HITACHI
Inspire the Next

For Windows Systems

Job Management Partner 1/Software Distribution

Description and Planning Guide

3020-3-S79-80(E)

■ Relevant program products

P-2642-1197 Job Management Partner 1/Software Distribution Manager version 09-51 (for Windows Server 2003, Windows XP Professional, and Windows 2000)

P-2642-1397 Job Management Partner 1/Software Distribution Client version 09-51 (for Windows Server 2003, Windows XP, Windows 2000, Windows NT 4.0, Windows Me, and Windows 98)

P-2A42-1197 Job Management Partner 1/Software Distribution Manager version 09-51 (for Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista)

P-2C42-1397 Job Management Partner 1/Software Distribution Client version 09-51 (for Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista)

P-1B42-2J72 Job Management Partner 1/Software Distribution Network Node Manager Linkage version 07-00 (for HP-UX)

P-2642-1C77 Job Management Partner 1/Software Distribution Internet Gateway version 07-00 (for Windows Server 2003, Windows XP Professional, Windows 2000, and Windows NT Server 4.0)

P-2642-1D77 Job Management Partner 1/Software Distribution HTTP Gateway version 07-00 (for Windows Server 2003, Windows XP, Windows 2000, Windows NT 4.0, Windows Me, and Windows 98)

■ Trademarks

■ Microsoft product screen shots

■ Restrictions

Information in this document is subject to change without notice and does not represent a commitment on the part of Hitachi. The software described in this manual is furnished according to a license agreement with Hitachi. The license agreement contains all of the terms and conditions governing your use of the software and documentation, including all warranty rights, limitations of liability, and disclaimers of warranty.

Material contained in this document may describe Hitachi products not available or features not available in your country.

Printed in Japan.

■ Issued

June 2013: 3020-3-S79-80(E)

■ Copyright

Summary of amendments

The following table lists changes in the manuals 3020-3-S79-80(E), 3020-3-S80-80(E), 3020-3-S81-80(E), and 3020-3-S82-80(E) for JP1/Software Distribution 09-51 and product changes related to these manuals.

Changes	Location
Windows 8 and Windows Server 2012 are now supported.	Desc. and Planning Guide: *1.3.6*, *2.2.1*, *2.2.2*, *2.5.2*, *2.5.3*, *2.5.4*, *2.5.5*, *2.5.6*, *2.5.8*, *2.7.1*, *2.7.2*, *2.7.6*, *2.13.3*, *2.13.7*, *2.14.5*, *5.1.5*, *6.6.1*, *Appendix A.2*, *Appendix C.23*, *C.61*, *C.62*, *Appendix F* Setup Guide: *1.1.1*, *1.1.2*, *2.1.4*, *2.1.6*, *2.1.25*, *3.1.16*, *4.6*, *5.4*, *6.3*, *7.3.2*, *7.4.1*, *7.4.5*, *7.5.1*, *7.5.4*, *9.5.2*, *11.1.1*, *11.1.2* Admin. Guide 1: *2.2.3*, *2.2.5*, *2.2.9*, *2.2.10*, *3.2.2*, *6.2.6*, *6.2.10*, *6.5.3*, *6.6.4*, *11.1.2*, *11.7*, *Appendix F* Admin. Guide 2: *1.1.1*, *4.26.20*, *4.28*, *6.6.4*, *6.6.7*, *7.2.1*, *Appendix A*, *A.1*, *A.2*, *A.3*, *A.4*, *A.5*, *A.6*, *Appendix E*
Microsoft SQL Server 2012 can now be used as a relational database program.	Desc. and Planning Guide: *2.6.5*, *5.2.6*, *5.4.2* Setup Guide:*7.1.1*, *7.3.2*, *7.5.4*, *7.6*, *11.1.1*, *11.1.2*, *Appendix A.2*, *Appendix F* Admin. Guide 2: *6.3.2*
Software information can now be collected for additional Microsoft Office products. In addition, greater detail about Microsoft Office products is now provided.	Desc. and Planning Guide: *2.2.1*
Software information can now be collected for additional anti-virus products.	Desc. and Planning Guide: *2.2.2*

Legend:

Desc. and Planning Guide: *Job Management Partner 1/Software Distribution Description and Planning Guide* (3020-3-S79(E)), for Windows systems

Setup Guide: *Job Management Partner 1/Software Distribution Setup Guide* (3020-3-S80(E)), for Windows systems

Admin. Guide 1: *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1* (3020-3-S81(E)), for Windows systems

Admin. Guide 2: *Job Management Partner 1/Software Distribution Administrator's Guide Volume 2* (3020-3-S82(E)), for Windows systems

In addition to the above changes, minor editorial corrections have been made.

Preface

(Note that this manual usually abbreviates *Job Management Partner 1* to *JP1*.)

This manual provides an overview of JP1/Software Distribution, and it describes how to install JP1/Software Distribution. This manual also introduces the JP1/Software Distribution facilities, provides examples of typical ways in which JP1/Software Distribution is used, and explains points you need to consider before you install and use JP1/Software Distribution.

Administrators who have not used JP1/Software Distribution before should read this manual first.

This manual is part of a related set of manuals for *JP1/Software Distribution for Windows*. The manuals in the set, including this manual, are listed below. Read the applicable manuals as needed.

Job Management Partner 1/Software Distribution Description and Planning Guide, for Windows systems

Read this manual first.

This manual provides an introductory overview of JP1/Software Distribution's concepts and facilities. It also provides examples of typical ways of setting up and using JP1/Software Distribution. The manual also includes important points to note before installing and using JP1/Software Distribution, and provides instructions on how to install JP1/Software Distribution.

Job Management Partner 1/Software Distribution Setup Guide, for Windows systems

This manual describes the installation and setup procedures for JP1/Software Distribution, database creation, and management of your system configuration.

Job Management Partner 1/Software Distribution Administrator's Guide Volume 1, for Windows systems

This manual describes in detail the facilities and operation of the managing server, such as for distributing software, acquiring and managing inventory, and collecting files. This manual also describes operations at a client.

Job Management Partner 1/Software Distribution Administrator's Guide Volume 2, for Windows systems

This manual describes how to link JP1/Software Distribution with other products, and how to take corrective action if a problem occurs. This manual also describes differences in functionality between the Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista Edition of JP1/Software Distribution Client.

Job Management Partner 1/Software Distribution Automatic Installation Tool Description and Reference, for Windows systems

This manual describes how to create AIT files and recorder files that are required for packaging non-Hitachi software.

Job Management Partner 1/Software Distribution Administrator Kit Description and Operator's Guide

This manual describes Job Management Partner 1/Software Distribution Administrator Kit, which is used for automatically installing JP1/Software Distribution Client.

Job Management Partner 1/Remote Control Description and Operator's Guide

This manual describes JP1/Remote Control and the remote control facility of JP1/Software Distribution.

■ Intended readers

This manual is intended for the following readers:

- Administrators who use JP1/Software Distribution to distribute software or to collect and manage asset information
- System administrators who intend to install and set up a JP1/Software Distribution system
- Users who have a basic understanding of Microsoft Windows operations
- Users who have a basic understanding of networks
- Users who have a basic understanding of relational databases
- Users who have a basic understanding of Microsoft SQL Server or Oracle (for those using Microsoft SQL Server or Oracle)

■ Related publications

This manual is part of a related set of manuals. The manuals in the set are listed below (with the manual numbers):

- *Job Management Partner 1/Software Distribution Setup Guide* (3020-3-S80(E)), for Windows systems#

- *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1* (3020-3-S81(E)), for Windows systems#
- *Job Management Partner 1/Software Distribution Administrator's Guide Volume 2* (3020-3-S82(E)), for Windows systems#
- *Job Management Partner 1/Software Distribution Automatic Installation Tool Description and Reference* (3020-3-S83(E)), for Windows systems#
- *Job Management Partner 1/Software Distribution Administrator Kit Description and Operator's Guide* (3020-3-S84(E))
- *Job Management Partner 1/Remote Control Description and Operator's Guide* (3020-3-S87(E))
- *Job Management Partner 1/Software Distribution Manager Description and Administrator's Guide* (3000-3-841(E))
- *Job Management Partner 1/Software Distribution Client Description and User's Guide* (3020-3-S85(E)), for UNIX systems
- *Job Management Partner 1/Asset Information Manager Description* (3020-3-S76(E))
- *Job Management Partner 1/Asset Information Manager Planning and Setup Guide* (3020-3-S77(E))
- *Job Management Partner 1/Asset Information Manager Administrator's Guide* (3020-3-S78(E))
- *Job Management Partner 1/Client Security Control Description, User's Guide and Operator's Guide* (3020-3-S71(E))
- *Job Management Partner 1/Automatic Job Management System 2 Description* (3020-3-K21(E))
- *Job Management Partner 1/Automatic Job Management System 2 Planning and Administration Guide* (3020-3-K22(E))
- *Job Management Partner 1/Automatic Job Management System 2 Operator's Guide* (3020-3-K24(E))
- *Job Management Partner 1/Automatic Job Management System 2 Command Reference* (3020-3-K25(E))
- *Job Management Partner 1/Automatic Job Management System 2 Linkage Guide* (3020-3-K27(E))
- *Job Management Partner 1/Automatic Job Management System 2 Messages* (3020-3-K28(E))
- *Job Management Partner 1/Automatic Job Management System 3 Introduction* (3020-3-S01(E))
- *Job Management Partner 1/Automatic Job Management System 3 Overview* (3020-3-S02(E))
- *Job Management Partner 1/Automatic Job Management System 3 System Design (Configuration) Guide* (3020-3-S03(E))
- *Job Management Partner 1/Automatic Job Management System 3 System Design (Work Tasks) Guide* (3020-3-S04(E))
- *Job Management Partner 1/Automatic Job Management System 3 Administration Guide* (3020-3-S07(E))
- *Job Management Partner 1/Automatic Job Management System 3 Troubleshooting* (3020-3-S08(E))
- *Job Management Partner 1/Automatic Job Management System 3 Operator's Guide* (3020-3-S09(E))
- *Job Management Partner 1/Automatic Job Management System 3 Command Reference 1* (3020-3-S10(E))
- *Job Management Partner 1/Automatic Job Management System 3 Command Reference 2* (3020-3-S11(E))
- *Job Management Partner 1/Automatic Job Management System 3 Linkage Guide* (3020-3-S12(E))
- *Job Management Partner 1/Automatic Job Management System 3 Messages 1* (3020-3-S13(E))
- *Job Management Partner 1/Automatic Job Management System 3 Messages 2* (3020-3-S14(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Automatic Job Management System 3 Overview* (3021-3-318(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Automatic Job Management System 3 System Design (Configuration) Guide* (3021-3-319(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Automatic Job Management System 3 System Design (Work Tasks) Guide* (3021-3-320(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Automatic Job Management System 3 Configuration Guide 1* (3021-3-321(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Automatic Job Management System 3 Configuration Guide 2* (3021-3-322(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Automatic Job Management System 3 Administration Guide* (3021-3-323(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Automatic Job Management System 3 Troubleshooting* (3021-3-324(E))

- *Job Management Partner 1 Version 10 Job Management Partner 1/Automatic Job Management System 3 Operator's Guide* (3021-3-325(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Automatic Job Management System 3 Command Reference 1* (3021-3-326(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Automatic Job Management System 3 Command Reference 2* (3021-3-327(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Automatic Job Management System 3 Linkage Guide* (3021-3-328(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Automatic Job Management System 3 Messages 1* (3021-3-329(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Automatic Job Management System 3 Messages 2* (3021-3-330(E))
- *Job Management Partner 1/Integrated Management - Manager Configuration Guide* (3020-3-R77(E))
- *Job Management Partner 1/Integrated Management - Manager Administration Guide* (3020-3-R78(E))
- *Job Management Partner Version 10 Job Management Partner 1/Integrated Management - Manager Configuration Guide* (3021-3-306(E))
- *Job Management Partner Version 10 Job Management Partner 1/Integrated Management - Manager Administration Guide* (3021-3-307(E))
- *Job Management Partner 1/Base User's Guide* (3020-3-R71(E))
- *Job Management Partner 1/Base Messages* (3020-3-R72(E))
- *Job Management Partner 1/Base Function Reference* (3020-3-R73(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Base User's Guide 1* (3021-3-301(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Base Messages* (3021-3-302(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Base Function Reference* (3021-3-303(E))
- *HiRDB Version 8 Messages* (3020-6-358(E))

#: This manual may omit common parts of manual names, such as *Job Management Partner 1/Software Distribution*.

■ How to use the manual

- Unless noted otherwise, this manual assumes that the version of the JP1/Software Distribution product that is used at the connection destination is JP1/Software Distribution Manager 09-51 for Windows or JP1/Software Distribution Manager 06-72 for UNIX, and that the version of JP1/Software Distribution Client for UNIX that is used is 09-00. If the system at the connection destination is using an earlier version of JP1/Software Distribution, only the facilities supported by that version are available.
- For details about the differences in terminology and facilities for JP1/Software Distribution for UNIX, see *D.2 Differences with JP1/Software Distribution for UNIX*.
- For details about the functional differences with the Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista Edition of JP1/Software Distribution Client, see *A. Functions Provided in the Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista Edition of JP1/Software Distribution Client* in the manual *Administrator's Guide Volume 2*.

■ About online Help

JP1/Software Distribution provides the following online Help.

JP1/Software Distribution online Help (for JP1/Software Distribution Manager and JP1/Software Distribution Client (relay system)):

This online Help combines the following manuals:

- *Job Management Partner 1/Software Distribution Description and Planning Guide*, for Windows systems
- *Job Management Partner 1/Software Distribution Setup Guide*, for Windows systems
- *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1*, for Windows systems

- *Job Management Partner 1/Software Distribution Administrator's Guide Volume 2*, for Windows systems
- *Job Management Partner 1/Software Distribution Automatic Installation Tool Description and Reference*, for Windows systems

JP1/Software Distribution Client online Help (for JP1/Software Distribution Client (client)):

This online Help contains information about clients. The information has been extracted from the above manuals.

This online Help enables the user to search the entire set of help documents for a desired item.

To access online Help, use the **Help** menu in any window of JP1/Software Distribution or the **Help** button in any dialog box. To use online Help, you must have Microsoft Internet Explorer 5.01 or later installed.

■ Conventions: Abbreviations for product names

This manual uses the following abbreviations for names of products associated with JP1/Software Distribution:

Abbreviation	Full name or meaning
HTTP Gateway	Job Management Partner 1/Software Distribution HTTP Gateway
Internet Gateway	Job Management Partner 1/Software Distribution Internet Gateway
JP1/Client Security Control or JP1/CSC	Job Management Partner 1/Client Security Control - Agent
	Job Management Partner 1/Client Security Control - Manager
JP1/Remote Control	Job Management Partner 1/Remote Control Agent
	Job Management Partner 1/Remote Control Manager
JP1/Software Distribution	Job Management Partner 1/Software Distribution Client
	Job Management Partner 1/Software Distribution Manager
Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista Edition of JP1/Software Distribution Client	The edition of JP1/Software Distribution Client that runs on Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista
Windows CE Edition of JP1/Software Distribution Client	The edition of JP1/Software Distribution Client that runs on Windows CE .NET 4.1

This manual uses the following abbreviations for the names of other products:

Abbreviation	Full name or meaning
AIX	AIX(R)
AMT	Intel Active Management Technology
HIBUN FDE	HIBUN AE - English version FDE
HP NNM	HP Network Node Manager Software version 6 or earlier
	HP Network Node Manager Starter Edition Software version 7.5 or earlier
InstallShield	InstallShield(R)
Itanium 2	Intel Itanium(R) 2 processor
JP1/AJS	Job Management Partner 1/Automatic Job Management System 2
	Job Management Partner 1/Automatic Job Management System 3
JP1/Asset Information Manager	Job Management Partner 1/Asset Information Manager

Abbreviation				Full name or meaning
JP1/Base				Job Management Partner 1/Base
JP1/IM	JP1/IM			Job Management Partner 1/Integrated Management - Manager
	JP1/IM - View			Job Management Partner 1/Integrated Management - View
JP1/PFM/SSO[#1]	JP1/PFM/SSO[#1]			Job Management Partner 1/Performance Management/ SNMP System Observer
	JP1/SSO			Job Management Partner 1/Server System Observer
Linux				Linux(R)
MBSA				Microsoft(R) Baseline Security Analyzer
Microsoft Internet Explorer				Microsoft(R) Internet Explorer(R)
				Windows(R) Internet Explorer(R)
Microsoft Internet Information Services				Microsoft(R) Internet Information Services 6.0
				Microsoft(R) Internet Information Services 7.0
Microsoft SQL Server				Microsoft(R) SQL Server(R) 2000
				Microsoft(R) SQL Server(R) 2005
				Microsoft(R) SQL Server(R) 2008
				Microsoft(R) SQL Server(R) 2012
				Microsoft(R) SQL Server(R) 7.0
MS-DOS				Microsoft(R) MS-DOS(R)
MSXML				Microsoft XML
NetWare				NetWare(R)
Oracle				Oracle9i
				Oracle8i
UNIX				UNIX(R)
Visual Test				Visual Test 4.0
				Visual Test 6.0
				Visual Test 6.5
Windows	Windows 98			Microsoft(R) Windows(R) 98 Operating System
	Windows Me			Microsoft(R) Windows(R) Millennium Edition Operating System
	Windows NT	Windows 2000	Windows 2000 Advanced Server	Microsoft(R) Windows(R) 2000 Advanced Server Operating System
			Windows 2000 Professional	Microsoft(R) Windows(R) 2000 Professional Operating System
			Windows 2000 Server	Microsoft(R) Windows(R) 2000 Server Operating System
		Windows 7		Microsoft(R) Windows(R) 7 Enterprise
				Microsoft(R) Windows(R) 7 Professional

Abbreviation				Full name or meaning
Windows	Windows NT	Windows 7		Microsoft(R) Windows(R) 7 Ultimate
		Windows 8		Microsoft(R) Windows(R) 8
				Microsoft(R) Windows(R) 8 Enterprise
				Microsoft(R) Windows(R) 8 Pro
		Windows NT 4.0	Windows NT Server 4.0	Microsoft(R) Windows NT(R) Server Network Operating System Version4.0
			Windows NT Workstation 4.0	Microsoft(R) Windows NT(R) Workstation Operating System Version4.0
		Windows Server 2003#2	Windows Server 2003#2	Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition
				Microsoft(R) Windows Server(R) 2003 R2, Standard Edition
				Microsoft(R) Windows Server(R) 2003, Datacenter Edition
				Microsoft(R) Windows Server(R) 2003, Enterprise Edition
				Microsoft(R) Windows Server(R) 2003, Standard Edition
			Windows Server 2003 (IPF)	Microsoft(R) Windows Server(R) 2003, Datacenter Edition for Itanium-based Systems
				Microsoft(R) Windows Server(R) 2003, Enterprise Edition for Itanium-based Systems
			Windows Server 2003 (x64)	Microsoft(R) Windows Server(R) 2003 R2, Datacenter x64 Edition
				Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition
				Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition
				Microsoft(R) Windows Server(R) 2003, Datacenter x64 Edition
				Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition
				Microsoft(R) Windows Server(R) 2003, Standard x64 Edition
		Windows Server 2008#3	Windows Server 2008#3	Microsoft(R) Windows Server(R) 2008 Datacenter
				Microsoft(R) Windows Server(R) 2008 Datacenter without Hyper-V(R)
				Microsoft(R) Windows Server(R) 2008 Enterprise
				Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(R)
				Microsoft(R) Windows Server(R) 2008 Standard
				Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(R)
			Windows Server 2008 R2	Microsoft(R) Windows Server(R) 2008 R2 Datacenter
				Microsoft(R) Windows Server(R) 2008 R2 Enterprise

Abbreviation				Full name or meaning
Windows	Windows NT	Windows Server 2008[#3]	Windows Server 2008 R2	Microsoft(R) Windows Server(R) 2008 R2 Standard
		Windows Server 2012		Microsoft(R) Windows Server(R) 2012 Datacenter
				Microsoft(R) Windows Server(R) 2012 Standard
		Windows Vista		Microsoft(R) Windows Vista(R) Business
				Microsoft(R) Windows Vista(R) Enterprise
				Microsoft(R) Windows Vista(R) Ultimate
		Windows XP	Windows XP Home Edition	Microsoft(R) Windows(R) XP Home Edition Operating System
			Windows XP Professional	Microsoft(R) Windows(R) XP Professional Operating System
Windows 95				Microsoft(R) Windows(R) 95 Operating System
WSUS	WSUS 2.0			Microsoft(R) Windows Server(R) Update Services 2.0
	WSUS 3.0			Microsoft(R) Windows Server(R) Update Services 3.0
WUA				Windows(R) Update Agent 2.0
				Windows(R) Update Agent 3.0

#1

In descriptions that are explicitly about JP1/SSO, any references to JP1/PFM/SSO do not apply to JP1/SSO.

#2

In descriptions that are explicitly about Windows Server 2003 (IPF) or Windows Server 2003 (x64), any references to Windows Server 2003 do not apply to Windows Server 2003 (IPF) or Windows Server 2003 (x64).

#3

In descriptions that are explicitly about Windows Server 2008 R2, any references to Windows Server 2008 do not apply to Windows Server 2008 R2.

■ Conventions: Acronyms

This manual also uses the following acronyms:

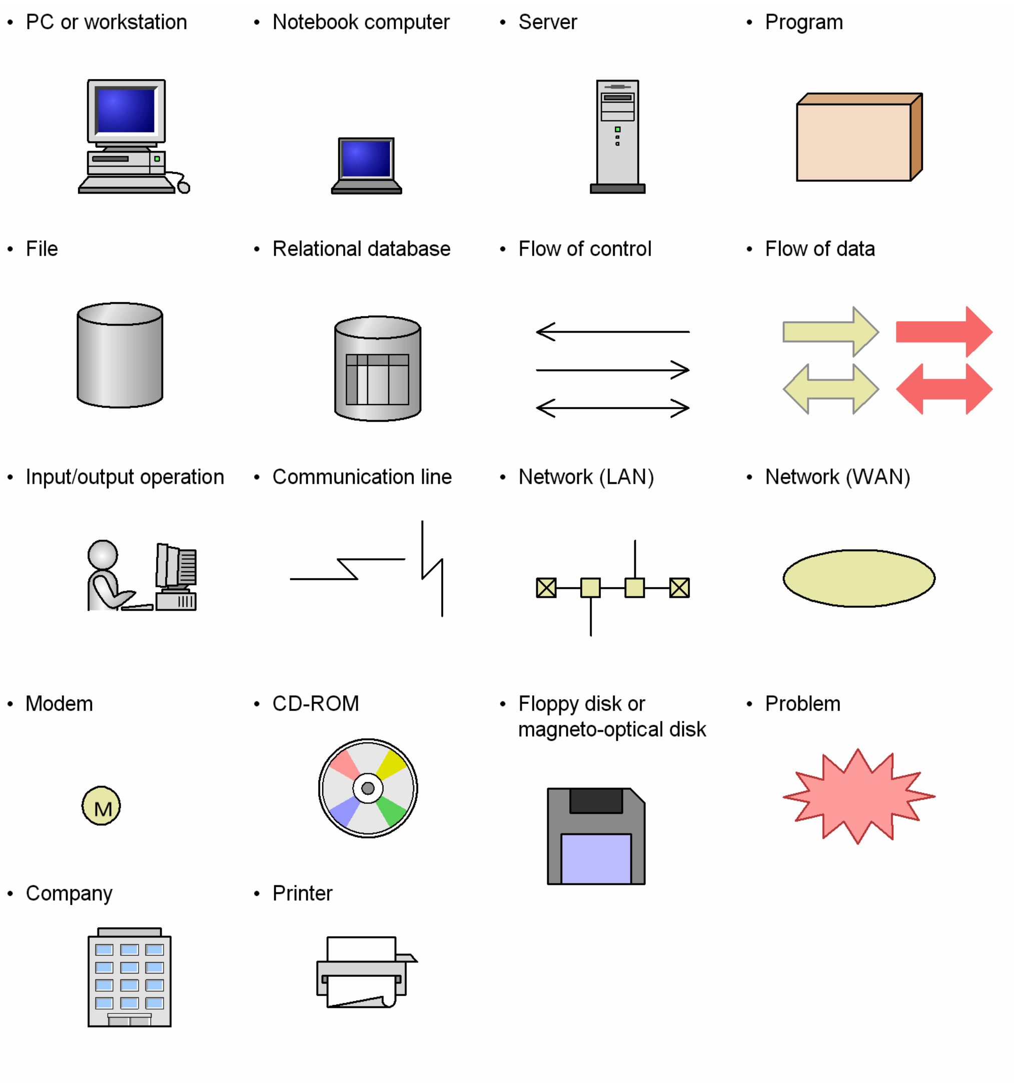
Acronym	Full name or meaning
AMD	Advanced Micro Devices
API	Application Programming Interface
BIOS	Basic Input Output System
CCMP	Counter mode with Cipher block chaining Message authentication code Protocol
CD-R	Compact Disc Recordable
CD-ROM	Compact Disc Read Only Memory
CF	Compact Flash
CGI	Common Gateway Interface
CPU	Central Processing Unit
CSV	Comma Separated Value
DB	Database

Acronym	Full name or meaning
DBA	Database Administrator
DHCP	Dynamic Host Configuration Protocol
DLL	Dynamic Linking Library
DNS	Domain Name System
DoS	Denial of Service
DVD	Digital Versatile Disk
FD	Floppy Disk
FTP	File Transfer Protocol
GUI	Graphical User Interface
HD	Hard Disk
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Security
ICMP	Internet Control Message Protocol
ID	Identifier
IEEE 1394	Institute of Electrical and Electronic Engineers 1394
IP	Internet Protocol
IPF	Itanium(R) Processor Family
ISAPI	Internet Server Application Programming Interface
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MIB	Management Information Base
MO	Magneto-Optical disk
MS-DOS	Microsoft Disk Operating System
NAS	Network Attached Storage
NAT	Network Address Translation
NFS	Network File System
NIC	Network Interface Card
OS	Operating System
OU	Organizational Unit
PC	Personal Computer
PDA	Personal Digital Assistant
PME	Power Management Event
PPP	Point to Point Protocol
RAS	Remote Access Service

Acronym	Full name or meaning
RPC	Remote Procedure Call
RSN	Robust Security Network
RWU	Remote-Wake-UP
SD	Secure Digital
SID	System Identifier
SMBIOS	System Management Basic Input Output System
SNMP	Simple Network Management Protocol
SOL	Serial Over LAN
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
USB	Universal Serial Bus
UTC	Coordinated Universal Time
UUID	Universally Unique Identifier
VPN	Virtual Private Network
WAN	Wide Area Network
WINS	Windows Internet Name Service
WMI	Windows Management Instrumentation
WPA	Wi-fi Protected Access
WS	Workstation
XML	Extensible Markup Language

■ Conventions: Diagrams

This manual uses the following conventions in diagrams:



■ Conventions: Facility, function, functionality

For consistency with earlier documentation, this manual usually (not always) uses the term *facility* instead of the more common terms *functionality* or *function*. Unless otherwise specified, these terms have the same meaning. For example, the following have the same meaning:

- JP1/Software Distribution facilities
- JP1/Software Distribution functionality

■ Conventions: Fonts and symbols

The following table explains the fonts used in this manual:

Font	Convention
Bold	**Bold** type indicates text on a window, other than the window title. Such text includes menus, menu options, buttons, radio box options, or explanatory labels. For example: • From the **File** menu, choose **Open**. • Click the **Cancel** button. • In the **Enter name** entry box, type your name.

Font	Convention
Italics	*Italics* are used to indicate a placeholder for some actual text to be provided by the user or system. For example: • Write the command as follows: `copy` *source-file target-file* • The following message appears: `A file was not found. (file =` *file-name*`)` *Italics* are also used for emphasis. For example: • Do *not* delete the configuration file.
`Code font`	A `code font` indicates text that the user enters without change, or text (such as messages) output by the system. For example: • At the prompt, enter `dir`. • Use the `send` command to send mail. • The following message is displayed: `The password is incorrect.`

The following table explains the symbols used in this manual:

Symbol	Convention
|	In syntax explanations, a vertical bar separates multiple items, and has the meaning of OR. For example: `A|B|C` means A, or B, or C.
{ }	In syntax explanations, curly brackets indicate that only one of the enclosed items is to be selected. For example: `{A|B|C}` means only one of A, or B, or C.
[ ]	In syntax explanations, square brackets indicate that the enclosed item or items are optional. For example: `[A]` means that you can specify `A` or nothing. `[B|C]` means that you can specify `B`, or `C`, or nothing.
...	In coding, an ellipsis (`...`) indicates that one or more lines of coding are not shown for purposes of brevity. In syntax explanations, an ellipsis indicates that the immediately preceding item can be repeated as many times as necessary. For example: `A, B, B, ...` means that, after you specify `A, B,` you can specify B as many times as necessary.

■ Conventions: KB, MB, GB, and TB

This manual uses the following conventions:

- 1 KB (kilobyte) is 1,024 bytes.
- 1 MB (megabyte) is 1,024^2 bytes.
- 1 GB (gigabyte) is 1,024^3 bytes.
- 1 TB (terabyte) is 1,024^4 bytes.

■ Conventions: References to other manuals

Within the group of manuals *Setup Guide*, *Administrator's Guide Volume 1*, *Administrator's Guide Volume 2*, and *Automatic Installation Tool Description and Reference*, a cross-reference in one manual to another manual is written as follows:

For details about *AAA*, see *n.n.n BBB* in the manual *CCC*.

Where*:*

- *AAA* is the topic to be referenced.
- *n.n.n* is the chapter or section number to be referenced. This number may be followed by a subsection number or letter in parentheses.
- *BBB* is the title of the chapter or section to be referenced.
- *CCC* is the abbreviated name of the manual to be referenced. Common parts of manual names, such as *Job Management Partner 1/Software Distribution* and *for Windows systems*, are omitted.

■ Conventions: Version numbers

The version numbers of Hitachi program products are usually written as two sets of two digits each, separated by a hyphen. For example:

- Version 1.00 (or 1.0) is written as 01-00.
- Version 2.05 is written as 02-05.
- Version 2.50 (or 2.5) is written as 02-50.
- Version 12.25 is written as 12-25.

The version number might be shown on the spine of a manual as *Ver. 2.00*, but the same version number would be written in the program as *02-00*.

Contents

1 About JP1/Software Distribution

A JP1/Software Distribution system distributes software and manages client resources over a network. JP1/Software Distribution automates client management, resulting in a significant reduction in the workload required for such tasks.

This chapter describes what you can do with JP1/Software Distribution, and gives an overview of how the JP1/Software Distribution programs are organized.

1.1 Features of JP1/Software Distribution

In recent years, networks have become more complex and software and hardware have become more diverse. As a result, there is an increasing need for tools that automate or reduce the amount of work required to distribute software and manage clients. Unless such tools are introduced to centrally manage systems in a network environment, the workload of system administrators will keep increasing (especially in large networks).

The conventional approach to operation and management poses problems such as the following:

Problems during software installation

- Software media must be transported to the installation site, and installation and setup must be performed for each client. Consequently, building a job environment requires significant effort and expense.
- Frequent software upgrades cannot be accommodated promptly.

Problems in collecting information from clients

- It is difficult to obtain information about each client's hardware and software.
- Collecting information from clients takes time, and there is no guarantee that up-to-date information is being obtained.

With JP1/Software Distribution, these tasks are executed in a batch in response to an instruction issued from a central server, thereby significantly reducing the workload of the system administrator. The features of JP1/Software Distribution are described below.

■ Standardization of software distribution and inventory management

Job programs and commercial software needed by clients are distributed in a batch from a central server. A distribution method appropriate to the particular system, such as schedule-based or group-based, can be selected. JP1/Software Distribution also supports multicast distribution to reduce the data volume during distribution.

Inventory information needed for management of client resources can be obtained in a batch in response to an instruction issued from the central server. Because the inventory information to be obtained from clients can include both hardware and software information as well as information about users, clients can be managed on the basis of either PC environments or users. Additionally, JP1/Software Distribution supports management of anti-virus products, which have become important as use of the Internet spreads.

■ Compatibility with systems and platforms of various sizes

JP1/Software Distribution can be applied to systems of various sizes, ranging from a few dozen clients to tens of thousands of clients. It can also handle systems in which Windows and UNIX platforms coexist.

JP1/Software Distribution can also be used in cluster systems and multi-LAN environments that improve system availability.

■ Linkage to other programs

By linking JP1/Software Distribution to other programs, such as JP1/Base, JP1/Asset Information Manager, JP1/Client Security Control, and JP1/IM, you can integrate software distribution and client resource management with your overall system management.

By setting up JP1/AJS to use the command interface provided by JP1/Software Distribution, you can also automate the tasks that use JP1/Software Distribution.

1.2 Facilities of JP1/Software Distribution

This section provides an overview of the *facilities* (that is, *functions* or *functionality*) of JP1/Software Distribution.

The main facilities provided by JP1/Software Distribution are listed below. By using these facilities effectively, you can achieve the precise operations that satisfy the varied needs of users.

- Software distribution (remote installation)

  This facility enables you to automatically distribute and install software over a network. You can specify a date and time for distribution and can target specific clients by specifying installation conditions.
- Inventory management

  This facility enables you to acquire and manage on a server inventory information from PCs being used on the network, including hardware information, OS settings information, and software information.
- File collection (remote collection)

  This facility enables you to collect client data on the server.
- Software operation status monitoring

  This facility enables you to acquire and manage client software operation status and file manipulation history. It also enables you to prohibit specific software programs from started and to allow only specified software programs to start.
- Client management

  This facility enables you to detect whether patches have been installed on a client and to monitor the system status. It also enables you to send messages from the server to a client. You can also use the AMT functionality to control any client computers that support AMT.
- Client remote control

  This facility enables you to respond to client problems by remote operations from the server. You can display, on the server screen, a screen from a remotely located client.
- Linkage to other programs

  By using the facilities of JP1/Software Distribution from other programs, you can carry out various tasks, such as resource management and security management.

1.2.1 Software distribution

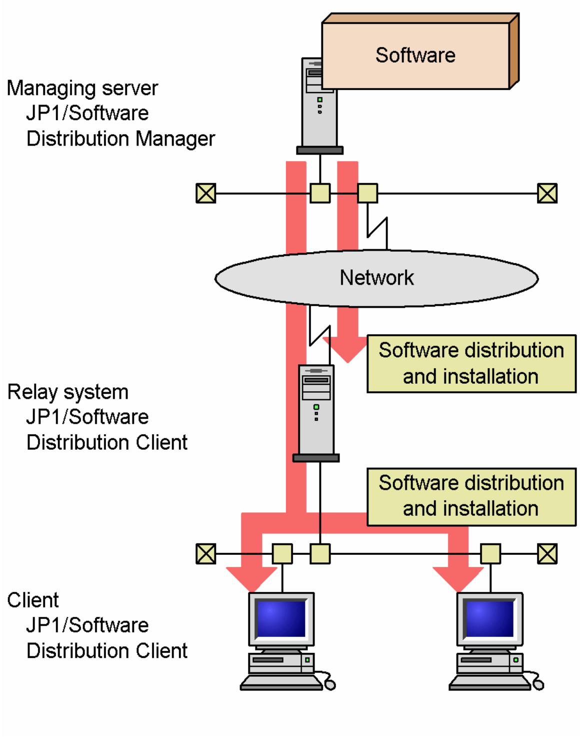
Using this facility, you can distribute and install software in batches into remote clients over the network, based on instructions from a central server. The installation results at the individual clients are automatically sent back to the server, where they can be centrally managed. You can also use this facility to install software on clients without using a network.

For details about the software distribution facility, see *2.1 Software distribution (remote installation)*.

(1) Facility overview

The software distribution facility distributes and installs software to a *client* from the central server (*managing server*), over a network. The client contains JP1/Software Distribution Client and the server contains JP1/Software Distribution Manager. If the network is large or the system consists of many clients, software can be distributed more efficiently if a *relay system* that uses JP1/Software Distribution Client is positioned between the managing server and clients. The following figure shows an overview of the software distribution facility.

Figure 1–1: Software distribution facility



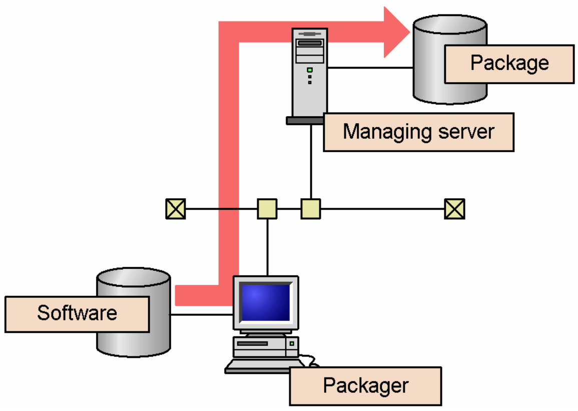
The software distribution procedure consists of three stages: preparation, execution, and confirmation, as described below.

To distribute software:

1. Register the software to be distributed (packaging).

   In the managing server, you first need to register the software to be distributed. This step is called *packaging*. To package software, you use a program called the *Packager*. Software that has been packaged and is ready to be distributed is called a *package*. When you package software, you can specify various types of information, such as installation conditions for the software to be distributed.

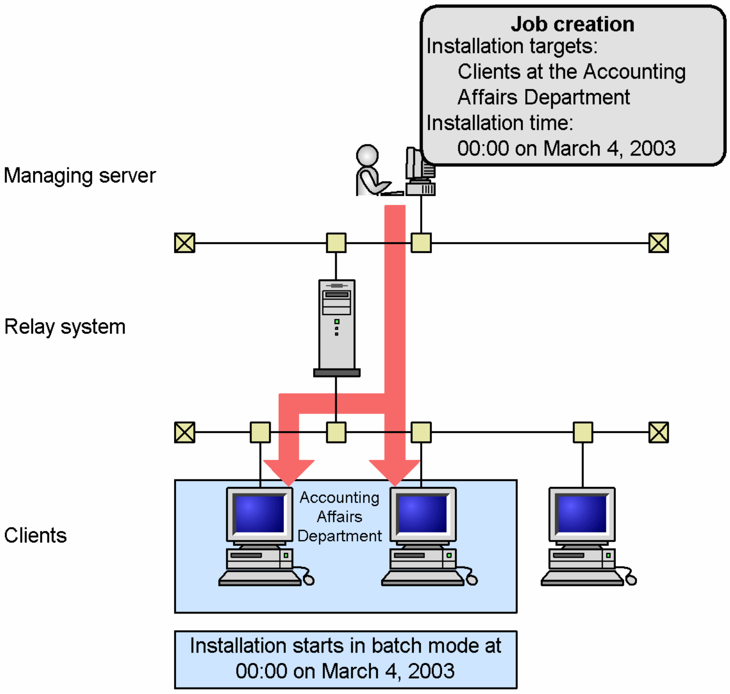
   Figure 1–2: Packaging

2. Specify software distribution (remote installation).

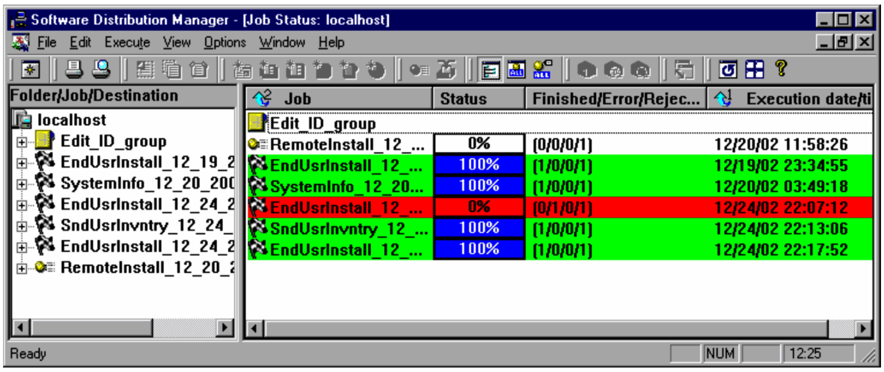
   Create and execute a job that specifies the clients to which the software is to be distributed and how the software is to be distributed. For example, you can create a job to distribute specified software to specified clients in specified departments, at a specified date and time. The software will be distributed and installed exactly as specified by the job.

Figure 1–3: Remote installation


Job creation
Installation targets:
Clients at the Accounting Affairs Department
Installation time:
00:00 on March 4, 2003
Managing server
Relay system
Clients
Accounting Affairs Department
Installation starts in batch mode at 00:00 on March 4, 2003

3. Confirm the installation status and results.
   You can easily check the status and results of the job from a window at the managing server:

Figure 1–4: Job Status window



Folder/Job/Destination
- localhost
  - Edit_ID_group
  - EndUsrInstall_12_19_2
  - SystemInfo_12_20_200
  - EndUsrInstall_12_24_2
  - SndUsrInvntry_12_24_
  - EndUsrInstall_12_24_2
  - RemoteInstall_12_20_2

Edit_ID_group

Job	Status	Finished/Error/Rejec...	Execution date/ti
RemoteInstall_12_...	0%	(0/0/0/1)	12/20/02 11:58:26
EndUsrInstall_12_...	100%	(1/0/0/1)	12/19/02 23:34:55
SystemInfo_12_20...	100%	(1/0/0/1)	12/20/02 03:49:18
EndUsrInstall_12_...	0%	(0/1/0/1)	12/24/02 22:07:12
SndUsrInvntry_12_...	100%	(1/0/0/1)	12/24/02 22:13:06
EndUsrInstall_12_...	100%	(1/0/0/1)	12/24/02 22:17:52

The facility for transferring a software package from the managing server to clients and installing it is called *remote installation*.

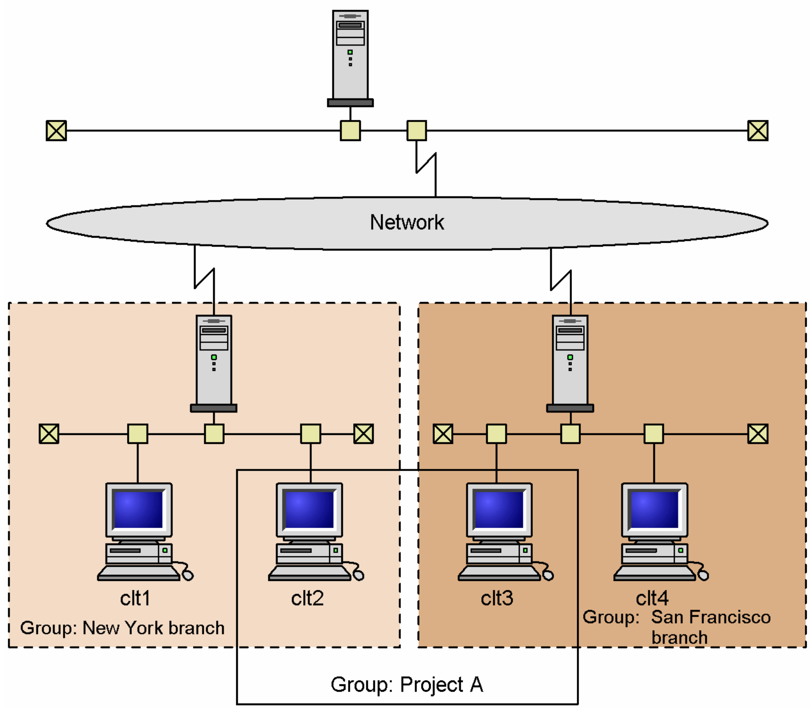
(2) Facilities for achieving efficient software distribution

JP1/Software Distribution provides various facilities to achieve efficient software distribution. This section describes some of these facilities.

(a) Grouping of distribution destinations

You can group the clients to which software is to be distributed so that the groups best match what you are trying to achieve. Because individual clients can belong to multiple groups, clients in different department groups can also be grouped into the same project group, as illustrated in the following figure.

Figure 1–5: Grouping of distribution destinations



By grouping the distribution destinations, you can specify a group (`project A`) as the target of software distribution instead of having to specify individual clients (`clt2` and `clt3`).

(b) Using a relay system

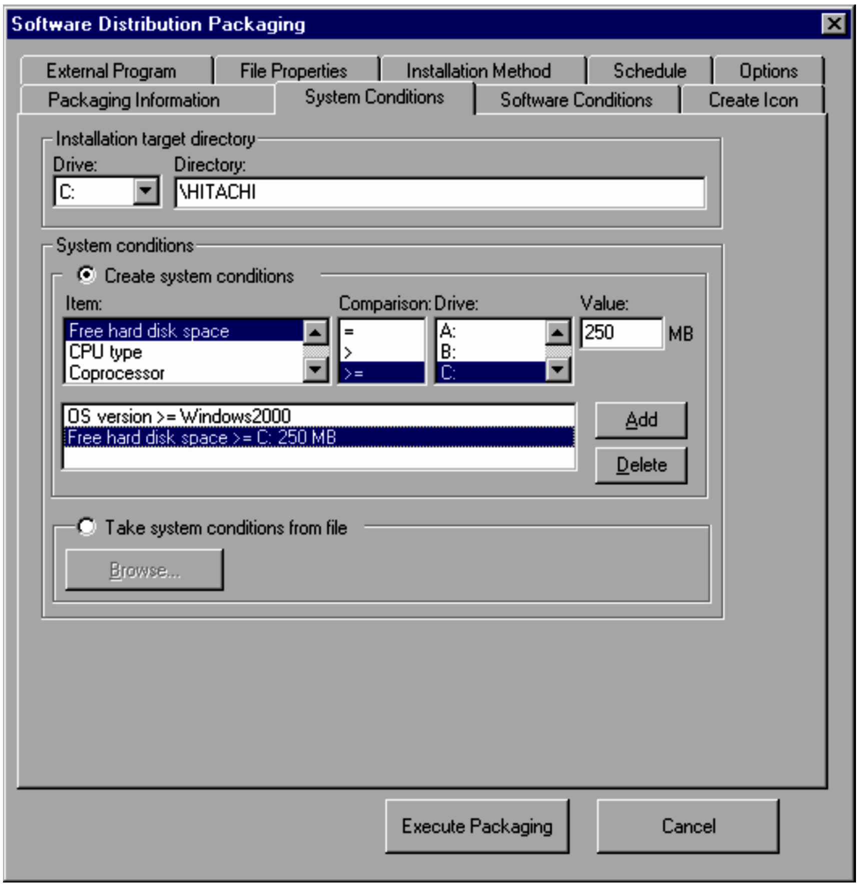
A relay system has functionality to act as a relay for software distribution as well to act as a managing server. Thus, software can be distributed by using the central server in a centralized arrangement and also by using relay systems as departmental servers in a distributed arrangement. Even in a distributed application, the central server can use a relay system to obtain the status of software that has been installed remotely. The central server can thus be used to centrally manage software information throughout the entire network.

Note that a relay system can also function as a client. The central server can execute remote installation for a relay system just as it can for any client.

(c) Installation conditions

When installing software remotely, you can check whether the software to be installed is appropriate for the destination clients. For example, while packaging software or creating a job, you can use the window shown below to specify conditions that the hardware must satisfy.

Figure 1–6: System Conditions page



Installation target directory

Drive: C:

Directory: \HITACHI

System conditions

● Create system conditions

Item:	Comparison:	Drive:	Value:
Free hard disk space CPU type Coprocessor	= > >=	A: B: C:	250 MB

OS version >= Windows2000

Free hard disk space >= C: 250 MB

○ Take system conditions from file

Specifying hardware conditions can prevent installation of software in clients where insufficient hard disk space or an incompatible operating system may cause the installation to fail.

In addition to hardware conditions, you can also check whether particular software has already been installed, or before installation you can start an external program to perform checks with your own specified conditions.

(d) Distribution time and installation time

The timing for remote installation can be divided into two stages: the time for distributing the software (that is, the data transmission time) and the time for installing the software onto the clients.

When you create a remote installation job, you specify a time for executing the job. This becomes the software distribution date and time (data transmission time). Specifying a time at night, when traffic on the network is relatively light, can result in more efficient transmission.

The time for installing the distributed software onto the clients is specified separately from the transmission time, and is specified for each package. This option is convenient for upgrading a program at all clients at a specific time.

(e) Split package distribution

You can split a package into multiple segments of specified sizes and distribute them separately. Because this facility allows a pause between transmissions of package segments, you can smooth out the workload on the network when you have a large package to distribute.

(f) Multicast distribution

In a multicast distribution, the system at a higher level than the clients sends the packets for a single job only, but the software is distributed to multiple lower-level clients. This facility reduces the number of packets sent when a large volume of software is distributed.

(g) Job suspension and restart

You can temporarily suspend job execution on a host during remote installation. For example, if a job is scheduled to be executed while an application is stopped, but the job has not been completed at the time the application is scheduled to resume, you can suspend job execution and restart it after the application has terminated.

(h) Use of client control facility

This facility enables you to use one PC to start, over a network, any other PC that supports AMT or Wake on LAN. It also enables you to shut down, over the network, any PC that supports automatic shutdown. Using this facility, JP1/Software Distribution can install software on remote PCs that have been turned off at night or on a weekend when network traffic is light.

(3) Software installation on stand-alone PCs

A JP1/Software Distribution system can distribute software and manage inventory over a network. It also enables you to install software on stand-alone PCs without using a network. This feature is useful when the PC where software is to be installed is not on the network, or is on the network but you do not want to increase the line load. JP1/Software Distribution supports stand-alone PCs (offline machines) on which JP1/Software Distribution Client is installed.

To install software on an offline machine, at the managing server you first create the files needed for installation, and then save them to storage media, such as CD-R or MO. You then transport this storage media to the location of the offline machine and execute the installation. This method of installing software without using a network is called *offline installation*.

1.2.2 Inventory management

The central server (managing server) can collect inventory information, such as the hardware and software configurations of the PCs being used in the network. If you create the media for acquiring inventory information, this facility can also acquire such information from PCs located outside the network.

Acquiring inventory information enables you to gain an accurate understanding of each client, which allows you to determine, for example, whether a client needs an additional hard disk, whether there is a problem with a client's OS security settings, or whether a client is missing software. This facility can also manage user information, such as the model numbers of the PCs and the user names.

To obtain inventory information, you must create and execute a job that instructs the managing server to collect the information, in the same manner that you create a job to perform software distribution. You can also use a relay system to collect inventory information.

If some inventory information is updated at a client, this facility can report the updated information whenever connection is established with the higher system. This increases the efficiency of inventory management because an up-to-date inventory is acquired without the administrator having to execute a job.

Other programs can use acquired inventory information as follows:

- The information can be used as JP1/Asset Information Manager asset information. JP1/Asset Information Manager can automatically apply the most recent inventory information collected by the managing server as asset information. For details about how to use inventory information as JP1/Asset Information Manager asset information, see the *Job Management Partner 1/Asset Information Manager Planning and Setup Guide*.
- The acquired inventory information can be viewed from the network monitoring windows of HP NNM version 7.5 or earlier.

For details about the inventory management facility, see *2.2 Acquiring inventory information* and *2.3 Managing inventory information*.

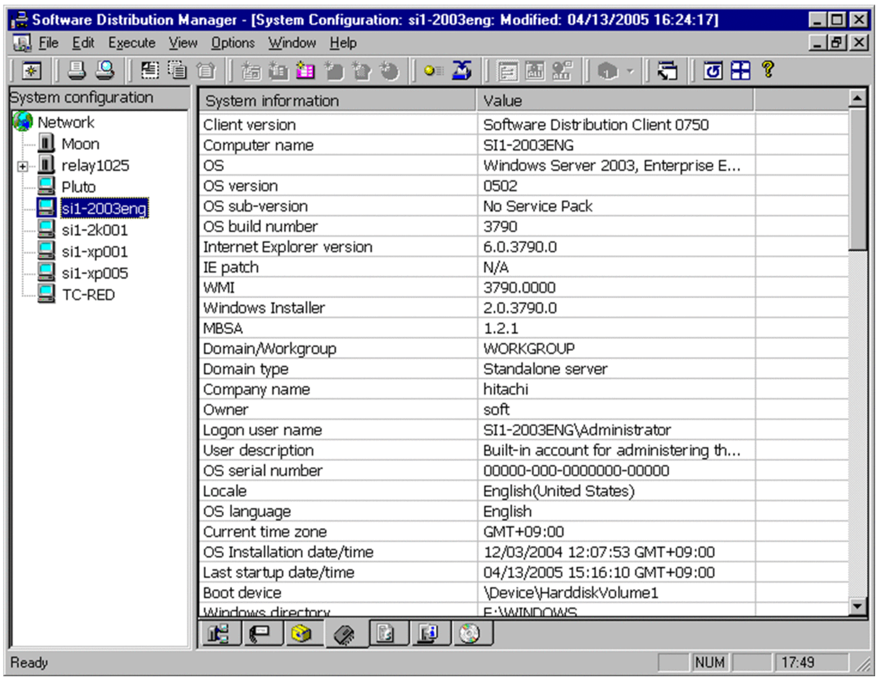
(1) Types of inventory information that can be obtained

You can obtain four types of inventory information:

System information

You can obtain information about the hardware at each client, such as the amount of available hard disk space, the type of operating system, and registry information:

Figure 1–7: System Configuration window (system information)


Software Distribution Manager - [System Configuration: si1-2003eng: Modified: 04/13/2005 16:24:17]
File Edit Execute View Options Window Help
System configuration
Network
Moon
relay1025
Pluto
si1-2003eng
si1-2k001
si1-xp001
si1-xp005
TC-RED
Ready
NUM
17:49

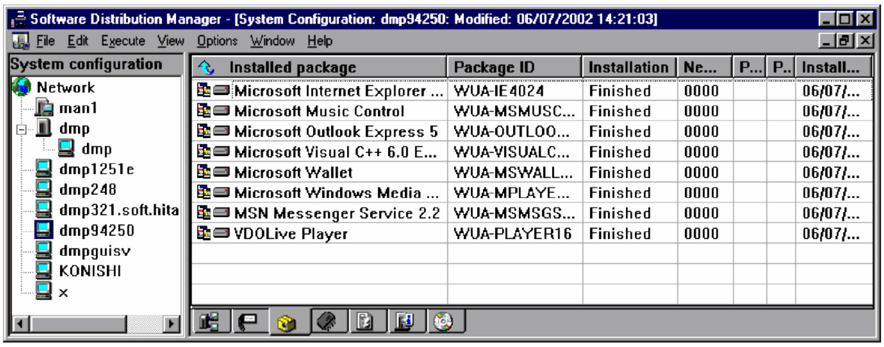
System information	Value
Client version	Software Distribution Client 0750
Computer name	SI1-2003ENG
OS	Windows Server 2003, Enterprise E...
OS version	0502
OS sub-version	No Service Pack
OS build number	3790
Internet Explorer version	6.0.3790.0
IE patch	N/A
WMI	3790.0000
Windows Installer	2.0.3790.0
MBSA	1.2.1
Domain/Workgroup	WORKGROUP
Domain type	Standalone server
Company name	hitachi
Owner	soft
Logon user name	SI1-2003ENG\Administrator
User description	Built-in account for administering th...
OS serial number	00000-000-0000000-00000
Locale	English(United States)
OS language	English
Current time zone	GMT+09:00
OS Installation date/time	12/03/2004 12:07:53 GMT+09:00
Last startup date/time	04/13/2005 15:16:10 GMT+09:00
Boot device	\Device\HarddiskVolume1
Windows directory	E:\WINDOWS

For details about the types of system information that you can obtain, see *2.2.1(1) System information that can be obtained from a Windows client* and *2.2.1(2) System information that can be obtained from a UNIX client*.

Software information

You can obtain the types and versions of the software products installed at each client. You can manage the software information that is shown in **Add/Remove Programs**, which is accessed from the Windows **Control Panel**, and search by file name for software that is installed at the clients. For anti-virus products, you can also obtain information such as the resident/nonresident settings and the version of the virus definition file. Additionally, you can obtain information about patches that have or have not been applied to the client computer, and manage such information in the same manner as the software information. WUA or MBSA 1.2.1 functionality is used to obtain patch information.

Figure 1–8: System Configuration window (software information)


Software Distribution Manager - [System Configuration: dmp94250: Modified: 06/07/2002 14:21:03]
File Edit Execute View Options Window Help
System configuration
Network
man1
dmp
dmp
dmp1251e
dmp248
dmp321.soft.hita
dmp94250
dmpguisv
KONISHI
x

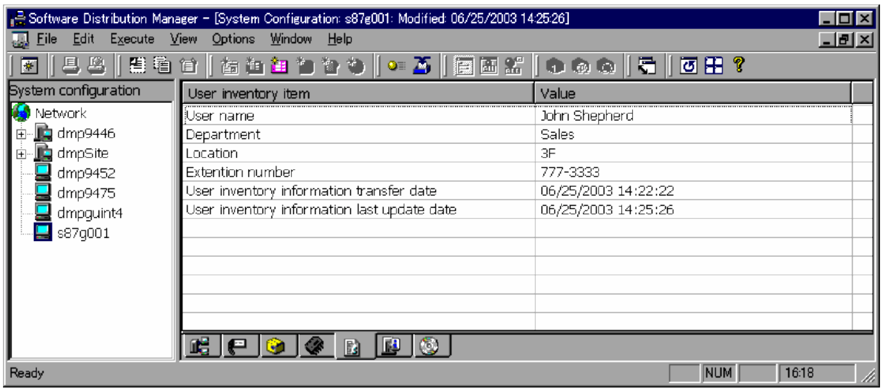
Installed package	Package ID	Installation	Ne...	P...	P..	Install...
Microsoft Internet Explorer ...	WUA-IE4024	Finished	0000			06/07/...
Microsoft Music Control	WUA-MSMUSC...	Finished	0000			06/07/...
Microsoft Outlook Express 5	WUA-OUTLOO...	Finished	0000			06/07/...
Microsoft Visual C++ 6.0 E...	WUA-VISUALC...	Finished	0000			06/07/...
Microsoft Wallet	WUA-MSWALL...	Finished	0000			06/07/...
Microsoft Windows Media ...	WUA-MPLAYE...	Finished	0000			06/07/...
MSN Messenger Service 2.2	WUA-MSMSGS...	Finished	0000			06/07/...
VDOLive Player	WUA-PLAYER16	Finished	0000			06/07/...

For details about the types of software information that can be obtained, see *2.2.2(1) Available software information*.

User inventory information

You can manage items of interest to the system administrator, such as user names and the serial numbers of computers. Although client users usually enter client information, a system administrator can also enter it in a batch operation.

Figure 1–9: System Configuration window (user inventory information)

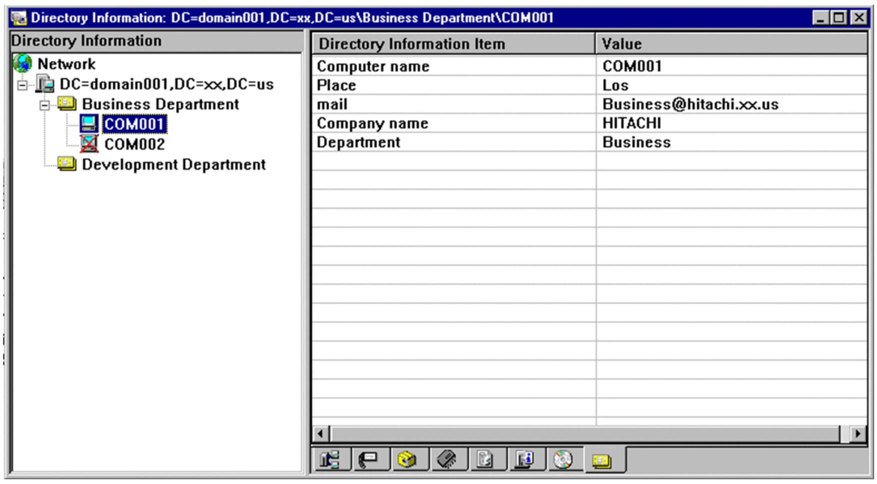


User inventory item	Value
User name	John Shepherd
Department	Sales
Location	3F
Extention number	777-3333
User inventory information transfer date	06/25/2003 14:22:22
User inventory information last update date	06/25/2003 14:25:26

Directory information

You can manage the user and computer information obtained from Active Directory according to the hierarchical structure in Active Directory.

Figure 1–10: Directory Information window (directory information)



Directory Information Item	Value
Computer name	COM001
Place	Los
mail	Business@hitachi.xx.us
Company name	HITACHI
Department	Business

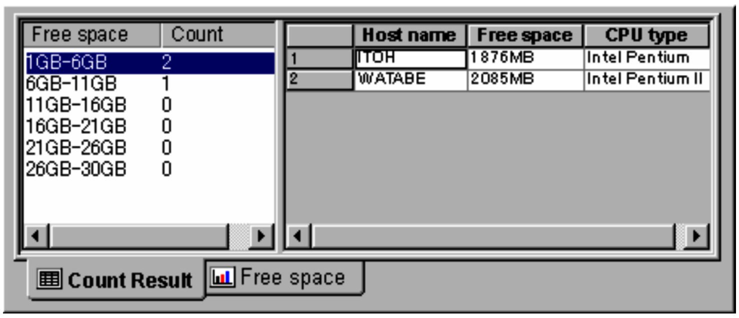
(2) Using inventory information

Once you have acquired inventory information, you can correlate inventory data and display the results in a graph. You can also save desired information to a CSV-format file, and print it. Some examples of using inventory information are given below.

Managing hardware and software usage status

You can use hardware or software information as a condition, and then count the number of clients that satisfy a particular condition. Counting the number of clients according to hard disk or memory capacity can be useful for planning purposes: for example, in developing a hardware-purchasing plan.

Figure 1–11: Count Clients window (counts for free hard disk space)



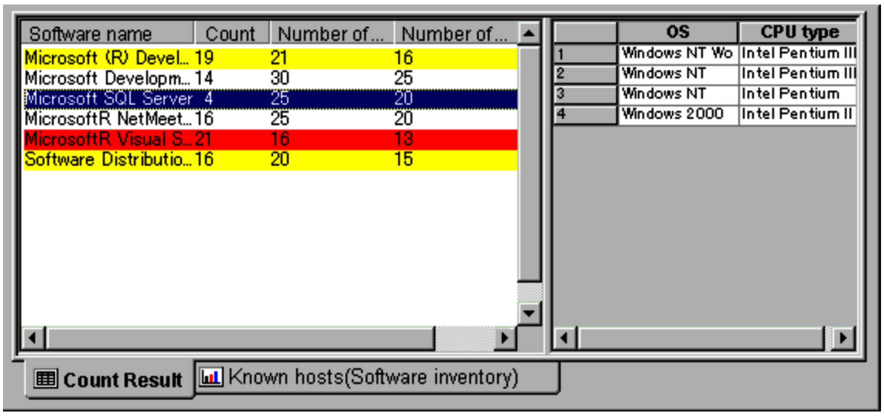
Free space	Count
1GB-6GB	2
6GB-11GB	1
11GB-16GB	0
16GB-21GB	0
21GB-26GB	0
26GB-30GB	0

	Host name	Free space	CPU type
1	ITOH	1876MB	Intel Pentium
2	WATABE	2085MB	Intel Pentium II

Managing software licenses

You can determine the number of clients in which a particular type of software is installed, and use this information to manage software licenses and upgrades.

Figure 1–12: Count Clients window (counts for each type of installed software)



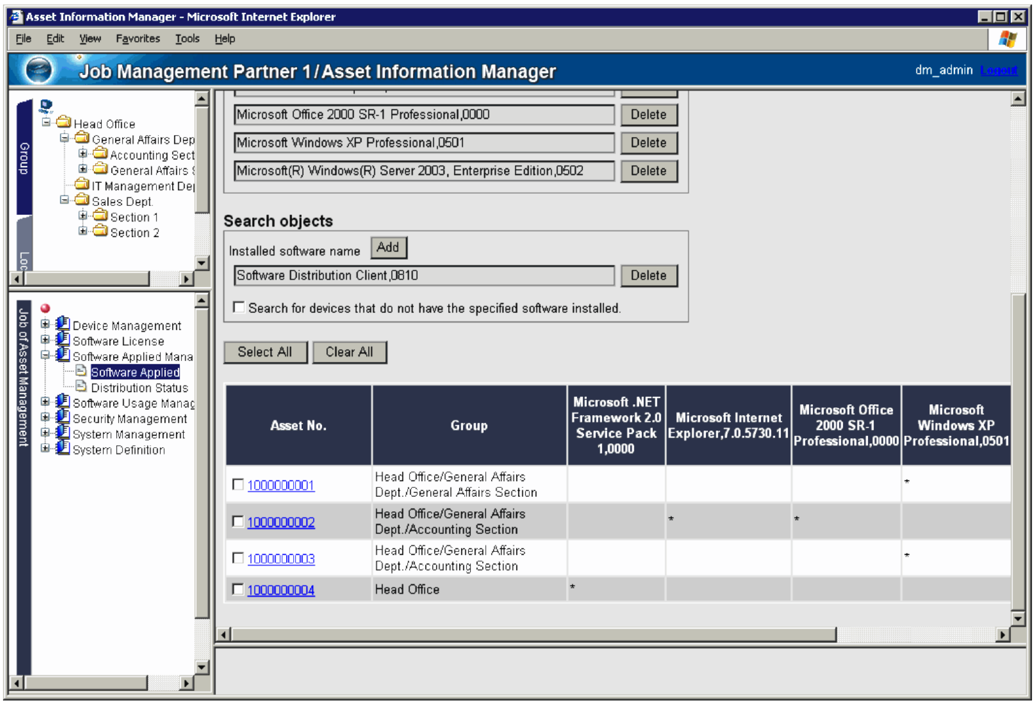
Software name	Count	Number of ...	Number of ...
Microsoft (R) Devel...	19	21	16
Microsoft Developm...	14	30	25
Microsoft SQL Server	4	25	20
MicrosoftR NetMeet...	16	25	20
MicrosoftR Visual S...	21	16	13
Software Distributio...	16	20	15

	OS	CPU type
1	Windows NT Wo	Intel Pentium III
2	Windows NT	Intel Pentium III
3	Windows NT	Intel Pentium
4	Windows 2000	Intel Pentium II

Counting according to job goal

By linking with client information, you can total the values provided for software installation statuses and operation statuses. Since search conditions are provided according to job goals, you can obtain precise counting results for each goal.

Figure 1–13: Software Applied window



Microsoft Office 2000 SR-1 Professional,0000 Delete

Microsoft Windows XP Professional,0501 Delete

Microsoft(R) Windows(R) Server 2003, Enterprise Edition,0502 Delete

Search objects

Installed software name Add

Software Distribution Client,0810 Delete

☐ Search for devices that do not have the specified software installed.

Select All Clear All

Asset No.	Group	Microsoft .NET Framework 2.0 Service Pack 1,0000	Microsoft Internet Explorer,7.0.5730.11	Microsoft Office 2000 SR-1 Professional,0000	Microsoft Windows XP Professional,0501
☐ 1000000001	Head Office/General Affairs Dept./General Affairs Section				*
☐ 1000000002	Head Office/General Affairs Dept./Accounting Section		*	*	
☐ 1000000003	Head Office/General Affairs Dept./Accounting Section				*
☐ 1000000004	Head Office	*			

Using inventory information as a resource management ledger

Because you can display or print required inventory information, you can use this information as a resource management ledger.

Editing and using inventory data

Inventory data can be output to a CSV-format file. This CSV data can then be input into spreadsheet software, which makes it easy for you to sort the information and create reports.

Using inventory information to group clients

You can create a group of clients that all have the same inventory information and specify the group as a destination for software distribution. For example, you can define all clients on which Microsoft Word 2000 is installed as a group and specify that group as a remote installation destination for Microsoft Word 2003.

(3) Acquiring inventory information from stand-alone PCs

A JP1/Software Distribution system distributes software and manages inventory over a network. It also enables you to obtain inventory information from stand-alone PCs without using a network. This facility is useful when you want to manage the inventory of PCs that are not on the network, as well as the PCs on the network. This facility is available for stand-alone PCs (offline machines) on which JP1/Software Distribution Client is installed.

To obtain inventory information from an offline machine, at the managing server you first create a program to obtain the inventory information and then save the program to storage media, such as a FD, CD-R, or MO. You then transport this media to the location of the offline machine and execute the program. Save the acquired inventory information to storage media and then input the information to the managing server where it can be managed.

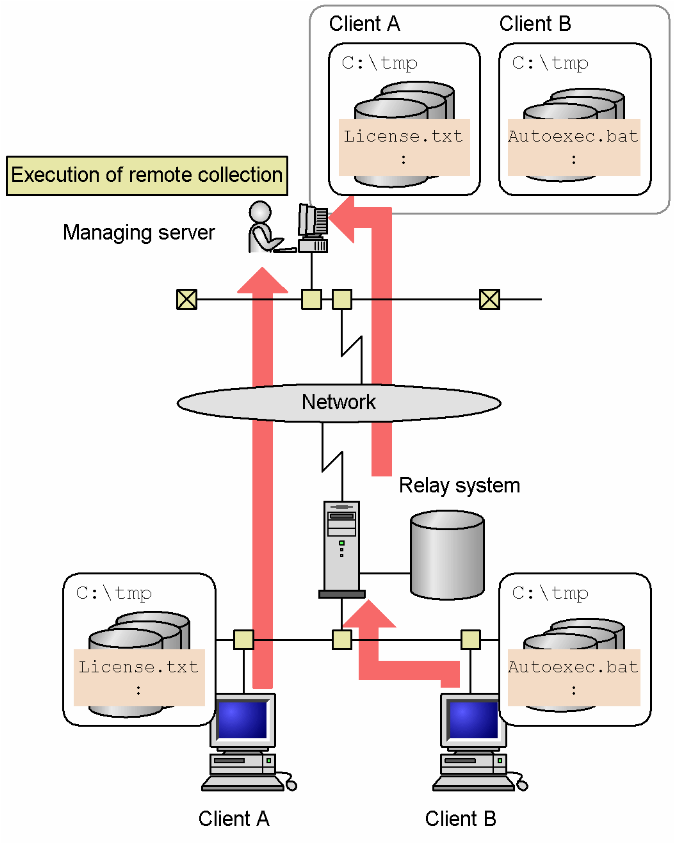
1.2.3 File collection

You use the file collection facility to collect client files at the central server. This is called (*remote collection*), and is used for tasks like the following:

- Collecting client job data in a batch, and then using it for a job.
- Collecting error and log information from client applications and analyzing it to facilitate troubleshooting.

To collect files, you create and execute a job from the managing server in the same way that you create a job to distribute software. You can place relay systems between the managing server and the clients to drive file collection and to transfer the collected files. The following figure shows an overview of the file collection facility.

Figure 1–14: File collection facility



Files are collected after being compressed or archived. Because remotely collected files that have been compressed or archived cannot be read directly, you must restore them to their original format by using the *unarchiver* facility of JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system).

For details about the file collection facility, see *2.4 Collecting files (by remote collection)*.

1.2.4 Software operation status monitoring

When you execute a job that monitors software operation status, you can suppress startup of software on clients and acquire software operation logs and operation times. For example, by preventing printing and copying of data into USB memory at a client, you can prevent confidential information from being leaked. You can also obtain Web site access logs, and monitor access to risky Web sites that might result in information leakage.

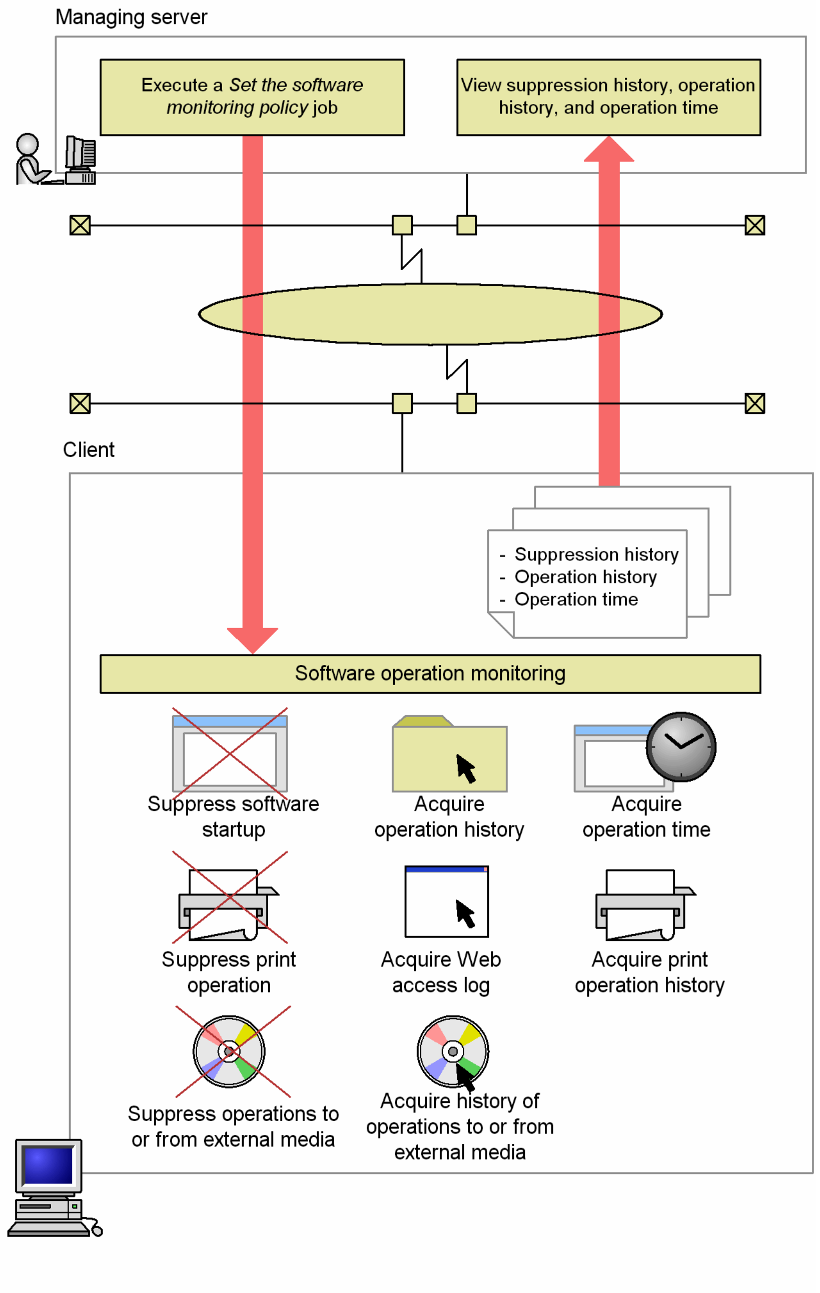
By displaying the acquired suppression logs and operation logs, you can check all operations or you can check only specific operations performed during a specified period of time. You can also trace the history of operations performed on specific files.

From the acquired operation times, you can check the usage status of each software asset.

Monitoring software operation statuses enables you to better understand overall software usage, and enables you to more easily trace and identify unauthorized use of software.

The following figure shows an overview of software operation monitoring.

Figure 1–15: Software operation monitoring


Managing server
Execute a *Set the software monitoring policy* job
View suppression history, operation history, and operation time
Client
- Suppression history
- Operation history
- Operation time
Software operation monitoring
Suppress software startup
Acquire operation history
Acquire operation time
Suppress print operation
Acquire Web access log
Acquire print operation history
Suppress operations to or from external media
Acquire history of operations to or from external media

For details about monitoring software operation status, see *2.5 Monitoring software operation statuses* and *2.6 Managing software operation information*.

The software operation status monitoring function can also acquire operation history, suppression history, and operation times from offline machines. For details about monitoring the operation status of offline machines, see *2.5.12 Monitoring the operation status of stand-alone PCs*.

1.2.5 Client management

JP1/Software Distribution enables you to obtain patches provided by Microsoft, and then distribute and apply these patches to clients. You can also collect and manage information about patches you have previously applied to clients.

By linking to WSUS, you can also manage security updates for clients. From the managing server, you can monitor the system status of clients and send messages to clients.

You can also use the AMT functionality to control any of your client computers that support AMT.

(1) Managing patch application status

JP1/Software Distribution enables you to use the managing server to obtain patches provided by Microsoft, such as security updates and service packs. You can then use the remote installation facility to apply the obtained patches to clients. You can also obtain information about the patches (*patch information*) that have already been applied to the clients (or not applied to clients). This means that you can use JP1/Software Distribution for centralized management of the entire operation flow from obtaining patches to managing their application status.

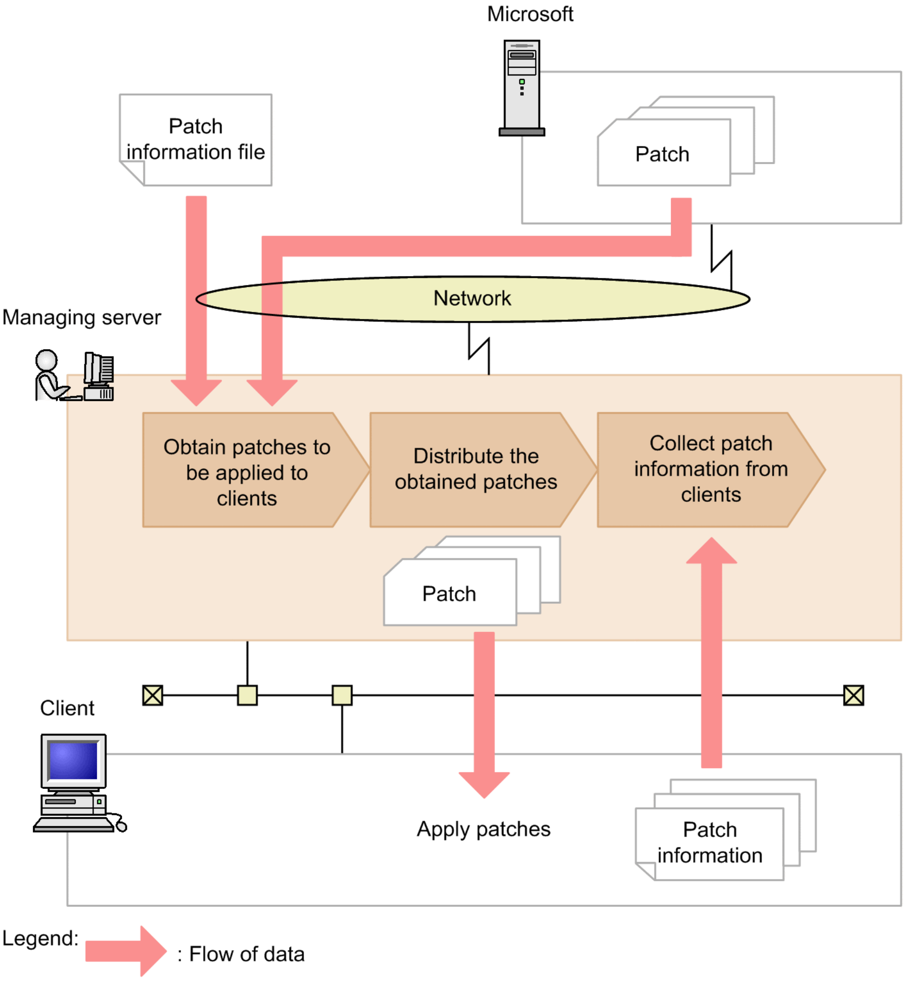
Thus, by using JP1/Software Distribution to manage the application status of patches, you can maintain system security based on the timely and accurate application of patches, without having to deploy WSUS.

To obtain patches, you first obtain a *patch information file*. For details about how to obtain the current patch information file, see the Readme file for JP1/Software Distribution Manager.

The patch information file contains information about patches available from Microsoft. You use this file to decide which patch data you wish to obtain. The patch information file is updated based on the patches that are currently being provided by Microsoft.

The following figure shows the operation flow for centralized management of patch application status.

Figure 1–16: Operation flow for centralized management of patch application status



Management of patch application status is separated into the following three operations:

- Obtaining patches to be applied to clients
- Distributing the obtained patches
- Detecting client patch information

The following subsections explain these operations.

(a) Obtaining patches to apply to clients

You obtain patches based on the information in the patch information file. JP1/Software Distribution enables you to manage patch acquisition status and to configure your system to obtain patches automatically. You can also automatically package the patches you have obtained.

For details about the patch acquisition feature, see *2.7.1 Obtaining patches to apply to clients*.

(b) Distributing the obtained patches

You use the software distribution facility to apply the obtained patches to the clients. A package can be created automatically when patches are obtained, which relieves you of having to perform the packaging work.

For details about the software distribution facility, see *2.1 Software distribution (remote installation)*.

(c) Detecting client patch information

You use WUA or MBSA 1.2.1 to detect information about patches at clients. Client patch information can be collected and managed as software information.

For details about the patch information detection feature, see *2.7.2 Detecting client patch information*.

(2) Linking with WSUS to manage security updates

Some WSUS security update management tasks can be distributed from JP1/Software Distribution.

By linking with WSUS, you can use JP1/Software Distribution to create a WSUS computer group and update the approval status of security updates, which reduces the burden of managing security updates.

For details about the functions that can be linked with WSUS, see *2.7.3 Linking with WSUS to manage security updates*.

(3) Monitoring a client system

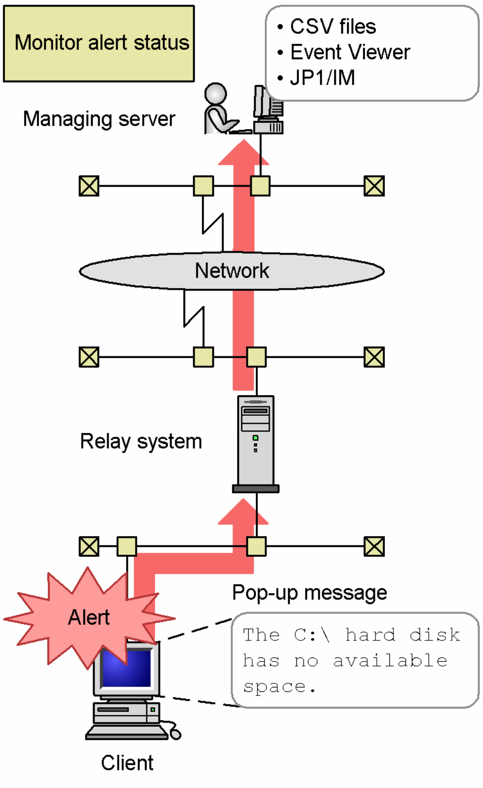
If a problem occurs with the available capacity in a hard disk or in memory at a client, the client system monitoring facility can send an alert to the central server and the system administrator can check the alert log file or use the Event Viewer to check the situation. This enables the system administrator to monitor the status of the entire client system.

The client user can also be alerted to a problem by a means such as a pop-up message, thus facilitating local system management.

To implement alerts, you start the *system monitoring facility* at each client and set it up so that alerts will be sent to a higher JP1/Software Distribution system. The alert information will be relayed if there is a relay system between the client and the managing server. This enables the managing server and relay system to monitor for any alert status in any of the lower-level clients.

The following figure gives an overview of client system monitoring.

Figure 1–17: Client system monitoring



```
The C:\ hard disk
has no available
space.
```

Managing server and relay system can check CSV files and the Windows NT Event Viewer for alert information. They can also send messages to JP1/IM.

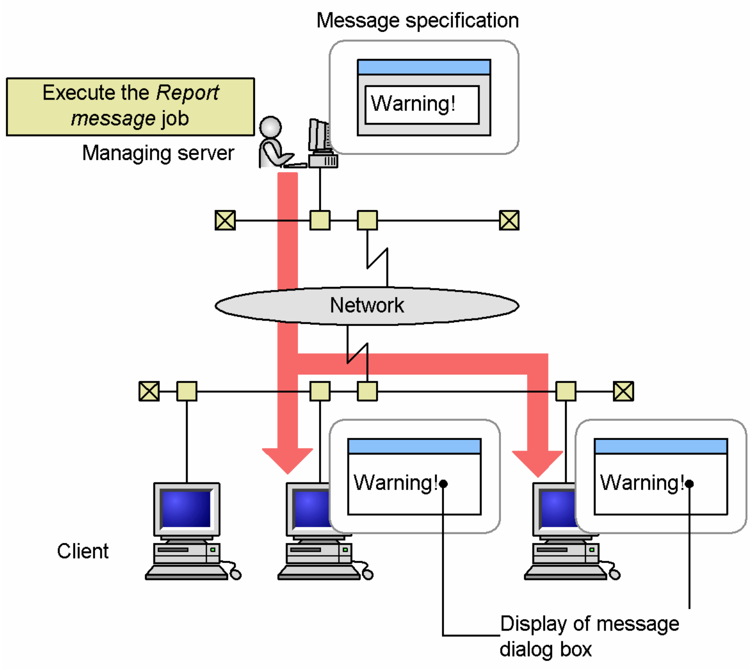
For details about monitoring client systems by means of alert reports, see *2.7.4 Monitoring client systems*.

(4) Sending messages to a client

To send information, such as notes and warnings, to a client, the administrator can execute the *Report message* job to send a message to the client at the job destination. Any information can be specified as the message. You can select whether to send the message in text format or in HTML format. This does not take up space in the client's PC memory because there is no need to send a package, and the message is deleted once it is read by the client. This facility is useful for sending a warning message to a specific client where there is a security problem, or for sending system maintenance information to multiple clients in the batch mode.

The following figure shows an overview of message transmission to a client.

Figure 1–18: Message transmission to a client



For details about sending messages to clients, see *2.7.5 Sending messages to clients*.

(5) Using AMT to control clients

AMT Linkage, which is provided as a component of JP1/Software Distribution, enables you to use AMT power control to control any of your client computers that support AMT. Note, however, that you cannot use this power control on clients that are in a wireless LAN environment.

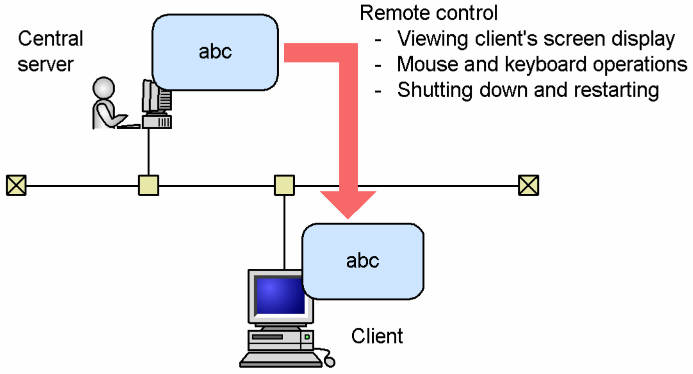
You can also set up AMT Linkage so that a client will always be recognized as the same asset, even after you have re-installed it. By remotely controlling a client whose power is turned off, you can set up its BIOS, or execute a diagnostic program from a floppy disk inserted in the central manager's computer.

For details about controlling clients that use AMT, see *2.7.6 Using AMT to control clients*.

1.2.6 Client remote control

The client remote control facility can display a client screen on the server screen so that the client screen can be managed by *remote control*. Not only can you use the server's keyboard or mouse to perform operations in an accessed client window, but you can also issue instructions to shut down and restart the client. The following figure shows an overview of the client remote control facility.

Figure 1–19: Remote control facility


Central server
abc
Remote control
- Viewing client's screen display
- Mouse and keyboard operations
- Shutting down and restarting
abc
Client

You can use this facility for purposes such as the following:

- Executing, from the server, corrective measures for a client error

  If an error occurs in a program running at a remote client, the cause of the error can be investigated and a corrective measure can be implemented from the server, without the need to travel to the remote site.
- Remote maintenance of a client

  From the server, you can set up, uninstall, or modify the configuration of programs installed at a client.

For details about the remote control facility, see the manual *Job Management Partner 1/Remote Control Description and Operator's Guide*.

1.2.7 Linkage to other programs

By linking JP1/Software Distribution to other programs, you can achieve the following management tasks:

- Managing users by linking with JP1/Base

  You can use the JP1/Base user management functionality to manage users of JP1/Software Distribution. By creating accounts that set permissions for each user type, you can limit the JP1/Software Distribution functions that can be used by specific users.

  For details about the facility for linking with JP1/Base, see *2.14.1 Managing users when JP1/Software Distribution is linked to JP1/Base*.
- Managing the application of software from JP1/Asset Information Manager

  This facility enables you to use the windows provided by JP1/Asset Information Manager to distribute software to devices managed by JP1/Asset Information Manager and to view the software distribution status.

  For details about the facility for linking with JP1/Asset Information Manager, see *2.14.2 Managing application of software from JP1/Asset Information Manager*.
- Managing security by linking with JP1/Client Security Control

  A security management system that has JP1/Client Security Control installed can monitor the status of clients' security handling, based on the inventory information collected by JP1/Software Distribution. If there is any problem in a client's security handling, you can use JP1/Software Distribution to take appropriate action.

  For details about linking with JP1/Client Security Control, see *2.14.3 Managing security by linking with JP1/Client Security Control*.
- Managing JP1/Software Distribution from JP1/IM

  This linkage enables you to use JP1/IM windows to distribute software and view the software distribution status.

  For details about linking with JP1/IM, see *2.14.4 Managing JP1/Software Distribution from JP1/IM*.
- Managing JP1/Software Distribution from HP NNM

  This linkage allows you to use the monitoring windows of HP NNM version 7.5 or earlier to view software distribution status and client inventory information.

  For details about the linking with HP NNM, see *2.14.5 Managing JP1/Software Distribution from HP NNM*.
- Executing jobs automatically by linking with JP1/AJS

  You can link JP1/Software Distribution with JP1/AJS to automate software distribution. JP1/Software Distribution provides a command interface for executing commands in the background. For details about linking JP1/AJS, see *2.14.6 Executing jobs automatically by linking with JP1/AJS*.

1.3 System components of JP1/Software Distribution

This section describes the components of a JP1/Software Distribution system. The section also describes the relationships between JP1/Software Distribution programs and system components, and the system components that the user must be familiar with for each operation method.

1.3.1 Basic system components

A JP1/Software Distribution system consists of the following components:

Managing server

The *managing server* is the system that is positioned at the top in the hierarchy; it executes the jobs that distribute software to lower systems and jobs that acquire inventory information.

In addition to executing jobs, you can use the managing server to manage lower-level systems. For example, you can use it check the status of job execution and to display and sum up the values in acquired inventory information.

Relay manager/system

A *relay manager/system* (relay manager and/or relay system) is positioned between a managing server and clients; it relays jobs from the managing server to lower-level systems.

In addition to the job relay functionality, a relay manager/system includes both managing server functionality for executing jobs in the lower-level systems, and client functionality for receiving jobs.

You can place not only clients under a relay manager/system, but also other relay managers/systems.

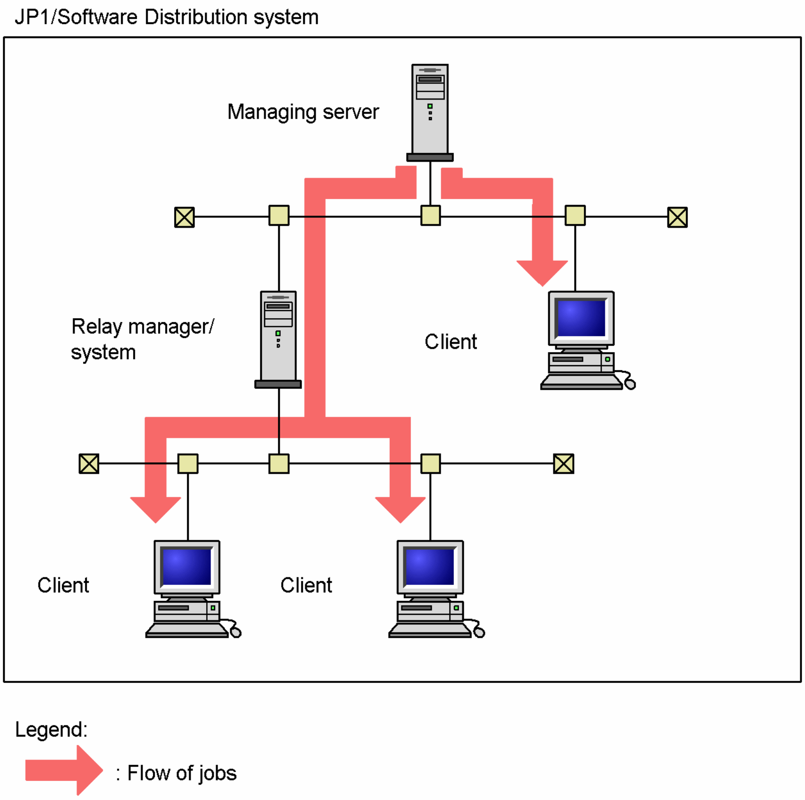
Client

A *client* is a system that is positioned under a managing server and a relay manager/system; it receives and executes jobs executed by the managing server and reports the execution results.

A client can install distributed software and report its inventory to the managing server.

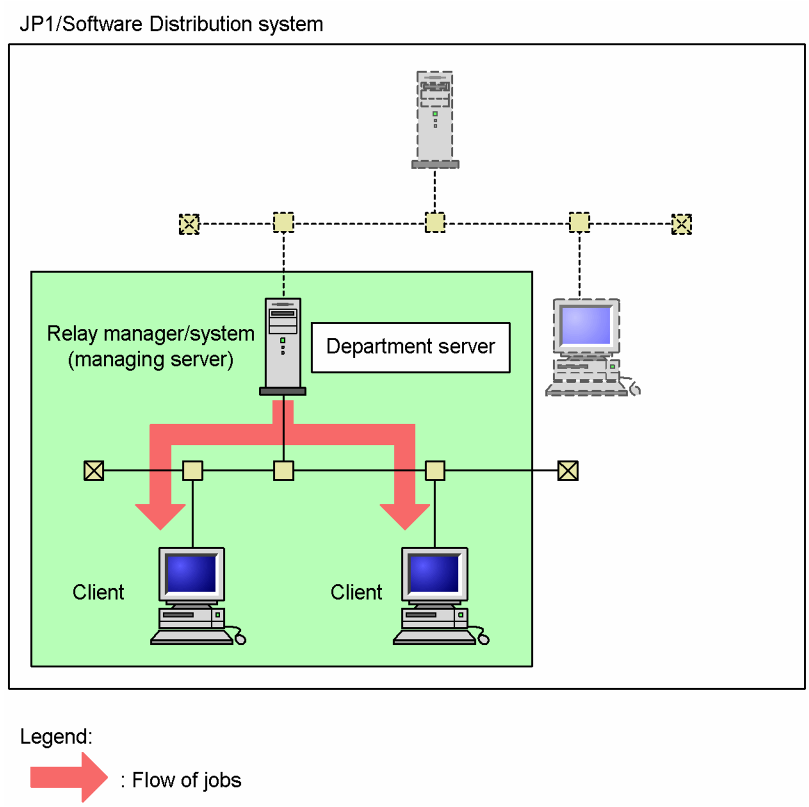
The following figure shows the relationships between a managing server, relay manager/system, and clients in a JP1/Software Distribution system:

Figure 1–20: Relationships between the JP1/Software Distribution system components



In a system managed by a single department server for the entire JP1/Software Distribution system, a relay manager/ system acts as the managing server in that system.

Figure 1‒21: Relationships between the JP1/Software Distribution system components (in a system managed by a department server)


JP1/Software Distribution system
Relay manager/system (managing server)
Department server
Client
Client
Legend:
: Flow of jobs

1.3.2 Relationships between programs and system components

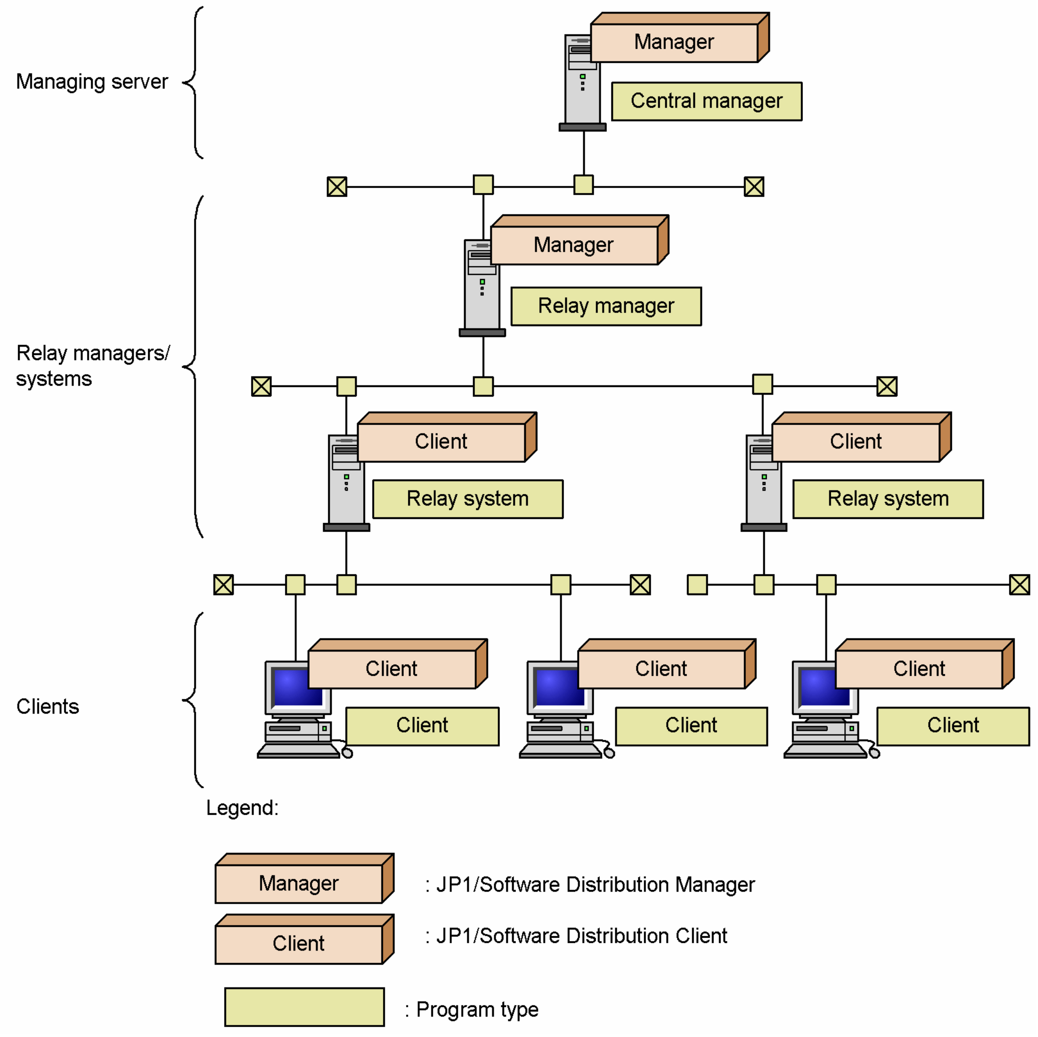
A JP1/Software Distribution system consists of the following two types of programs:

- JP1/Software Distribution Manager
- JP1/Software Distribution Client

When you create a JP1/Software Distribution system, you install appropriate programs on each system component, such as the managing server, the relay managers/systems, and the clients.

The following figure shows the relationships between the JP1/Software Distribution programs and the system components:

Figure 1–22: Relationships between programs and system components



The following describes the types of programs and the programs that can be used in each system component.

(1) Types of programs

This subsection describes each JP1/Software Distribution program.

(a) JP1/Software Distribution Manager

JP1/Software Distribution Manager can use all the resource and distribution management facilities provided by JP1/Software Distribution. It manages the relay managers/systems and the clients positioned under them. The JP1/Software Distribution Manager positioned at the top of a system is called the *central manager*.

JP1/Software Distribution Manager can also be a relay manager/system. A JP1/Software Distribution Manager used as a relay manager/system is called a *relay manager*.

(b) JP1/Software Distribution Client

JP1/Software Distribution Client is used as a relay manager/system or as a client in a JP1/Software Distribution system. When you install JP1/Software Distribution Client, you select whether it is to be used as a relay manager/system or as a client. JP1/Software Distribution Client used as a relay manager/system is called a *relay system*.

(2) Programs that can be used in the system components

The following table lists the programs that can be used in the system components (managing server, relay manager/system, and client) and their types:

Table 1–1: Programs that can be used in the system components

System component	Applicable program	Type#
Managing server	JP1/Software Distribution Manager	• Central manager • Relay manager
	JP1/Software Distribution Client	Relay system
Relay manager/system	JP1/Software Distribution Manager	Relay manager
	JP1/Software Distribution Client	Relay system
Client	JP1/Software Distribution Client	Client

#: You select the type when you install the program. For details about program installation, see *2. Installing JP1/Software Distribution Manager* or *3. Installing JP1/Software Distribution Client* in the *Setup Guide*.

(a) Programs that can be used in the managing server

Basically, the managing server uses JP1/Software Distribution Manager, which is a program for administrators. You can use JP1/Software Distribution Manager to manage the entire JP1/Software Distribution system such as a central server at the headquarters.

You can also position JP1/Software Distribution Client at the top of the system and use it as the managing server. However, compared to using JP1/Software Distribution Manager as the managing server, there are limitations when using JP1/Software Distribution Client in this role, such as the number of clients that can be managed. Therefore, this usage should be employed only in a small system in which only a few dozen clients are to be managed.

For details about the functional differences between JP1/Software Distribution Manager and JP1/Software Distribution Client, see *D.1 Functional differences between JP1/Software Distribution Manager and JP1/Software Distribution Client (relay system)*.

(b) Programs that can be used in a relay manager/system

You can use JP1/Software Distribution Manager (relay manager) or JP1/Software Distribution Client (relay system) for a relay manager/system.

You choose the one you will use during program installation.

Compared to a relay manager, a relay system has limitations, such as on the number of clients that can be managed and the available functions. To manage clients from a relay manager/system in the same manner as when JP1/Software Distribution Manager is used as the managing server, you should use a relay manager. For details about the functional differences between a relay manager and a relay system, see *D.1 Functional differences between JP1/Software Distribution Manager and JP1/Software Distribution Client (relay system)*.

(c) Programs that can be used in a client

Only JP1/Software Distribution Client can be used as a client.

1.3.3 System components required for distributing software

The system configuration required for software distribution consists of all the basic system components plus *Packager*, which is registered in the managing server used to distribute software.

Packager

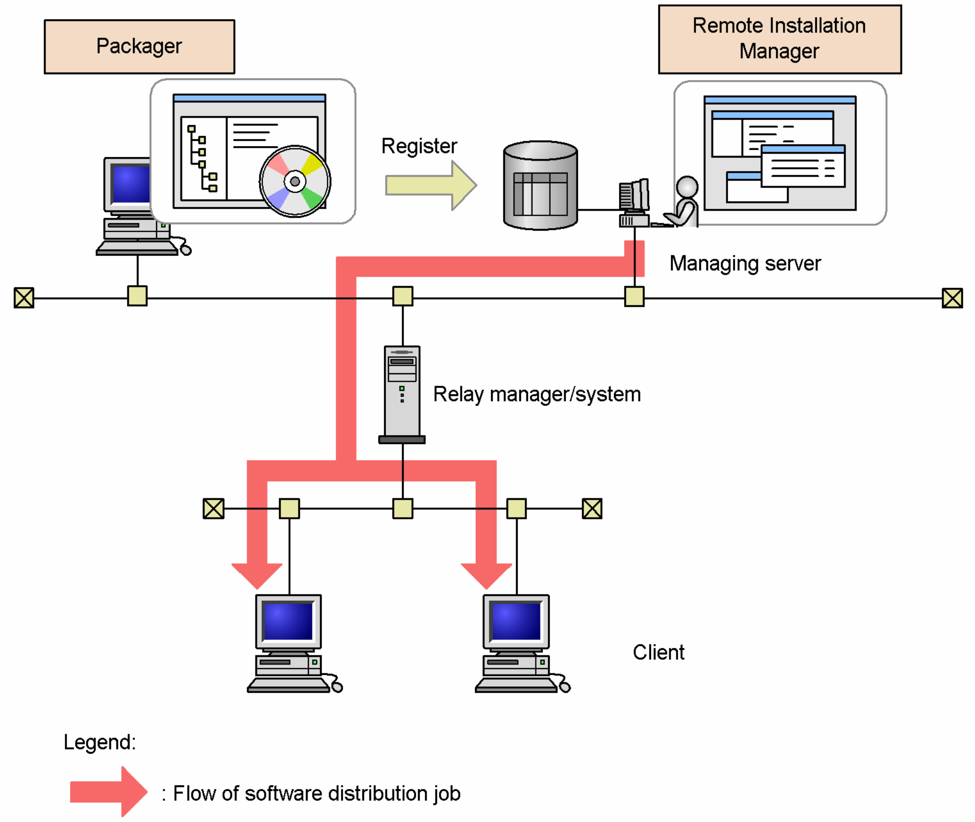
A program on a managing server that registers software for remote installation is called a *Packager*. You can install a Packager on the same PC as the managing server, on any relay manager/system, or on clients, or you can have a PC dedicated as the Packager.

The managing server installs the software registered by the Packager on the remote clients (remote installation).

To use the managing server's GUI to create and execute a job for executing remote installation, you must use *Remote Installation Manager*. You use Remote Installation Manager not only for software distribution but also for inventory management and software operation status monitoring.

The following shows the system configuration required for software distribution.

Figure 1–23: System configuration required for software distribution



1.3.4 System components required for managing inventory

The basic system configuration required for inventory management consists of a managing server, relay manager/system, and clients. To collect inventory data from a PC outside the network, you must add two more components:

Offline machine

An offline machine is a PC on which JP1/Software Distribution Client is installed but which is not registered in the JP1/Software Distribution system configuration. The following are examples:

- Stand-alone machines on which JP1/Software Distribution Client has been installed
- PCs that are in the network and on which JP1/Software Distribution Client is installed, but which are not registered as part of the JP1/Software Distribution system configuration

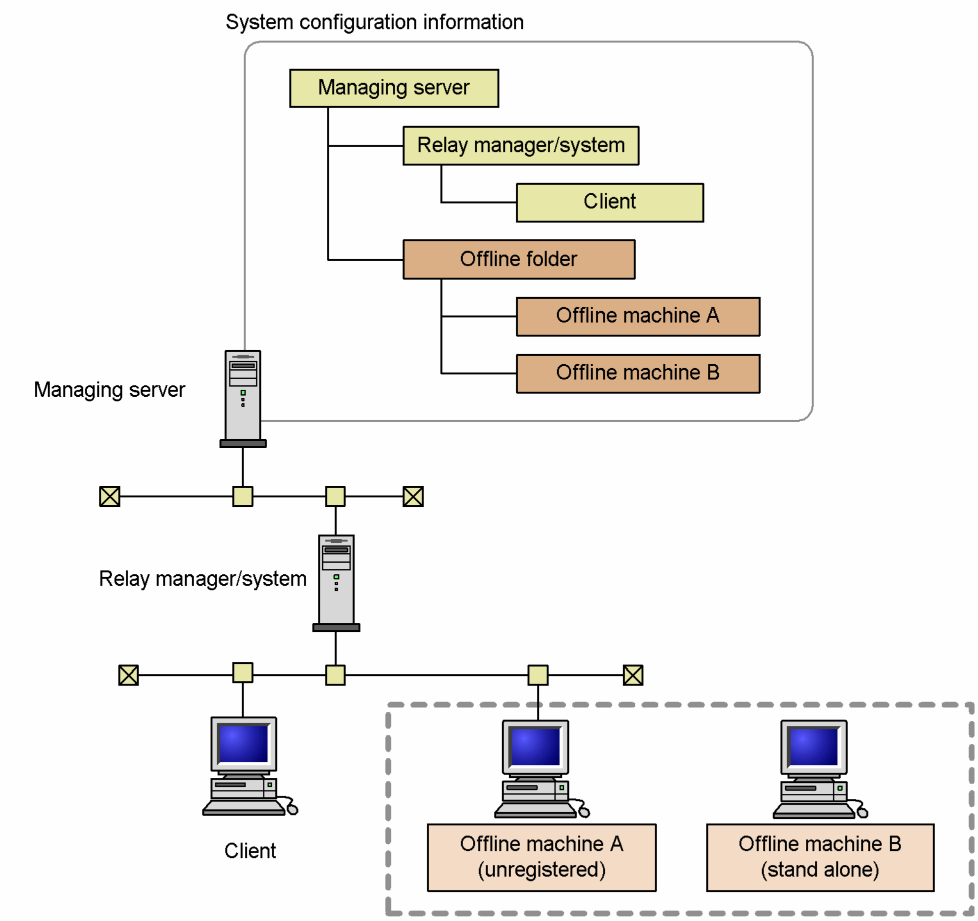
You can collect inventory data from such machines, even though they are not registered in the system configuration. You can also install software on the PCs that have not been registered in the system configuration information.

Offline folder

An offline folder is used to manage inventory data collected from offline machines. An offline folder is shown under the name `{OFFLINE}` in the system configuration information. Because is treated as a virtual relay system without an actual machine, you cannot rename it or change its hierarchical position.

The following figure shows a system configuration for managing inventory data.

Figure 1–24: System configuration for managing inventory



The system configuration shown in Figure 1-24 enables inventory data to be retrieved from clients and offline machines. The collected inventory data is managed by the managing server. Inventory data collected from offline machines is stored in the offline folder.

1.3.5 System components required for managing software operation statuses

The basic system configuration required for software operation status management consists of a managing server, relay manager/system, and clients.

Asset Information Manager Subset has been added to this basic system configuration, which extends the software operation status management functionality.

Asset Information Manager Subset

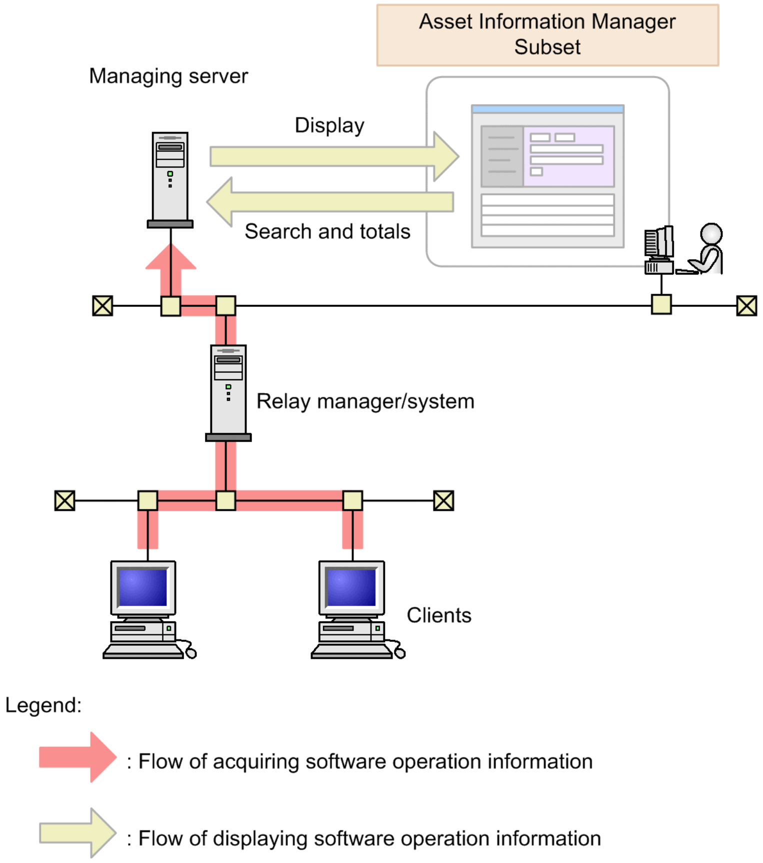
This is a JP1/Software Distribution Manager component that provides the GUI for summing up and viewing inventory information.

By installing this component, from Remote Installation Manager you can start the window for displaying software operation information. From this window, you can perform operations such as specifying search conditions and searching for operation information, and displaying the operation information summation results.

If you install Asset Information Manager Subset, you must also install Remote Installation Manager on the same PC.

The following figure shows the system components required for software operation status management:

Figure 1–25: System configuration required for software operation status management


Asset Information Manager Subset
Managing server
Display
Search and totals
Relay manager/system
Clients
Legend:
: Flow of acquiring software operation information
: Flow of displaying software operation information

1.3.6 System components required for using the remote control facility

The system configuration required for using the remote control facility consists of the local system (*Remote Control Manager*) and the remote system (*Remote Control Agent*).

Remote Control Manager

This program calls the remote client's window information and controls the client. It is one of the components of JP1/Software Distribution Manager.

Remote Control Agent

This is a remote program that provides the local system's window information to the Remote Control Manager to be controlled. It is one of the components of JP1/Software Distribution Manager (relay manager) and JP1/Software Distribution Client.

You can install the Remote Control Manager and Remote Control Agent on a PC on which other JP1/Software Distribution facilities, such as a client or a managing server, are installed. You can also install the Remote Control Manager on a PC that is not used as the managing server or a relay manager/system. If you are using the remote control facility only, you can use JP1/Remote Control.

The following table lists the operating environment for remote control.

Table 1–2: Operating environment for remote control

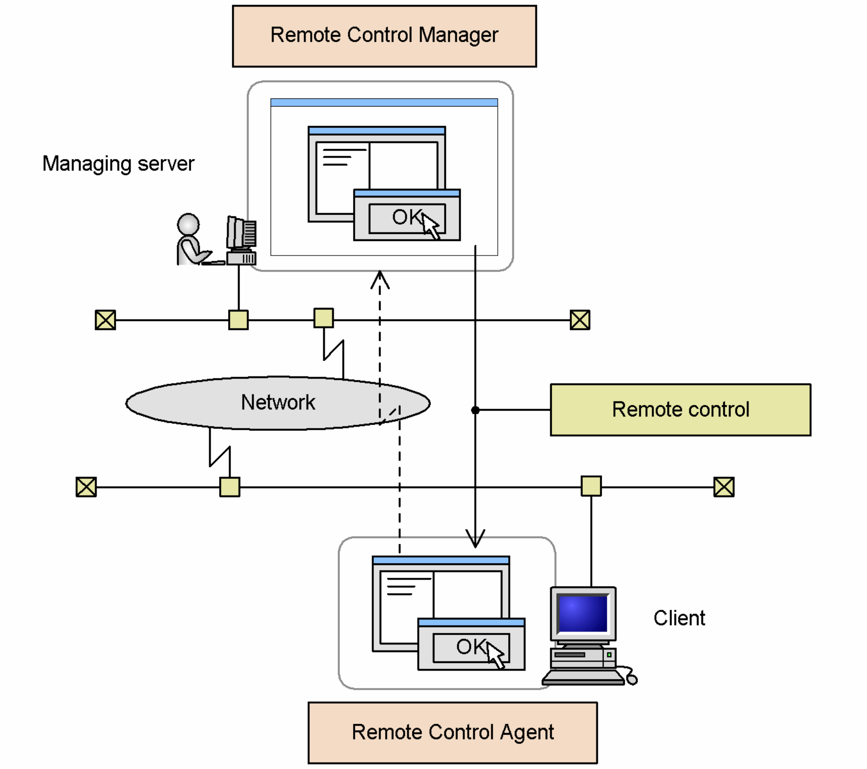
Program	Remote Control Manager	Remote Control Agent	Operating environment
JP1/Software Distribution Manager (central manager)	Y	N	• Windows 8 • Windows Server 2012 • Windows 7

Program	Remote Control Manager	Remote Control Agent	Operating environment
JP1/Software Distribution Manager (central manager)	Y	N	• Windows Server 2008 • Windows Vista • Windows Server 2003 • Windows XP Professional • Windows 2000
JP1/Software Distribution Manager (relay manager)	Y	Y	• Windows 8 • Windows Server 2012 • Windows 7 • Windows Server 2008 • Windows Vista • Windows Server 2003 • Windows XP Professional • Windows 2000
JP1/Software Distribution Client (relay system)	N	Y	• Windows 8 • Windows Server 2012 • Windows 7 • Windows Server 2008 • Windows Vista • Windows Server 2003 • Windows XP Professional • Windows 2000 • Windows NT 4.0
JP1/Software Distribution Client (client)	N	Y	Windows

Legend:
Y: Can be installed.
N: Cannot be installed.

The following figure shows the system configuration required for using the remote control facility.

Figure 1–26: System configuration required for using the remote control facility



2 Facilities of JP1/Software Distribution

This chapter provides details about the facilities of JP1/Software Distribution.

(For consistency with earlier documentation, this manual usually uses the term *facility* instead of the more common terms *functionality* or *function*.)

2.1 Software distribution (remote installation)

JP1/Software Distribution's *remote installation facility* enables you to distribute programs, such as Hitachi program products and other companies' software, to clients.

With this facility, you can specify the date and time that software distribution is to be executed, or you can distribute only to those clients that satisfy specified conditions. The facility also enables a client to specify the software to be distributed and software to be installed on a stand-alone PC on which JP1/Software Distribution has been installed.

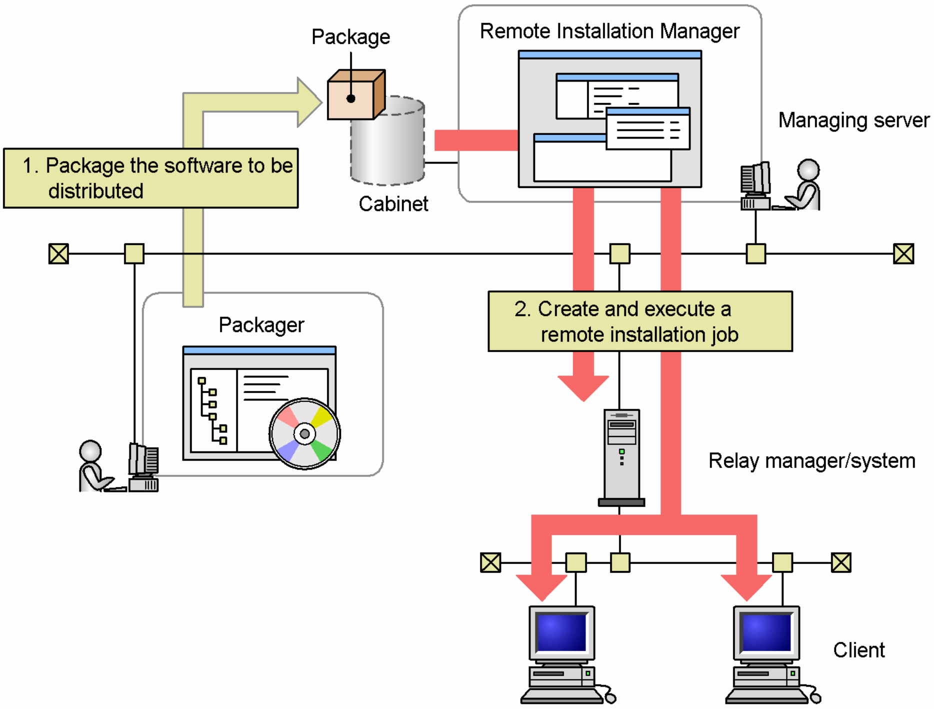
This section provides an overview of the remote installation facility.

2.1.1 General procedure for remote installation

The remote installation procedure consists of two stages: registering the software to be installed (packaging), and distributing and installing the registered package (remote installation).

The following figure shows the general procedure for remote installation.

Figure 2–1: General procedure for remote installation


Package
Remote Installation Manager
Managing server
1. Package the software to be distributed
Cabinet
Packager
2. Create and execute a remote installation job
Relay manager/system
Client

(1) Packaging the software to be distributed

To execute remote installation, in the managing server you must first register (package) the software that is to be installed. You can use the Packager to package software.

In a storage location on the managing server called a *cabinet*, the Packager stores the software subject to remote installation as well as information needed for installation. Software stored in this manner is called a *package*.

The Packager and the managing server can both reference and delete packages stored in a cabinet. However, a package cannot be renamed or moved to a different cabinet, so carefully check the cabinet configuration before you begin packaging. You can create a package on the managing server in advance, or you can use the Packager to create a new package at the time of packaging.

For details about the packaging procedure, see *2.1 Packaging procedure* in the manual *Administrator's Guide Volume 1*.

(2) Creating and executing a remote installation job

After you finish packing the software, at the managing server you create a job that provides instructions for remote installation, and then you execute that job. You can execute remote installation from Remote Installation Manager. For details about the remote installation procedure, see *2.3 Executing remote installation* in the manual *Administrator's Guide Volume 1*.

The remote installation tasks include not only creating and executing jobs, but also managing cabinets and packages, and deleting packages from relay systems. For details about managing cabinets and packages, see *2.1.7 Managing cabinets and packages*; for details about deleting packages from a relay system, see *2.1.8 Deleting packages from a relay system*.

The way remote installation works typically is that the client simply waits for the software to be installed automatically. However, there are some preparations and installation procedures required at the client side. For the client system to function appropriately to the needs of its users, attention must be paid to various procedures at the client. These procedures include selecting and installing only required software, and receiving software at a time appropriate to the client's schedule. For details about the operations at the client, see *2.13 Client facilities*.

2.1.2 Types of software available for distribution

JP1/Software Distribution classifies the software subject to remote installation into the following three types, called *package types*:

- Hitachi program products
- Other companies' software
- User programs and data

When software is packaged, the Packager automatically determines whether the software is in the category *Hitachi program products* or in the category *Other companies' software*. If the software does not belong to either of these categories, the Packager handles it as *User programs and data*.

Some packages require an *AIT file* (file created by the Automatic Installation Tool) or a *recorder file* (file created by Visual Test) during remote installation. For details about remote installation using an AIT or recorder file, see the manual *Automatic Installation Tool Description and Reference*.

(1) Hitachi program products

Remote installation applies to multiple-license pack products. For other program products, remote installation is permitted only for program upgrades. Note that remote installation is not available for some program products (such as communications software). To determine whether a program product can be installed remotely, check the accompanying documentation or release notes.

Remote installation for JP1/Software Distribution:

- JP1/Software Distribution Manager
  You cannot install this product in a remote installation.
- JP1/Software Distribution Client (relay system)
  You can install this product in a remote installation unless Automatic Installation Tool has been installed on the target PC. If Automatic Installation Tool has been installed on the target PC, Automatic Installation Tool is not overwritten, so you must manually install Automatic Installation Tool.
- JP1/Software Distribution Client (client)
  You can install this product in a remote installation unless *Startup Kit Support Tool* has been installed on the target PC. If Automatic Installation Tool has been installed on the target PC, Automatic Installation Tool is not overwritten, so you must manually install Startup Kit Support Tool and Automatic Installation Tool.

(2) Other companies' software

The term *other companies' software* refers to commercially available programs that are provided by companies other than Hitachi. Most multiple-license pack products from other companies qualify for remote installation. However, remote installation might not be permitted because of the type of software or the licensing agreement. If you cannot determine this from the software agreement or the other software's documentation, obtain permission from the applicable software company.

An AIT file or recorder file is required to automate responses if you use an interactive installer from another company for remote installation.

(3) User programs and data

You can use remote installation to install some or all files in a directory. The data created with an application such as a spreadsheet program is also handled as user data.

2.1.3 Installation conditions that can be set during packaging

To install software by remote installation, you must specify details of the intended installation during packaging. Such information might include the installation date and time, programs required for installation, and a recorder file to be used for installation. This is called the *installation conditions*.

You specify the installation conditions in the Software Distribution Packaging dialog box during packaging. During remote installation (at job creation), you can modify these conditions in the Change Installation Conditions dialog box.

This subsection describes the supported installation conditions on each page of the Software Distribution Packaging dialog box. For details about the settings, see *2.2 Specifying the packaging details* in the manual *Administrator's Guide Volume 1*.

(1) System Conditions

You can specify hardware requirements, such as the minimum hard disk space required for installation and the amount of memory to be available after installation. Specify any necessary information, such as the condition that there must be 10-20 MB of free space available after installation. Specifying memory requirements can prevent certain operation errors that can occur after installation.

(2) Software Conditions

If the software to be installed requires a specific version of another software program, you can specify software version information for purposes of checking that the correct programs are already installed. You can also specify a condition that remote installation is to be executed only if certain software is not installed on the client.

(3) File Properties

You can specify the access permission and owner of a file after remote installation.

(4) Schedule

You can specify the date/time for installation, and the timings of the installation. There are two installation timings:

- **Normal installation**
  The package is to be installed at the time the job is executed or at the specified installation date/time.
- **Install when system starts**
  The package is to be installed when the client's system starts.

(5) Installation Method

If the client's OS is Windows, you can specify an installation mode (installation method suitable for the software installer). There are two installation modes:

- **GUI installation mode**
  This installation mode uses a special installer (such as an interactive installer). When the package type is **Hitachi program products** or **Other companies' software**, the installation method is always set to the GUI installation mode.
- **Background installation mode**

This installation mode does not use any special installer. Use this mode when installation can be completed simply by copying files.

(6) Options

You can specify the following options for remote installation:

- **Compress package data**
  You use this option to compress and package software. Compressing a package speeds up its transfer and saves cabinet space needed for saving the package. However, compression and decompression take time during packaging and remote installation.
- **Restore old version when upgrade failed**
  You can use the *backup/restore facility* to protect the previous version of software in the event of a remote installation error. When this facility is used, the client also makes a backup copy of the previous version during remote installation for program upgrading. If remote installation fails, this backup copy is used to restore the previous version.
- **Restart computer after installation**
  You can set a client's computer to be restarted automatically after the package has been installed.
- **Display processing message**
  You can specify whether a processing message is to be displayed at the client while the package is being installed. The message is a dialog box indicating that downloading or installation is in progress.

(7) Create Icon

If the package type is **User programs and data**, you can set an icon or shortcut for the user programs.

(8) External Program

You can start execution of external programs at the client immediately before and after installation and in the event of an installation error. This feature enables you to:

- Set an icon or shortcut to be created when a user program, data, or differing-components package is installed.
- Use an external program to start an installed program product.

(9) Setup Information

If the package type is **Other companies' software**, you can specify desired setup information, such as the setup method, company name, and owner name.

(10) AIT File Settings

If you use an AIT file during remote installation, you can monitor the responses from the installation process.

(11) Recorder File

If you use a recorder file during remote installation, you must set the directory that contains the recorder file.

(12) Select Components

When packaging JP1/Software Distribution Client, you can select the components that are not to be packaged.

2.1.4 Job types for executing remote installation

After creating a package to be distributed, you must create and execute a job that provides instructions for remote installation by the managing server. There are three types of jobs related to remote installation, which are referred to as *job types*.

This subsection describes the job types for executing remote installation.

(1) Install package job

This is the basic job type. Jobs of this job type distribute a package from the managing server (or relay system) to clients, and then install the software. The managing server initiates package distribution and installation.

(2) Transfer package to relay system job

Jobs of this job type transfer a package from the managing server to relay systems only. The distribution and installation from the relay systems can be handled by the relay system administrators or initiated from the managing server. An *Install package* job is used to distribute the package to the clients.

When a *Transfer package to relay system* job and an *Install package* job are combined for remote installation from the managing server, the execution dates/times for these jobs become the package distribution times from the managing server to the relay systems and from the relay systems to the clients, respectively.

A package transferred by a *Transfer package to relay system* job is saved at the relay systems. Therefore, the managing server will not redistribute a package that has been saved at relay systems until its expiration date. When you package software, you can specify how long the package is to be saved. If you wish to change how long a package that has already been transferred to relay systems is to be saved, you must transfer the changed package to the relay systems again.

Note that a *Transfer package to relay system* job cannot be specified from a relay system.

(3) Send package, allow client to choose job

Jobs of this job type grant, to the clients, permission to decide whether to install the software. Each client determines which provided software will be installed and when.

Use normal remote installation only if the software must be installed at all clients. In other cases, software might be installed unnecessarily. Often, a *Send package, allow client to choose* job is the most efficient job to use.

For details about checking the software distributed by a job of this job type and installing it at the client, see *2.1.5 Executing installation according to a client user's schedule*.

2.1.5 Executing installation according to a client user's schedule

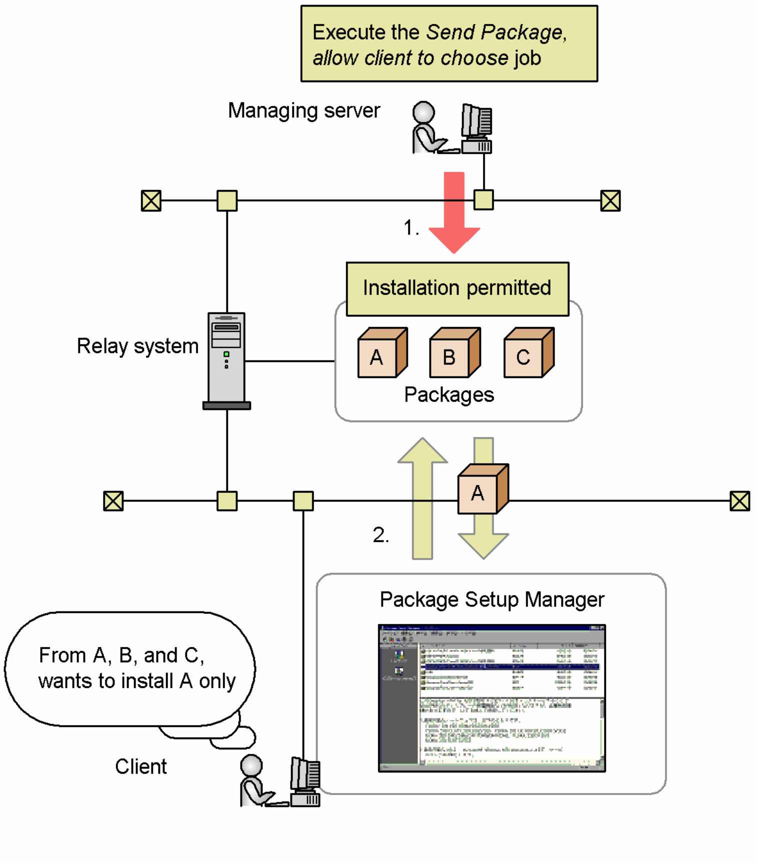
Remote installation initiated from the managing server is convenient for clients, but might result in unnecessary software being installed on a client or installation being executed at a time that is inconvenient for a client. You can avoid this by using a job of the job type *Send package, allow client to choose*.

When the managing server executes a job whose job type is *Send package, allow client to choose*, the client is granted permission to decide whether to install the package. The client can use Package Setup Manager to check which software is permitted to be installed, and then install only the necessary software.

This is also useful when the user at the client chooses to interact with the installer to install desired software.

The following figure shows the procedure for performing a remote installation in accordance with a client user's schedule.

Figure 2–2: Procedure for a remote installation in accordance with a client user's schedule


Execute the *Send Package, allow client to choose* job
Managing server
1.
Installation permitted
Relay system
A
B
C
Packages
A
2.
Package Setup Manager
From A, B, and C, wants to install A only
Client

To perform remote installation in accordance with a client user's schedule:

1. At the managing server, execute the *Send package, allow client to choose* job.
   Permission to install the package is granted to the client that was specified as the target (destination) of the job.
   At this point, the package is not distributed to the client; instead, it is held at the managing server or the relay system.
2. Use the client's Package Setup Manager to select desired software, and then execute installation.
   The selected software is downloaded to the client and its installation begins.

For details about how to operate Package Setup Manager, see *11.4 Using Package Setup Manager* in the manual *Administrator's Guide Volume 1*.

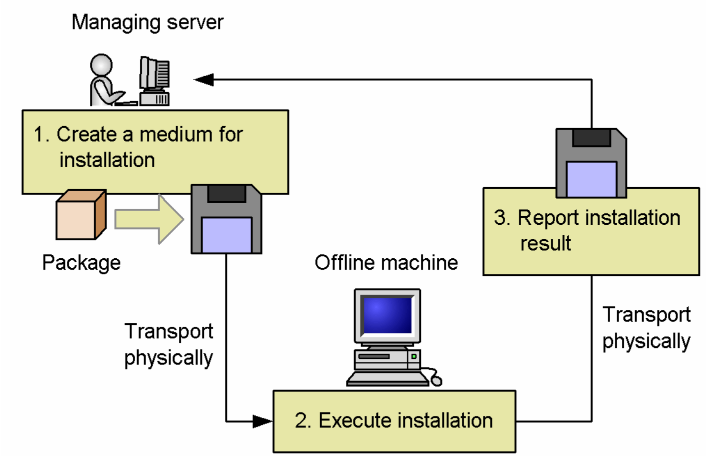
2.1.6 Installing software on a stand-alone PC

By using storage media such as a CD-R or MO disk, you can install software on a stand-alone machine (offline machine) in which JP1/Software Distribution Client is installed, without using a network. This is called offline installation. Offline installation can also be executed for a client where job execution is suspended by an instruction from a higher-order system.

For details about the offline installation method, see *7.7.1 Offline installation* in the manual *Administrator's Guide Volume 1*.

The following figure provides the general procedure for offline installation.

Figure 2–3: General procedure for offline installation



Offline installation is useful in the following cases:

- When you want to install a package on a PC outside the network
- When package transfer will take a long time, such as when the connected network's line speed is slow or the package is very large

To execute offline installation using a managing server and offline machine, the following conditions must be satisfied:

On the managing server:

- Windows JP1/Software Distribution Manager 07-50 or later (relational database version) has been installed
- Remote Installation Manager is used on the PC where the above JP1/Software Distribution Manager is running

On the offline machine:

Windows JP1/Software Distribution Client 07-50 or later has been installed

Note that the following actions cannot be performed in an offline installation:

- Installing JP1/Software Distribution Client#
- Specifying an installation schedule
- Restarting the computer following installation
- Installing from the Package Setup Manager
- Performing a split distribution or multicast distribution

#

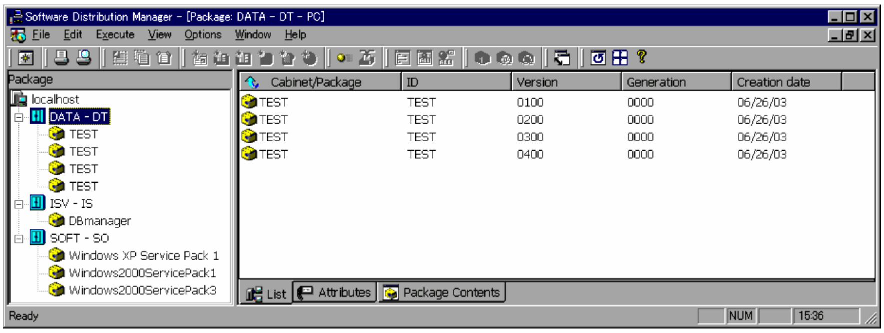
To install JP1/Software Distribution Client by overwriting the existing version without using a network, you can use JP1/Software Distribution Administrator Kit.

2.1.7 Managing cabinets and packages

Managing cabinets and packages is basically the managing server's (or relay system's) responsibility. You can use the Remote Installation Manager's Package window to check and edit packages as required. It is convenient to create cabinets in advance for different types of software and purposes (such as commercial software, user data, and anti-virus products).

The following is an example of the Package window:

Figure 2–4: Package window



Package

- localhost
  - DATA - DT
    - TEST
    - TEST
    - TEST
    - TEST
  - ISV - IS
    - DBmanager
  - SOFT - SO
    - Windows XP Service Pack 1
    - Windows2000ServicePack1
    - Windows2000ServicePack3

Cabinet/Package	ID	Version	Generation	Creation date
TEST	TEST	0100	0000	06/26/03
TEST	TEST	0200	0000	06/26/03
TEST	TEST	0300	0000	06/26/03
TEST	TEST	0400	0000	06/26/03

Cabinets and packages are listed in the Package window in the left-hand frame with the following icons:

- : Cabinet (for Windows client)
- : Cabinet (for UNIX client)
- : Package (successfully packaged)
- : Package (error occurred or currently being processed)
- : Package (differing-components packages#)

#

This icon is displayed for a differing-components package created by a JP1/Software Distribution version earlier than 7i. JP1 Version 8 or later does not support remote installation of differing-components packages.

In the Package window, you can perform the following operations on cabinets and packages:

- Check cabinets and packages
- Create cabinets
- Rename cabinets
- Delete cabinets and packages

For details about how to manage cabinets and packages, see *2.4 Managing cabinets and managing packages* in the manual *Administrator's Guide Volume 1*.

2.1.8 Deleting packages from a relay system

A relay system first stores the package files to be transferred to each client system. This might cause a shortage of disk space because the package files not deleted until the **Package expiration at the relay system** specified with the Packager is reached. If a hard disk space shortage occurs at a relay system, relaying of jobs will terminate with an error during job execution. If this happens, you must do one of the following to delete unneeded packages:

- From Remote Installation Manager in the relay system, delete the unneeded packages.
  From Remote Installation Manager in the relay system, select the unneeded packages and delete them.
- From the managing server, execute a *Batch delete packages on relay system* job.
  The *Batch delete packages on relay system* job deletes all the packages stored in the target relay system. This method is effective when all packages can be deleted from the relay system.
- From the managing server, select a package in the relay system and delete it.
  This method enables you to delete an unneeded package in a relay system by using the Remote Installation Manager in the managing server. For details about this facility, see *2.4.5 Deleting packages from a relay system* in the manual *Administrator's Guide Volume 1*.

2.2 Acquiring inventory information

By executing a job or a command from the managing server, you can acquire information about the clients (*inventory information*). The following inventory information can be acquired:

- System information
- Software information
- User inventory information
- Directory information

This section provides the details of the inventory information that can be acquired and gives an overview of how to acquire the inventory information.

It also describes how to use the acquired inventory information, explains the facility for acquiring inventory information from a stand-alone PC where JP1/Software Distribution is installed, and provides notes about managing inventory information.

2.2.1 Acquiring system information

You can obtain the system information used to manage clients' system usage status and the registry information for the clients. For details about how to acquire system and registry information, see *3.1 Collecting system information* in the manual *Administrator's Guide Volume 1*.

The following provides the details about the system and registry information that can be acquired.

(1) System information that can be obtained from a Windows client

You can obtain the information shown in *Tables 2-1* through *2-6* from a Windows client.

(a) System information that can be obtained (For JP1/Software Distribution version 06-53 or earlier)

For the system information that can be obtained from JP1/Software Distribution 06-53 or earlier, see *Table 2-1* and *Table 2-2*. These tables use the same legend and remarks.

Table 2–1: Available system information 1 (available from JP1/Software Distribution version 06-53 or earlier)

Available system information	Target OS						
	Windows						
	XP	Svr 2003	Vista	Svr 2008	7	Svr 2012	8
Client version	Y	Y	Y	Y	Y	Y	Y
Computer name	Y	Y	Y	Y	Y	Y	Y
Machine type	--	--	--	--	--	--	--
OS	Y	Y	Y	Y	Y	Y	Y
Name of OS family[#1]	Y	Y	Y	Y	Y	Y	Y
OS version	Y	Y	Y	Y	Y	Y	Y
OS sub-version	Y	Y	Y	Y	Y	Y	Y
OS build number/OS patch[#2]	Y	Y	Y	Y	Y	Y	Y
WMI[#3]	Y	Y	Y	Y	Y	Y	Y
Domain type	Y	Y	Y	Y	Y	Y	Y

Available system information	Target OS						
	Windows						
	XP	Svr 2003	Vista	Svr 2008	7	Svr 2012	8
Company name	Y	Y	Y#4	Y#4	Y#4	Y#4	Y#4
Owner	Y	Y	Y	Y	Y	Y	Y
CPU type#5	Y	Y	Y	Y	Y	Y	Y
Coprocessor	Y	Y	Y	Y	Y	Y	Y
CPU clock speed#5, #6	Y	Y	Y	Y	Y	Y	Y
Number of processors	Y	Y	Y	Y	Y	Y	Y
Real memory size	Y	Y	Y	Y	Y	Y	Y
Usable user memory size	Y	Y	Y	Y	Y	Y	Y
Usable system resource size	Y	Y	Y	Y	Y	Y	Y
Maker name	Y	Y	Y	Y	Y	Y	Y
Model	Y	Y	Y	Y	Y	Y	Y
Drive type#7, #8	Y	Y	Y	Y	Y	Y	Y
Free hard disk space#9	Y#7	Y#7	Y	Y	Y	Y	Y
Total disc capacity#8	Y#7	Y#7	Y	Y	Y	Y	Y
Video driver	Y	Y	Y	Y	Y	Y	Y
Video chip	Y	Y	Y	Y	Y	Y	Y
VRAM size	Y	Y	Y	Y	Y	Y	Y
Display	Y	Y	Y#10	Y#10	Y#10	Y#10	Y#10
Network adapter	Y	Y	Y	Y	Y	Y	Y
Subnet mask	Y	Y	Y	Y	Y	Y	Y
Default router address	Y	Y	Y	Y	Y	Y	Y
MAC address	Y	Y	Y	Y	Y	Y	Y

Table 2–2: Available system information 2 (available from JP1/Software Distribution version 06-53 or earlier)

Available system information	Target OS				
	Windows				
	NT 4.0	2K	95	98	Me
Client version	Y	Y	Y	Y	Y
Computer name	Y	Y	Y	Y	Y
Machine type	--	--	--	--	--
OS	Y	Y	Y	Y	Y
Name of OS family#1	W	Y	--	--	--

Available system information	Target OS				
	Windows				
	NT 4.0	2K	95	98	Me
OS version	Y	Y	Y	Y	Y
OS sub-version	Y	Y	Y	Y	Y
OS build number/OS patch[#2]	Y	Y	--	--	--
WMI[#3]	Y	Y	Y	Y	Y
Domain type	W	Y	N/A	N/A	N/A
Company name	Y	Y	Y	Y	Y
Owner	Y	Y	Y	Y	Y
CPU type[#5]	Y	Y	Y	Y	Y
Coprocessor	Y	Y	Y	Y	Y
CPU clock speed[#5, #6]	Y	Y	Y	Y	Y
Number of processors	Y	Y	Y	Y	Y
Real memory size	Y	Y	Y	Y	Y
Usable user memory size	Y	Y	Y	Y	Y
Usable system resource size	Y	Y	Y	Y	Y
Maker name	W	Y	W	W	Y
Model	W	Y	W	W	Y
Drive type[#7, #8]	Y	Y	Y	Y	Y
Free hard disk space[#9]	Y[#7]	Y[#7]	Y	Y	Y
Total disc capacity[#8]	Y[#7]	Y[#7]	Y	Y	Y
Video driver	Y	Y	Y	Y	Y
Video chip	Y	Y	Y	Y	Y
VRAM size	Y	Y	W	W	Y
Display	Y	Y	Y	Y	Y
Network adapter	Y	Y	W	Y	Y
Subnet mask	Y	Y	W	Y	Y
Default router address	Y	Y	W	Y	Y
MAC address	Y	Y	Y[#9]	Y	Y

Legend:

2K: 2000

Svr: Server

Y: Available.

--: Not available.

N/A: The OS does not include any applicable item.

W: Available when the following prerequisite programs are installed on the client:

For Windows 95:

- DCOM95 for Windows 95 or Microsoft Internet Explorer 5.01 or later
- Windows Management Instrumentation (WMI) CORE

For Windows 98 or Windows NT 4.0:

- Windows Management Instrumentation (WMI) CORE

You can download these prerequisite programs from the Microsoft web site.

#1

Displayed in the OS field.

#2

The OS build number is obtained for a Windows client.

#3

The WMI field shows the client's WMI version. This is the version of the WMI service, not of the WMI core component. When the installed WMI core component is version 1.5, the WMI version is 1085.0005.

If WMI is unavailable, `N/A` (Not Available) is shown in the WMI field.

It might not be possible to obtain the information if you have logged on as a user without administrator permissions. For details, see *(4) System information that cannot be obtained without administrator permissions*.

#4

If this information is not present on the client, the company name might not be collected.

#5

Only one value is obtained for a multi-processor host. `Pentium II` or `Pentium III` might be displayed for some Pentium II Xeon or Pentium III Xeon processors.

#6

The CPU clock speed is obtained for a Pentium processor. The displayed value is the maximum CPU clock speed that has been obtained so far.

For a mobile processor installed in a laptop PC, the displayed CPU clock speed might be different from the clock speed in the technical specifications published for that laptop PC. Furthermore, depending on the processor type, the obtained CPU clock speed might be incorrect.

You can customize the obtained CPU clock speed value. For details, see *3.1.6 Customizing the CPU clock speed that is reported* in the manual *Administrator's Guide Volume 1*.

#7

Not obtained for a network drive or a drive for which there is no access right.

#8

Information is obtained for each drive. These items are grouped together and displayed for each drive.

#9

For a machine in which a RAS client is installed, the dummy address might be displayed in addition to the MAC address of the network adapter. The MAC address is not obtained unless NetBIOS is being used.

#10

The settings of the last user who logged on are obtained.

Additionally, after you have initialized the client by specifying the asterisk (`*`) wildcard for the new installation or setup destination, you must log on again before you can obtain the information.

(b) System information that can be obtained (For JP1/Software Distribution version 06-71 through 08-10)

For the system information that can be obtained from JP1/Software Distribution 06-71 through 08-10, see *Table 2-3* and *Table 2-4*. These tables use the same legend and remarks.

Table 2–3: Available system information 1 (additional information that is available from JP1/Software Distribution 06-71 through 08-10)

Available system information	Target OS						
	Windows						
	XP	Svr 2003	Vista	Svr 2008	7	Svr 2012	8
Computer description	Y	Y	Y	Y	Y	Y	Y
Internet Explorer version	Y	Y	Y	Y	Y	Y	Y
Windows Installer[#1]	Y	Y	Y	Y	Y	Y	Y
MBSA[#2]	Y	Y	N/A	N/A	N/A	N/A	N/A
Windows Update Agent[#3]	Y	Y	Y	Y	Y	Y	Y
IE batch information	Y	Y	Y	Y	Y	Y	Y
Domain/workgroup	Y	Y	Y	Y	Y	Y	Y
Logon user name[#4]	Y	Y	Y	Y	Y	Y	Y
Full name of user[#4, #5]	Y	Y	Y	Y	Y	Y	Y
User description[#4, #5]	Y	Y	Y	Y	Y	Y	Y
OS serial number	Y	Y	Y	Y	Y	Y	Y
Locale	Y	Y	Y	Y	Y	Y	Y
OS language	Y	Y	Y	Y	Y	Y	Y
Current time zone	Y	Y	Y	Y	Y	Y	Y
OS installation date/time	Y	Y	Y	Y	Y	Y	Y
Last startup date/time	Y	Y	Y	Y	Y	Y	Y
Boot device	Y	Y	Y	Y	Y	Y	Y
Windows directory	Y	Y	Y	Y	Y	Y	Y
System directory	Y	Y	Y	Y	Y	Y	Y
Speed of external clock for CPU	Y	Y	Y	Y	Y	Y	Y
Memory slot capacity	Y	Y	Y	Y	Y	Y	Y
Available physical memory	Y	Y	Y	Y	Y	Y	Y
Total virtual memory size	Y	Y	Y	Y	Y	Y	Y
Available virtual memory	Y	Y	Y	Y	Y	Y	Y
Page file size	Y	Y	Y	Y	Y	Y	Y
Machine UUID[#6]	Y	Y	Y	Y	Y	Y	Y
Machine serial number[#7]	Y	Y	Y	Y	Y	Y	Y

Available system information	Target OS						
	Windows						
	XP	Svr 2003	Vista	Svr 2008	7	Svr 2012	8
BIOS manufacturer	Y	Y	Y	Y	Y	Y	Y
BIOS release date/time	Y	Y	Y	Y	Y	Y	Y
BIOS version	Y	Y	Y	Y	Y	Y	Y
BIOS version (SMBIOS)	Y	Y	Y	Y	Y	Y	Y
AMT firmware version#8	Y	Y	Y	Y	Y	--	Y
Type of primary bus	Y	Y	Y	Y	Y	Y	Y
Type of secondary bus	Y	Y	Y	Y	Y	Y	Y
Keyboard	Y	Y	Y	Y	Y	Y	Y
Mouse	Y	Y	Y	Y	Y	Y	Y
Number of mouse buttons	Y	Y	Y#4, #9	Y#4, #9	Y#4, #9	Y#4, #9	Y#4, #9
File system#10	Y	Y	Y	Y	Y	Y	Y
Model of hard disk	Y	Y	Y	Y	Y	Y#14	Y
Hard disk capacity	Y	Y	Y	Y	Y	Y#14	Y
Hard disk interface	Y	Y	Y	Y	Y	Y#14	Y
Number of hard disk partitions	Y	Y	Y	Y	Y	Y#14	Y
CD-ROM drive	Y	Y	Y	Y	Y	Y	Y
Monitor type	Y	Y	Y	Y	Y	Y	Y
Sound card manufacturer	Y	Y	Y	Y	Y	Y	Y
Product name of sound card	Y	Y	Y	Y	Y	Y	Y
IP address	Y	Y	Y	Y	Y	Y	Y
Primary DNS server address	Y	Y	Y	Y	Y	Y	Y
Secondary DNS server address	Y	Y	Y	Y	Y	Y	Y
DHCP	Y	Y	Y	Y	Y	Y	Y
DHCP server address	Y	Y	Y	Y	Y	Y	Y
DHCP lease expiration date/time	Y	Y	Y	Y	Y	Y	Y
DHCP lease acquisition date/time	Y	Y	Y	Y	Y	Y	Y
WINS server address#11	Y	Y	Y	Y	Y	Y	Y
Printer name#4	Y	Y	Y	Y	Y	Y	Y

Available system information	Target OS						
	Windows						
	XP	Svr 2003	Vista	Svr 2008	7	Svr 2012	8
Printer driver[#4]	Y	Y	Y	Y	Y	Y	Y
Printer paper size[#4]	Y	Y	Y	Y	Y	Y	Y
Printer type[#4, #12]	Y	Y	Y	Y	Y	Y	Y
Shared name of printer[#4]	Y	Y	Y	Y	Y	Y	Y
Printer server name[#4]	Y	Y	Y	Y	Y	Y	Y
Printer port[#4, #13]	Y	Y	Y	Y	Y	Y	Y

Table 2–4: Available system information 2 (additional information that is available from JP1/Software Distribution 06-71 through 08-10)

Available system information	Target OS				
	Windows				
	NT 4.0	2K	95	98	Me
Computer description	N/A	N/A	W	W	Y
Internet Explorer version	Y	Y	Y	Y	Y
Windows Installer[#1]	Y	Y	--	Y	Y
MBSA[#2]	Y	Y	N/A	N/A	N/A
Windows Update Agent[#3]	N/A	Y	N/A	N/A	N/A
IE batch information	Y	Y	Y	Y	Y
Domain/workgroup	W	Y	W	W	Y
Logon user name[#4]	W	Y	W	W	Y
Full name of user[#4, #5]	W	Y	N/A	N/A	N/A
User description[#4, #5]	W	Y	N/A	N/A	N/A
OS serial number	W	Y	W	W	Y
Locale	W	Y	W	W	Y
OS language	W	Y	W	W	Y
Current time zone	W	Y	W	W	Y
OS installation date/time	W	Y	W	W	Y
Last startup date/time	--	--	--	--	--
Boot device	W	Y	W	W	Y
Windows directory	Y	Y	Y	Y	Y
System directory	Y	Y	Y	Y	Y
Speed of external clock for CPU	W	Y	W	W	Y
Memory slot capacity	W	Y	W	W	Y

Available system information	Target OS				
	Windows				
	NT 4.0	2K	95	98	Me
Available physical memory	W	Y	W	W	Y
Total virtual memory size	W	Y	W	W	Y
Available virtual memory	W	Y	W	W	Y
Page file size	W	Y	W	W	Y
Machine UUID#6	W	Y	W	W	Y
Machine serial number#7	W	Y	W	W	Y
BIOS manufacturer	W	Y	W	W	Y
BIOS release date/time	W	Y	W	W	Y
BIOS version	W	Y	W	W	Y
BIOS version (SMBIOS)	W	Y	W	W	Y
AMT firmware version#8	--	--	--	--	--
Type of primary bus	W	Y	W	W	Y
Type of secondary bus	W	Y	W	W	Y
Keyboard	W	Y	W	W	Y
Mouse	W	Y	W	W	Y
Number of mouse buttons	W	Y	W	W	Y
File system#10	W	Y	W	W	Y
Model of hard disk	W	Y	W	W	Y
Hard disk capacity	W	Y	W	W	Y
Hard disk interface	W	Y	W	W	Y
Number of hard disk partitions	W	Y	W	W	Y
CD-ROM drive	W	Y	W	W	Y
Monitor type	W	Y	W	W	Y
Sound card manufacturer	W	Y	W	W	Y
Product name of sound card	W	Y	W	W	Y
IP address	Y	Y	W	Y	Y
Primary DNS server address	W	Y	W	W	Y
Secondary DNS server address	W	Y	W	W	Y
DHCP	W	Y	W	W	Y
DHCP server address	W	Y	W	W	Y
DHCP lease expiration date/time	W	Y	W	W	Y
DHCP lease acquisition date/time	W	Y	W	W	Y
WINS server address#11	W	Y	--	--	Y

Available system information	Target OS				
	Windows				
	NT 4.0	2K	95	98	Me
Printer name[#4]	Y	Y	Y	Y	Y
Printer driver[#4]	Y	Y	Y	Y	Y
Printer paper size[#4]	Y	Y	Y	Y	Y
Printer type[#4, #12]	Y	Y	Y	Y	Y
Shared name of printer[#4]	Y	Y	Y	Y	Y
Printer server name[#4]	Y	Y	Y	Y	Y
Printer port[#4, #13]	Y	Y	Y	Y	Y

Legend:

2K: 2000

Svr: Server

Y: Available.

--: Not available.

N/A: The OS does not include any applicable item.

W: Available when the following prerequisite programs are installed on the client:

For Windows 95:

- DCOM95 for Windows 95 or Microsoft Internet Explorer 5.01 or later
- Windows Management Instrumentation (WMI) CORE

For Windows 98 or Windows NT 4.0:

- Windows Management Instrumentation (WMI) CORE

You can download these prerequisite programs from the Microsoft web site.

#1

The version information of the Windows Installer installed on the client is collected. If none is installed, `N/A` (Not Available) is displayed.

#2

Information is collected on the product version of the MBSA command line interface (`mbsacli.exe` file) stored in the installation directory `\CLIENT\MBSA` of the client. If the information has not been stored but WUA has been installed, `N/A (The Windows Update is available)` is displayed; if WUA has not been installed, `N/A` (Not Available) is displayed.

#3

WUA product version information is obtained. If the obtained value is `5.4.3790.1000` or greater, WUA2.0 has been installed. If WUA has not been installed, `N/A` (Not Available) is displayed.

#4

The settings of the last user who logged on are obtained.

Additionally, after you have initialized the client by specifying the asterisk (`*`) wildcard for the new installation or setup destination, you must log on again before you can obtain the logon user name, full name of user, and user description information.

#5

You can obtain the user description only when the computer is participating in a work group. You cannot obtain this information if the computer is participating in a domain.

#6

The machine's UUID obtained by WMI is displayed. If a UUID cannot be obtained, a UUID consisting entirely of zeros is displayed.

#7

The machine's serial number obtained by WMI is displayed. The machine's serial number is arbitrarily set up for each hardware vendor, so it might sometimes differ from the PC's manufacturing number. If no information is available, N/A (Not Available) is displayed.

#8

This item is not displayed for clients on which AMT Linkage is not installed. Also, because there is no value to collect, N/A (not available) is displayed in the following cases even when AMT Linkage is installed:

- The PC being used does not support AMT.
- Authentication of an AMT management user failed.
- Microsoft .NET Framework 1.1 or later has not been installed.

#9

The value 0 is displayed if more than one mouse is connected.

#10

Information is obtained for each driver. Items such as total disk size are grouped together and displayed for each drive.

#11

Information can be obtained only on the primary and secondary WINS servers.

#12

This information is obtained during a logon.

#13

This information can be obtained only for a local printer.

#14

When you configure a virtual disk with Windows Server 2012 Storage Service, this is displayed as physical disk information.

(c) System information that can be obtained (For JP1/Software Distribution version 08-51 or later versions)

For the system information that can be obtained from JP1/Software Distribution 08-51 or later versions, see *Table 2-5* and *Table 2-6*. These tables use the same legend and remarks.

Table 2–5: Available system information 1 (additional information available from JP1/Software Distribution 08-51 or later versions)

Available system information	Target OS						
	Windows						
	XP	Svr 2003	Vista	Svr 2008	7	Svr 2012	8
Guest account	Y	Y	Y	Y	Y	Y	Y
Weak password#1#2	Y	Y	Y	Y	Y	Y	Y
Elapsed days since a password modification#3	Y	Y	Y	Y	Y	Y	Y
Non-expiring password	Y#4	Y#4	Y#4	Y#4	Y#4	Y#4	Y#4
Autologon setting#5	Y	Y	Y	Y	Y	Y	Y
Shared folder#2	Y	Y	Y	Y	Y	Y	Y
Anonymous connection#5	Y	Y	Y	Y	Y	Y	Y
Screensaver#5, #6, #7	Y	Y	Y	Y	Y	Y	Y

Available system information	Target OS						
	Windows						
	XP	Svr 2003	Vista	Svr 2008	7	Svr 2012	8
Screensaver password protection function[#5, #6, #7, #8]	Y	Y	Y	Y	Y	Y	Y
Power on password	Y	Y	Y	Y	Y	Y	Y
Windows Firewall settings[#5, #9]	Y[#10]	Y[#10]	Y	Y[#7]	Y	Y	Y
Windows Automatic Updates[#5]	Y	Y	Y	Y	Y	Y	Y
Unnecessary service[#11]	Y	Y	Y	Y	Y	Y	Y
Turn off monitor (AC)[#12]	Y	Y	Y	Y	Y	Y	Y
Turn off monitor (DC)[#12]	Y	Y	Y	Y	Y	Y	Y
Processor Throttle (AC)[#12]	Y	Y	Y	Y	Y	Y	Y
Processor Throttle (DC)[#12]	Y	Y	Y	Y	Y	Y	Y
Turn off hard disks (AC)[#12]	Y	Y	Y	Y	Y	Y	Y
Turn off hard disks (DC)[#12]	Y	Y	Y	Y	Y	Y	Y
System standby/Sleep (AC)[#12]	Y	Y	Y	Y	Y	Y	Y
System standby/Sleep (DC)[#12]	Y	Y	Y	Y	Y	Y	Y
System hibernates (AC)[#12]	Y	Y	Y	Y	Y	Y	Y
System hibernates (DC)[#12]	Y	Y	Y	Y	Y	Y	Y
BitLocker-based encryption information[#2, #13, #14]	N/A	N/A	Y[#15]	Y	Y[#15]	--	Y[#15]
HIBUN FDE-based encryption information[#13, #16]	Y[#17]	--	Y[#17]	--	Y[#17]	--	Y[#17]

Table 2–6: Available system information 2 (additional information available from JP1/Software Distribution 08-51 or later versions)

Available system information	Target OS				
	Windows				
	NT 4.0	2K	95	98	Me
Guest account	Y	Y	N/A	N/A	N/A

Available system information	Target OS				
	Windows				
	NT 4.0	2K	95	98	Me
Weak password[#1#2]	Y	Y	N/A	N/A	N/A
Elapsed days since a password modification[#3]	Y	Y	N/A	N/A	N/A
Non-expiring password	Y	Y[#4]	N/A	N/A	N/A
Autologon setting[#5]	Y	Y	N/A	N/A	N/A
Shared folder[#2]	Y	Y	--	Y	Y
Anonymous connection[#5]	Y	Y	N/A	Y	Y
Screensaver[#5, #6, #7]	Y	Y	--	Y	Y
Screensaver password protection function[#5, #6, #7, #8]	Y	Y	--	Y	Y
Power on password	W	Y	N/A	W	Y
Windows Firewall settings[#5, #9]	N/A	N/A	N/A	N/A	N/A
Windows Automatic Updates[#5]	N/A	Y	N/A	N/A	N/A
Unnecessary service[#11]	Y	Y	N/A	N/A	N/A
Turn off monitor (AC)[#12]	N/A	Y	N/A	Y	Y
Turn off monitor (DC)[#12]	N/A	Y	N/A	Y	Y
Processor Throttle (AC)[#12]	N/A	N/A	N/A	N/A	N/A
Processor Throttle (DC)[#12]	N/A	N/A	N/A	N/A	N/A
Turn off hard disks (AC)[#12]	N/A	Y	N/A	Y	Y
Turn off hard disks (DC)[#12]	N/A	Y	N/A	Y	Y
System standby/Sleep (AC)[#12]	N/A	Y	N/A	Y	Y
System standby/Sleep (DC)[#12]	N/A	Y	N/A	Y	Y
System hibernates (AC)[#12]	N/A	Y	N/A	Y	Y
System hibernates (DC)[#12]	N/A	Y	N/A	Y	Y
BitLocker-based encryption information[#2, #13, #14]	N/A	N/A	N/A	N/A	N/A
HIBUN FDE-based encryption information[#13, #16]	--	--	--	--	--

Legend:

2K: 2000

Svr: Server

Y: Available.

--: Not available.

N/A: The OS does not include any applicable item.

W: Available when Windows Management Instrumentation (WMI) CORE is installed on the client. You can download Windows Management Instrumentation (WMI) CORE from the Microsoft Web site.

#1

- In the initial settings, you cannot obtain this information. To acquire this information, you must edit the `security.ini` file. For details about how to edit the `security.ini` file, see *3.1.7 Customizing the reported security-related inventory information* in the manual *Administrator's Guide Volume 1*.
- The maximum number of accounts that can be checked is 30,000.
- The system does not check invalid, expired, or already-locked accounts.
- If **Audit account management** in **Audit Policy** under **Local Policies** in the **Local Security Settings** window is enabled (accessed in Windows by choosing **Administrative Tools**, and then **Local Security Policy** (local environment, domain environment)), an event log is output when a weak password check is performed.

#2

It might not be possible to obtain the information if you have logged on as a user without administrator permissions. For details, see *(4) System information that cannot be obtained without administrator permissions*.

#3

- The system does not check invalid or expired accounts. For all other accounts, the number of days elapsed is obtained.
- Define a threshold to use for determining whether a password is weak. Define the threshold in the `security.ini` file. For details on how to define the `security.ini` file, see *3.1.7 Customizing the reported security-related inventory information* in the manual *Administrator's Guide Volume 1*.

#4

If **Maximum password age** in **Password Policy** under **Account Policies** in the Group Policy window is set to 0 days (accessed in Windows by choosing **Control Panel**, and then **Administrative Tools**), you might not be able to obtain the non-expiring password information.

#5

If accurate data cannot be read because the acquisition-target registry does not exist or is damaged, `Invalid` is displayed.

#6

The settings that were in effect when the last logon occurred are displayed. If multiple users were logged on when the information was obtained, the settings that were in effect when the last user logged on are displayed.

#7

This information is obtained during a logon.

#8

If the client's OS is Windows 7 or Windows Server 2008 R2, this information corresponds to **On resume, display logon screen** accessed by choosing **Control Panel**, and then **Screen Saver Settings**.

#9

If Service Pack is not applied, `Invalid` is displayed.

#10

Information can be obtained for Windows XP Service Pack 2, Windows Server 2003 Service Pack 1, or a newer version that supports Windows Firewall.

#11

To check the operation status of an unnecessary service, in the `security.ini` file you must define which service is to be monitored as an unnecessary service. For details on how to define the `security.ini` file, see *3.1.7 Customizing the reported security-related inventory information* in the manual *Administrator's Guide Volume 1*.

#12

- If information cannot be obtained for some reason (for example, because of an error), `Unknown` is displayed.
- If the client's OS is Windows 7, Windows Server 2008 or Windows Vista, the settings of the last user who logged on are obtained. For all other OSs, the settings of the last user who logged on with administrator permissions are obtained.
- The obtained settings might be different from the settings that are displayed on the client side. In this case, the obtained values have been applied to the client settings.
- If the Power Options feature is not available, the information acquired may be incorrect.

#13

These items are grouped together and displayed as *Drive Encryption*.

#14

Applies to the drives displayed on the **BitLocker Drive Encryption** page, accessed by choosing **Control Panel**, and then **System and Security**.

#15

Information can be obtained when the client's OS is one of the following:

- Microsoft Windows 7 Enterprise
- Microsoft Windows 7 Ultimate
- Microsoft Windows Vista Enterprise
- Microsoft Windows Vista Ultimate

#16

Information can be obtained when one of the following versions of HIBUN FDE is installed on the client:

- 09-01
- 09-10

#17

Information can be obtained when the client's OS is one of the following:

- Microsoft Windows 7 Enterprise
- Microsoft Windows 7 Professional
- Microsoft Windows 7 Ultimate
- Microsoft Windows Vista Business
- Microsoft Windows Vista Enterprise
- Microsoft Windows XP Professional Operating System

(2) System information that can be obtained from a UNIX client

The following table shows the system information that can be obtained from a UNIX client.

Table 2–7: Available system information (UNIX client)

Available system information	Target OS		
	UNIX		
	HP-UX	Solaris	AIX
Client version	Y	Y	Y
Computer name#1	Y	Y	Y
Workstation type	Y	Y	Y
OS	Y	Y	Y
Name of OS family	N/A	N/A	N/A
Distribution	N/A	N/A	N/A
OS version	Y	Y	Y
OS sub-version	N/A	N/A	N/A
OS build number/OS patch#2	Y	Y	Y
OS license#3	--	--	--
WMI	N/A	N/A	N/A

Available system information	Target OS		
	UNIX		
	HP-UX	Solaris	AIX
Domain type	N/A	N/A	N/A
Company name	N/A	N/A	N/A
Owner	N/A	N/A	N/A
CPU type#4	Y	Y	Y
Existence of coprocessor	N/A	N/A	N/A
CPU clock speed#4	Y	Y	Y
Number of processors	Y	Y	Y
Installed RAM	Y	Y	Y
Usable user memory size	Y	Y	Y
Usable system resource size	--	--	--
Maker name	--	Y	--
Model	Y	N/A	Y
Drive type	N/A	N/A	N/A
Free space#5	Y	Y	Y
Partition size#5	Y	Y	Y
Video driver	--	--	--
Video chip	--	--	--
VRAM	--	--	--
Display	--	--	Y
Network adapter	Y	--	Y
Subnet mask	Y	Y	Y
Default router address	Y	Y	Y
MAC address	Y	Y	Y
Computer description	N/A	N/A	N/A
Internet Explorer version	N/A	N/A	N/A
Windows Installer	N/A	N/A	N/A
MBSA	N/A	N/A	N/A
Windows Update Agent	N/A	N/A	N/A
IE patch	N/A	N/A	N/A
Domain/Workgroup	N/A	N/A	N/A
Logon user name	N/A	N/A	N/A
Full name of user	N/A	N/A	N/A
User description	N/A	N/A	N/A

Available system information	Target OS		
	UNIX		
	HP-UX	Solaris	AIX
OS serial number	--	--	--
Locale	--	--	--
OS language	--	--	--
Current time zone	Y	Y	Y
OS installation date/time	--	--	--
Last startup date/time	Y	Y	Y
Boot device	--	--	Y
Windows directory	N/A	N/A	N/A
System directory	--	--	--
Clock speed of the external CPU	--	--	--
Memory slot capacity	--	--	--
Available physical memory	Y	--	Y[#6]
Total capacity of virtual memory	--	--	--
Available virtual memory	--	--	--
Page file capacity	Y	--	Y
Machine UUID	--	--	--
Machine serial number	Y[#7]	--	Y
BIOS manufacturer	--	--	--
BIOS release date/time	--	--	--
BIOS version	--	--	--
BIOS version (SMBIOS)	--	--	--
AMT firmware version	--	--	--
Type of primary bus	--	--	--
Type of secondary bus	--	--	--
Keyboard	--	--	Y
Mouse	--	--	Y
Number of mouse buttons	--	--	Y
File system[#8]	Y	Y	Y
Model of hard disk	--	--	Y
Hard disk capacity	--	--	Y
Hard disk interface	--	--	Y
Number of hard disk partitions	--	--	--
CD-ROM drive	--	Y	Y

Available system information	Target OS		
	UNIX		
	HP-UX	Solaris	AIX
Monitor type	--	--	Y
Sound card manufacturer	--	--	Y
Product name of sound card	--	--	Y
IP address	Y	Y	Y
Primary DNS server address	Y	Y	Y
Secondary DNS server address	Y	Y	Y
DHCP	--	--	--
DHCP server address	--	--	--
Expiration date/time of DHCP lease	--	--	--
Acquired date/time of DHCP lease	--	--	--
WINS server address	N/A	N/A	N/A
Printer name	--	--	--
Printer driver	--	--	--
Printer sheet size	--	--	--
Printer type	--	--	--
Shared name of printer	--	--	--
Printer server name	--	--	--
Printer port	--	--	--
Guest account	N/A	N/A	N/A
Weak password	N/A	N/A	N/A
Elapsed days since a password modification#9	Y	Y	Y
Non-expiring password	N/A	N/A	N/A
Autologon setting	N/A	N/A	N/A
Shared folder#10	Y	Y	Y
Anonymous connection	N/A	N/A	N/A
Screensaver	N/A	N/A	N/A
Screensaver password protection function	N/A	N/A	N/A
Power on password	N/A	N/A	N/A
Windows Firewall settings	N/A	N/A	N/A
Windows Automatic Updates	N/A	N/A	N/A
Unnecessary service	N/A	N/A	N/A

Legend:

Y: Available.

--: Not available.

N/A: The OS does not include any applicable item.

#1

The computer name is the same as the host name in the system configuration information.

#2

In the case of Solaris, OS patch information is obtained. If the client's OS is HP-UX, AIX, or HP Tru64 UNIX, a value determined using the command `uname -v` is obtained.

#3

Obtained only when the client's OS is HI-UX/WE2.

#4

Only a single value is obtained if multiple CPUs are used in a single host.

#5

Information is obtained for each partition. These items are summarized and displayed as information for each partition.

#6

Can be obtained only when Workload Manager is installed.

#7

This information might not be obtained for HP-UX11i in some cases.

#8

Information is obtained for each partition. Items such as *Total disk capacity* are summarized and displayed as information for each partition.

#9

In the initial setting, only the information for the root account is obtained. No information is obtained if a shadow password is not used, or if no last password update date/time is specified for a shadow password that is used.

#10

Obtain information on whether an NFS-mounted directory is present. However, if auto-mounting is used, no information is obtained on directories that are not mounted while system information is being obtained.

(3) Available registry information

You can collect registry information for each client. You can use this information to restore a PC in the event of an error.

You can obtain the following registry paths:

- `HKEY_CLASSES_ROOT`
- `HKEY_LOCAL_MACHINE`

Note that registry information cannot be collected for a client whose version is 05-20 or earlier.

When the OS obtains registry information from a Windows 8, Windows Server 2012, Windows 7, Windows Server 2008 or Windows Vista client via a relay manager whose version is 08-10 or later, the following restrictions apply:

- When executing a *Transfer registry collection definition* job, choose **Any** under **Operating system** in the Edit dialog box.
- You cannot obtain registry information if the *item-name* + *registry-path* exceeds 315 characters.

(4) System information that cannot be obtained without administrator permissions

If you logged on as a user without administrator permissions, when you use the following system acquisition methods you might fail to obtain some system information.

System information acquisition methods

- Using Local System Viewer to obtain system information
- Using an offline machine information acquisition media to obtain system information
- Sending user inventory information from the Software Distribution - Update User Information dialog box to a higher-order system to obtain system information
- When the **Run the client with non-Administrator user permissions** check box is cleared on the **Role** page in the Client Setup dialog box, a system information acquisition job is executed using one of the following operations:
    - Click the **Execute Job Backlog** icon

- Starting Package Setup Manager

Items for which information cannot be obtained

- WMI
- Weak password
- Shared folder
- BitLocker-based encryption information

2.2.2 Acquiring software information

JP1/Software Distribution enables you to obtain the installed software and version information for each client. You can acquire information about various items of software, such as those that were installed by JP1/Software Distribution, those that are recorded in **Add/Remove Programs** in the Windows **Control Panel**, and those that are in the search list provided by JP1/Software Distribution. You can also search installed software by file name. In the case of anti-virus products, you can obtain their resident/nonresident status and their virus definition file versions.

Additionally, you can acquire information about patches that have been installed at the client computers as well as patches that have not been installed, and you can manage patch information in the same manner as you manage software information.

For details about how to acquire software information, see *3.2 Collecting software information* in the manual *Administrator's Guide Volume 1*.

(1) Available software information

You can acquire software information for each relay manager/system and host where clients are run.

When acquiring software information, you can use one of the following six types of search methods:

- Search software installed by Software Distribution
- Search all software
- Search for software in **Add/Remove Programs**
- Search for a file
- Search for Microsoft Office products
- Search for anti-virus products

The software information that can be acquired using each of these search methods is explained below.

The search methods, Search for Microsoft Office products and Search for anti-virus products are performed based on the search information files for Microsoft Office products and anti-virus products. When you upgrade Job Management Partner 1/Software Distribution, see the notes on the upgrade in *3.2.3 Notes on collecting software information* in the manual *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1*.

(a) Search software installed by Software Distribution

You can collect information about software installed by JP1/Software Distribution.

(b) Search all software

This method acquires the following software information:

- Software in *software search lists*
- Software listed in **Add/Remove Programs** of the Windows **Control Panel**
- Software patches that have been installed at the computer
- Software patches that have not been installed at the computer
- Hitachi program products recorded in the registry (other than the ones installed by JP1/Software Distribution)

Software search lists enable you to search software set as standard search targets by JP1/Software Distribution and software that has been set locally as search targets. For details about the acquisition of software information using software search lists, see *(2) Acquiring software information by using software search lists*.

(c) Search for software in "Add/Remove Programs"

This method obtains the software information shown in **Add/Remove Programs** of the Windows **Control Panel** and the patches that have or have not been installed at the client.

In the default, information is not acquired on Hitachi program products that contain any of the character strings listed below in the name displayed in **Add/Remove Programs**. This prevents duplication with the information acquired by the *search all software* method.

- `GROUPMAX`
- `JP1`
- `NETM/DM`
- `Software Distribution`
- `Remote Control Agent`
- `Remote Control Manager`

Using the method *search software listed in* **Add/Remove Programs** to acquire information on Hitachi program products containing these character strings requires client setup. For details about client setup, see *6.2.10(6) Include Hitachi program products in the "Add/Remove Programs" software* in the *Setup Guide*.

The same information as that collected by the *search all software* method is collected from clients whose version is 06-01 or earlier.

(d) Search for a file

This method searches the client for installed software on the basis of a file name. Use this method for a software search after other methods have failed to acquire the desired software information.

If the client version is 05-20 or earlier, JP1/Software Distribution collects only the information about software installed by JP1/Software Distribution.

You can use the *software inventory dictionary* to manage the obtained software information by setting it as a target for management. By setting a license count threshold for the software that is found, on the **Count Result** page of Inventory Viewer you can check for software that has exceeded or is nearing its license count threshold. For details about the software inventory dictionary, see *(3) Managing software information by using the software inventory dictionary*.

(e) Search for Microsoft Office products

You can obtain information on the Microsoft Office products listed in the table below. You can also obtain the owner name, company name, and product ID that were registered during installation.

Note that information cannot be acquired if the client version is 07-00 or earlier or if Microsoft Office `DISK1` has not been installed.

Furthermore, if the client's OS is the 64-bit version of Windows 8, the 64-bit version of Windows 7, the 64-bit version of Windows Server 2012, the 64-bit version of Windows Server 2008, or the 64-bit version of Windows Vista or Windows Server 2003 (x64), you can obtain information only for Microsoft Office products whose version is 2003, 2007, or 2010.

You can obtain information on Microsoft Office products if the product's language matches that of JP1/Software Distribution. For example, if an English version of a Microsoft Office product is installed in the Japanese version of JP1/Software Distribution, sometimes you might be unable to obtain information on the Microsoft Office product.

The following *tables 2.8* to *2.9* show Microsoft Office products for which information can be obtained from a Windows client.

Table 2–8: Microsoft Office products for which information can be obtained from a Windows client

Product name	version	Edition	Software name	Software version	Company name	Language	Path	Size
Microsoft Office	2000	Premium	Y	Y	Y	Y	Y	Y
		Standard	Y	Y	Y	Y	Y	Y
		Professional	Y	Y	Y	Y	Y	Y
		Developer	Y	N	Y	N	N	N
	XP	Standard	Y	Y	Y	Y	Y	Y
		Professional	Y	Y	Y	Y	Y	Y
		Professional with FrontPage	Y	Y	Y	Y	Y	Y
		Developer	Y	Y	Y	Y	Y	Y
	2003	Standard Edition	Y	Y	Y	Y	Y	Y
		Professional Enterprise Edition	Y	Y	Y	Y	Y	Y
		Small Business Edition	Y	Y	Y	Y	Y	Y
	2007	Standard	Y	Y	Y	Y#1	Y	Y
		Small Business	Y	Y	Y	Y#1	Y	Y
		Professional	Y	Y	Y	Y#1	Y	Y
		Ultimate	Y	Y	Y	Y#1	Y	Y
		Professional Plus	Y	Y	Y	Y#1	Y	Y
		Enterprise	Y	Y	Y	Y#1	Y	Y
	2010#2	Home and Business (32bit/ 64bit)	Y	Y	Y	Y#1	Y	Y
		Standard (32bit/ 64bit)	Y	Y	Y	Y#1	Y	Y
		Professional (32bit/64bit)	Y	Y	Y	Y#1	Y	Y
		Professional Plus (32bit/ 64bit)	Y	Y	Y	Y#1	Y	Y
	2013#2	Standard (32bit/ 64bit)	Y	Y	Y	Y#1	Y	Y
		Professional Plus (32bit/ 64bit)	Y	Y	Y	Y#1	Y	Y
Microsoft Word	2000		Y	Y	Y	Y	Y	Y
	2002		Y	Y	Y	Y	Y	Y
	2003		Y	Y	Y	Y	Y	Y

Product name	version	Edition	Software name	Software version	Company name	Language	Path	Size
Microsoft Word	2007		Y	Y	Y	Y#1	Y	Y
	2010 (32bit/64bit)#2		Y	Y	Y	Y#1	Y	Y
	2013 (32bit/64bit)#2		Y	Y	Y	Y#1	Y	Y
Microsoft Excel	2000		Y	Y	Y	Y	Y	Y
	2002		Y	Y	Y	Y	Y	Y
	2003		Y	Y	Y	Y	Y	Y
	2007		Y	Y	Y	Y#1	Y	Y
	2010 (32bit/64bit)#2		Y	Y	Y	Y#1	Y	Y
	2013 (32bit/64bit)#2		Y	Y	Y	Y#1	Y	Y
Microsoft Outlook	2000		Y	Y	Y	Y	Y	Y
	2002		Y	Y	Y	Y	Y	Y
	2003	Standard	Y	Y	Y	Y	Y	Y
		Professional	Y	Y	Y	Y	Y	Y
	2007		Y	Y	Y	Y#1	Y	Y
	2010 (32bit/64bit)#2		Y	Y	Y	Y#1	Y	Y
	2013 (32bit/64bit)#2		Y	Y	Y	Y#1	Y	Y
Microsoft PowerPoint	2000		Y	Y	Y	Y	Y	Y
	2002		Y	Y	Y	Y	Y	Y
	2003		Y	Y	Y	Y	Y	Y
	2007		Y	Y	Y	Y#1	Y	Y
	2010 (32bit/64bit)#2		Y	Y	Y	Y#1	Y	Y
	2013 (32bit/64bit)#2		Y	Y	Y	Y#1	Y	Y
Microsoft Access	2000		Y	Y	Y	Y	Y	Y
	2002		Y	Y	Y	Y	Y	Y
	2003		Y	Y	Y	Y	Y	Y
	2007		Y	Y	Y	Y#1	Y	Y
	2010 (32bit/64bit)#2		Y	Y	Y	Y#1	Y	Y
	2013 (32bit/64bit)#2		Y	Y	Y	Y#1	Y	Y
Microsoft FrontPage	2000		Y	Y	Y	Y	Y	Y
	2002		Y	Y	Y	Y	Y	Y
	2003		Y	Y	Y	Y	Y	Y
Microsoft Publisher	2000		Y	Y	Y	Y	N	Y
	2002		Y	Y	Y	Y	Y	Y
	2003		Y	Y	Y	Y	Y	Y

Product name	version	Edition	Software name	Software version	Company name	Language	Path	Size
Microsoft Publisher	2007		Y	Y	Y	Y[#1]	Y	Y
	2010 (32bit/64bit)[#2]		Y	Y	Y	Y[#1]	Y	Y
	2013 (32bit/64bit)[#2]		Y	Y	Y	Y[#1]	Y	Y
Microsoft Visio	2000		Y	Y	Y	Y	N	Y
	2002	Standard	Y	Y	Y	Y	Y	Y
		Professional	Y	Y	Y	Y	Y	Y
	2003	Standard	Y	Y	Y	Y	Y	Y
		Professional	Y	Y	Y	Y	Y	Y
	2007	Standard	Y	Y	Y	Y[#1]	Y	Y
		Professional	Y	Y	Y	Y[#1]	Y	Y
	2010[#2, #3, #4]	Standard (32bit/64bit)	Y	Y	Y	Y[#1]	Y	Y
		Professional (32bit/64bit)	Y	Y	Y	Y[#1]	Y	Y
		Premium (32bit/64bit)	Y	Y	Y	Y[#1]	Y	Y
	2013[#2]	Standard (32bit/64bit)	Y	Y	Y	Y[#1]	Y	Y
		Professional (32bit/64bit)	Y	Y	Y	Y[#1]	Y	Y
Microsoft Project	2000		Y	Y	Y	Y	N	Y
	2002	Standard	Y	Y	Y	Y	Y	Y
		Professional	Y	Y	Y	Y	Y	Y
	2003	Standard	Y	Y	Y	Y	Y	Y
		Professional	Y	Y	Y	Y	Y	Y
	2007	Standard	Y	Y	Y	Y[#1]	Y	Y
		Professional	Y	Y	Y	Y[#1]	Y	Y
	2010[#2]	Standard (32bit/64bit)	Y	Y	Y	Y[#1]	Y	Y
		Professional (32bit/64bit)	Y	Y	Y	Y[#1]	Y	Y
	2013[#2]	Standard (32bit/64bit)	Y	Y	Y	Y[#1]	Y	Y
		Professional (32bit/64bit)	Y	Y	Y	Y[#1]	Y	Y
Microsoft InfoPath	2007		Y	Y	Y	Y[#1]	Y	Y
	2010 (32bit/64bit)[#2]		Y	Y	Y	Y[#1]	Y	Y
	2013 (32bit/64bit)[#2]		Y	Y	Y	Y[#1]	Y	Y

Product name	version	Edition	Software name	Software version	Compan y name	Languag e	Path	Size
Microsoft InterConnect	2007		Y	Y	Y	Y[#1]	Y	Y
Microsoft Groove	2007		Y	Y	Y	Y[#1]	Y	Y
Microsoft SharePoint	2010[#2]	Workspace (32bit/64bit)	Y	Y	Y	Y[#1]	Y	Y
Microsoft OneNote	2007		Y	Y	Y	Y[#1]	Y	Y
	2010 (32bit/64bit)[#2]		Y	Y	Y	Y[#1]	Y	Y
	2013 (32bit/64bit)[#2]		Y	Y	Y	Y[#1]	Y	Y
Microsoft Lync	2010 (32bit/64bit)[#5]		Y	Y	Y	Y[#1]	Y	Y
	2013 (32bit/64bit)[#5]		Y	Y	Y	Y[#1]	Y	Y

Legend:

Y: Can be obtained.

N: Cannot be obtained.

#1

This information is obtained as a neutral language (Locale:0x000).

#2

The destination from which the information is acquired will vary if either of the following methods is used to install the product on the client:

- Running setup.exe in the x86 folder or on the media (including automatic installation)
- Running setup.exe in the x64 folder

#3

This can be installed as Visio Standard, Visio Professional, or Visio Premium based on a product key. The edition of the product can be changed after the installation.

#4

JP1/Software Distribution is unable to determine which edition is installed on the client because GUID is not unique. Therefore, the edition information is not displayed. (The edition is registered in the registry during the installation. However, if it is changed in #3, the registered edition is not changed.)

#5

This is 32 or 64-bit specific software depending on the client OS version. (The 32-bit product cannot be installed on the 64-bit OS, nor vice versa.)

Table 2–9: Microsoft Office products for which information can be obtained from a Windows client

Product name	version	Edition	Search date	Installati on date/ time	Product ID	Register ed company name	Register ed owner name	Compon ent Name
Microsoft Office	2000	Premium	Y	Y	Y	Y	Y	Y
		Standard	Y	Y	Y	Y	Y	Y
		Professional	Y	Y	Y	Y	Y	Y
		Developer	Y	N	N	N	N	N
	XP	Standard	Y	Y	Y	Y	Y	Y
		Professional	Y	Y	Y	Y	Y	Y
		Professional with FrontPage	Y	Y	Y	Y	Y	Y

Product name	version	Edition	Search date	Installation date/ time	Product ID	Registered company name	Registered owner name	Component Name
Microsoft Office	XP	Developer	Y	Y	Y	Y	Y	N
	2003	Standard Edition	Y	Y	Y	Y	Y	Y
		Professional Enterprise Edition	Y	Y	Y	Y	Y	Y
		Small Business Edition	Y	Y	Y	Y	Y	Y
	2007	Standard	Y	Y	Y#1	Y#2	Y#2	Y
		Small Business	Y	Y	Y#1	Y#2	Y#2	Y
		Professional	Y	Y	Y#1	Y#2	Y#2	Y
		Ultimate	Y	Y	Y#1	Y#2	Y#2	Y
		Professional Plus	Y	Y	Y#1	Y#2	Y#2	Y
		Enterprise	Y	Y	Y#1	Y#2	Y#2	Y
	2010#3	Home and Business (32bit/ 64bit)	Y	Y	Y	Y	Y	Y
		Standard (32bit/ 64bit)	Y	Y	Y	Y	Y	Y
		Professional (32bit/64bit)	Y	Y	Y	Y	Y	Y
		Professional Plus (32bit/ 64bit)	Y	Y	Y	Y	Y	Y
	2013#3	Standard (32bit/ 64bit)	Y	Y	N	Y	Y	Y
		Professional Plus (32bit/ 64bit)	Y	Y	N	Y	Y	Y
Microsoft Word	2000		Y	Y	Y	Y	Y	N
	2002		Y	Y	Y	Y	Y	N
	2003		Y	Y	Y	Y	Y	N
	2007		Y	Y	Y#1	Y#2	Y#2	N
	2010 (32bit/64bit)#3		Y	Y	Y	Y	Y	N
	2013 (32bit/64bit)#3		Y	Y	N	Y	Y	N
Microsoft Excel	2000		Y	Y	Y	Y	Y	N
	2002		Y	Y	Y	Y	Y	N
	2003		Y	Y	Y	Y	Y	N
	2007		Y	Y	Y#1	Y#2	Y#2	N

Product name	version	Edition	Search date	Installation date/time	Product ID	Registered company name	Registered owner name	Component Name
Microsoft Excel	2010 (32bit/64bit)#3		Y	Y	Y	Y	Y	N
	2013 (32bit/64bit)#3		Y	Y	N	Y	Y	N
Microsoft Outlook	2000		Y	Y	Y	Y	Y	N
	2002		Y	Y	Y	Y	Y	N
	2003	Standard	Y	Y	Y	Y	Y	N
		Professional	Y	Y	Y	Y	Y	N
	2007		Y	Y	Y#1	Y#2	Y#2	N
	2010 (32bit/64bit)#3		Y	Y	Y	Y	Y	N
	2013 (32bit/64bit)#3		Y	Y	N	Y	Y	N
Microsoft PowerPoint	2000		Y	Y	Y	Y	Y	N
	2002		Y	Y	Y	Y	Y	N
	2003		Y	Y	Y	Y	Y	N
	2007		Y	Y	Y#1	Y#2	Y#2	N
	2010 (32bit/64bit)#3		Y	Y	Y	Y	Y	N
	2013 (32bit/64bit)#3		Y	Y	N	Y	Y	N
Microsoft Access	2000		Y	Y	Y	Y	Y	N
	2002		Y	Y	Y	Y	Y	N
	2003		Y	Y	Y	Y	Y	N
	2007		Y	Y	Y#1	Y#2	Y#2	N
	2010 (32bit/64bit)#3		Y	Y	Y	Y	Y	N
	2013 (32bit/64bit)#3		Y	Y	N	Y	Y	N
Microsoft FrontPage	2000		Y	Y	Y	Y	Y	N
	2002		Y	Y	Y	Y	Y	N
	2003		Y	Y	Y	Y	Y	N
Microsoft Publisher	2000		Y	Y	Y	Y	Y	N
	2002		Y	Y	Y	Y	Y	N
	2003		Y	Y	Y	Y	Y	N
	2007		Y	Y	Y#1	Y#2	Y#2	N
	2010 (32bit/64bit)#3		Y	Y	Y	Y	Y	N
Microsoft Visio	2000		Y	Y	Y	Y	Y	N
	2002	Standard	Y	Y	Y	Y	Y	N
		Professional	Y	Y	Y	Y	Y	N
	2003	Standard	Y	Y	Y	Y	Y	N

Product name	version	Edition	Search date	Installation date/time	Product ID	Registered company name	Registered owner name	Component Name
Microsoft Visio	2003	Professional	Y	Y	Y	Y	Y	N
	2007	Standard	Y	Y	Y#1	Y#2	Y#2	N
		Professional	Y	Y	Y#1	Y#2	Y#2	N
	2010#3, #4, #5	Standard (32bit/64bit)	Y	Y	Y	Y	Y	N
		Professional (32bit/64bit)	Y	Y	Y	Y	Y	N
		Premium (32bit/64bit)	Y	Y	Y	Y	Y	N
	2013#3	Standard (32bit/64bit)	Y	Y	N	Y	Y	N
		Professional (32bit/64bit)	Y	Y	N	Y	Y	N
Microsoft Project	2000		Y	Y	Y	Y	Y	N
	2002	Standard	Y	Y	Y	Y	Y	N
		Professional	Y	Y	Y	Y	Y	N
	2003	Standard	Y	Y	Y	Y	Y	N
		Professional	Y	Y	Y	Y	Y	N
	2007	Standard	Y	Y	Y#1	Y#2	Y#2	N
		Professional	Y	Y	Y#1	Y#2	Y#2	N
	2010#3	Standard (32bit/64bit)	Y	Y	Y	Y	Y	N
		Professional (32bit/64bit)	Y	Y	Y	Y	Y	N
	2013#3	Standard (32bit/64bit)	Y	Y	N	Y	Y	N
		Professional (32bit/64bit)	Y	Y	N	Y	Y	N
Microsoft InfoPath	2007		Y	Y	Y#1	Y#2	Y#2	N
	2010 (32bit/64bit)#3		Y	Y	Y	Y	Y	N
	2013 (32bit/64bit)#3		Y	Y	N	Y	Y	N
Microsoft InterConnect	2007		Y	Y	Y#1	Y#2	Y#2	N
Microsoft Groove	2007		Y	Y	Y#1	Y#2	Y#2	N
Microsoft SharePoint	2010#3	Workspace (32bit/64bit)	Y	Y	Y	Y	Y	N
Microsoft OneNote	2007		Y	Y	Y#1	Y#2	Y#2	N
	2010 (32bit/64bit)#3		Y	Y	Y	Y	Y	N

Product name	version	Edition	Search date	Installation date/time	Product ID	Registered company name	Registered owner name	Component Name
Microsoft OneNote	2013 (32bit/64bit)#3		Y	Y	N	Y	Y	N
Microsoft Lync	2010 (32bit/64bit)#6		Y	Y	Y	N	N	N
	2013 (32bit/64bit)#3		Y	Y	N	Y	Y	N

Legend:

Y: Can be obtained.

N: Cannot be obtained.

#1

This information cannot be obtained before the product key is entered. The product ID is not generated until it is entered.

#2

If the product key is not entered during the installation and is entered later, the company name and the owner name are not registered and therefore the information is not available.

#3

The destination from which the information is acquired will vary if either of the following methods is used to install the product on the client:

- Running setup.exe in the x86 folder or on the media (including automatic installation)
- Running setup.exe in the x64 folder

#4

This can be installed as Visio Standard, Visio Professional, or Visio Premium based on a product key. The edition of the product can be changed after the installation.

#5

JP1/Software Distribution is unable to determine which edition is installed on the client because GUID is not unique. Therefore, the edition information is not displayed. (The edition is registered in the registry during the installation. However, if it is changed in #4, the registered edition is not changed.)

#6

This is 32 or 64-bit specific software depending on the client OS version. (The 32-bit product cannot be installed on the 64-bit OS, nor vice versa.)

Table 2–10: Microsoft Office products for which information is available

Product name	How product is provided			Displayed name
	Volume license version	Packaged version	Pre-installed version	
Microsoft Office 2000 Professional	Y	N	N	Office 2000 Professional
Microsoft Office 2000 Standard	Y	N	N	Office 2000 Standard
Microsoft Office 2000 Premium	Y	N	N	Office 2000 Premium
Microsoft Office 2000 Developer	Y	N	N	Office 2000 Developer
Microsoft Office XP Professional	Y	N	N	Office XP Professional
Microsoft Office XP Standard	Y	N	N	Office XP Standard
Microsoft Office XP Professional with FrontPage	Y	N	N	Office XP Professional with FrontPage
Microsoft Office XP Developer	Y	N	N	Office XP Developer
Microsoft Office Professional Enterprise Edition 2003	Y	N	N	Office Professional 2003

Product name		How product is provided			Displayed name
		Volume license version	Packaged version	Pre-installed version	
Microsoft Office Standard Edition 2003		Y	N	N	Office Standard 2003
Microsoft Office Small Business Edition 2003		Y	N	N	Office Small Business 2003
Microsoft Office Standard 2007		Y	N	N	Office Standard 2007
Microsoft Office Small Business 2007		Y	N	N	Office Small Business 2007
Microsoft Office Professional 2007		Y	N	N	Office Professional 2007
Microsoft Office Ultimate 2007		Y	N	N	Office Ultimate 2007
Microsoft Office Professional Plus 2007		Y	N	N	Office Professional Plus 2007
Microsoft Office Enterprise 2007		Y	N	N	Office Enterprise 2007
Microsoft Office Home and Business 2010	32-bit	Y	N	N	Office Home and Business 2010
	64-bit	Y	N	N	Office Home and Business 2010 64bit
Microsoft Office Standard 2010	32-bit	Y	N	N	Office Standard 2010
	64-bit	Y	N	N	Office Standard 2010 64bit
Microsoft Office Professional 2010	32-bit	Y	N	N	Office Professional 2010
	64-bit	Y	N	N	Office Professional 2010 64bit
Microsoft Office Professional Plus 2010	32-bit	Y	N	N	Office Professional Plus 2010
	64-bit	Y	N	N	Office Professional Plus 2010 64bit
Microsoft Office Standard 2013	32-bit	Y	N	N	Office Standard 2013
	64-bit	Y	N	N	Office Standard 2013 64bit
Microsoft Office Professional Plus 2013	32-bit	Y	N	N	Office Professional Plus 2013
	64-bit	Y	N	N	Office Professional Plus 2013 64bit
Microsoft Word 2000		Y	N	N	Word 2000
Microsoft Word 2002		Y	N	N	Word 2002
Microsoft Word 2003		Y	N	N	Word 2003
Microsoft Word 2007		Y	N	N	Word 2007
Microsoft Word 2010	32-bit	Y	N	N	Word 2010
	64-bit	Y	N	N	Word 2010 64bit
Microsoft Word 2013	32-bit	Y	N	N	Word 2013
	64-bit	Y	N	N	Word 2013 64bit
Microsoft Excel 2000		Y	N	N	Excel 2000
Microsoft Excel 2002		Y	N	N	Excel 2002
Microsoft Excel 2003		Y	N	N	Excel 2003

Product name		How product is provided			Displayed name
		Volume license version	Packaged version	Pre-installed version	
Microsoft Excel 2007		Y	N	N	Excel 2007
Microsoft Excel 2010	32-bit	Y	N	N	Excel 2010
	64-bit	Y	N	N	Excel 2010 64bit
Microsoft Excel 2013	32-bit	Y	N	N	Excel 2013
	64-bit	Y	N	N	Excel 2013 64bit
Microsoft Outlook 2000		Y	N	N	Outlook 2000
Microsoft Outlook 2002		Y	N	N	Outlook 2002
Microsoft Outlook Professional 2003		Y	N	N	Outlook Professional 2003
Microsoft Outlook Standard 2003		Y	N	N	Outlook Standard 2003
Microsoft Outlook 2007		Y	N	N	Outlook 2007
Microsoft Outlook 2010	32-bit	Y	N	N	Outlook 2010
	64-bit	Y	N	N	Outlook 2010 64bit
Microsoft Outlook 2013	32-bit	Y	N	N	Outlook 2013
	64-bit	Y	N	N	Outlook 2013 64bit
Microsoft PowerPoint 2000		Y	N	N	PowerPoint 2000
Microsoft PowerPoint 2002		Y	N	N	PowerPoint 2002
Microsoft PowerPoint 2003		Y	N	N	PowerPoint 2003
Microsoft PowerPoint 2007		Y	N	N	PowerPoint 2007
Microsoft PowerPoint 2010	32-bit	Y	N	N	PowerPoint 2010
	64-bit	Y	N	N	PowerPoint 2010 64bit
Microsoft PowerPoint 2013	32-bit	Y	N	N	PowerPoint 2013
	64-bit	Y	N	N	PowerPoint 2013 64bit
Microsoft Access 2000		Y	N	N	Access 2000
Microsoft Access 2002		Y	N	N	Access 2002
Microsoft Access 2003		Y	N	N	Access 2003
Microsoft Access 2007		Y	N	N	Access 2007
Microsoft Access 2010	32-bit	Y	N	N	Access 2010
	64-bit	Y	N	N	Access 2010 64bit
Microsoft Access 2013	32-bit	Y	N	N	Access 2013
	64-bit	Y	N	N	Access 2013 64bit
Microsoft FrontPage 2000		Y	N	N	FrontPage 2000
Microsoft FrontPage 2002		Y	N	N	FrontPage 2002
Microsoft FrontPage 2003		Y	N	N	FrontPage 2003

Product name		How product is provided			Displayed name
		Volume license version	Packaged version	Pre-installed version	
Microsoft Publisher 2000		Y	N	N	Publisher 2000
Microsoft Publisher 2002		Y	N	N	Publisher 2002
Microsoft Publisher 2003		Y	N	N	Publisher 2003
Microsoft Publisher 2007		Y	N	N	Publisher 2007
Microsoft Publisher 2010	32-bit	Y	N	N	Publisher 2010
	64-bit	Y	N	N	Publisher 2010 64bit
Microsoft Publisher 2013	32-bit	Y	N	N	Publisher 2013
	64-bit	Y	N	N	Publisher 2013 64bit
Microsoft Visio 2000		Y	N	N	Visio 2000
Microsoft Visio 2002 Standard		Y	N	N	Visio 2002 Standard
Microsoft Visio 2002 Professional		Y	N	N	Visio 2002 Professional
Microsoft Visio Standard 2003		Y	N	N	Visio Standard 2003
Microsoft Visio Professional 2003		Y	N	N	Visio Professional 2003
Microsoft Visio Standard 2007		Y	N	N	Visio Standard 2007
Microsoft Visio Professional 2007		Y	N	N	Visio Professional 2007
Microsoft Visio 2010 Standard/Professional/ Premium	32-bit	Y	N	N	Visio 2010
	64-bit	Y	N	N	Visio 2010 64bit
Microsoft Visio Standard 2013	32-bit	Y	N	N	Visio Standard 2013
	64-bit	Y	N	N	Visio Standard 2013 64bit
Microsoft Visio Professional 2013	32-bit	Y	N	N	Visio Professional 2013
	64-bit	Y	N	N	Visio Professional 2013 64bit
Microsoft Project 2000		Y	N	N	Project 2000
Microsoft Project 2002 Standard		Y	N	N	Project 2002 Standard
Microsoft Project 2002 Professional		Y	N	N	Project 2002 Professional
Microsoft Project Standard 2003		Y	N	N	Project Standard 2003
Microsoft Project Professional 2003		Y	N	N	Project Professional 2003
Microsoft Project Standard 2007		Y	N	N	Project Standard 2007
Microsoft Project Professional 2007		Y	N	N	Project Professional 2007
Microsoft Project Standard 2010	32-bit	Y	N	N	Project Standard 2010
	64-bit	Y	N	N	Project Standard 2010 64bit
Microsoft Project Professional 2010	32-bit	Y	N	N	Project Professional 2010
	64-bit	Y	N	N	Project Professional 2010 64bit

Product name		How product is provided			Displayed name
		Volume license version	Packaged version	Pre-installed version	
Microsoft Project Standard 2013	32-bit	Y	N	N	Project Standard 2013
	64-bit	Y	N	N	Project Standard 2013 64bit
Microsoft Project Professional 2013	32-bit	Y	N	N	Project Professional 2013
	64-bit	Y	N	N	Project Professional 2013 64bit
Microsoft InfoPath 2007		Y	N	N	InfoPath 2007
Microsoft InfoPath 2010	32-bit	Y	N	N	InfoPath 2010
	64-bit	Y	N	N	InfoPath 2010 64bit
Microsoft InfoPath 2013	32-bit	Y	N	N	InfoPath 2013
	64-bit	Y	N	N	InfoPath 2013 64bit
Microsoft InterConnect 2007		Y	N	N	InterConnect 2007
Microsoft Groove 2007		Y	N	N	Groove 2007
Microsoft SharePoint Workspace 2010	32-bit	Y	N	N	SharePoint Workspace 2010
	64-bit	Y	N	N	SharePoint Workspace 2010 64bit
Microsoft OneNote 2007		Y	N	N	OneNote 2007
Microsoft OneNote 2010	32-bit	Y	N	N	OneNote 2010
	64-bit	Y	N	N	OneNote 2010 64bit
Microsoft OneNote 2013	32-bit	Y	N	N	OneNote 2013
	64-bit	Y	N	N	OneNote 2013 64bit
Microsoft Lync 2010	32-bit	Y	N	N	Lync 2010
	64-bit	Y	N	N	Lync 2010 64bit
Microsoft Lync 2013	32-bit	Y	N	N	Lync 2013
	64-bit	Y	N	N	Lync 2013 64bit

Legend:

Y: Can be obtained

N: Cannot be obtained

(f) Search for anti-virus products

You can obtain information on the anti-virus products listed in the table below. You can also obtain version information on the virus detection engines, virus definition files, and resident/nonresident settings.

Table 2–11: Anti-virus products for which information can be obtained from a Windows client

Product name, version, etc.			Display in JP1/Software Distribution
Symantec AntiVirus Corporate Edition	9.0		AntiVirus Corporate Edition 9.0
	10.0	32-bit	AntiVirus Corporate Edition 10.0
		64-bit	Symantec AntiVirus Win64
	10.1	32-bit	AntiVirus Corporate Edition 10.1

Product name, version, etc.			Display in JP1/Software Distribution
Symantec AntiVirus Corporate Edition	10.1	64-bit	Symantec AntiVirus Win64
	10.2	32-bit	AntiVirus Corporate Edition 10.2
		64-bit	Symantec AntiVirus Win64
Symantec Client Security	2.0	Client	Symantec Client Security
		Server	AntiVirus Corporate Edition 9.0
	3.0	32-bit	Symantec Client Security
		64-bit	Symantec AntiVirus Win64
	3.1	32-bit	Symantec Client Security
		64-bit	Symantec AntiVirus Win64
Symantec Endpoint Protection	11.0	32-bit	Symantec Endpoint Protection 11.0
		64-bit	Symantec Endpoint Protection 11.0 64bit
	12.1	32-bit	Symantec Endpoint Protection 12.1
		64-bit	Symantec Endpoint Protection 12.1 64bit
Norton AntiVirus#1	2009	32-bit	Norton AntiVirus 2009
		64-bit	Norton AntiVirus 2009 64bit
	2010	32-bit	Norton AntiVirus 2010
		64-bit	Norton AntiVirus 2010 64bit
	2011	32-bit	Norton AntiVirus 2011
		64-bit	Norton AntiVirus 2011 64bit
	2012	32-bit	Norton AntiVirus 2012
		64-bit	Norton AntiVirus 2012 64bit
	(20.1.0.24)	32-bit	Norton AntiVirus
		64-bit	Norton AntiVirus 64bit
McAfee VirusScan	4.5.1		VirusScan 4.5.1
McAfee VirusScan Enterprise	8.0i#2		VirusScan Enterprise 8.0i
	8.5i	32-bit	VirusScan Enterprise 8.5i
		64-bit	VirusScan Enterprise 8.5i 64bit
	8.7i	32-bit	VirusScan Enterprise 8.7i
		64-bit	VirusScan Enterprise 8.7i 64bit
	8.8	32-bit	VirusScan Enterprise 8.8
		64-bit	VirusScan Enterprise 8.8 64bit
McAfee VirusScan Thin Client	6.1.0		VirusScan TC 6.1.0
McAfee NetShield	4.5		NetShield 4.5
McAfee Managed Total Protection	4.7, 5.0	32-bit	Managed Total Protection
		64-bit	Managed Total Protection 64bit
McAfee SaaS Endpoint Protection	5.2	32-bit	SaaS Endpoint Protection

Product name, version, etc.			Display in JP1/Software Distribution
McAfee SaaS Endpoint Protection	5.2	64-bit	SaaS Endpoint Protection 64bit
PC-cillin	2002		PC-cillin 2002
	2003		PC-cillin 2003
	2009	32-bit	PC-cillin 2009
		64-bit	PC-cillin 2009 64bit
	2010	32-bit	PC-cillin 2010
		64-bit	PC-cillin 2010 64bit
Trend Micro Titanium Internet Security	32-bit		Trend Micro Titanium Internet Security
	64-bit		Trend Micro Titanium Internet Security 64bit
Trend Micro Titanium Internet Security 2012	32-bit		Trend Micro Titanium Internet Security 2012
	64-bit		Trend Micro Titanium Internet Security 2012 64bit
Trend Micro Titanium Internet Security 2013	32-bit		Trend Micro Titanium Internet Security 2013
	64-bit		Trend Micro Titanium Internet Security 2013 64bit
Office Scan Corporate Edition	5.5, 5.58, 6.5, 7.0		**If the OS is Windows NT:** OfficeScan Corp. WinNT **If the OS is Windows Me or Windows 98:** OfficeScan Corp. Win9*x*
	7.3		**If the OS is the 32-bit version of Windows NT:** OfficeScan Corp. WinNT **If the OS is the 64-bit version of Windows NT:**[#3] OfficeScan Corp. WinNT 64bit **If the OS is Windows Me or Windows 98:** OfficeScan Corp. Win9*x*
	8.0	32-bit	OfficeScan Corp. WinNT
		64-bit	OfficeScan Corp. WinNT 64bit
	10.0	32-bit	OfficeScan Corp. WinNT 10.0
		64-bit	OfficeScan Corp. WinNT 10.0 64bit
	10.5	32-bit	OfficeScan Corp. WinNT 10.5
		64-bit	OfficeScan Corp. WinNT 10.5 64bit
	10.6	32-bit	OfficeScan Corp. WinNT 10.6
		64-bit	OfficeScan Corp. WinNT 10.6 64bit
ServerProtect for Microsoft Windows/Novell NetWare	5.56		ServerProtect Normal Server
ServerProtect for Windows NT/Netware	5.7, 5.8	32-bit	ServerProtect Normal Server
		64-bit	ServerProtect Normal Server 64bit
F-Secure Anti-Virus Client Security[#1]	5.7, 6.01		F-Secure Anti-Virus Client Security
F-Secure Client Security[#1]	7.0[#4], 7.1[#5]		F-Secure Client Security
	8.01[#6]	32-bit	F-Secure Client Security 8.01

Product name, version, etc.			Display in JP1/Software Distribution
F-Secure Client Security[#1]	8.01[#6]	64-bit	F-Secure Client Security 8.01 64bit
	9.00[#7]	32-bit	F-Secure Client Security 9.00
		64-bit	F-Secure Client Security 9.00 64bit
	9.01	32-bit	F-Secure Client Security 9.01
		64-bit	F-Secure Client Security 9.01 64bit
	9.10	32-bit	F-Secure Client Security 9.10
		64-bit	F-Secure Client Security 9.10 64bit
	9.11	32-bit	F-Secure Client Security 9.11
		64-bit	F-Secure Client Security 9.11 64bit
	9.20	32-bit	F-Secure Client Security 9.20
		64-bit	F-Secure Client Security 9.20 64bit
	9.31	32-bit	F-Secure Client Security 9.31
		64-bit	F-Secure Client Security 9.31 64bit
	9.32	32-bit	F-Secure Client Security 9.32
		64-bit	F-Secure Client Security 9.32 64bit
	10.00	32-bit	F-Secure Client Security 10.00
		64-bit	F-Secure Client Security 10.00 64bit
Microsoft Forefront Client Security	1.5	32-bit	Forefront Client Security
		64-bit	Forefront Client Security 64bit
Avira AntiVir Professional	9.0, 10	32-bit	Avira AntiVir Professional
		64-bit	Avira AntiVir Professional 64bit
Avira Professional Security	13.0.0.3185	32-bit	Avira Professional Security
		64-bit	Avira Professional Security 64bit
Avira AntiVir Server	10.0.0.1824	32-bit	Avira AntiVir Server
		64-bit	Avira AntiVir Server 64bit
Avira Server Security	13.0.0.3185	32-bit	Avira Server Security
		64-bit	Avira Server Security 64bit
Kaspersky Open Space Security[#1]	6.0.3.837, 6.0.4.1424	32-bit	Kaspersky Anti-Virus 6.0 for Windows Server
			Kaspersky Anti-Virus 6.0 for Windows Workstations
		64-bit	Kaspersky Anti-Virus 6.0 for Windows Server 64bit
			Kaspersky Anti-Virus 6.0 for Windows Workstations 64bit
Kaspersky Endpoint Security 8 for Windows	8.1.0.646, 8.1.0.831	32-bit	Kaspersky Endpoint Security 8 for Windows
		64-bit	Kaspersky Endpoint Security 8 for Windows 64bit
ESET NOD32 Antivirus[#1]	4.2.71.2, 5.0.93.0,	32-bit	ESET NOD32 Antivirus

Product name, version, etc.			Display in JP1/Software Distribution
ESET NOD32 Antivirus[1]	5.0.94.0, 5.0.95.0, 5.2.9.1, 5.2.15.0, 6.0.308.0, 6.0.314.0	64-bit	ESET NOD32 Antivirus 64bit

#1

The version of the virus detection engine cannot be obtained.

#2

Information about 64-bit products can also be acquired. The names displayed in JP1/Software Distribution are the same as for the 32-bit versions.

#3

Information is output when the version is 8.0 or later.

#4

7.10 will be obtained as "Software version".

#5

7.42 will be obtained as "Software version".

#6

8.30 will be obtained as "Software version".

#7

9.20 will be obtained as "Software version".

If the client version is earlier than 07-00, the job will result in an error and you will not obtain any information.

The following *tables 2.12* to *2.13* show anti-virus products for which information can be obtained from a Windows client.

Table 2–12: Anti-virus products for which information can be obtained from a Windows client

Product name, version, etc.		Software name	Software version	Company name	Language	Path	Size	Search date
Symantec AntiVirus Corporate Edition 9.0		Y	Y	Y	Y	Y	Y	Y
Symantec AntiVirus Corporate Edition 10.0	32bit	Y	Y	Y	Y	Y	Y	Y
	64bit							
Symantec AntiVirus Corporate Edition 10.1	32bit	Y	Y	Y	Y	Y	Y	Y
	64bit							
Symantec AntiVirus Corporate Edition 10.2	32bit	Y	Y	Y	Y	Y	Y	Y
	64bit							
Symantec Client Security 2.0	Client	Y	Y	Y	Y	Y	Y	Y
	Server							
Symantec Client Security 3.0	32bit	Y	Y	Y	Y	Y	Y	Y
	64bit							
Symantec Client Security 3.1	32bit	Y	Y	Y	Y	Y	Y	Y
	64bit							
Symantec Endpoint Protection 11.0	32bit	Y	Y	Y	Y	Y	Y	Y
	64bit							

Product name, version, etc.		Software name	Software version	Company name	Language	Path	Size	Search date
Symantec Endpoint Protection 12.1	32bit	Y	Y	Y	Y	Y	Y	Y
	64bit							
Norton AntiVirus 2009	32bit	Y	Y	Y	N	Y	N	Y
	64bit							
Norton AntiVirus 2010	32bit	Y	Y	Y	N	Y	N	Y
	64bit							
Norton AntiVirus 2011	32bit	Y	Y	Y	N	Y	N	Y
	64bit							
Norton AntiVirus 2012	32bit	Y	Y	Y	N	Y	N	Y
	64bit							
Norton AntiVirus (20.1.0.24)	32bit	Y	Y	Y	N	Y	N	Y
	64bit							
McAfee VirusScan 4.5.1		Y	Y	Y	Y	Y	Y	Y
McAfee VirusScan Thin Client 6.1.0		Y	Y	Y	Y	Y	Y	Y
McAfee NetShield 4.5		Y	Y	Y	Y	Y	Y	Y
McAfee VirusScan Enterprise 8.0i		Y	Y	Y	Y#1	Y	Y	Y
McAfee VirusScan Enterprise 8.5i	32bit	Y	Y	Y	Y#1	Y	Y	Y
	64bit							
McAfee VirusScan Enterprise 8.7i	32bit	Y	Y	Y	Y#1	Y	Y	Y
	64bit							
McAfee VirusScan Enterprise 8.8	32bit	Y	Y	Y	Y#1	Y	Y	Y
	64bit							
McAfee Managed Total Protection 4.7	32bit	Y	Y	Y	N	Y	N	Y
	64bit							
McAfee Managed Total Protection 5.0	32bit	Y	Y	Y	N	Y	N	Y
	64bit							
McAfee SaaS Endpoint Protection 5.2	32bit	Y	Y	Y	N	Y	N	Y
	64bit							
PC-cillin 2002		Y	Y	Y	Y#1	Y	Y	Y
PC-cillin 2003		Y	Y	Y	Y#1	Y	Y	Y
PC-cillin 2009	32bit	Y	Y	Y	Y	Y	Y	Y
	64bit							
PC-cillin 2010	32bit	Y	Y	Y	Y	Y	Y	Y
	64bit							

Product name, version, etc.		Software name	Software version	Company name	Language	Path	Size	Search date
Trend Micro Titanium Internet Security	32bit	Y	Y	Y	Y	Y	Y	Y
	64bit							
Trend Micro Titanium Internet Security 2012	32bit	Y	Y	Y	Y	Y	Y	Y
	64bit							
Trend Micro Titanium Internet Security 2013	32bit	Y	Y	Y	Y	Y	Y	Y
	64bit							
OfficeScan Corporate Edition 5.5	Windows NT	Y	Y	N	N	Y	N	Y
	Windows Me or Windows 98							
OfficeScan Corporate Edition 5.58	Windows NT	Y	Y	N	N	Y	N	Y
	Windows Me or Windows 98							
OfficeScan Corporate Edition 6.5	Windows NT	Y	Y	N	N	Y	N	Y
	Windows Me or Windows 98							
OfficeScan Corporate Edition 7.0	Windows NT	Y	Y	N	N	Y	N	Y
	Windows Me or Windows 98							
OfficeScan Corporate Edition 7.3	Windows NT 32bit	Y	Y	N	N	Y	N	Y
	Windows NT 64bit							
	Windows Me or Windows 98							
OfficeScan Corporate Edition 8.0	Windows NT	Y	Y	N	N	Y	N	Y

Product name, version, etc.		Software name	Software version	Company name	Language	Path	Size	Search date
OfficeScan Corporate Edition 8.0	Windows Me or Windows 98	Y	Y	N	N	Y	N	Y
OfficeScan Corporate Edition 10.0	Windows NT	Y	Y	Y	N	Y	N	Y
	Windows Me or Windows 98				Y[#2]		Y[#2]	
OfficeScan Corporate Edition 10.5	Windows NT	Y	Y	Y	N	Y	N	Y
	Windows Me or Windows 98				Y[#2]		Y[#2]	
OfficeScan Corporate Edition 10.6	Windows NT	Y	Y	Y	N	Y	N	Y
	Windows Me or Windows 98				Y[#2]		Y[#2]	
ServerProtect for Microsoft Windows/Novell NetWare 5.56		Y	Y	Y	N	Y	N	Y
ServerProtect for Microsoft Windows/Novell NetWare 5.7	32bit	Y	Y	Y	N	Y	N	Y
	64bit							
ServerProtect for Microsoft Windows/Novell NetWare 5.8	32bit	Y	Y	Y	N	Y	N	Y
	64bit							
F-Secure Anti-Virus Client Security 5.7		Y	Y	Y	N	Y	N	Y
F-Secure Anti-Virus Client Security 6.01		Y	Y	Y	N	Y	N	Y
F-Secure Client Security 7.0		Y	Y	Y	N	Y	N	Y
F-Secure Client Security 7.1		Y	Y	Y	N	Y	N	Y
F-Secure Client Security 8.01	32bit	Y	Y	Y	N	Y	N	Y
	64bit							
F-Secure Client Security 9.00	32bit	Y	Y	Y	N	Y	N	Y
	64bit							
F-Secure Client Security 9.01	32bit	Y	Y	Y	N	Y	N	Y
	64bit							
F-Secure Client Security 9.10	32bit	Y	Y	Y	N	Y	N	Y
	64bit							
F-Secure Client Security 9.11	32bit	Y	Y	Y	N	Y	N	Y

Product name, version, etc.		Software name	Software version	Company name	Language	Path	Size	Search date
F-Secure Client Security 9.11	64bit	Y	Y	Y	N	Y	N	Y
F-Secure Client Security 9.20	32bit	Y	Y	Y	N	Y	N	Y
	64bit							
F-Secure Client Security 9.31	32bit	Y	Y	Y	N	Y	N	Y
	64bit							
F-Secure Client Security 9.32	32bit	Y	Y	Y	N	Y	N	Y
	64bit							
F-Secure Client Security 10.00	32bit	Y	Y	Y	N	Y	N	Y
	64bit							
Forefront Client Security 1.5	32bit	Y	Y	Y	Y	Y	Y	Y
	64bit							
Avira AntiVir Professional 9	32bit	Y	Y	Y	Y[#1]	Y	N	Y
	64bit							
Avira AntiVir Professional 10	32bit	Y	Y	Y	Y[#1]	Y	Y	Y
	64bit							
Avira Professional Security 13.0.0.3185	32bit	Y	Y	Y	Y[#1]	Y	Y	Y
	64bit							
Avira AntiVir Server 10.0.0.1824	32bit	Y	Y	Y	Y[#3]	Y	N	Y
	64bit							
Avira Server Security 13.0.0.3185	32bit	Y	Y	Y	N	Y	Y	Y
	64bit							
Kaspersky Open Space Security 6.0.3.837	32bit	Y	Y	Y	Y	Y	Y	Y
	64bit							
Kaspersky Open Space Security 6.0.4.1424	32bit	Y	Y	Y	Y	Y	Y	Y
	64bit							
Kaspersky Endpoint Security 8 for Windows 8.1.0.646	32bit	Y	Y	Y	Y	Y	Y	Y
	64bit							
Kaspersky Endpoint Security 8 for Windows 8.1.0.831	32bit	Y	Y	Y	Y	Y	Y	Y
	64bit							
ESET NOD32 Antivirus 4.2.71.2	32bit	Y	Y	Y	Y	Y	Y	Y
	64bit							
ESET NOD32 Antivirus 5.0.93.0	32bit	Y	Y	Y	Y	Y	Y	Y
	64bit							
ESET NOD32 Antivirus 5.0.94.0	32bit	Y	Y	Y	Y	Y	Y	Y
	64bit							

Product name, version, etc.		Software name	Software version	Company name	Language	Path	Size	Search date
ESET NOD32 Antivirus 5.0.95.0	32bit	Y	Y	Y	Y	Y	Y	Y
	64bit							
ESET NOD32 Antivirus 5.2.9.1	32bit	Y	Y	Y	Y	Y	Y	Y
	64bit							
ESET NOD32 Antivirus 5.2.15.0	32bit	Y	Y	Y	Y	Y	Y	Y
	64bit							
ESET NOD32 Antivirus 6.0.308.0	32bit	Y	Y	Y	Y	Y	Y	Y
	64bit							
ESET NOD32 Antivirus 6.0.314.0	32bit	Y	Y	Y	Y	Y	Y	Y
	64bit							

Legend:

Y: Can be obtained.

N: Cannot be obtained.

#1

This information is obtained as a neutral language (Locale:0x000).

#2

If the anti-virus product is installed on the client with an installation package in MSI format created by Trend Micro Client Packager, this information can be obtained.

#3

This information is obtained as a neutral language (Locale:0x00000009).

Table 2–13: Anti-virus products for which information can be obtained from a Windows client

Product name, version, etc.		Installation date/time	Registered company name	Registered owner name	Virus detecting engine version	Virus definition file version	Virus detection resident/nonresident setup
Symantec AntiVirus Corporate Edition 9.0		Y	N	N	Y	Y	Y
Symantec AntiVirus Corporate Edition 10.0	32bit	Y	N	N	Y	Y	Y
	64bit						
Symantec AntiVirus Corporate Edition 10.1	32bit	Y	N	N	Y	Y	Y
	64bit						
Symantec AntiVirus Corporate Edition 10.2	32bit	Y	N	N	Y	Y	Y
	64bit						
Symantec Client Security 2.0	Client	Y	N	N	Y	Y	Y
	Server						
Symantec Client Security 3.0	32bit	Y	N	N	Y	Y	Y
	64bit						
Symantec Client Security 3.1	32bit	Y	N	N	Y	Y	Y
	64bit						

Product name, version, etc.		Installation date/ time	Registered company name	Registered owner name	Virus detecting engine version	Virus definition file version	Virus detection resident/ nonresident setup
Symantec Endpoint Protection 11.0	32bit	Y	N	N	Y	Y	Y
	64bit						
Symantec Endpoint Protection 12.1	32bit	Y	N	N	Y	Y	Y
	64bit						
Norton AntiVirus 2009	32bit	N	N	N	N	Y	N
	64bit						
Norton AntiVirus 2010	32bit	Y	N	N	N	Y	N
	64bit						
Norton AntiVirus 2011	32bit	Y	N	N	N	Y	N
	64bit						
Norton AntiVirus 2012	32bit	Y	N	N	N	Y	N
	64bit						
Norton AntiVirus (20.1.0.24)	32bit	Y	Y	Y	Y	Y	Y
	64bit	Y	Y	Y	Y	Y	N
McAfee VirusScan 4.5.1		Y	Y	Y	Y	Y	Y
McAfee VirusScan Thin Client 6.1.0		Y	Y	Y	Y	Y	N
McAfee NetShield 4.5		Y	Y	Y	Y	Y	Y
McAfee VirusScan Enterprise 8.0i		Y	Y	Y	Y	Y	Y
McAfee VirusScan Enterprise 8.5i	32bit	Y	Y	Y	Y	Y	Y
	64bit						
McAfee VirusScan Enterprise 8.7i	32bit	Y	Y	Y	Y	Y	Y
	64bit						
McAfee VirusScan Enterprise 8.8	32bit	Y	Y	Y	Y	Y	Y
	64bit						
McAfee Managed Total Protection 4.7	32bit	N	N	N	Y	Y	N
	64bit						
McAfee Managed Total Protection 5.0	32bit	N	N	N	Y	Y	N
	64bit						
McAfee SaaS Endpoint Protection 5.2	32bit	N	N	N	Y	Y	Y
	64bit						
PC-cillin 2002		Y	Y	Y	Y	Y	Y
PC-cillin 2003		Y	Y	Y	Y	Y	Y
PC-cillin 2009	32bit	Y	Y	Y	Y	Y	Y
	64bit						

Product name, version, etc.		Installation date/ time	Registered company name	Registered owner name	Virus detecting engine version	Virus definition file version	Virus detection resident/ nonresident setup
PC-cillin 2010	32bit	Y	Y	Y	Y	Y	Y
	64bit						
Trend Micro Titanium Internet Security	32bit	Y	N	N	Y	Y	Y
	64bit						
Trend Micro Titanium Internet Security 2012	32bit	Y	N	N	Y	Y	Y
	64bit						
Trend Micro Titanium Internet Security 2013	32bit	Y	N	N	Y	Y	Y
	64bit						
OfficeScan Corporate Edition 5.5	Windows NT	Y	Y	Y	Y	Y	Y
	Windows Me or Windows 98						
OfficeScan Corporate Edition 5.58	Windows NT	Y	N	N	Y	Y	Y
	Windows Me or Windows 98						
OfficeScan Corporate Edition 6.5	Windows NT	Y	N	N	Y	Y	Y
	Windows Me or Windows 98						
OfficeScan Corporate Edition 7.0	Windows NT	Y	N	N	Y	Y	Y
	Windows Me or Windows 98						
OfficeScan Corporate Edition 7.3	Windows NT 32bit	Y	N	N	Y	Y	Y
	Windows NT 64bit						
	Windows Me or Windows 98						
OfficeScan Corporate Edition 8.0	Windows NT	Y	N	N	Y	Y	Y

Product name, version, etc.		Installation date/time	Registered company name	Registered owner name	Virus detecting engine version	Virus definition file version	Virus detection resident/nonresident setup
OfficeScan Corporate Edition 8.0	Windows Me or Windows 98	Y	N	N	Y	Y	Y
OfficeScan Corporate Edition 10.0	Windows NT	Y	N	N	Y	Y	Y
	Windows Me or Windows 98						
OfficeScan Corporate Edition 10.5	Windows NT	Y	N	N	Y	Y	Y
	Windows Me or Windows 98						
OfficeScan Corporate Edition 10.6	Windows NT	Y	N	N	Y	Y	Y
	Windows Me or Windows 98						
ServerProtect for Microsoft Windows/Novell NetWare 5.56		N	Y	Y	Y	Y	Y
ServerProtect for Microsoft Windows/Novell NetWare 5.7	32bit	N	Y	Y	Y	Y	Y
	64bit						
ServerProtect for Microsoft Windows/Novell NetWare 5.8	32bit	N	Y	Y	Y	Y	Y
	64bit						
F-Secure Anti-Virus Client Security 5.7		N	N	N	N	Y	N
F-Secure Anti-Virus Client Security 6.01		N	N	N	N	Y	N
F-Secure Client Security 7.0		N	N	N	N	Y	N
F-Secure Client Security 7.1		N	N	N	N	Y	N
F-Secure Client Security 8.01	32bit	N	N	N	N	Y	N
	64bit						
F-Secure Client Security 9.00	32bit	N	N	N	N	Y	N
	64bit						
F-Secure Client Security 9.01	32bit	N	N	N	N	Y	N
	64bit						
F-Secure Client Security 9.10	32bit	N	N	N	N	Y	N
	64bit						
F-Secure Client Security 9.11	32bit	N	N	N	N	Y	N
	64bit						

Product name, version, etc.		Installation date/time	Registered company name	Registered owner name	Virus detecting engine version	Virus definition file version	Virus detection resident/nonresident setup
F-Secure Client Security 9.20	32bit	N	N	N	N	Y	N
	64bit						
F-Secure Client Security 9.31	32bit	N	N	N	N	Y	N
	64bit						
F-Secure Client Security 9.32	32bit	N	N	N	N	Y	N
	64bit						
F-Secure Client Security 10.00	32bit	N	N	N	N	Y	N
	64bit						
Forefront Client Security 1.5	32bit	Y	N	N	Y	Y	Y
	64bit						
Avira AntiVir Professional 9	32bit	N	N	N	Y	Y	N
	64bit						
Avira AntiVir Professional 10	32bit	N	N	N	Y	Y	N
	64bit						
Avira Professional Security 13.0.0.3185	32bit	N	N	N	Y	Y	N
	64bit						
Avira AntiVir Server 10.0.0.1824	32bit	Y	N	N	Y	Y	N
	64bit						
Avira Server Security 13.0.0.3185	32bit	N	N	N	Y	Y	N
	64bit						
Kaspersky Open Space Security 6.0.3.837	32bit	Y	N	N	N	N	Y
	64bit						
Kaspersky Open Space Security 6.0.4.1424	32bit	Y	N	N	N	N	Y
	64bit						
Kaspersky Endpoint Security 8 for Windows 8.1.0.646	32bit	Y	N	N	N	N	Y
	64bit						
Kaspersky Endpoint Security 8 for Windows 8.1.0.831	32bit	Y	N	N	N	N	Y
	64bit						
ESET NOD32 Antivirus 4.2.71.2	32bit	Y	N	N	N	Y	N
	64bit						
ESET NOD32 Antivirus 5.0.93.0	32bit	Y	N	N	N	Y	N
	64bit						
ESET NOD32 Antivirus 5.0.94.0	32bit	Y	N	N	N	Y	N
	64bit						

Product name, version, etc.		Installation date/ time	Registered company name	Registered owner name	Virus detecting engine version	Virus definition file version	Virus detection resident/ nonresident setup
ESET NOD32 Antivirus 5.0.95.0	32bit	Y	N	N	N	Y	N
	64bit						
ESET NOD32 Antivirus 5.2.9.1	32bit	Y	N	N	N	Y	N
	64bit						
ESET NOD32 Antivirus 5.2.15.0	32bit	Y	N	N	N	Y	N
	64bit						
ESET NOD32 Antivirus 6.0.308.0	32bit	Y	N	N	N	Y	N
	64bit						
ESET NOD32 Antivirus 6.0.314.0	32bit	Y	N	N	N	Y	N
	64bit						

Legend:

Y: Can be obtained.

N: Cannot be obtained.

■ Settings that allow judgment of the resident/nonresident status

In anti-virus product software information, JP1/Software Distribution can obtain the resident/nonresident status for some products but not all. Whether an anti-virus product is resident or nonresident is judged based on whether a certain setting of the anti-virus product is enabled during inventory information acquisition.

Table 2-14 shows the settings used to judge the resident/nonresident status of each anti-virus product.

Table 2–14: Settings that allow judgment of the resident/nonresident status of the Windows version of anti-virus products

Product name	Judging the resident/nonresident status
Symantec AntiVirus Corporate Edition	Judged to be resident when **Enable Auto-Protect** is on.
Symantec Client Security	
Symantec Endpoint Protection	Judged to be resident when **Enable File System Auto-Protect** is on.
Norton AntiVirus	N/A
McAfee VirusScan	Judged to be resident when **Enable System scan** is on.
McAfee VirusScan Enterprise (Version 8.0i, 8.5i, or 8.7i)	Judged to be resident when **Enable on-access scanning at system startup** is on.
McAfee VirusScan Enterprise (Version 8.8)	Judged to be resident when **Enabled** or **Disable** is set for **On-access scanning** in **Open Console**.
McAfee VirusScan Thin Client	N/A
McAfee NetShield	Judged to be resident when **Enable on-access scanning at system startup** is on.
McAfee Managed Total Protection (Version 4.7 or 5.0)	N/A
McAfee Managed Total Protection (Version 5.2)	Judged to be resident when **Enabled** or **Disable** is set for **On-access scanning** in **Open Console**.
PC-cillin (Version 2002 or 2003)	Judged to be resident when **Enable Real-time Scan** is on.

Product name	Judging the resident/nonresident status
PC-cillin (Version 2009 or 2010)	Judged to be resident when **Infected files and suspected spyware** is on.
Trend Micro Titanium Internet Security	Judged to be resident when **Protection Against Viruses & Spyware** is on.
Trend Micro Titanium Internet Security(Version 2012 or later)	
OfficeScan Corporate Edition (Version 7.0 or 7.3)	When the management server's **Real-time Scan Settings** - **Enable Real-time Scan** (**Enable real-time scan** in the case of Version 5.5 or 5.58) is turned off and the setting is applied to clients, real-time searching of clients stops. When this occurs, the product is judged to be nonresident.
OfficeScan Corporate Edition (Version 8.0, 10.0, 10.5, or 10.6)	Judged to be resident when the management server's **Real-time Scan Settings** - **Enable virus/malware scan** is turned on.
ServerProtect for Microsoft Windows/Novell NetWare	When the information server's **Real-time Scan** - **Enable Real-time Scan** is turned off and the setting is applied to general servers, real-time searching of general servers stops. When this occurs, the product is judged to be nonresident.
F-Secure Anti-Virus Client Security	N/A
F-Secure Client Security(Version 7.0, 7.1, or 8.01)	N/A
F-Secure Client Security(Version 9.00 or later)	Judged to be resident when **Turn on real-time scanning** is on. To select this option, in the Open F-Secure Client Security dialog box, select **Tasks**, **Settings**, **Virus and spyware scanning**, and then **Turn on real-time scanning**.
Microsoft Forefront Client Security	Judged to be resident when **Use real-time protection (recommended)** is on.
Avira AntiVir Professional	N/A
Avira Professional Security	N/A
Avira AntiVir Server	N/A
Avira Server Security	N/A
Kaspersky Open Space Security	Becomes resident when Enable protection is on.
Kaspersky Endpoint Security 8 for Windows	Judged to be non-resident when **Pause protection and control..** is on.
ESET NOD32 Antivirus	N/A

Legend:
N/A: The resident/nonresident status cannot be obtained.

(2) Acquiring software information by using software search lists

A *Get software information from client* job with the *search all software* method specified during job creation enables you to use software search lists to search the software installed on the client. There are two types of software search lists:

- Standard retrieve list

  This search list is provided by JP1/Software Distribution. It contains the software programs that are searched for by JP1/Software Distribution by default. The contents of the standard retrieve list cannot be edited.

  The standard retrieve list is included in a standard installation in all JP1/Software Distribution systems.

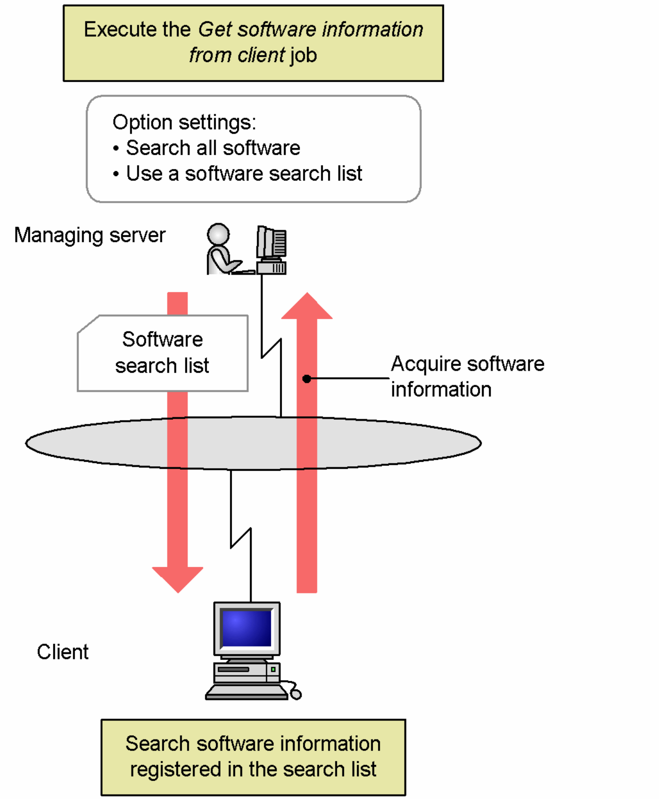
- Optional software list

  This type of search list enables you to register any software that you want to search for.

  You can optionally create multiple software lists. For example, you can create different optional software lists for different types of clients or for different client OSs.

The following figure illustrates the concept of using software search lists to acquire software information.

Figure 2–5: Using software search lists to acquire software information


Execute the *Get software information from client* job
Option settings:
• Search all software
• Use a software search list
Managing server
Software search list
Acquire software information
Client
Search software information registered in the search list

For details about how to make software search lists, see *3.2.4 Creating a software search list* in the manual *Administrator's Guide Volume 1*.

(3) Managing software information by using the software inventory dictionary

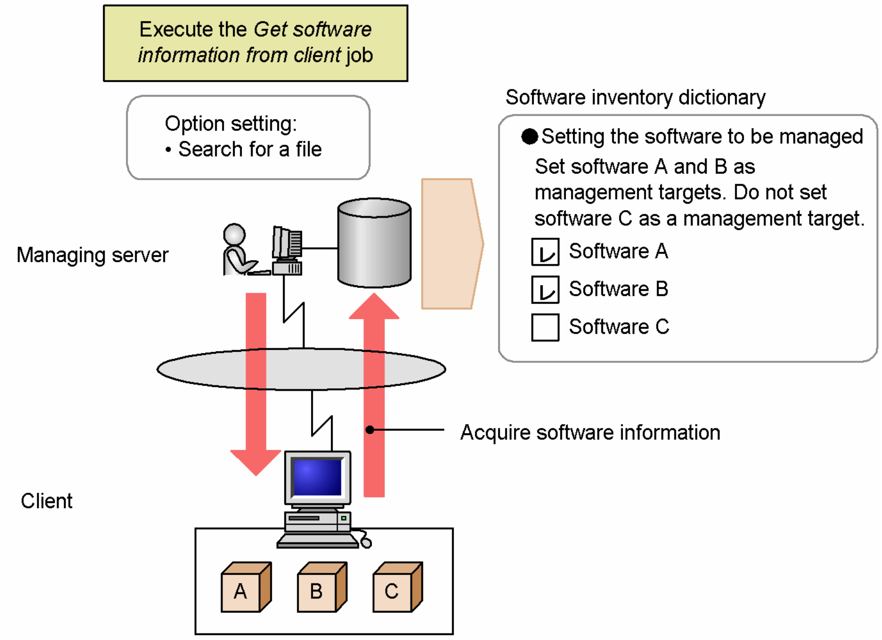
A software inventory dictionary is created when you collect software information using the *search for a file* method in a *Get software information from client* job. In the software dictionary, you must specify whether each software program is to be managed and, if so, under what name it will be managed.

When you display a host's software inventory information in the System Configuration, Destination, or Directory Information window, the window displays only the software that was specified as managed in the software inventory dictionary. You can use the **Count Result** page of Inventory Viewer to check the software that has exceeded or is nearing its license count threshold.

For details about how to edit the software inventory dictionary, see *3.2.5 Filtering a software inventory* in the manual *Administrator's Guide Volume 1*.

The following figure shows the concept of using the software inventory dictionary to manage software information.

Figure 2–6: Using the software inventory dictionary to manage software information


Execute the *Get software information from client* job
Option setting:
• Search for a file
Managing server
Software inventory dictionary
● Setting the software to be managed
Set software A and B as management targets. Do not set software C as a management target.
☑ Software A
☑ Software B
□ Software C
Acquire software information
Client
A
B
C

2.2.3 Acquiring user inventory information

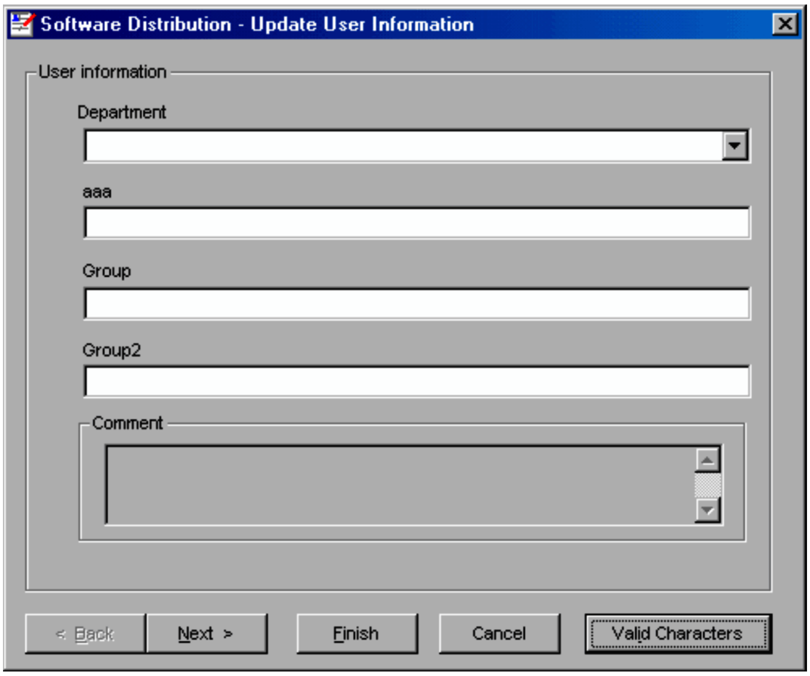
You can use JP1/Software Distribution to manage the information required for managing clients, such as clients' user names and PC resource numbers, in the same way that hardware and system information is managed. The user can specify the information to be managed; the information that is managed or specified by the user is called *user inventory information*.

User inventory information enables you to manage user-defined information as well as the client itself under an easy-to-manage name. For example, if you use the user inventory information to manage host users, the managing server can identify each host by its user name.

You can have the client users enter information in the Software Distribution - Update User Information dialog box, and then you can collect this information as user inventory information by executing a *Get system information from client* job or a *Get user inventory information* job from the managing server.

Note that a *Get user inventory information* job cannot be executed from JP1/Software Distribution Client (relay system).

Figure 2–7: JP1/Software Distribution - Update User Information dialog box

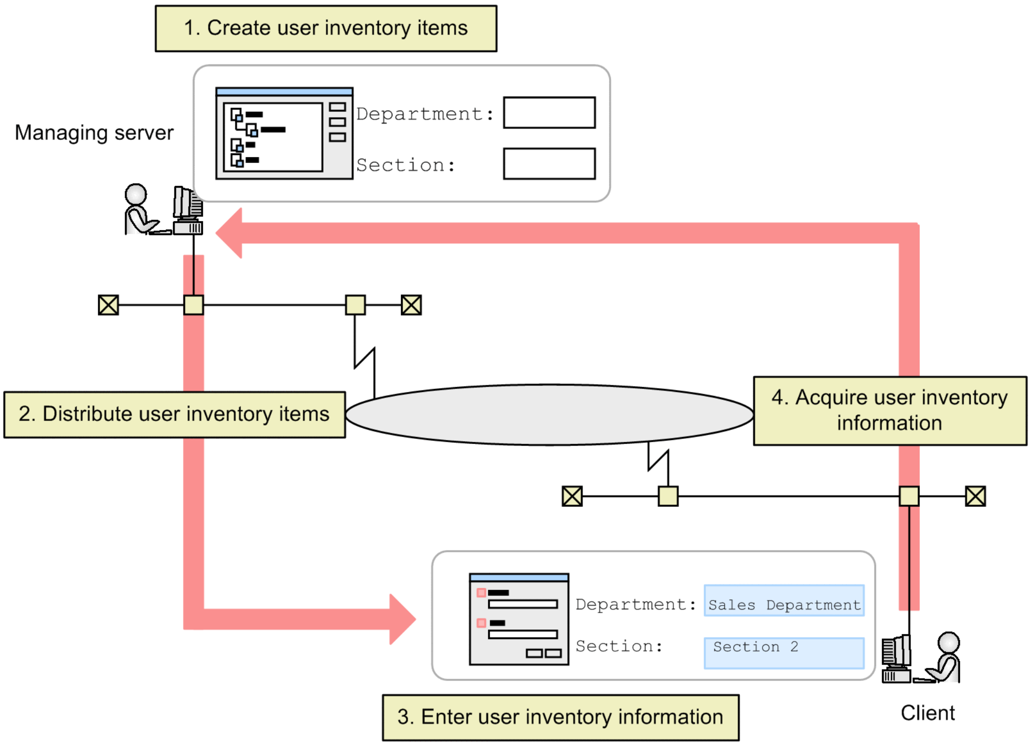


The user can set desired information in the items (*user inventory items*) in the Software Distribution - Update User Information dialog box. The user inventory items must be created in advance on the managing server and distributed to the applicable clients by a *Transfer user inventory schema to client* job.

To have the clients always set user inventory information, you can suppress startup of Package Setup Manager until the clients have specified their user inventory information.

The following figure shows the general procedure for acquiring user inventory information.

Figure 2–8: General procedure for acquiring user inventory information



1. Create user inventory items
Managing server
Department:
Section:
2. Distribute user inventory items
4. Acquire user inventory information
Department: Sales Department
Section: Section 2
3. Enter user inventory information
Client

For details about how to acquire user inventory information, see *3.3 Collecting user inventory information* in the manual *Administrator's Guide Volume 1*.

2.2.4 Acquiring directory information

You can acquire the information necessary for client management, such as client user information and computer information, from Active Directory, and use it in the managing server. The user information and computer information acquired from Active Directory is called *directory information*.

To acquire directory information from Active Directory, you execute the directory information acquisition command (`dcmadsync.exe`).

By acquiring directory information, you can use the user and computer information that is being managed by Active Directory as is. This means that you can import the user and computer information without having to acquire user inventory information. You can specify the acquired directory information as a job destination, or view it as client information in Inventory Viewer. Furthermore, by periodically executing the directory information acquisition command, you can keep the directory information up-to-date in sync with Active Directory updates.

You can specify whether to link to Active Directory during setup of JP1/Software Distribution Manager. The default is that Active Directory is not linked. Therefore, you must specify linkage to Active Directory if you plan to acquire directory information from Active Directory.

(1) Directory information that can be acquired

The directory information listed below can be acquired from Active Directory. You can also acquire the property information that is set in each type of information.

- Domain
- Organizational unit (OU)
- Group
- Computer
- User
- InetOrgPerson
  To acquire this information in an environment that uses Windows 2000, you need Windows 2000 inetOrgPerson Kit.

You specify which types of information to acquire from Active Directory in the parameter file that used when executing the directory information acquisition command (`dcmadsync.exe`). For details on how to create a parameter file, see *3.4.4 Creating a parameter file* in the manual *Administrator's Guide Volume 1*.

(2) How to use directory information

By specifying the destination from the directory information, you can execute the following jobs:

- *Install package*
- *Collect files from client*
- *Send package, allow client to choose*
- *Get system information from client*
- *Get software information from client*
- *Get user inventory information*
- *Transfer registry collection definition*
- *Transfer user inventory schema to client*
- *Report message*
- *Set the software monitoring policy*
- *Get software monitoring information from the client*

In addition to acquiring system information, software information, and user inventory information, you can also count clients and print the results. For details about counting clients and printing the results, see *2.2.7 Uses of inventory information*.

2.2.5 How to acquire inventory information

You can use the following methods to collect system information, software information, and user inventory information from clients:

- Collecting inventory information by executing jobs
- Automatically collecting inventory information

You can use a command to acquire directory information from the computer that is managing the Active Directory information.

These methods are described below.

(1) Collecting inventory information by executing jobs

You can collect system information, software information and user inventory information by executing the following jobs from the managing server:

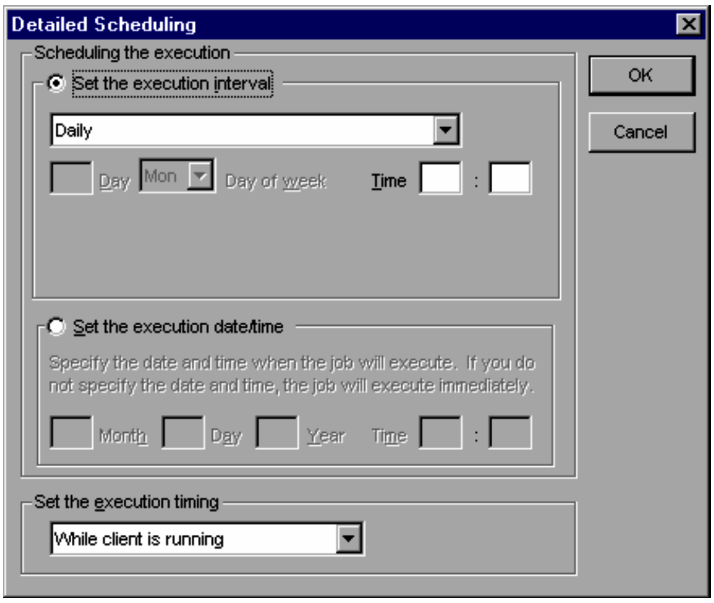
- *Get system information from client* job
  Collects system information (system and registry information) and user inventory information.
- *Get software information from client* job
  Collects software information.
- *Get user inventory information* job
  Collects user inventory information.

The following subsections describe examples of efficiently collecting inventory information.

(a) Collecting inventory information periodically

You can execute a job for collecting system information, software information, and user inventory information periodically at a client. You specify the collection interval in the Detailed Scheduling dialog box. Open this dialog box when you create the inventory collection job. From the **Schedule** page, choose **Options**. The available intervals are **Daily**, **Weekly**, and **Monthly**.

Figure 2–9: Detailed Scheduling dialog box



Detailed Scheduling

Scheduling the execution

● Set the execution interval

Daily

○ Set the execution date/time

Specify the date and time when the job will execute. If you do not specify the date and time, the job will execute immediately.

Set the execution timing

While client is running

Once the system administrator specifies the job, this facility automatically updates the inventory information managed by the managing server to its current status.

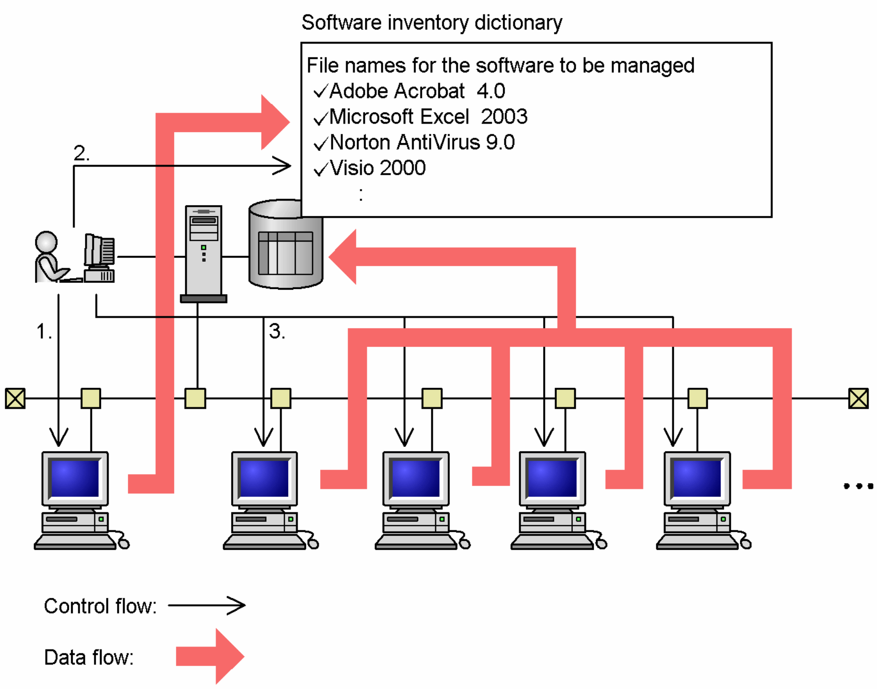
When you create a *Get user inventory information* job to collect user inventory information, you can execute the job periodically. You can also have the job report modified information to the managing server whenever there is a change in the client user's user inventory information. This facility enables the managing server to always maintain up-to-date user inventory information.

(b) Collecting inventory information while reducing the burden on the network and relational database

Using a wildcard (*) to search many clients might collect unnecessary information, placing a heavy burden on the network, and might cause the size of the relational database to expand excessively. In this case, you can use a software inventory dictionary to narrow the file search, thereby reducing the burden on the network and relational database.

The following figure shows how to use a software inventory dictionary to search for files.

Figure 2–10: File search method that uses a software inventory dictionary



1. Generate a software inventory dictionary by using the asterisk (*) wildcard to find all applicable files in one or several machines in which you know the software you want to manage is already installed.

   The software information collected through a file search is registered in the software inventory dictionary.

2. Edit the software inventory dictionary.

   From the list of registered software, select the software you want to manage.

3. Execute a file search with the inventory dictionary edited in step 2 specified on all the clients having inventory information you want to manage.

   This search finds only the software targeted for management, so the burden on the network is reduced. You can also prevent unneeded information from being loaded into the relational database.

For details about file search using the asterisk wildcard, see *3.2.2 Setting the Options page* in the manual *Administrator's Guide Volume 1*. For details about how to edit the software inventory dictionary, see *3.2.5 Filtering a software inventory* in the manual *Administrator's Guide Volume 1*.

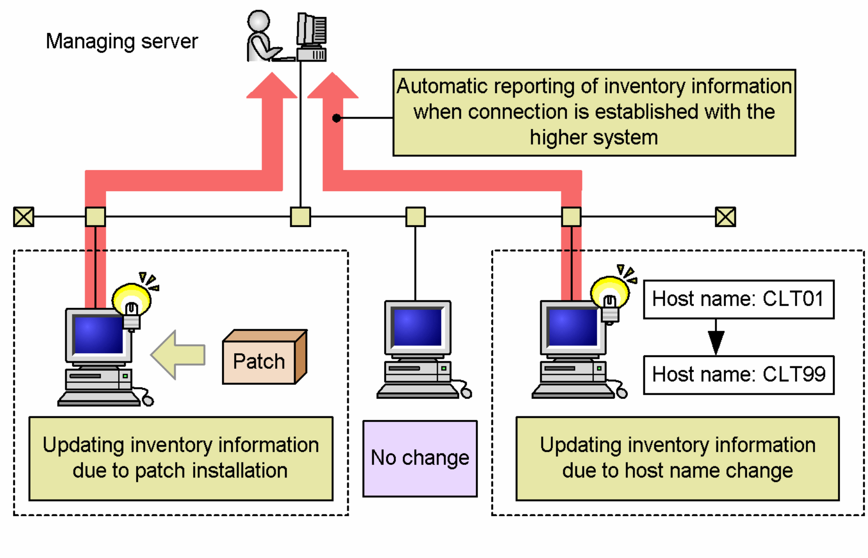
(2) Automatically collecting the latest inventory information

You can keep managed inventory information current by having the clients report their inventory information automatically to the managing server whenever given types of inventory information are updated at the clients.

Because this method enables you to collect inventory information without having to execute a job, it is especially effective for managing inventory information.

The following figure shows the facility for automatically collecting update inventory information.

Figure 2‒11: Facility for automatically collecting updated inventory information


Managing server
Automatic reporting of inventory information when connection is established with the higher system
Patch
Host name: CLT01
Host name: CLT99
Updating inventory information due to patch installation
No change
Updating inventory information due to host name change

This facility enables you to collect part of the system information and software information. To collect all system information, software information, and user inventory information, you must execute a job.

For details about the function for automatic reporting of inventory information to the higher system and the inventory information that can be collected, see *2.13.4 Reporting inventory information from clients*.

(3) Collecting inventory information by executing a command

You can collect directory information by executing a command instead of a job. The following gives the general procedure for collecting directory information from Active Directory.

To collect directory information from Active Directory:

1. Extract the information necessary for connecting to Active Directory, and the information to be collected from Active Directory.

   Extract the information necessary for connecting to Active Directory, such as the host name and port number of the Active Directory from which directory information is to be collected, and the items to be collected from Active Directory.

2. In a map file, define the names to be displayed in the window.

   In the map file, define the names to be displayed in the managing server window when displaying items collected from Active Directory. Defining the display names here ensures that the items acquired are displayed in the window. In the map file, define names that will be easy for you to manage.

3. Define in parameter files the information necessary for connecting to Active Directory, and the information to be collected from Active Directory.

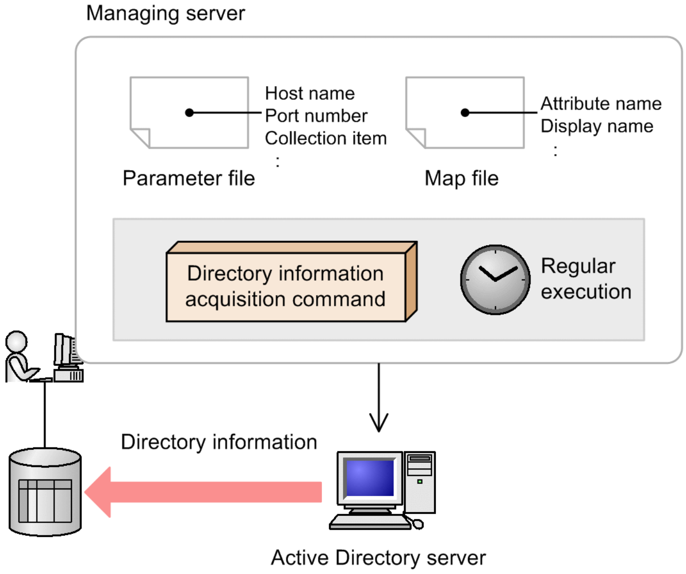
   Define in parameter files the information necessary for connecting to Active Directory, such as the host name and port number of the Active Directory from which directory information is to be collected, and the items to be collected from Active Directory.

4. Execute the directory information acquisition command (`dcmadsync.exe`).

   By registering this command as a task in the Windows Task Scheduler or by linking it to JP1/AJS, you can execute it periodically. Whenever Active Directory is updated, update the directory information as well.

The following figure shows the general procedure for collecting directory information.

Figure 2–12: General procedure for collecting directory information



Notes on collecting directory information

- The password information managed by Active Directory is excluded from the information that can be collected.
- If collection items are added or deleted during collection, the computer and user information is not reflected in the directory information until the applicable entries in Active Directory are updated.
- For directory information collection, require the use of a host name for the ID key for operations. Even when an IP address is to be used for the ID key for operations, make the entry of a host name mandatory.
- The maximum size of the LDAP identifier (Distinguished Name) and attribute values that can be collected from Active Directory is 2,000 bytes. If an OU whose LDAP identifier is 2,000 bytes or longer is specified as the target, the job might not execute correctly.
- Offline machines or non-Software Distribution hosts are not mapped to the directory information.

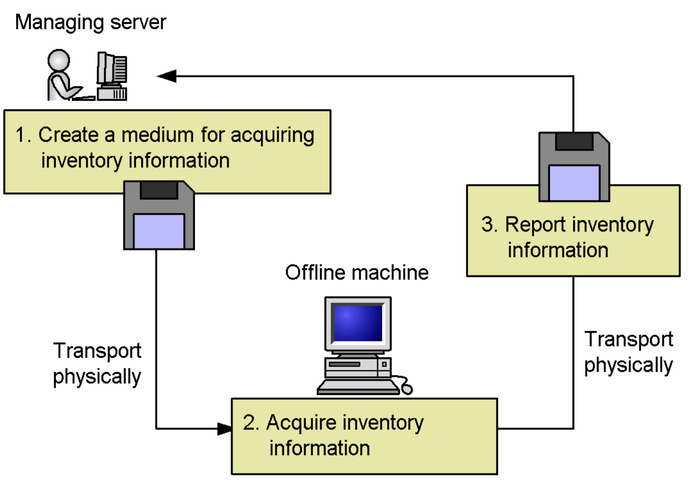
For details about the relationship between the collected directory information and the system configuration information on the managing server, see *2.10.3 Relationship between system configuration information and directory information*. For details about how to collect directory information, see *3.4 Acquiring directory information* in the manual *Administrator's Guide Volume 1*.

2.2.6 Acquiring inventory information from stand-alone PCs

Inventory information can be collected from clients outside the network as well as from connected clients. An unconnected client or other client not registered in the JP1/Software Distribution system configuration is known as an *offline machine*. You can collect inventory information from an offline machine by email or by using storage media such as a floppy disk, CD-R, or MO disk.

The following figure shows the concept of acquiring inventory information from an offline machine.

Figure 2–13: Acquiring inventory information from an offline machine


Managing server
1. Create a medium for acquiring inventory information
3. Report inventory information
Offline machine
Transport physically
Transport physically
2. Acquire inventory information

For details about how to acquire inventory information from offline machines, see *7.7.2 Collecting inventory and operation information from offline machines* in the manual *Administrator's Guide Volume 1*.

To collect inventory information from an offline machine, the JP1/Software Distribution system must be using:

- A relational database
- Host IDs
- Remote Installation Manager running on the same machine as the central manager

Note that you cannot collect only modified inventory information from an offline machine. Also, when you install JP1/Software Distribution Client on a computer to be managed as an offline machine, you must set a question mark (`?`) as the host name or IP address of the connection destination.

The inventory information collected from offline machines is managed in an *offline folder*. This folder is handled as a virtual relay system; there is no actual machine. In the System Configuration window and Destination window, the name `{OFFLINE}` represents an offline folder.

If an offline machine for which inventory information was previously managed in an offline folder is registered into the system configuration, that client is moved from the offline folder as soon as the system configuration information is reported from the client to the central manager.

If you use the facility for collecting inventory information from an offline machine to acquire inventory information from a client registered in the system configuration, that client is not moved to the offline folder; only its inventory information is updated.

2.2.7 Uses of inventory information

Inventory Viewer provided by JP1/Software Distribution Manager enables you to manage and use acquired inventory information for a variety of purposes. This subsection provides an overview of the uses of inventory information. For details about how to use inventory information, see *2.3 Managing inventory information*.

(1) Counting inventory information

You can count the total number of hosts corresponding to each type of inventory item. Obtaining the totals for different types of inventory information is useful for managing software licenses and managing hardware usage in the network. You can also display the counting results as graphs.

(a) Counting hosts by software program

You can count the number of hosts at which each software program is installed. This information enables you to determine whether any license limitations have been exceeded.

(b) Counting hosts by system information

You can count the number of hosts to which various types of system information are applicable.

This information helps you manage hardware resources and utilization status.

The following are examples of system information counting:

- Checking the hard disk space

  You can classify hosts by the amount of available hard disk space. If you want to install a software program that requires 80 MB of free space, you can identify and exclude the hosts that have less than 80 MB of free space available and avoid creating space shortages at those hosts during remote installation.

- Checking memory size

  You can classify hosts by memory size in order to avoid creating space shortages as a result of remote installation of a software program that requires a large amount of memory.

- Checking the OS

  You can classify hosts by OS. For example, if you are migrating the OS on clients from Windows 98 to Windows 2000, you can check the OS status by counting hosts by OS type.

- Checking the version information of the JP1/Software Distribution Client programs installed on clients

  You can classify hosts by the version of JP1/Software Distribution Client or UNIX JP1/Software Distribution Client running on the client systems. Because available facilities depend on the product version, this information helps you determine which hosts can support a desired facility.

(c) Counting the number of relay systems and clients

You can count the number of relay systems and clients. This information helps you understand the size of the network managed by JP1/Software Distribution.

(d) Counting hosts by user inventory

You can obtain the number of applicable hosts for each user-managed inventory item, such as by the number of client users in each department or project.

(2) Outputting to a CSV file

You can export the collected inventory information to a CSV file. You can open this CSV file with a spreadsheet program, so you can easily sort the information or create management documents.

You can use Inventory Viewer or the CSV output utility to export inventory information to a CSV file. For details, see *4.5.2 Exporting to a CSV-formatted file* and *9.1 Using the CSV output utility to output information to a file* in the manual *Administrator's Guide Volume 1*.

(3) Printing inventory information

You can print acquired inventory information in list format. By adding a header, footer, and other additional information, you can create a finished document or report.

For details about how to print inventory information, see *4.5.3 Printing* in the manual *Administrator's Guide Volume 1*.

(4) Managing inventory information from HP NNM

The HP OpenView linkage enables you to manage inventory information from outside the managing server that manages JP1/Software Distribution.

For details about how to manage inventory information for JP1/Software Distribution by linking with HP NNM, see *3. Managing JP1/Software Distribution from HP NNM* in the manual *Administrator's Guide Volume 2*.

2.2.8 Notes on managing inventory information

(1) Central manager for managing inventory information

Within a JP1/Software Distribution system, you should use only one central manager to manage inventory information. If you use more than one, inconsistencies in the inventory information might develop. However, if an error occurs in the central manager, you might have to use another central manager temporarily to manage the inventory information. If you temporarily change the central manager because of some problem, you should re-collect all the managed inventory information at the first central manager after the problem has been corrected.

(2) Notes on inventory information of hosts not in the system configuration

Even after you have deleted a host from the system configuration, the inventory information of the deleted host might still remain in the database. You can delete this inventory information by using Database Manager. For details about how to delete inventory information and the types of inventory information that can be deleted by Database Manager, see *7.5.6 Deleting unneeded inventory information from the database* in the *Setup Guide*.

2.3 Managing inventory information

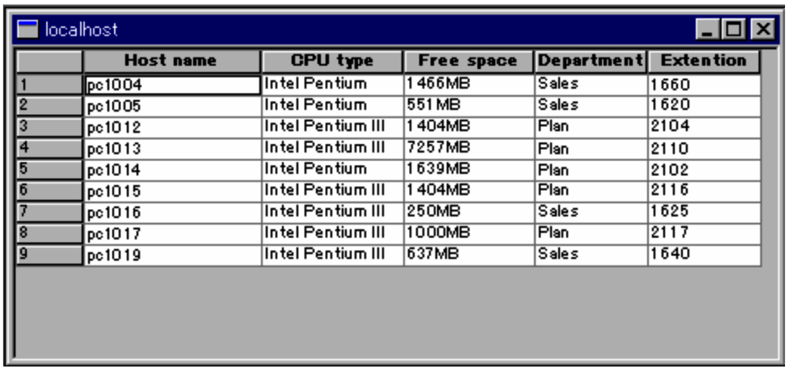
You can use JP1/Software Distribution Manager's Inventory Viewer to display the inventory information acquired from clients and to count clients. You can also display count results in graph format or output them to CSV files.

This section provides an overview of using Inventory Viewer to manage inventory information.

2.3.1 Displaying inventory information

You can display inventory information from all clients in a table-format window. You can sort or filter the listed items to suit your viewing needs and preferences.

Figure 2–14: Example of displaying inventory information



	Host name	CPU type	Free space	Department	Extention
1	pc1004	Intel Pentium	1466MB	Sales	1660
2	pc1005	Intel Pentium	551MB	Sales	1620
3	pc1012	Intel Pentium III	1404MB	Plan	2104
4	pc1013	Intel Pentium III	7257MB	Plan	2110
5	pc1014	Intel Pentium	1639MB	Plan	2102
6	pc1015	Intel Pentium III	1404MB	Plan	2116
7	pc1016	Intel Pentium III	250MB	Sales	1625
8	pc1017	Intel Pentium III	1000MB	Plan	2117
9	pc1019	Intel Pentium III	637MB	Sales	1640

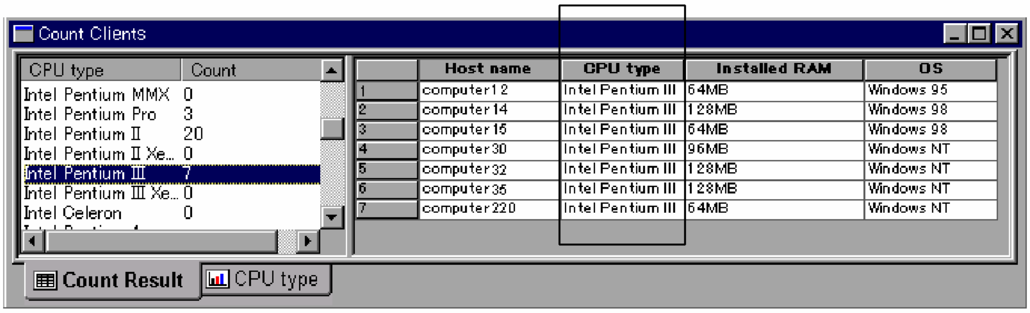
You can display system information, software information, and user inventory information for all clients in table format. You can also display only the inventory items you need or only the clients that have specific information.

For details about how to display inventory information, see *4.3 Displaying inventory information* in the manual *Administrator's Guide Volume 1*.

2.3.2 Counting hosts by inventory items

You can count the total number of client computers for each item of inventory information. For example, the inventory information you collect might include the total number of relay systems and clients, the total number of installed software products, and other system information. In addition to the count results, at the same time you can also display detailed client information for any item of inventory information. For example, you can count the number of hosts for each CPU type and display the hosts that have an Intel Pentium II CPU.

Figure 2–15: Example of counting hosts for each CPU type



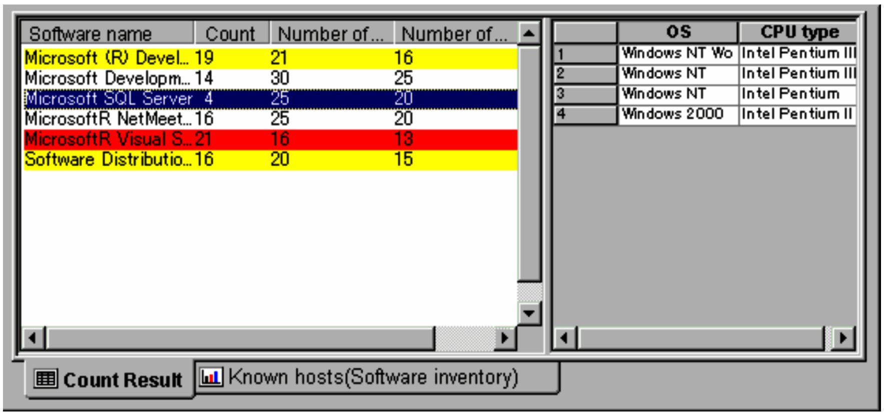
CPU type	Count
Intel Pentium MMX	0
Intel Pentium Pro	3
Intel Pentium II	20
Intel Pentium II Xe...	0
Intel Pentium III	7
Intel Pentium III Xe...	0
Intel Celeron	0

	Host name	CPU type	Installed RAM	OS
1	computer12	Intel Pentium III	64MB	Windows 95
2	computer14	Intel Pentium III	128MB	Windows 98
3	computer15	Intel Pentium III	64MB	Windows 98
4	computer30	Intel Pentium III	96MB	Windows NT
5	computer32	Intel Pentium III	128MB	Windows NT
6	computer35	Intel Pentium III	128MB	Windows NT
7	computer220	Intel Pentium III	64MB	Windows NT

You can combine several inventory items and specify detailed information to create a set of conditions for counting, so you can efficiently manage the information you need. For example, you can combine **CPU type** and **OS** to count the number of hosts whose CPU type is Intel Pentium 4 and OS is Windows XP.

If you already set the number of software licenses in advance, you can determine software license usage status from counting results.

Figure 2–16: Example of software license usage status



Software name	Count	Number of...	Number of...
Microsoft (R) Devel...	19	21	16
Microsoft Developm...	14	30	25
Microsoft SQL Server	4	25	20
MicrosoftR NetMeet...	16	25	20
MicrosoftR Visual S...	21	16	13
Software Distributio...	16	20	15

	OS	CPU type
1	Windows NT Wo	Intel Pentium III
2	Windows NT	Intel Pentium III
3	Windows NT	Intel Pentium
4	Windows 2000	Intel Pentium II

For details about how to count hosts by inventory items, see *4.2 Counting hosts by inventory items* in the manual *Administrator's Guide Volume 1*.

2.3.3 Using a template to display and count

If you save the inventory information display or count conditions that were set by using the View wizard or Count Clients wizard as templates, you can easily perform displays and counts again based on the same conditions. Templates are useful if you repeatedly display or count data using the same conditions.

Templates contain the following information specified with the View wizard or Count Clients wizard:

- View wizard:
  Display conditions and the inventory items to be displayed
- Count Clients wizard:
  Count conditions and the inventory items to be displayed in the **Details** pane

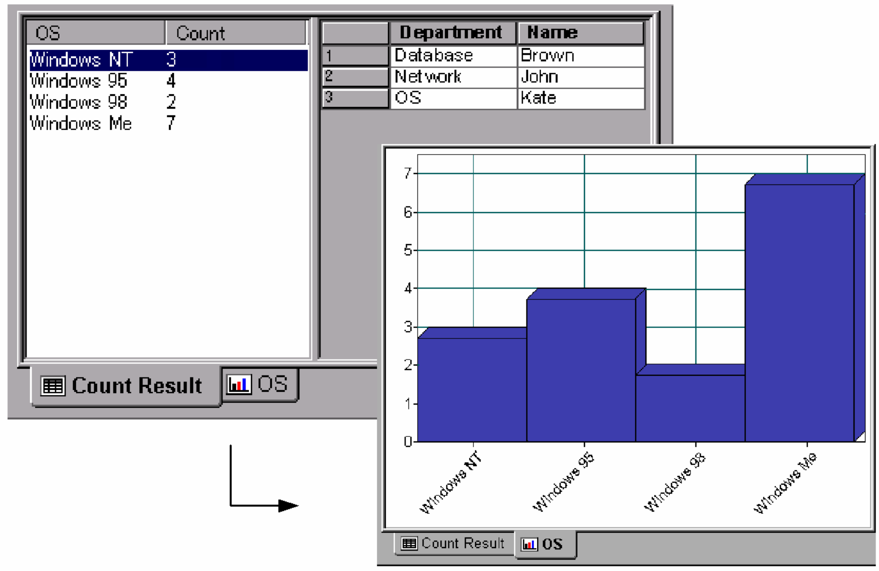
You can edit the conditions in an existing template to create a new template.

For details about how to use templates to display and count data, see *4.4 Using templates* in the manual *Administrator's Guide Volume 1*.

2.3.4 Displaying count results as a graph

Count results can be displayed easily as a graph. You can also copy created graphs and use them in other applications.

Figure 2–17: Displaying count results as a graph



OS	Count
Windows NT	3
Windows 95	4
Windows 98	2
Windows Me	7

	Department	Name
1	Database	Brown
2	Network	John
3	OS	Kate

You can select a 3-dimensional bar graph or a 3-dimensional circle graph; the default is a bar graph. You can change the fonts of the labels displayed in a graph.

For details about how to display count results as a graph and how to change the labels font, see *4.2.6 Displaying count results as a graph* in the manual *Administrator's Guide Volume 1*.

2.3.5 Grouping hosts based on count results

You can create a host group of found hosts in order to group hosts that share the same inventory information. For example, after you count hosts by *Installed package* to create a host group of the hosts that contain Microsoft Word 2000, you can remote-install Microsoft Word 2003 onto all members in that host group.

You can create a new host group or add hosts to an existing host group. You can also remove all hosts from an existing host group, and then add hosts to the group.

For details about how to group hosts based on count results, see *4.2.7 Creating a host group from count results* the manual *Administrator's Guide Volume 1*.

2.3.6 Output of inventory information

You can export the results of sorting inventory information and count results to a CSV file and print the information.

For details about how to output inventory information, see *4.5 Outputting inventory information* in the manual *Administrator's Guide Volume 1*.

(1) Exporting to a CSV file

You can export to a CSV file all the information, including the column names, displayed in a table-format window or in the Count Clients window. In the Count Clients window, you can select whether to save the information from the **Count** pane or the **Details** pane.

You can copy selected information to the clipboard in CSV format. This method is useful for exporting part of the information to another program, such as a spreadsheet program, without having to handle files.

(2) Printing

You can print all the information, including the column names, displayed in a table-format window or in the **Count** pane of the Count Clients window. You can also add a header and footer to the printouts from a table-format window or Count Clients window.

2.4 Collecting files (by remote collection)

You can use the remote collection facility to collect client files onto the managing server. For example, this facility can collect user data created with an application program such as a spreadsheet program and the error logs of application programs.

Note that remote collection can be used for user programs and data only, and cannot be used for Hitachi program products or to other companies' software.

This section provides an overview of remote collection.

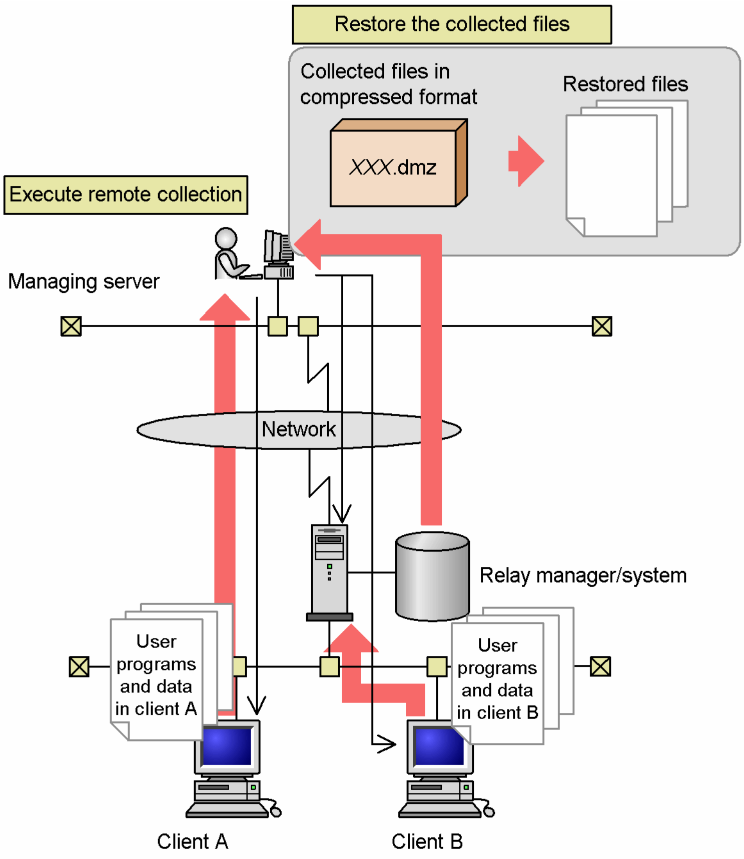
2.4.1 General procedure for remote collection

To collect files (user programs and data) from clients, at the managing server you create and execute a job for executing remote collection.

The *collected files* are saved in archive or compressed format on the managing server. You must restore the files to their original format before you can use them at the managing server.

The following figure gives the general procedure for remote collection.

Figure 2–18: General procedure for remote collection

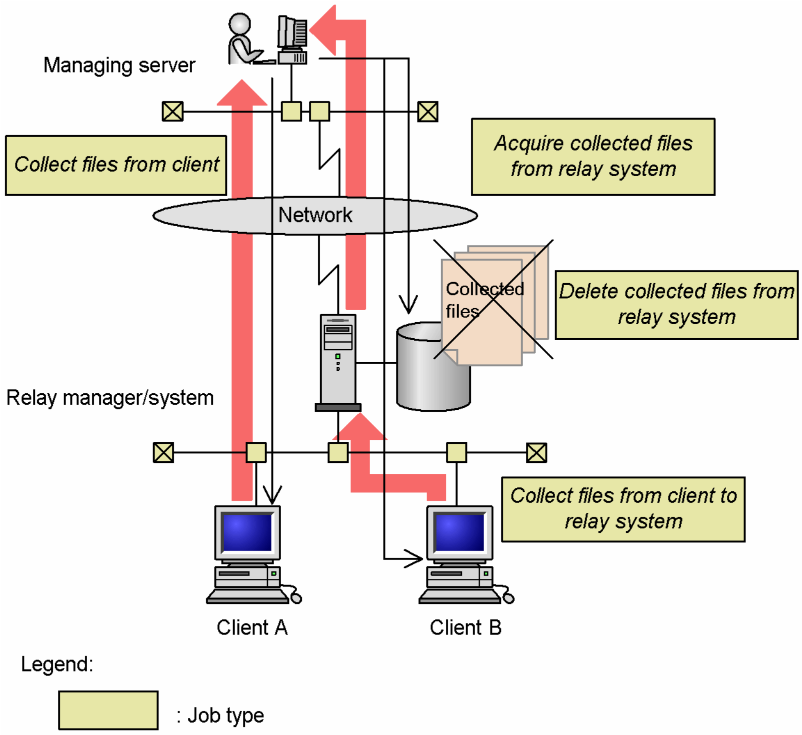

Restore the collected files
Collected files in compressed format
XXX.dmz
Restored files
Execute remote collection
Managing server
Network
Relay manager/system
User programs and data in client A
User programs and data in client B
Client A
Client B

For details about how to execute remote collection, see *5.1 Remote collection procedures* in the manual *Administrator's Guide Volume 1*.

2.4.2 Types of remote collection jobs

Four types of jobs are available for performing remote collection; you should use the type that is appropriate for your network and purpose.

Figure 2–19: Types of remote collection jobs


Managing server
Collect files from client
Acquire collected files from relay system
Network
Collected files
Delete collected files from relay system
Relay manager/system
Collect files from client to relay system
Client A
Client B
Legend:
: Job type

When you create a *Collect files from client* job or a *Collect files from client to relay system* job, you can specify remote collection options, such as the collection time at the client, whether to compress the files, and startup of an external program.

For details about how to set these options, see *5.1.1 Executing remote collection* in the manual *Administrator's Guide Volume 1*.

The following describes each type of job:

(1) "Collect files from client" job

This job collects files from a client onto the managing server, via a relay manager/system. You can also use this type of job without using a relay manager/system, as well as to collect files between a client and the relay manager/system, or to collect files between the relay manager/system and the managing server.

(2) "Collect files from client to relay system" job

On instruction from the managing server, this job collects files and stores the collected files at the relay manager/system connected to the managing server where the job was executed. If the relay manager/system is in a hierarchy of systems, the collected files are stored at the relay manager/system that is directly under the managing server where the job was executed.

You can process or use the collected data at the relay manager/system. You can also transfer all the data to the managing server by executing this job and then an *Acquire collected files from relay system* job.

(3) "Acquire collected files from relay system" job

This job transfers, to the managing server, files that were collected at the relay manager/system by a *Collect files from client to relay system* job.

Because remote collection results in a high workload on the network between the relay manager/system and the managing server, you can collect files more efficiently by storing them temporarily at the relay manager/system with a *Collect files from client to relay system* job, and then later, such as at night when the network traffic is low, transferring them to the managing server by executing this job. Note that when the relay manager/system has a hierarchical structure, even if the relay manager/system that is not directly under the managing server is specified as the job destination, the files are collected from the relay manager/system that is directly under the managing server.

(4) "Delete collected files from relay system" job

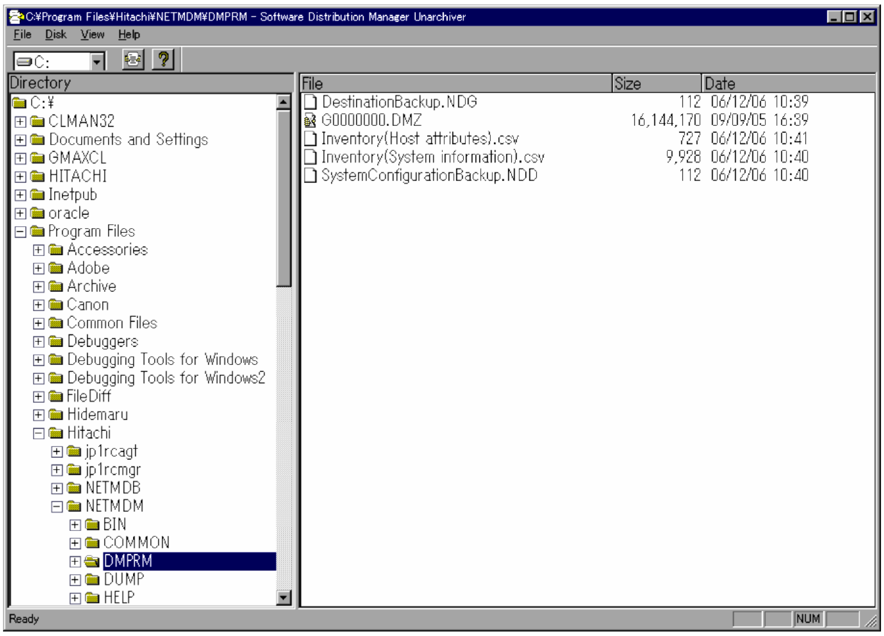
This job deletes files collected at the relay manager/system by a *Collect files from client to relay system* job. Note that when the relay manager/system has a hierarchical structure, even if the relay manager/system that is not directly under the managing server is specified as the job destination, the files are deleted from the relay manager/system that is directly under the managing server.

2.4.3 Restoring collected files

Collected files cannot be read or written directly because they are stored in an archived or compressed format at the managing server. To use these files at the managing server, you must restore them to their original format.

To restore a file, you use a program called *Unarchiver*. The Unarchiver restores a file to its original format after it has been archived or compressed during remote collection (archive file).

Figure 2–20: JP1/Software Distribution Manager Unarchiver window



File	Size	Date
DestinationBackup.NDG	112	06/12/06 10:39
G0000000.DMZ	16,144,170	09/09/05 16:39
Inventory(Host attributes).csv	727	06/12/06 10:41
Inventory(System information).csv	9,928	06/12/06 10:40
SystemConfigurationBackup.NDD	112	06/12/06 10:40

For details about how to restore collected files, see *5.1.2 Restoring collected files* in the manual *Administrator's Guide Volume 1*.

2.4.4 Setting restrictions on executing remote collection at a client

A remote collection job can collect files from any client on which JP1/Software Distribution Client is installed. Thus, there is a risk that unplanned or inappropriate remote collection might be performed on a client by a higher system. To prevent this from happening, you can set restrictions on remote collection when you set up a client.

By setting execution restrictions, you can block all remote collection jobs at a client, or allow only remote collection jobs from a specified higher system.

For details about how to set restrictions on executing remote collection, see *6.2.12 Remote Collect Options page* in the *Setup Guide*.

2.5 Monitoring software operation statuses

By executing a job at a client from the managing server, you can suppress startup of specific software packages, printing, or operations using USB memory devices, and you can collect an operation history by monitoring file operations and Web access. You can also obtain log data about file operations such as the copying, renaming, and printing of files. You can also collect the operation times of specified software.

Using these facilities, you can prohibit the use of unlicensed software, and prevent illegal use of computers and software. Furthermore, by collecting the file operation history, you can monitor for unauthorized removal of confidential information and the import of non-business data. To investigate and locate errors, you can search the collected operation log data by narrowing the search conditions in the Operation Log List window.

This section provides an overview of the facilities for monitoring the software operation statuses of clients.

2.5.1 General procedure for monitoring software operations

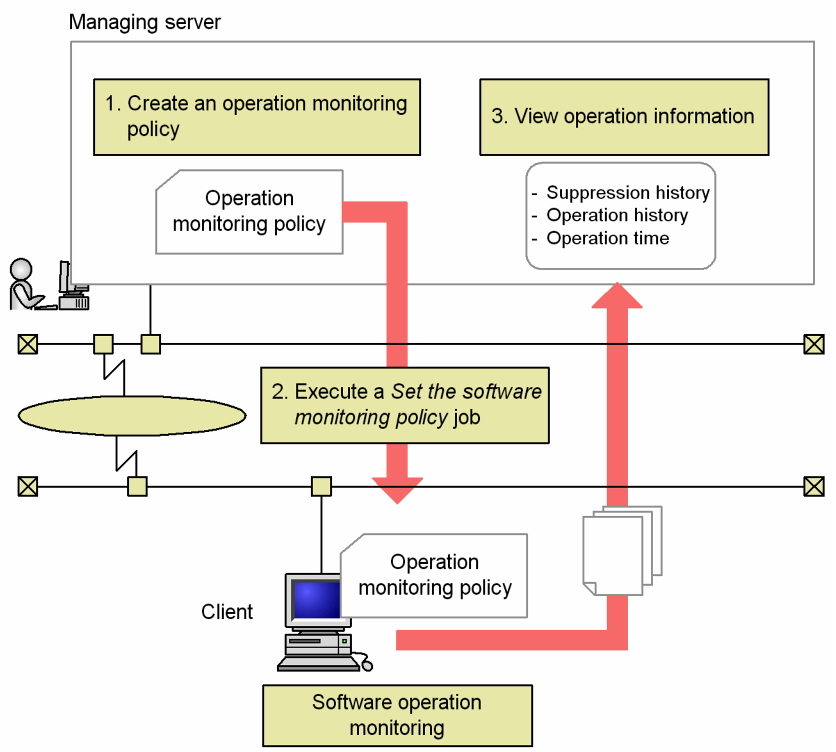
To monitor software operation statuses, you must create at the managing server an operation monitoring policy that specifies the following items:

- Operations for which history is to be collected
- Software to be monitored
- Software whose startup is to be suppressed
- Software whose operation times are to be collected
- Whether to collect Web access history
- Whether to collect print operation history
- Whether to suppress print operations
- Whether to collect external media operation history
- External media whose operations are to be suppressed
- Whether to collect device operation history
- Devices whose operations are to be suppressed

By applying the created operation monitoring policy to a client, you can monitor the client's operation status. Also, by applying the operation monitoring policy to a virtual environment, you can monitor the operation status of that virtual environment. For details about virtual environments, see *2.5.2 Prerequisites for monitoring operation status*.

The figure below shows the general procedure for monitoring software operation statuses. For details about each procedure, see *6. Monitoring Software Operation Status* in the manual *Administrator's Guide Volume 1*.

Figure 2–21: General procedure for monitoring software operation statuses


Managing server
1. Create an operation monitoring policy
3. View operation information
Operation monitoring policy
- Suppression history
- Operation history
- Operation time
2. Execute a *Set the software monitoring policy* job
Operation monitoring policy
Client
Software operation monitoring

To monitor software operation status:

1. Create a software operation monitoring policy.

   At the managing server, create an operation monitoring policy that specifies the software whose startup is to be suppressed and the operations for which history information is to be collected.

2. Specify the clients whose operation is to be monitored and execute a *Set the software monitoring policy* job.

   By executing a job that applies your operation monitoring policy to clients, you can monitor the software operation status at those clients according to the policy.

   Although the operation log data is reported from the clients periodically, you can also acquire it by executing a job from the managing server.

3. View the software operation information.

   To view the software startup prevention history and operation history, use the Software Operation Information window.

   You can view the software operation times in the Software Operation Status window of Asset Information Manager Subset.

   If you have installed Asset Information Manager Subset, you can also view suppression and operation log data from the Operation Log List window and Operation Log Total window.

   You cannot use the Software Operation Status window to view Web access log data or histories of print operations, external media operations, or device operations. Use the Operation Log List window or the Operation Log Total window instead.

If an environment uses a relay manager, you can set it up so that policies created by the central manager can be exported to and used by the relay manager, or so that the operation history collected by the relay manager can be communicated to the central manager. For details on how to monitor the operation status in an environment that uses a relay manager, see *2.5.11 Monitoring the operation status in a large-scale system*.

2.5.2 Prerequisites for monitoring operation status

The items whose operation status can be monitored vary depending on the version of JP1/Software Distribution that is used.

The following table shows the operation statuses that can be monitored by the various versions of JP1/Software Distribution for Windows.

Table 2–15: JP1/Software Distribution versions required for each item whose operation status is monitored

Item whose operation status is monitored		Required JP1/Software Distribution version
Software startup suppression		• JP1/Software Distribution Manager (08-00 or later) • JP1/Software Distribution Client (07-50 or later)
Print suppression		• JP1/Software Distribution Manager (08-51 or later) • JP1/Software Distribution Client (08-51 or later)
External media operation suppression		• JP1/Software Distribution Manager (08-51 or later) • JP1/Software Distribution Client (08-51 to 09-00)
Device operation suppression		• JP1/Software Distribution Manager (09-50 or later) • JP1/Software Distribution Client (09-50 or later)
Operation history	• Start process • Stop process • Change caption • Change active window • Machine start/stop • Logon/logoff	• JP1/Software Distribution Manager (08-00 or later) • JP1/Software Distribution Client (07-50 or later)
	• File operation[#1]	• JP1/Software Distribution Manager (08-00 or later) • JP1/Software Distribution Client (08-00 or later)
	• Web access[#2] • Print operation	• JP1/Software Distribution Manager (08-51 or later) • JP1/Software Distribution Client (08-51 or later)
	• External media operation[#3]	• JP1/Software Distribution Manager (08-51 or later) • JP1/Software Distribution Client (08-51 to 09-50)
	• Device operation[#4]	• JP1/Software Distribution Manager (09-50 or later) • JP1/Software Distribution Client (09-50 or later)
Software operation time		• JP1/Software Distribution Manager (08-10 or later) • JP1/Software Distribution Client (08-10 or later)

#1

To collect a file operation history when the client's OS is Windows Vista, you must use a client whose JP1/Software Distribution version is 08-11 or later.

#2

The client's Microsoft Internet Explorer must be version 5.01, 5.5, 6.0, 7.0, 8.0, 9.0 or 10.0.

Furthermore, for Microsoft Internet Explorer version 6.0 or later, in the dialog box displayed by choosing **Tools**, and then **Internet Options** in Microsoft Internet Explorer, you must click the **Advanced** tab and then select the **Enable third-party browser extensions** check box.

#3

If the client's OS is Windows NT 4.0, no external media operation history is collected.

Furthermore, if the client's OS is Windows 7, Windows Server 2008, or Windows Vista, no histories are collected for operations on either a USB-connected CD/DVD drive or an internal CD/DVD drive.

#4

If the client's OS is Windows 8 (Basic Edition), the facility to suppress writing operations on the device is not supported.

You can limit the items whose operation status is monitored, provided that you have indicated JP1/Software Distribution for each destination of operation status monitoring listed in Table 2-15. For example, to monitor only software operation time, you need JP1/Software Distribution Manager version 08-10 or later and JP1/Software Distribution Client. You do not need other programs.

Note that a system for relaying jobs requires one of the programs listed below, common to all monitored items.

- Windows version of JP1/Software Distribution Manager version 07-50 or later
- Windows and UNIX versions of JP1/Software Distribution SubManager version 07-50 or later
- Windows version of JP1/Software Distribution Client version 08-00 or later
- UNIX version of JP1/Software Distribution Client version 09-00 or later

Prerequisites for operation monitoring in a virtual environment

With the following versions, you can monitor operation statuses in a virtual environment.

- JP1/Software Distribution Manager version 09-50 or later (relay manager)
- JP1/Software Distribution Client version 09-50 or later (relay system and client)

The following table shows the virtual environments and OSs supported by the operation monitoring facility.

Table 2–16: Virtual environments and OSs supported by the operation monitoring facility

Virtual environment	OS	Recommended OS
Quick User Switching Feature#1	• Windows Server 2008 • Windows Server 2012	• Windows Server 2003 (x64) • Windows Server 2008 (x64) • Windows Server 2008 R2 • Windows Server 2012
Terminal server#1	• Windows Server 2003#2 • Windows Server 2008 • Windows Server 2012	• Windows Server 2003 (x64) • Windows Server 2008 (x64) • Windows Server 2008 R2 • Windows Server 2012
Citrix XenApp#1, #3	• Windows Server 2003#2 • Windows Server 2008	• Windows Server 2003 (x64) • Windows Server 2008 (x64) • Windows Server 2008 R2
Windows XP Mode#4	Windows 7	

#1

The maximum number of supported users who can concurrently log on to a virtual environment is 60. If the number of concurrently logged-on users exceeds 60, you can acquire operation monitoring information only from the first 60 users who logged on.

For the 61st or subsequent user who logs on, some of the facilities do not work. For these users, some of the facilities continue to be disabled even when other users log off and the number of concurrently logged-on users falls to or below 60. Such subsequent users must log on again, and if at that time the number of concurrently logged-on users is 60 or fewer, all of the operation monitoring facilities become enabled.

#2

Windows Server 2003 (IPF) is not included.

#3

Only Open Desktop is supported.

#4

In the Windows XP Mode environment, the versions that can be used to monitor operation statuses vary. For details about operating JP1/Software Distribution Client (client) in the Windows XP Mode environment, see *C. Using JP1/Software Distribution Client (Client) in a Windows XP Mode Environment* in the *Setup Guide*.

Notes on virtual environments

If you are using the software operation monitoring facility to acquire a history for file operations, change caption, or change active window, or if you are applying a software operation monitoring policy that suppresses software startup, an application error might occur in the operation monitoring process (`smcusapp.exe`).

To avoid this problem, remove `smcusapp.exe` from the targets of data execution prevention (DEP) on the PC to which the policy was applied. Note that when you uninstall JP1/Software Distribution and reinstall it in a different path, you must also reset the DEP target.

Setting method (common to Windows OSs)

1. In the System Properties dialog box, click the **Advanced** tab, then under **Performance**, click **Settings**.
2. Click the **Data Execution Prevention** tab and select the radio button **Turn On DEP for all programs and services except those I select**, and then add `smcusapp.exe`.

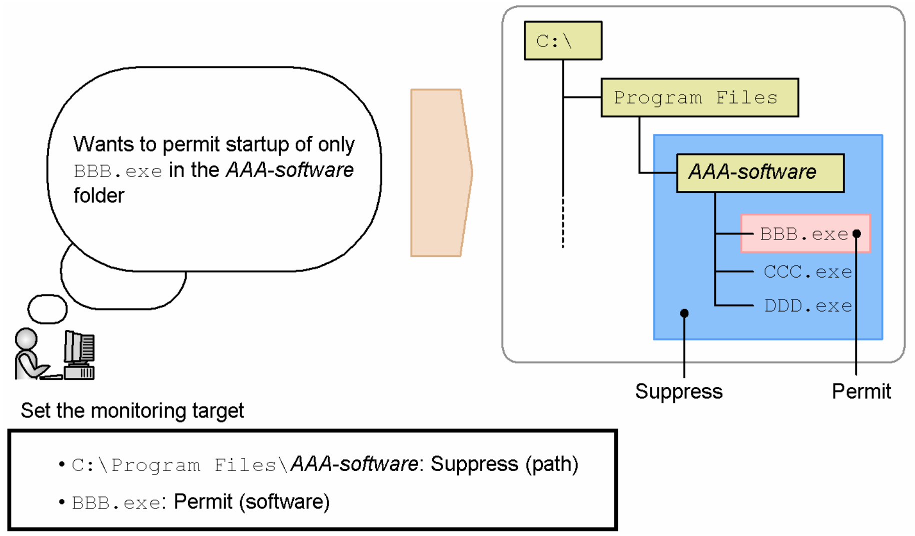
2.5.3 Preventing software from starting

You can monitor software that clients attempt to start, and permit or prevent programs from starting according to specified conditions.

For example, you can suppress startup of programs that are not needed for your company's work or suppress all programs other than the ones provided by JP1/Software Distribution, and permit startup of specified programs only.

The following figure provides an overview of suppressing software startup.

Figure 2–22: Overview of suppressing software startup


Wants to permit startup of only BBB.exe in the *AAA-software* folder
C:\
Program Files
AAA-software
BBB.exe
CCC.exe
DDD.exe
Suppress
Permit
Set the monitoring target
• C:\Program Files*AAA-software*: Suppress (path)
• BBB.exe: Permit (software)

Software whose startup is to be monitored and its path are referred to as a *monitoring target program*. You can specify programs with the following file extensions as monitoring target programs:

- `exe`
- `com`
- `scr`

To monitor startup of a program, you must specify its file name or formal file name.

In the case of a monitoring target program whose startup is suppressed, you can also specify conditions (called *permitted conditions*) to be used to determine when startup of the program is to be permitted. Because you can specify a user type and time as start conditions, you can, for example, allow game programs to start only during lunch hours. If a specified time span is set as the permitted condition, the program stops when the time is over. You can also display a termination warning dialog box before the program stops.

If APPLocker and JP1/Software Distribution suppress startup of the same software when the client's OS is Windows 8, Windows Server 2012, Windows 7 or Windows Server 2008 R2, APPLocker suppresses startup first. Consequently, startup suppression history cannot be collected. Neither the Suppress Startup dialog box nor the Pre-alert Notification dialog box is displayed.

In this section, when there is no need to differentiate between the Suppress Startup dialog box and the Pre-alert Notification dialog box, they are generically referred to as warning dialog boxes.

Note on suppressing software startup

If the client's OS is Windows 8 or Windows Server 2012, dialog boxes related to startup suppression appear on the desktop.

Notes on virtual environments

Note the following when you suppress software startup in a virtual environment:

- The display of the warning dialog box differs as described below, depending on the software startup method and the OS.
  - When a user directly starts the software
    The dialog box is displayed to the user who starts the software.
  - When a service starts the software
    In Windows Server 2003, if there is a user who has logged onto a console session, the dialog box is displayed to that user. If no user has logged onto a console session, the dialog box is not displayed anywhere.
    In Windows Server 2012 or Windows Server 2008, the dialog box is not displayed.

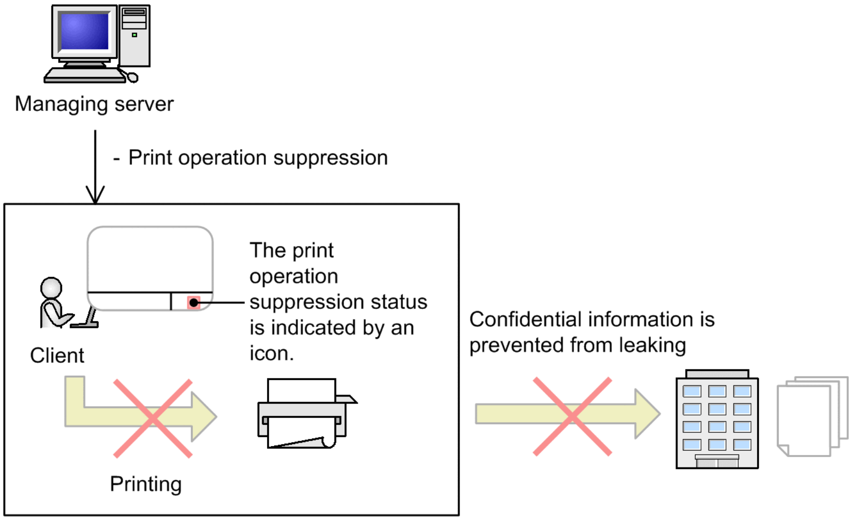
2.5.4 Suppressing printing

By suppressing printing at a client, you can prevent leakage of confidential information.

When an attempt to print data is made on a client PC for which printing is suppressed, a message indicating print suppression is displayed and no data can be printed. Therefore, we recommend that you notify a client before suppressing printing at that client. When a policy is applied to suppress printing, an icon is displayed in the client PC's task tray, indicating that printing is suppressed.

The following figure provides an overview of print suppression.

Figure 2–23: Print suppression overview


Managing server
- Print operation suppression
Client
The print operation suppression status is indicated by an icon.
Printing
Confidential information is prevented from leaking

(1) Prerequisites for the client OS

Printing can be suppressed when the client OS is one of the following:

- Windows NT 4.0
- Windows 2000
- Windows Server 2003
- Windows XP
- Windows Vista
- Windows Server 2008

- Windows 7
- Windows Server 2012
- Windows 8

Printing cannot be suppressed if the client OS is Windows 98 or Windows Me.

(2) Printer types for which printing can be suppressed

The following table shows the printer types for which printing can be suppressed.

Table 2–17: Printer types for which printing can be suppressed

Printer type	Port used	Print suppression
Local printer	LPT port	Y
	Local port	Y
	USB port	Y
	File port	N
	TCP/IP port	Y
	LAN Manager port	N
Shared network printer or printer connected to another PC	N/A	Y
Internet printer	N/A	N
Virtual printer	N/A	Y#

Legend:

Y: Can be used

N: Cannot be used

N/A: Not applicable

#

With some virtual printers, it might not be possible to suppress printing.

Prerequisites for shared network printers

- When you suppress printing, check the printer access privileges from the PC that acts as the printer server. Make sure that in the printer's Properties dialog box, **Manage Documents** is enabled under the **Security** tab. By default, it is enabled.
- If there is a client whose OS is Windows Vista or later, or a client on which File and Printer Sharing for Microsoft Networks is not installed:
  - When you create an operation monitoring policy, you must configure the settings for collecting print operation logs and suppressing print operations. For details about configuring the settings for collecting print operation logs and suppressing print operations, see *6.2.9 Setup for collecting print logs and for suppressing print operations* in the manual *Administrator's Guide Volume 1*.
- If the client's OS is Windows 8 or Windows Server 2012, the icons and dialog boxes related to suppressing print operations or releasing such print suppression appear on the desktop.
  - If you use single-byte characters to specify the name of a shared network printer, the number of characters must not exceed 199. If the printer name contains double-byte characters, you can specify 200 or more characters.
- If no client's OS is Windows Vista or later, and all clients have File and Printer Sharing for Microsoft Networks installed:
  - When you create an operation monitoring policy, check the settings for collecting print operation logs and suppressing print operations. For details about the settings for collecting print operation logs and suppressing

print operations, see *6.2.9 Setup for collecting print logs and for suppressing print operations* in the manual *Administrator's Guide Volume 1*.

- To suppress printing, the printer server uses RPC to communicate with the client PC. If RPC communication is not possible, the problem might be caused by one of the following:
  - The printer server's OS is Windows 95, Windows 98, or Windows Me.
  - The printer server's OS is not Windows.
  - The printer server is a printer based on the Internet Printing Protocol (IPP).
  - A firewall or proxy is present between the printer server and the client PC.
  - The client PC is controlled by NAT.
  - The printer server cannot resolve the name of the client PC.
  - The client PC's Windows firewall is enabled and **File and Printer Sharing** is not set to **Exceptions**.

(3) Notes on suppressing printing

- If the printer server has suppressed printing in an environment in which a shared network printer is used, printing cannot be enabled even if the client PC releases print suppression.
- You might not be able to suppress printing in the following cases:
  - If Windows does not recognize a print operation as a print job
  - When a test print is performed during printer installation
  - If printing is performed before the software operation status monitoring facility is activated
- Depending on the printer, a dialog box indicating print job deletion might be displayed when printing is suppressed. The content of the displayed message differs depending on the application.
- If a single print operation is processed as multiple print jobs, print suppression applies to all of these jobs.
- If there is a client whose OS is Windows Vista or later, or a client on which File and Printer Sharing for Microsoft Networks is not installed, note the following:
  - When you create an operation monitoring policy, you must configure the settings for collecting print operation logs and suppressing print operations. For details about configuring the settings for collecting print operation logs and suppressing print operations, see *6.2.9 Setup for collecting print logs and for suppressing print operations* in the manual *Administrator's Guide Volume 1*.
  - If a print job is not reported via WMI, printing cannot be suppressed.
  - If an operation monitoring policy for suppressing print operations is applied when a print job is in the print queue of a shared network printer, that print job is suppressed. A dialog box indicating print suppression might also be displayed.
- When a shared network printer is used and there is no client whose OS is Windows Vista or later, or there is no client without File and Printer Sharing for Microsoft Networks installed, check the settings for collecting print operation logs and suppressing print operations when you create an operation monitoring policy. For details about the settings for collecting print operation logs and suppressing print operations, see *6.2.9 Setup for collecting print logs and for suppressing print operations* in the manual *Administrator's Guide Volume 1*.

Notes on virtual environments

Note the following when suppressing printing in a virtual environment:

- The display of the warning dialog box differs depending on the number of logged-on users.
  - When only a single user has logged on

    The warning dialog box is displayed to the user who logged on.
  - When two or more users have logged on

    The warning dialog box is not displayed.
- If a user who has logged onto a virtual environment enters the password for releasing print suppression and releases print suppression, print suppression is released for all users who have logged onto that virtual environment.
- If a printer connected to a PC that is executing a Remote Desktop connection is specified to be used by a terminal server, that printer behaves in the same way as a local printer.

2.5.5 Suppressing external media operations

By suppressing external media operations at a client, you can prevent the leakage of confidential information and the entry of undesirable information from external systems. This facility is available when the client version is between 08-51 and 09-00.

During external media operation suppression, writing and reading data via the following external media is suppressed:

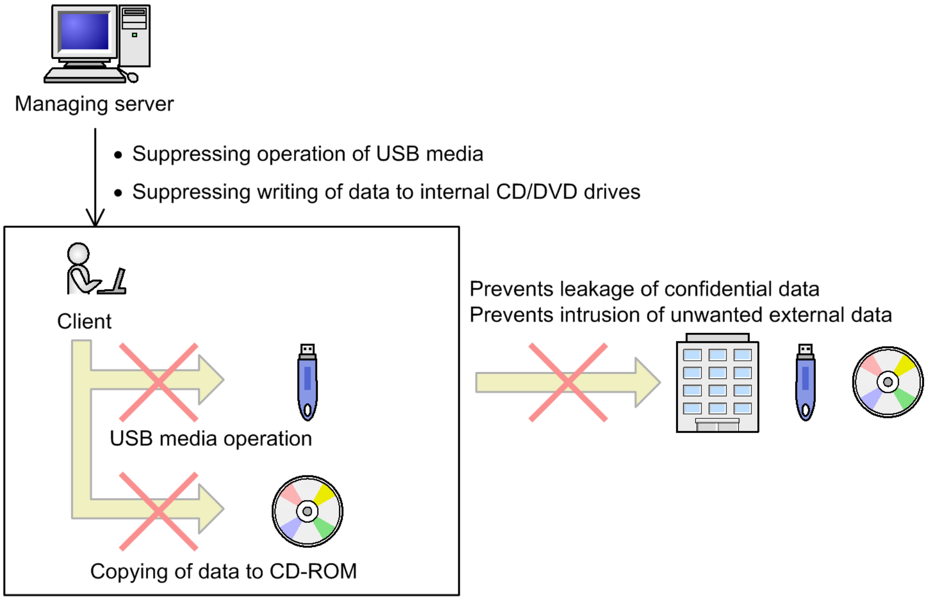
- USB media
- Internal CD/DVD drive
- Internal floppy disk drive
- IEEE 1394-connected media
- Internal SD card slot

Select the media whose operations are to be suppressed based on factors such as the frequency of use by jobs and the risk for information leakage.

If the client version is 09-50 or later, you can suppress these external media operations by suppressing device operations. For details about how to suppress device operations, see *2.5.6 Suppressing device operations*.

The following figure provides an overview of external media operation suppression.

Figure 2–24: Overview of external media operation suppression


Managing server
• Suppressing operation of USB media
• Suppressing writing of data to internal CD/DVD drives
Client
USB media operation
Copying of data to CD-ROM
Prevents leakage of confidential data
Prevents intrusion of unwanted external data

(1) Prerequisites for the client OS

To suppress external media operations, match the client OS to the prerequisites. If the client's OS is Windows NT 4.0, Windows 98, or Windows Me, suppression of external media operations is not supported.

Facility	Windows					
	2000	Server 2003	XP	Vista	Server 2008	7
Suppression of USB-connected media operations (write- and read-disabled)#1, #2	Y	Y	Y	Y	Y#3	Y
Exclusion of specific USB-connected media from suppression#4, #5	Y	Y	Y	Y	Y	Y

Facility	Windows					
	2000	Server 2003	XP	Vista	Server 2008	7
Suppression of USB-connected media operations (only write-disabled)#1, #2	N	N	Y	N	N	N
Suppression of writing data to internal CD/DVD drive	N	Y	Y	Y	N	Y
Suppression of internal floppy disk operations	Y	Y	Y	Y	N	Y
Suppression of IEEE 1394-connected media operations#1	Y	Y	Y	Y	N	Y
Suppression of internal SD card clot operations#1	N	N	Y	Y	N	Y

Legend:

Y: Supported

N: Not supported

#1

The USB-connected media, IEEE 1394-connected media, and SD cards to be suppressed are those media that are displayed as follows when device components are displayed from the Safely Remove Hardware dialog box.

- **USB Mass Storage Device**
- **IEEE 1394 SBP2 Drive**
- **Secure Digital Storage Device**

#2

In some cases, a USB-connected media device that is not displayed as a **USB Mass Storage Device** in the Safely Remove Hardware dialog box may be suppressed. In such a case, exclude the client PC or the suppressed USB-connected media from suppression. When you suppress USB-connected media operations (only write-disabled), you cannot exclude specific USB-connected media devices from suppression.

#3

If the OS of the client PC is Windows Server 2008, the suppressed items are USB storage devices.

#4

If the **Exclude the specified media from suppression** check box is selected, the items suppressed by suppressing USB-connected media operations (write- and read-disabled) are USB storage devices.

#5

With JP1/Software Distribution Client version 08-51 and earlier, you cannot exclude specific media from suppression.

The operations that can be suppressed differ depending on the OS of the client PC, as indicated below.

- When both of the following conditions are met and a file is being copied to a USB-connected hard disk or floppy disk drive, operation of the USB-connected media device cannot be suppressed until file copying is completed:
  - The client's OS is Windows 7 or Windows Server 2008 R2.
  - An operation monitoring policy for suppressing operation of USB-connected media device is applied while file copying is being performed.
- When an operation monitoring policy is applied that excludes a specific USB-connected media device from suppression based on its friendly name, that USB-connected media device is suppressed when it is connected to the client PC for the first time. In this case, reconnect the USB-connected media device. It will not be suppressed the second and subsequent times.
- If the OS of the client PC is Windows 7 or Windows Vista, the following types of suppression cannot be specified separately:

  - Suppression of USB-connected media operations (when the **Exclude the specified media from suppression** check box is cleared)
  - Suppression of IEEE 1394-connected media operations
  - Suppression of internal SD card slot operations

  If either of these is specified, both writing data to and reading data from USB-connected media, IEEE 1394-connected media, an internal SC card, and removable disks on the client are suppressed.

- If the OS of the client PC is Windows 7, Windows Server 2008, or Windows Vista, and the version of JP1/Software Distribution Client is 09-00 or later: when you exclude specified media from suppression during suppression of USB-connected media operations, do not specify suppression of operations of IEEE 1394-connected media or the internal SD card slot. Specifying suppression of these individual operations will invalidate the setting of the **Exclude the specified media from suppression** check box, and both writing data to and reading data from all USB-connected media will be suppressed.
- If you suppress writing data to an internal CD/DVD drive when the OS of the client PC is Windows 7 or Windows Vista, writing data to not only the internal CD/DVD drive but also to USB-connected CD/DVD drives will be suppressed. Similarly, if you allow writing data to USB-connected CD/DVD drives, USB-connected media operations are not suppressed.
- If you suppress writing data to and reading data from an internal floppy disk drive when the OS of the client PC is Windows 7 or Windows Vista, writing data to and reading data from not only the internal floppy disk drive but also to USB-connected floppy disk drives are suppressed. Similarly, if you allow writing data to USB-connected floppy disk drives, USB-connected media operations are not suppressed.
- The setting that suppresses only writing data to USB-connected media does not go into effect if the OS of the client PC is one of those listed below. Therefore, if a setting that suppresses only writing data to USB-connected media is applied, a setting that suppresses both writing and reading is applied to the client PC instead.

  Windows 7, Windows Server 2008, Windows Vista, Windows Server 2003, Windows XP (without any service pack, or with Service Pack 1), and Windows 2000
- If the OS of the client PC is Windows XP, the setting that suppresses only writing data to USB-connected media is supported by Service Pack 2 or later only.
- If the **Exclude the specified media from suppression** check box is selected when the OS of the client PC is Windows 2000, you cannot suppress the operations of a USB-connected floppy disk or hard disk drive that was connected before you logged onto the system. To suppress operations of such USB-connected media, clear the check box.

(2) Notes on suppressing external media operations

- If you suppress only writing data to USB-connected media when the auto-playback function of CD/DVD is disabled in the Windows settings, writing data to USB-connected CD/DVD drive might not be suppressed.
- Even when you specify suppression of external media operations, the operations of any external media that were already connected will not be suppressed. The suppression setting goes into effect after the media are disconnected (removed).
- Suppression of writing data to and reading data from an internal SD card slot goes into effect after the client PC is rebooted.
- Suppression of external media operations is not released even if the operation-monitoring service is stopped. To release the suppression of external media operations, do one of the following:
  - Create an operation monitoring policy that does not suppress external media operations, and apply it.
  - Uninstall JP1/Software Distribution Client.
- If the operation of an internal floppy disk drive is suppressed when the client OS is Windows Server 2003, Windows XP, or Windows 2000, the internal floppy disk drive itself is treated as nonexistent. Consequently, if you collect inventory information from a client whose internal floppy disk operations are suppressed, no information is collected from the internal floppy disk drive.
- JP1/Software Distribution cannot be used concurrently with other products that limit the use of external media (such as Windows Group Policy or Active Directory Policy). If such a product and JP1/Software Distribution are used concurrently on the same client, JP1/Software Distribution's setting for suppressing external media operations might be modified by the other product. JP1/Software Distribution might also modify the setting of the other product.

- There is a risk that the setting for suppressing external media operations might be modified by Active Directory or operator actions. Therefore, the setting for suppressing external media operations is reset according to the operation monitoring policy when the operation monitoring service is restarted. However, if the setting for suppressing external media operations has not been used at all, it will not be reset when the operation monitoring service is restarted. Additionally, no settings related to external media operations are made when an operation monitoring policy that does not suppress external media operations is applied.
- If the OS of the client PC is Windows 7, Windows Server 2008, or Windows Vista, the setting for suppressing external media operations goes into effect after the OS is restarted. Regardless of the OS of the client PC type, when a specific USB-connected media device is excluded from suppression, the setting for suppressing USB-connected media operations and the setting for excluding the specific USB-connected media device from suppression go into effect after the OS is restarted.
- To release external media operation from suppression, perform reinstallation or take a similar action to make sure that the device driver is running normally.
- To suppress the use of a USB-connected link cable, specify operation suppression according to the USB device recognized by the OS. Note that depending on the device, it might not be possible to suppress the use of a USB-connected link cable.
- If you select the **Safely Remove Hardware** icon on the client PC, or if you right-click each USB-connected media device in **Device Manager** (accessed by choosing **Control Panel**, **Administrative Tools**, and then **Computer Management**), and choose **Delete**, suppression of USB-connected media operations might not function normally.
- If you connect USB-connected media targeted for suppression to a client PC, auto-playback might fail and an error message might be displayed even if the auto playback function for USB-connected media is enabled.
- If the **Exclude the specified media from suppression** check box is selected when the OS of the client PC is Windows 2000, you cannot suppress USB-connected floppy disk drive operations. To suppress the operations of this USB-connected media device, clear the check box.
- If the **Exclude the specified media from suppression** check box is selected and the auto-playback function is enabled in the Windows settings when the OS of the client PC is Windows 7, Windows Server 2008, or Windows Vista, you cannot suppress the operations of USB-connected floppy disk or hard disk drives. To suppress the operations of these USB-connected media, clear the check box or disable the auto-playback function.
- The OS might display an error message in the following cases:
    - You connect USB-connected media targeted for suppression when the OS of the client PC is Windows 2000 and no device driver has been installed.
    - An operation monitoring policy for suppressing the operation of USB-connected media is applied while the USB-connected media are operating.
- It might not be possible to suppress the operation of USB-connected media that are connected before the function for monitoring the operating status of software starts.
- If the **Enable CD recording on this drive** check box under the **Recording** tab in **Properties** is cleared when the OS of the client PC is Windows Server 2003 or Windows XP, you cannot suppress recording to the internal CD/ DVD. When recording on DVD-RAM, you need to clear the **Enable CD recording on this drive** check box. Therefore, you cannot suppress recording.

Notes on suppressing external media operations at an offline machine

Do not suppress the operation of external media that will be used to apply an operation monitoring policy or collect operating information. If you suppress the operation of such external media, you will not be able to apply an operation monitoring policy or collect operating information.

Notes on virtual environments

Note the following when an operation monitoring policy for suppressing external media operations is applied to a virtual environment:

- The warning dialog box, which indicates that the connection of USB-connected media has been suppressed, is displayed only to users connected to a console session.
- If all of the following conditions are satisfied, operation of the redirected drive cannot be suppressed even if a security policy for suppressing external media has been applied to the terminal server:
    1. A security policy for suppressing external media connection has not been applied to a PC remotely connected to the terminal server.

2. The drive connected to the PC in condition 1 is set to be used by the terminal server.

To suppress such a drive, disable redirection on the terminal server side. However, doing so will disable redirection for all drives. The procedure for disabling redirection for a terminal server in Windows Server 2008 is as follows.

- **For Windows Server 2008:**

1. From Windows **Terminal Service Configuration**, open the **RDP-Tcp** property.
2. Under the **Client Settings** tab, choose **Drive** in **Redirection**.

- **For Windows Server 2008 R2:**

1. From Windows **RD Session Host configuration**, open the **RDP-Tcp** property.
2. Under the **Client Settings** tab, choose **Drive** in **Redirection**.

2.5.6 Suppressing device operations

By suppressing device operations at a client, you can prevent the leakage of confidential information and the entry of undesirable information from external systems. This functionality is available when the client version is 09-50 or later.

Operation of the following can be suppressed:

- USB storage devices
- Internal CD/DVD drives
- Internal floppy disk drives
- IEEE1394-connected devices
- Internal SD cards
- Bluetooth devices
- Imaging devices

You can suppress the use of various devices (writing data to or reading data from these devices), and you can exclude specific devices from suppression. You also have the option of suppressing only writing data to a device. The following table shows the operations that can be suppressed for various devices.

Table 2–18: Operations that can be suppressed for various devices

Device type	Can use of the device be suppressed?	Can specific devices be excluded from suppression?	Can only recording to a device be suppressed?#1, #6
USB storage device	Y	Y	Y#2
Internal CD/DVD drive	Y	N	Y#3
Internal floppy disk drive	Y	N	Y#4
IEEE1394-connected device	Y	N	Y#4
Internal SD card#5	Y	N	Y#4
Bluetooth device	Y	Y	N
Imaging device	Y	Y	N

Legend:

Y: Supported

N: Not supported

#1

You cannot suppress recording only by device type. The devices for which you can suppress recording only are those devices whose use is not suppressed, or those that are excluded from suppression.

#2

Recording can be suppressed only if the client's OS is Windows XP Service Pack 2, Windows XP Service Pack 3, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2012, or Windows 8.

#3

Recording can be suppressed only if the client's OS is Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2012, or Windows 8.

#4

Recording can be suppressed only if the client's OS is Windows Vista, Windows Server 2008, Windows 7, Windows Server 2012, or Windows 8.

#5

With an SD card connected, from Windows **Device Manager**, open the Properties dialog box for each SD card. If `SD` or `RIMMPTSK` is displayed for **Enumerator** under the **Details** tab, that SC card is supported. Depending on how the SD card in the PC is connected to the PC main unit, something other than `SD` or `RIMMPTSK` might be displayed for **Enumerator**. If something other than `SD` or `RIMMPTSK` is displayed for **Enumerator**, that SD card is not supported.

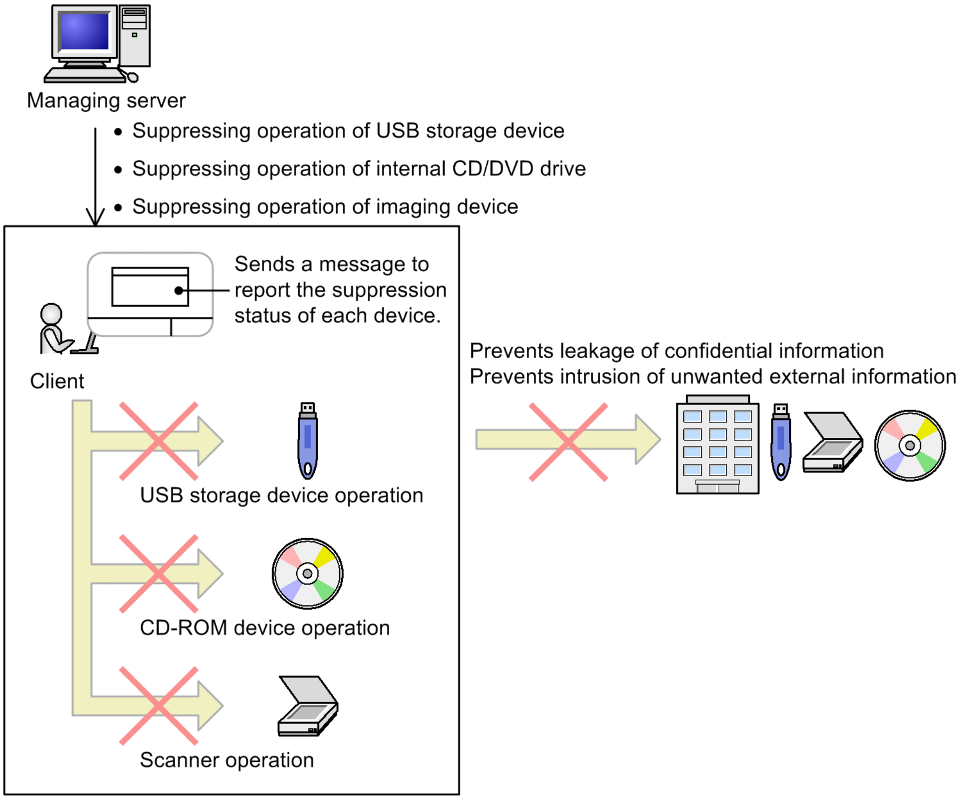
#6

If the client's OS is Windows 8 (Basic Edition), this facility is not supported.

Select the devices whose operations you want to suppress, based on factors such as the frequency of their use by jobs and the risk of information leakage.

The following figure provides an overview of device operation suppression.

Figure 2–25: Overview of device operation suppression


Managing server
• Suppressing operation of USB storage device
• Suppressing operation of internal CD/DVD drive
• Suppressing operation of imaging device
Sends a message to report the suppression status of each device.
Client
USB storage device operation
CD-ROM device operation
Scanner operation
Prevents leakage of confidential information
Prevents intrusion of unwanted external information

(1) Prerequisites for the client OS

You can suppress device operations when the client's OS is one of the following:

- Windows 2000
- Windows Server 2003
- Windows XP
- Windows Vista

- Windows Server 2008
- Windows 7
- Windows Server 2012
- Windows 8

Operation suppression is not supported if the client's OS is Windows NT 4.0, Windows 98, or Windows Me.

(2) Notes on suppressing device operations

- You may not be able to suppress the operation of devices that were connected before operation monitoring started, such as immediately following startup of the client PC.
- JP1/Software Distribution cannot be used concurrently with other products that limit the use of external media (such as Windows Group Policy or Active Directory Policy). If such a product and JP1/Software Distribution are used concurrently on the same client, JP1/Software Distribution's setting for suppressing external media operations might be modified by the other product. JP1/Software Distribution might also modify the setting of the other product.
- Operation suppression does not go into effect on devices that were connected before an operation monitoring policy was applied. To enable device operation suppression for these devices, you must restart the client PC.
- If you make any of the following modifications to the operation monitoring policy, restart the client PC:
  - Changing the setting from operation suppression to operation enabling
  - Changing the setting for an already-connected device to operation suppression
  - Enabling or disabling the setting that suppresses recording only
- If the OS of the client PC is Windows 2000, you cannot suppress operation of USB-connected hard disk and floppy disk drives that were connected before the user logged in.
- If you suppress a device for which the auto-playback function is enabled, an error message indicating auto-playback failure might be displayed.
- If an operation monitoring policy for suppressing the operation of a device is applied while that device is operating, the OS might display an error message.
- When a suppressed device is connected to the client PC for the first time, the OS might display an error message indicating a device driver installation failure.
- Devices such as USB scanners might be recognized as imaging devices even when they are USB-connected.
- You cannot suppress devices that cannot be recognized as USB storage devices, Bluetooth devices, or imaging devices even when they are USB-connected. You cannot exclude them from suppression, either.
- You cannot suppress only writing of data to DVD RAM.
- If you suppress only writing of data to a USB storage device equipped with an encryption function, reading of data from that device might also be disabled.
- To suppress only writing of data when the OS of the client PC is Windows Vista or later, you need to start **Portable Device Enumerator service** in the Services window (accessed by choosing **Control Panel**, **Administrative Tools**, and then **Services**).
- If a device that has multiple device instance IDs is connected, the dialog box showing its suppression status might be displayed multiple times for that single device.
- If driver installation is performed after a suppressed device is connected to the client PC for the first time, the dialog box indicating that device connection was suppressed might be displayed multiple times.
- When you suppress a USB-connected CD/DVD drive, the tray of the suppressed CD/DVD drive might open.
- When you connect a suppressed device to the client for the first time, you might not be able to install the device driver.

  In this case, no history of device connection, disconnection, and connection suppression is collected. The warning dialog box indicating device connection suppression is not displayed, either.
- When both of the following conditions are satisfied and a file is being copied to a USB-connected hard disk or floppy disk drive, operation of a USB storage device cannot be suppressed until file copying is completed:
  - The OS of the client PC is Windows 8, Windows Server 2012, Windows 7 or Windows Server 2008 R2.

    - An operation monitoring policy for suppressing the operation of a USB storage device is applied while file copying is being performed.

- If an operation monitoring policy is applied that excludes a specific USB storage device from suppression based on its friendly name, when that USB storage device is connected to the client PC for the first time, any device whose friendly name cannot be acquired might be suppressed. In this case, reconnect the USB storage device.
- If you suppress the operation of a device, the suppressed device is no longer recognized as a drive, and consequently you will not be able to collect that device's system information.
- If the auto-playback function is enabled in Windows settings, you cannot suppress the operation of USB-connected hard disk or floppy disk drives. To suppress the operation of these drives, disable the auto-playback function.
- If you suppress internal SD cards, the operation of the following devices is also suppressed:
    - Devices for which `RIMMPTSK` is displayed for **Enumerator** under the **Details** tab in the device's Properties dialog box (displayed by choosing from **Administrative Tools**, **Computer Management**, and then **Device Manager**)
- If you specify an operation monitoring policy that suppresses the operation of a device that is already connected, the suppression dialog box for that device might be displayed when you connect a different device to the client PC.
- Even when it is necessary to restart the client PC to enable an operation monitoring policy for suppressing operation, the suppression dialog box is displayed when the operation monitoring policy is set.
- When the OS of the client PC is Windows Vista or later, if you apply an operation monitoring policy that suppresses one or more devices, an error-level event log might be output.

  The following example shows the event log that is output when an internal CD/DVD is suppressed.

```
Source: Service Control Manager Eventlog Provider
Event ID: 7026
The following boot-start drive or system-start drive could not be loaded: cdrom
```

  Note that in Windows 7 and Windows Server 2008 R2, the source is `Service Control Manager`.

- If you suppress a Bluetooth device, the use of the mouse or keyboard connected using Bluetooth will also be suppressed.
- When you connect a Bluetooth device to a PC, the registry `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB\` (the Bluetooth device's hardware ID) is created. The device control facility treats a device as a Bluetooth device when the `Class` value in this registry is `Bluetooth`, `BTW`, or `BTM`. You can check the hardware ID from the OS's device manager. We have confirmed that the Bluetooth devices listed below can be suppressed.

Manufacturer	Model No.
Planex Communications	BT-Micro3E1X
	BT-MicroEDR2X
Logitech	LBT-UAN03C2BK
	LBT-UAN01C1
Corega	CG-BT2USB01CB
	CG-BT2USB02CB
Sanwa Supply	MM-BTUD26
	MM-BTUD23
Buffalo	BSHSBD04BK
	BSHSBD02BK
I-O Data	USB-BT21

- If the client's OS is Windows 8 or Windows Server 2012, dialog boxes related to device suppression appear on the desktop.

- If the client's OS is Windows 8 or Windows Server 2012, you cannot suppress operations on a USB storage device to which a storage pool is assigned.

Notes on suppressing device operations at an offline machine

Do not suppress the operation of the device that will be used to apply an operation monitoring policy or to collect operating information. If you suppress such a device, you will not be able to apply an operation monitoring policy or collect operating information.

Notes on virtual environments

- When an operation monitoring policy for suppressing device operations is applied to a virtual environment, a warning dialog box indicating that the connection of the device has been suppressed is displayed only to users connected to a console session. If no users are connected to a console session, the warning dialog box is not displayed.
- If both of the following conditions are satisfied, operation of the redirected drive cannot be suppressed even if a security policy for suppressing devices has been applied to the terminal server:
  1. A security policy for suppressing device operations has not been applied to a PC remotely connected to the terminal server.
  2. The drive connected to the PC in condition 1 is set to be used by the terminal server.

  To suppress such a drive, disable redirection on the terminal server side. However, making this setting will disable redirection for all drives. The procedure for disabling redirection for a terminal server in Windows Server 2012 or Windows Server 2008 is as follows.

  - **For Windows Server 2008:**

  1. From Windows **Terminal Service Configuration**, open the **RDP-Tcp** property.
  2. Under the **Client Settings** tab, select **Drive** in **Redirection**.

  - **For Windows Server 2008 R2:**

  1. From Windows **Remote Desktop Session Host Configuration**, open the **RDP-Tcp** property.
  2. Under the **Client Settings** tab, select **Drive** in **Redirection**.

  - **For Windows Server 2012:**

  1. In Windows Local Group Policy Editor, choose **Device and Resource Redirection** (**Computer configuration - Administrative Templates - Windows Components - Remote Desktop Services - Remote Desktop Session Host**)
  2. Enable **Do not allow drive redirection**.

Notes on upgrading JP1/Software Distribution from versions between 08-51 and 09-00 inclusive to version 09-50 or later

An operation monitoring policy for suppressing external media operation is not applied to clients whose version is 09-50 or later. You need to specify an operation monitoring policy for suppressing device operation.

However, an operation monitoring policy for suppressing external media operations is applied when the following two conditions are satisfied:

- No operation monitoring policy that was edited following an upgrade has ever been applied.
- An operation monitoring policy that suppresses the operation of pre-upgrade external media is applied without being edited.

2.5.7 Reporting invalid operations

When an invalid operation is detected at a client PC, you can alert the administrator with a JP1 event.

(1) Using an alert event to report connection of a device whose operation is suppressed

When a device whose operation is suppressed is connected to the client PC, an operation-monitoring alert event for an invalid device connection can be reported as a JP1 alert event.

If the client version is 09-50, a JP1 event can be reported only when USB-connected media whose operation is suppressed are connected to the client PC. However, if the client version is 09-00 or earlier, no alert event is reported.

To report the operation-monitoring alert event for an invalid device connection, specify the settings as described below. For details about the settings for the relay manager and relay system, see *(4) Notes on reporting invalid operations*.

For details about the information that is output in this JP1 event, see *2.2.2 JP1 event attributes* in the manual *Administrator's Guide Volume 2*.

Managing server or relay manager

- During the server setup, on the **Event Service** page, select the **Enable the event service** and **Unauthorized operation event in operation monitoring** check boxes.

  For details about the **Event Service** page, see *4.2.11 Event Service page* in the *Setup Guide*.
- Select the **Notify suppression event immediately** check box in the Edit Software Operation Monitoring Policy dialog box (for uploading operation monitoring results).

  For details about the Edit Software Operation Monitoring Policy dialog box (for uploading operation monitoring results), see *6.2.4 Setup for uploading the operation monitoring result* in the manual *Administrator's Guide Volume 1*.
- Specify either of the following:
  - Select the **Exclude the specified media from suppression** check box in the Edit Software Operation Monitoring Policy dialog box (for collecting external media operation log and setting suppression).

    For details about the Edit Software Operation Monitoring Policy dialog box (for collecting external media operation log and setting suppression), see *6.2.10 Setup for collecting logs of operations with external media and for suppressing operations with external media* in the manual *Administrator's Guide Volume 1*.
  - In the Control Settings dialog box, select the **Suppress usage** and **Send alerts** check boxes.

    For details about the Control Settings dialog box, see *6.2.11 Setup for collecting device operation logs and for suppressing device operations* in the manual *Administrator's Guide Volume 1*.

(a) Notes on reporting an operation-monitoring alert event for an invalid device connection

Notes when the client version is 09-00

- If USB-connected media with multiple device instance IDs are connected to a client PC, multiple operation-monitoring alert events for an invalid device connection might be reported.
- When USB-connected media are connected to a client PC for the first time, a device driver might be installed. When this occurs, multiple operation-monitoring alert events for an invalid device connection might be reported.
- No operation-monitoring alert event for an invalid device connection is reported for USB-connected media that are connected before the software operation status monitoring facility starts.
- If the OS of the client PC is Windows 2000, an operation-monitoring alert event for an invalid device connection cannot be reported for a USB-connected floppy disk drive.
- Depending on the type of USB-connected link cable, it might not be possible to report an operation-monitoring alert event for an invalid operation.
- Even when an operation-monitoring alert event for an invalid device connection is reported, the operation history and suppression history might not be reported to the managing server. To check the operation history and suppression history, either execute a *Get software operation monitoring history* job, or wait for lower systems to report the operation history and suppression history.
- If USB-connected media are connected to the client PC when an operation monitoring policy is applied, it might not be possible to acquire the correct information to be output in an operation-monitoring alert event for an invalid device connection.
- If one of the notes on suppressing external media operations is applicable and the operation of external media cannot be suppressed, no operation-monitoring alert event for an invalid device connection is reported.

  For notes on suppressing external media operations, see *2.5.5(2) Notes on suppressing external media operations*.

Notes when the client version is 09-50 or later

- If a device for which multiple device instance IDs are set is connected to the client PC, multiple operation-monitoring alert events for an invalid device connection might be reported.
- When a device is connected to the client PC for the first time, a device driver might be installed. When this occurs, multiple operation-monitoring alert events for an invalid device connection might be reported.
- No operation-monitoring alert event for an invalid device connection is reported for a device that is connected before the software operation status monitoring facility starts.
- Even when it is necessary to restart the client PC to enable an operation monitoring policy for suppressing operations, an operation-monitoring alert event for an invalid operation is reported when the operation monitoring policy is set.
- Even when a product other than JP1/Software Distribution changes the device setting and device connection or when disconnection is detected, an operation-monitoring alert event for an invalid device connection is reported.
- If one of the notes on suppressing device operations is applicable and the operation of a device cannot be suppressed, no operation-monitoring alert event for an invalid device connection is reported.

  For notes on suppressing device operations, see *2.5.6(2) Notes on suppressing device operations*.
- Because an operation-monitoring alert event for an invalid device connection is reported after device operation is suppressed (the device is disconnected), it might not be possible to acquire the following items (expanded attributes of the operation-monitoring alert event for an invalid device connection):
  - Device type
  - Friendly name
  - Device instance ID by type
  - Device instance ID of controller

(2) Using an alert event to report software startup suppression

When a client suppresses software startup, an operation-monitoring alert event for software startup suppression can be reported as a JP1 alert event. However, no alert event is reported if the client version is 09-00 or earlier.

To report the operation-monitoring alert event for software startup suppression, specify the settings as described below. For details about the settings for the relay manager and relay system, see *(4) Notes on reporting invalid operations*.

For details about the information that is output in this JP1 event, see *2.2.2 JP1 event attributes* in the manual *Administrator's Guide Volume 2*.

If software startup cannot be suppressed, no operation-monitoring alert event for software startup suppression is reported. For details about cases in which software startup cannot be suppressed, see *2.5.3 Preventing software from starting*.

Managing server or relay manager

- During the server setup, on the **Event Service** page, select the **Enable the event service** and **Unauthorized operation event in operation monitoring** check boxes.

  For details about the **Event Service** page, see *4.2.11 Event Service page* in the *Setup Guide*.
- Select the **Notify suppression event immediately** check box in the Edit Software Operation Monitoring Policy dialog box (for uploading operation monitoring results).

  For details about the Edit Software Operation Monitoring Policy dialog box (for uploading operation monitoring results), see *6.2.4 Setup for uploading the operation monitoring result* in the manual *Administrator's Guide Volume 1*.
- In the **Monitoring target program list** in the Edit Software Operation Monitoring Policy dialog box (for specifying monitoring target programs), set **Operation** for the software to be suppressed to **Suppression**.

  For details about the Edit Software Operation Monitoring Policy dialog box (for specifying monitoring target programs), see *6.2.6 Specifying the programs to be monitored* in the manual *Administrator's Guide Volume 1*.

(3) Using an alert event to report print suppression

When a client suppresses print operations, an operation-monitoring alert event for print suppression can be reported as a JP1 alert event. However, no alert event is reported if the client version is 09-00 or earlier.

To report the operation-monitoring alert event for print suppression, specify the settings as described below. For details about the settings for the relay manager and relay system, see *(4) Notes on reporting invalid operations*.

For details about the information that is output in this JP1 event, see *2.2.2 JP1 event attributes* in the manual *Administrator's Guide Volume 2*.

If printing could not be suppressed, no operation-monitoring alert event for print suppression is reported. For details about cases in which printing cannot be suppressed, see *2.5.4(3) Notes on suppressing printing*.

Managing server or relay manager

- During the server setup, select the **Enable the event service** and **Unauthorized operation event in operation monitoring** check boxes in the **Event Service** page.

  For details about the **Event Service** page, see *4.2.11 Event Service page* in the *Setup Guide*.
- Select the **Notify suppression event immediately** check box in the Edit Software Operation Monitoring Policy dialog box (for uploading operation monitoring results).

  For details about the Edit Software Operation Monitoring Policy dialog box (for uploading operation monitoring results), see *6.2.4 Setup for uploading the operation monitoring result* in the manual *Administrator's Guide Volume 1*.
- Select the **Suppress printing** check box in the Edit Software Operation Monitoring Policy dialog box (for configuring collection of print operation logs and suppression of print operations).

  For details about the Edit Software Operation Monitoring Policy dialog box (for configuring collection of print operation logs and suppression of print operations), see *6.2.9 Setup for collecting print logs and for suppressing print operations* in the manual *Administrator's Guide Volume 1*.

(4) Notes on reporting invalid operations

- To report invalid operations, you need to specify the settings described below in the relay manager. Note that these settings are not required if JP1 events are to be reported from the relay manager.
  - In the basic settings for the relay manager, on the **Report To Higher System** page, select the **When result is received from managed hosts** radio button.
  - In the basic settings for the relay manager on the **Report To Higher System** page, if both the **Specify whether to relay operation monitoring history to the higher system** check box and the **Relay** radio button are selected, select the **Startup suppression information** check box.

    For details about the **Report To Higher System** page, see *4.3.2 Report To Higher System page* in the *Setup Guide*.
- To report invalid operations, you must specify the following in the relay system:
  - In the basic settings for the relay system, on the **Report To Higher System** page, select the **When result is received from managed hosts** radio button.

    For details about the **Report To Higher System** page, see *5.2.5 Report To Higher System page* in the *Setup Guide*.
- If you specify that the operation monitoring history be saved at the relay manager, use a version of relay manager that is the same as or newer than lower systems.

  If a relay manager of version 08-10 or earlier receives an operation-monitoring alert event for an invalid device connection, suppression history containing only dates ends up being stored in the operation monitoring log database.

2.5.8 Collecting operation history and suppression history

You can collect the operation history and suppression history of software programs used at clients.

To collect the operation history and suppression history, you must specify in an operation monitoring policy those events whose history you wish to collect. The follow table shows the event types that can be collected as operation history and suppression history.

Table 2–19: Event types that can be collected as operation history and suppression history

Event	Operation target	Description
`Start process`	Software	Program start event
`Stop process`		Program stop event
`Change caption`#1, #2, #3		Window title change event
`Change active window`#1, #3		Active window change event
`Start/Stop of machine`		PC start or stop event
`Logons/logoffs`#4		Logon or logoff event
`Web access`#3		Web page downloading completion event in Microsoft Internet Explorer
`Software startup suppression`		Software startup suppression event
`Print operation`#3, #5		Print execution event from software
`External media operation`	External media	External media connection or disconnection event (can be collected from clients whose version is between 08-51 and 09-00)
`Device operation`		Connection or disconnection event for various types of devices (can be collected from clients whose version is 09-50 or later)
`USB media connection permission`		USB media connection permission event (can be collected from clients whose version is between 08-51 and 09-00)
`USB media connection suppression`		USB media connection suppression event (can be collected from clients whose version is between 08-51 and 09-00)
`Device connection permission`		Connection event for various types of devices (can be collected from clients whose version is 09-50 or later)
`Device connection suppression`		Connection suppression event for various types of devices (can be collected from clients whose version is 09-50 or later)
`File operations`#3	File	File manipulation event on Windows Explorer

#1

If a client's OS is Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, or Windows Vista, change events in the active window cannot be collected, nor can the caption for a process for which user permissions have been upgraded.

#2

Caption change events might not be collectable for software created in Java or Visual Basic.

#3

Depending on the logon timing, the logon user name might be displayed as `SYSTEM`.

#4

To collect the logoff operation history when the client's OS is Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, or Windows Vista, do not stop the Terminal Services service.

#5

In the case of a virtual printer, printing might not have been suppressed even if a print suppression event has been output to the log.

The details of the information to be collected are given below.

(1) Information collected in the software operation log and suppression log

This subsection explains the information that is collected in the software operation log and suppression log.

(a) Information collected in a software operation log

Information collected in a software operation log differs depending on the event that occurs. The following information is collected. For details about the information that is collected, see *6.5.3 Items displayed in an operation log* in the manual *Administrator's Guide Volume 1*.

Table 2–20: Information collected in a software operation log

Event	Time	Type	Logon user	Window title	Program name	File version	Account
Start process	Y	Y	Y	--	Y	Y	Y
Stop process	Y	Y	Y	--	Y	Y	Y
Change caption	Y	Y	Y	Y	Y	Y	Y
Change active window	Y	Y	Y	Y	Y	Y	Y
Start/Stop of machine	Y	Y	--	--	--	--	--
Logons/Logoffs	Y	Y	Y	--	--	--	--

Legend:
Y: Collected.
--: Not collected.

(b) Information collected in the software startup suppression log

The types of data listed below are collected in the software startup suppression log. For details about the information that is collected, see *6.5.1 Viewing software startup suppression logs* in the manual *Administrator's Guide Volume 1*.

- Date and time
- Program name
- File version
- File language
- Software name
- Product version
- Account
- Logon user

(2) Information collected in a Web access log

The following Web access log information is collected:

- Execution date/time
  Date/time when a Web access was executed
- Type
  Web access
- Title
  Title of the accessed Web page
- URL
  URL of the accessed Web page
- Logon user
  User who logged onto Windows

Notes on collecting a Web access log

- A Web access log may result in a massive volume of data. Therefore, set up filtering conditions so that the history of Web pages that are frequently used in business is not collected.
- Information about images on Web pages cannot be collected.
- When a Web access is made from an inline frame, it might not be possible to collect the access destination information.
- If multiple Web accesses are made within 1 second, it might not be possible to collect a Web access log.
- If multiple copies of Microsoft Internet Explorer start concurrently, it might not be possible to collect a Web access log.
- If Microsoft Internet Explorer is started immediately after either logon to Windows or the application of an operation monitoring policy, it might not be possible to collect a Web access log.
- If a Web page or file that is divided into frames is accessed, log data is collected for each frame (with the total number of log entries equaling the number of Web accesses generated to configure the page). In this case, the title and URL of the main window are used as the log title and URL, respectively.
- A Web access log is also collected when files and folders are opened with Microsoft Internet Explorer.
- A Web access log might be collected even when a Web access attempt ends in a connection error due to factors such as a communication error or non-existent URL.

(3) Information collected in the print operation and print suppression logs

The information collected in the print operation and print suppression logs varies depending on the events that occur. The following table shows the information collected in the print operation and print suppression logs.

Table 2–21: Information collected in the print operation and print suppression logs

Event	Execution date/time	Type	Document name	Logon user	Name of the printer used	Result
Print	Y	Y	Y	Y	Y	--
Print suppression	Y	Y	Y	Y	Y	--
Print suppression released	Y	Y	--	Y	--	Y

Legend:
Y: Collected.
--: Not collected.

- Execution date/time

  Date and time when printing, print suppression, and print suppression release were performed
- Type

  `Printed`, `Printing suppression`, or `Print suppression released`
- Document name

  Name of the document that was printed or whose printing was suppressed
- Logon user

  User who logged onto Windows

  For a virtual environment, the logon user will vary depending on the event and the number of logon users.

  - Printing and print suppression events

    If there is only one logon user, the name of the user who performed printing is collected.

    If two or more users used a local printer, the names of the users who performed printing are collected. If a user starts software from a user account that is different from that of the logon user and performs printing, the name of the user who performed printing is collected.

    If a network printer is used, `Network Printer` is displayed.
  - Print suppression released event

    The name of the user who released print suppression is collected.

- Name of the printer used

  Name of the printer used for print operations. This is the printer name that is set up by the PC that executes printing. Therefore, if a user has changed this name, it might be different from the printer product name.

- Result

  Success or failure

  Note that a print suppression log is acquired when a print operation is suppressed. For the printer types for which print operations can be suppressed, see *2.5.4(2) Printer types for which printing can be suppressed*. The following table shows the printer types from which print operation logs can be acquired.

Table 2–22: Printer types from which print operation logs can be acquired

Printer type	Port used	Print operation log acquisition
Local printer	LPT port	Y
	Local port	Y
	USB port	Y
	File port	Y
	TCP/IP port	Y
	LAN Manager port	N
Shared network printer or printer connected to another PC	N/A	Y
Internet printer	N/A	N
Virtual printer	N/A	Y

Legend:
Y: Can be used
N: Cannot be used
N/A: Not applicable

Prerequisites for shared network printers

- If there is a client whose OS is Windows Vista or later, or a client on which File and Printer Sharing for Microsoft Networks is not installed
  - When you create an operation monitoring policy, you must configure the settings for collecting print operation logs and suppressing print operations. For details about configuring the settings for collecting print operation logs and suppressing print operations, see *6.2.9 Setup for collecting print logs and for suppressing print operations* in the manual *Administrator's Guide Volume 1*.
  - To acquire a print operation log, WMI must be active on the client PC.
  - If you use single-byte characters to specify the name of a shared network printer, the number of characters must not exceed 199. If the printer name contains double-byte characters, you can specify 200 or more characters.
- If no client's OS is Windows Vista or later, and all clients have File and Printer Sharing for Microsoft Networks installed
  - When you create an operation monitoring policy, check the settings for collecting print operation logs and suppressing print operations. For details about the settings for collecting print operation logs and suppressing print operations, see *6.2.9 Setup for collecting print logs and for suppressing print operations* in the manual *Administrator's Guide Volume 1*.
  - To acquire a print operation log, the printer server uses RPC to communicate with the client PC. If RPC communication is not possible, the problem might be caused by one of the following:
    - The printer server's OS is Windows 95, Windows 98, or Windows Me.
    - The printer server's OS is not Windows.
    - The printer server is a printer based on the Internet Printing Protocol (IPP).
    - A firewall or proxy is present between the printer server and the client PC.

- The client PC is controlled by NAT.
- The printer server cannot resolve the name of the client PC.
- The client PC's Windows firewall is enabled and **File and Printer Sharing** is not set to **Exceptions**.

Notes on collecting print operation and print suppression logs

- In the following cases, printing is not performed, but print operation and print suppression logs might be collected:
  - If Windows does not recognize a print operation as a print job
  - When a test print is performed during printer installation
  - If printing is performed before the software operation status monitoring facility is activated
  - If printing is cancelled immediately following print execution
- When a print job is in the print queue of a shared network printer
- If an operation monitoring policy for suppressing print operations is applied, that print job is suppressed and a print operation suppression log might be collected in some cases.
- If a print job is completed before the print operation is reported to the managing server

  The print operation log cannot be collected.
- If a print job is cancelled before the print operation is reported to the managing server

  The print operation log cannot be collected.
- When **Hide extensions for known file types** is enabled in the Windows folder options

  No extension is displayed in document names. This is the same as the content displayed in the window that displays the print queue in Windows.
- If a single print operation is processed as multiple print jobs

  Multiple print operation logs are collected.
- If printing is performed in a specific application

  An application name, instead of a document name, might be displayed in some cases. This is the same as the content displayed in the window that displays the print queue in Windows.
- If the printer server is suppressing printing in an environment in which a shared network printer is used

  Printing cannot be performed even if print suppression is released at the client PC, but a print job log is collected at the client PC.
- If a shared network printer is used, and there is a client whose OS is Windows Vista or later or a client on which File and Printer Sharing for Microsoft Networks is not installed:

  When you create an operation monitoring policy, you must configure the settings for collecting print operation logs and suppressing print operations. For details about configuring the settings for collecting print operation logs and suppressing print operations, see *6.2.9 Setup for collecting print logs and for suppressing print operations* in the manual *Administrator's Guide Volume 1.*
  - If an operation monitoring policy is applied when a print job is in the print queue of a shared network printer, the print job might be reported and a print operation log might be collected in some cases.
- If no client's OS is Windows Vista or later, and all clients have File and Printer Sharing for Microsoft Networks installed
  - When you create an operation monitoring policy, check the settings for collecting print operation logs and suppressing print operations. For details about the settings for collecting print operation logs and suppressing print operations, see *6.2.9 Setup for collecting print logs and for suppressing print operations* in the manual *Administrator's Guide Volume 1.*
- If multiple users who have logged onto a virtual environment simultaneously print a file having the same name from the same printer

  Only a single print operation log might be collected in some cases.
- If a user who has logged onto a virtual environment performs a print operation

  Depending on the operation timing, the same log might be collected more than once.

(4) Log data collected for operations to or from external media

The following types of log data are collected for operations to or from external media:

- Operation date/time
  Date/time when external media was connected or disconnected
- Type
  `Connected` or `Disconnected`
- Logon user
  User who logged onto Windows
  For a virtual environment, the logon user will vary depending on whether there is a user who logged onto a console session.
    - When there is a user who logged onto a console session
      The logon user indicates the user who logged onto a console session.
    - When there is no user who logged onto a console session
      No logon user information is collected.
- External media type
  External media type (`Local disk`, `Removable`, `CDROM`, or `Other (Collection failure)`)
- External media drive name
  Name of the drive to which external media was connected or from which it was disconnected

Notes on collecting log data for operations to or from external media

- If the client's OS is Windows 7, Windows Server 2008, or Windows Vista, log data cannot be collected for operations in a USB-connected CD/DVD drive or an internal CD/DVD drive.
- If the CD/DVD auto-playback function is disabled in the Windows settings, log data cannot be collected for operations in a USB-connected CD/DVD drive or an internal CD/DVD drive.
- If an external media device is removed from the client PC, the applicable drive is considered non-existent, and as a result `Other (Collection failure)` might be output as the external media type.
- Log data for operations to or from external media is output based on the information that is received from Windows. Therefore, if the following types of information are reported from Windows, the communicated information is output as log data for operations to or from external media:
    - When USB-connected media for which serial numbers are supported is connected to the client PC, the drive name (drive letter) that was used during the previous connection is assigned to the USB-connected media. In this case, even if an operation such as drive name duplication causes a connection failure, the drive name that was used during the previous connection is reported as log data.
    - If there is a connected device such as a multi-slot memory card, to which multiple drives are assigned when they are connected, Windows reports multiple items of connection log data for each drive. However, when the same device is disconnected (removed), Windows reports disconnection log data for a single drive only.
    - When external media is connected to a client PC for the first time, a single connection might cause Windows to report multiple items of connection and disconnection (removal) log data.
    - If the client's OS is Windows Me and a USB-connected CD/DVD drive is disconnected (removed), Windows might report multiple items of disconnection log data.
    - If the client's OS is Windows XP and a USB-connected CD/DVD drive is connected with a CD/DVD in the drive, Windows might report multiple items of log data.
    - If the client's OS is Windows NT 4.0, log data for operations to or from external media is not collected. However, operation log data for a CD/DVD drive might be reported in some cases.
- If the operation of USB-connected media is suppressed, a log might not be collected from the file operations inside the USB-connected media even if operation log collection is specified.

(5) Information collected in the connection permission log and connection suppression logs for USB-connected media

The information collected in the connection permission log and connection suppression log for USB-connected media varies depending on the event that occurs. The following table shows the information that is collected.

Table 2–23: Information collected in the connection permission log and connection suppression log for USB-connected media

Event	Type	Op D/T	Frndly name	ID: DD	ID: USB	Cond	User
USB media connection permission	Y	Y	Y	Y	Y	Y	Y
USB media connection suppression	Y	Y	Y	Y	Y	N	Y

Legend:

Op D/T: Operation date/time
Frndly name: Friendly name
ID: DD: Device instance name: CD/DVD drive
ID: USB: Device instance name: USB drive
Cond: Permission condition
User: Logon user
Y: Collected
N: Not collected

- Type

  `Connection permission` or `Connection suppression`

- Operation date/time

  The date/time on which an operation was performed on USB-connected media that is permitted or not permitted to be connected is collected in the following format:

  YYYYMMDDhhmmss

- Friendly name

  Friendly name of the USB-connected media

- Device instance ID-DD

  Device instance ID in the disk drive of the USB-connected media. This device instance ID is located under the device manager's disk drive.

- Device instance ID-USB

  Device instance ID in the USB controller of the USB-connected media. This device instance ID is located under the device manager's USB controller.

- Permission condition

  The permission condition for the USB-connected media specified in an operation monitoring policy is collected in the following format:

  Permission condition: *type_match-condition_condition-string*

  Each of the collected items is explained below.

  - The following table shows the information collected as *type*.

    Table 2–24: Information collected as "type"

Type	Explanation
`DevID-DD`	Device instance ID of the disk drive
`DevID-USB`	Device instance ID of the USB controller
`FriendlyName`	Friendly name

  - The following table shows the information collected as *match-condition*.

    Table 2–25: Information collected as "match condition"

Match condition	Explanation
`Full`	Full-match

Match condition	Explanation
`Pre`	Starts-with
`Post`	Ends-with
`Middle`	Contains
`PreAndPost`	Starts and ends with

- A condition string is the string that is specified in the operation monitoring policy.

Shown below is a collection example when the device instance ID of the disk drive starts with the condition string `ABC`.

Permission condition: `DevID-DD_Pre_ABC`

- Logon user

  Name of the logon user who performed the operation on the target USB-connected media. However, if the user has not logged onto a console session in a virtual environment, no logon user name is collected.

  For a virtual environment, the logon user that will be acquired will vary depending on the logon destination.

  - When the user logged onto a console session

    User name in the console session

  - When the user did not log onto a console session

    No logon user name is collected.

Notes on collecting the connection permission and connection suppression logs for USB-connected media

In the following cases, it might not be possible to collect the connection permission and connection suppression logs for USB-connected media:

- When *type* or *operation-date-time* cannot be collected

  No connection permission or connection suppression log for the USB-connected media is collected.

- When none of the following can be collected: *friendly-name*, *device-instance-ID-DD*, *device-instance-ID-USB*, or *permission-condition*

  No connection permission log for the USB-connected media is collected.

- When none of the following can be collected: *friendly-name*, *device-instance-ID-DD*, or *device-instance-ID-USB*

  No connection suppression log for the USB-connected media is collected.

(6) Information collected in the connection, disconnection, connection permission, and connection suppression logs for devices

The information collected in the connection, disconnection, connection permission, and connection suppression logs for various devices varies depending on the event that occurs. The following table shows the information that is collected.

Table 2–26: Information collected in the connection, disconnection, connection permission, and connection suppression logs for devices

Collected item	Device connection	Device disconnection	Device connection permission	Device connection suppression
Type	Y	Y	Y	Y
Execution date/time	Y	Y	Y	Y
Device type	Y	Y	Y	Y
Drive type	Y	Y	Y	N
Drive letter	Y	Y	Y	N
Friendly name	Y	Y	Y	Y

Collected item	Device connection	Device disconnection	Device connection permission	Device connection suppression
Device instance ID by type	Y	Y	Y	Y
Device instance ID of controller	Y	Y	Y	Y
Permission condition	N	N	Y	N
User name	Y	Y	Y	Y

Legend:
Y: Collected
N: Not collected

- Type
  `Connection`, `Disconnection`, `Connection permission`, or `Connection suppression`
- Execution date/time
  The date/time on which the device was connected, disconnected, given connection permission, or prevented from connecting
- Device type
  The following table shows the information collected as *device-type*.

Table 2–27: Information collected as "device type"

Device type	Explanation
USB storage device	USB-connected storage device
Internal CD/DVD	Internal CD/DVD drive
Internal floppy disk	Internal floppy disk drive
IEEE1394	IEEE1394-connected device
Internal SD card	Internal SD card drive
Bluetooth	Internal or USB-connected Bluetooth device
Imaging device	Internal or USB-connected imaging device
Unknown	Unknown device type

- Drive type
  Drive type (`Local`, `Removable`, `CD ROM`, or `Other media`) of the device
- Drive letter
  Drive name of the device
- Friendly name
  Friendly name of the device
- Device instance ID by type
  Device instance ID under the device type (disk drive, DVD/CD-ROM, or the like)
- Device instance ID of controller
  Device instance ID under the device controller
- Permission condition
  The permission condition for the device specified in an operation monitoring policy is collected in the following format:
  Permission condition: *condition-type_match-condition_condition-string*
  Each of the collected items is explained below.
  - The following table shows the information collected as *condition-type*.

Table 2–28: Information collected as "condition type"

Condition type	Explanation
`DevID-Class`	Various types of device instance IDs
`DevID-Ctrl`	Device instance ID of the controller
`FriendlyName`	Friendly name

- The following table shows the information collected as *match-condition*.

Table 2–29: Information collected as "match condition"

Match condition	Explanation
`Full`	Full-match
`Pre`	Starts-with
`Post`	Ends-with
`Middle`	Contains
`PreAndPost`	Starts and ends with

Note: If *condition-type* is `FriendlyName`, `Full` is collected.

- A condition string is the string that is specified in the operation monitoring policy.

Shown below is a collection example when the device instance ID of the disk drive starts with the condition string `ABC`.

Permission condition: `DevID-Class_Pre_ABC`

- User name

  Name of the user who logged on to Windows

  For a virtual environment, the user name that is acquired varies depending on whether the user logged on to a console session.

  - When the user logged on to a console session

    User name in the console session

  - When the user did not log on to a console session

    No user name is collected.

Notes on collecting the device operation log

- If *device-type* is `Internal CD/DVD`, `Internal FD`, `IEEE1394`, or `Internal SD`, a device connection permission log is not collected.
- If *type* or *execution-date/time* cannot be collected, connection permission, connection suppression, connection, and disconnection logs for the device are not collected.
- When none of the following can be collected, a device connection permission log is not collected: *friendly-name*, *device-instance-ID-by-type*, *controller-device-instance-ID*.
- When none of the following can be collected, a device connection suppression log is not collected: *friendly-name*, *device-instance-ID-by-type*, or *controller-device-instance-ID*.
- For the disconnection log, it might not be possible to collect the following items depending on the timing:
  - Device type
  - Drive type
  - Drive letter
  - Friendly name
  - Device instance ID by type
  - Device instance ID of controller

- If you try to collect a connection log while the device is disconnected or suppressed, you might not be able to collect log information since the device is disconnected. In this case, *drive-type* is displayed as `Other`.
- You cannot collect log data indicating that a device was connected to, or disconnected from the client PC (Device connection or disconnection logs) before operation monitoring starts, such as immediately following the startup of the client PC. However, you can collect the device connection and disconnection logs that are recorded after operation monitoring starts.
- If *device-type* is `Internal FD`, `Drive type` is `Other`. Additionally, no drive letter is collected.
- If either of the following operations is performed in an internal CD/DVD drive or USB-connected CD/DVD drive, a connection or disconnection log might not be collected in some cases.
    - Insertion of CD or DVD media
    - Ejection of CD or DVD media
- If the OS of the client PC is Windows 8, Windows Server 2012, Windows Vista, Windows Server 2008, or Windows 7, an operation log cannot be collected from an internal CD/DVD drive or USB-connected CD/DVD drive.
- If an floppy disk or SD card is inserted, a connection or disconnection log is not collected.
- If a device for which multiple device instance IDs are set is connected, multiple operation logs are collected from the single device. However, only a single disconnection log is collected.
- When a device is connected to the client PC for the first time, a device driver might be installed. When this occurs, multiple operation logs might be collected.
- Even when it is necessary to restart the client PC in order to enable an operation monitoring policy for suppressing operations, an operation suppression log is collected when the operation monitoring policy is set.
- Even when a product other than JP1/Software Distribution changes the device setting and device connection, or when disconnection is detected, a device operation log is collected.
- You cannot collect operation logs from devices that cannot be recognized as USB storage devices, Bluetooth devices, or imaging devices even when they are USB-connected.
- If a CD/DVD drive with a CD or DVD already inserted is connected to the client PC, multiple connection logs might be collected in some cases.
- If the client PC is restarted in order to enable an operation monitoring policy for suppressing operation, a device disconnection log might not be collected.
- If you specify an operation monitoring policy that suppresses the operation of a device that is already connected, the suppression log for that device might be collected when you connect a different device to the client PC.

(7) Data collected in a file operation log

A file operation event occurs when one of the operations listed below is performed on a file or folder. For details about the information to be collected, see *6.5.3 Items displayed in an operation log* in the manual *Administrator's Guide Volume 1*.

- Copying
- Migration
- Renaming
- Deletion
- Creation
- File opening

Data collected in a file operation log differs depending on the operation that is performed. The following types of data are collected.

Table 2–30: Data collected in a file operation log

Operation	Time	Type	Logon user	Drive type	File name	Drive type after change	File name after change	Program name	Account
Copying	Y	Y	Y	Y	Y	Y	Y	Y	Y
Migration	Y	Y	Y	Y	Y	Y	Y	Y	Y
Renaming	Y	Y	Y	Y	Y	--	Y	Y	Y
Deletion	Y	Y	Y	Y	Y	--	--	Y	Y
Creation	Y	Y	Y	Y	Y	--	--	Y	Y
File opening#	Y	Y	Y	Y	Y	--	--	Y	Y

Legend:
Y: Collected.
--: Not collected.

#: If the OS of the client PC is one of the following, a log for file opening operation cannot be collected.

- Windows 8
- Windows Server 2012
- Windows 7
- Windows Server 2008
- Windows Vista

(a) Notes on collecting file operation log data

Note the following when collecting file operation log data:

- When a folder is copied, moved, or deleted, log data is also collected for all files and subfolders that are under that folder.
  When a folder name is changed, the path to the files and folders under that folder is changed. However, no log data is collected.
- After a file or folder operation, if an Undo operation is performed by using the **Undo** menu or by pressing the **Ctrl** + **Z** keys, the following operation log data is collected:

Operation before Undo	Operation log data collected during the Undo operation
Copying	Deletion of the copied file or folder
Migration	Return of the moved file or folder to its original location
Renaming	Name change back to the original file name or folder name
Deletion	Moving of the deleted file or folder to its original location

- If you cancel a copy operation in the dialog box for confirming overwriting, the following occurs: If the update date of the copy-source file is the same as the update date of a file having the same name in the copy-destination folder, log data is collected, assuming the latter file to be a copy.
- When you consecutively copy the same file or folder, a log might be collected for creation operations instead of copying operations.
- When you move a file or folder to Windows Recycle Bin, log data is collected assuming that the file or folder has been deleted rather than having been moved.
- When you delete a file or folder from Windows Recycle Bin, the file name or folder name collected in the log data might differ from the name before deletion.
- If you select multiple files, file deletion log data might not be collected in some cases.

- Collection of operation log data for compressed (zip format) folders is not supported. However, log data might be collected for some operations.
- If the move-destination file is overwritten during a file move, or if a file move is undone, log data indicating the deletion of the move-source file might be collected in addition to log data indicating a file move.
- If a large number of files or folders are overwritten during a copying operation, log data might not be collected in some cases.
- If an operation monitoring policy that specifies to suppress operations on USB media is applied, history for operations performed on the USB media files may not be acquired.
- Immediately following the start of operation monitoring, you might not be able to acquire some of the file operations, or the output might be invalid. In either of these cases, perform a restart or logoff at the client. For the operation for starting operation monitoring, see *6. Monitoring Software Operation Status* in the manual *Administrator's Guide Volume 1*.
- When multiple users are performing file operations in a virtual environment, if a user manipulates a file, it is considered that all users who are displaying that same file in Windows Explorer have performed the same operation, and logs are collected accordingly.

(b) Notes on collecting file operation log data from a client whose OS is Windows 8, Windows Server 2012, Windows 7, Windows Server 2008 or Windows Vista

When you collect file operation log data from a client whose OS is Windows 8, Windows Server 2012, Windows 7, Windows Server 2008 or Windows Vista, note the following points in addition to those described under (a):

- If a file or folder is manipulated from an application or from the command prompt on a client whose OS is Windows 8, Windows Server 2012, Windows 7, Windows Server 2008 or Windows Vista, log data might be collected for some of the operations.
- Collection of operation log data for file restoration from a shadow copy or backup is not supported. However, log data might be collected for some of the operations.
- If you use Remote Installation Manager or Asset Information Manager Subset to view a file operation log collected from a client whose OS is Windows 8, Windows Server 2012, Windows 7, Windows Server 2008 or Windows Vista, use JP1/Software Distribution Manager version 08-51 or later. JP1/Software Distribution Manager of Version 08-10 or earlier might not display the log data correctly.
- If the file operation log collection facility is being used, the memory usage by `smcusapp.exe` might continue to be large, but this will not affect the operation.
- If files or folders were restored by the File History feature of Windows 8, some file operation logs on them might be collected.

Note the following points on each type of operation for which log data can be collected.

Notes on collecting copy operation log data

- When a file is overwritten by a copy operation, if you choose **Copy, but keep both files** in the Confirm File Replace dialog box, note the following points:
  - Log data is collected in which the file name after the copying operation is *pre-copy-file-name* (*n*) (where *n* is an arbitrary number).
  - If the copy-source file is deleted after the copying operation, extra log data for a file move might be output.
  - If the copy-source file and the file to be overwritten have the same update date/time, extra copy log data is output in which the pre-copy and post-copy file names are the same.
- If the dialog box for confirming a file overwrite is displayed multiple times for a single copy operation, extra folder or file copy log data might be output.
- If a file or folder whose name contains parentheses (( )) is copied, log data might not be correctly collected.
- When multiple files or folders whose name contains (*n*) (where *n* is an arbitrary number) are selected and overwritten during a copying operation, if you choose **Copy, but keep both files** in the Confirm File Replace dialog box, log data might not be correctly collected.
- When files or folders whose name contains (*n*) (where *n* is an arbitrary number) are continuously copied, log data is collected indicating a file or folder creation for the second or subsequent copy operations.

- Following an Undo operation, if you perform a Redo operation in the **Redo Copy** menu or by using the **Ctrl** + **Y** keys, no file operation log data is output. For a Redo operation on a folder, log data is collected indicating a folder copy operation.
- If multiple files or folders, or a folder containing multiple files or folders are selected and copied, log data might not be collected in some cases.

Notes on collecting move operation log data

- When a file is overwritten by a move operation, if you choose **Move, but keep both files** in the Move File dialog box, log data is collected in which the file name after the move operation is *pre-move-file-name* (*n*) (where *n* is an arbitrary number). Additionally, extra move log data is output in which the pre-move and post-move file names are the same.
- When multiple files or folders whose name contains (*n*) (where *n* is an arbitrary number) are selected and moved, if you choose **Move, but keep both files** in the Confirm File Replace dialog box, log data might not be correctly collected.
- If a file is overwritten by a move operation, note the following points when you consolidate folders by clicking the **Yes** button in the Confirm File Replace dialog box:
    - If the move-source and move-destination folders contain files that have the same name, only the file is moved during folder consolidation, and the move-source folder is not deleted. In this case, copy log data is collected for the move-source folder.
    - When **Move and replace** is selected during file replacement confirmation, if the move-source file and the file to be overwritten have the same update date/time, file copy and deletion log data is collected instead of file move log data.
    - If **Move, but keep both files** is selected during file replacement confirmation, log data is collected in which the file name after the move operation is *pre-move-file-name* (*n*) (where *n* is an arbitrary number). If the pre-move file and the file to be overwritten have the same update date/time, file copy and deletion log data is collected in addition to file move log data. If the pre-move file and the file to be overwritten have different update dates/times, extra move log data is output in which the pre-move and post-move file names are the same.
- If the folder replacement confirmation dialog box is displayed multiple times for a single move operation, extra folder and file move log data might be collected.
- If a file whose name contains parentheses (( )) is moved, log data might not be correctly collected.
- If an Undo operation is performed following a file move, log data is collected for the movement of the file back to its original location and a file deletion. If an Undo operation is performed on a folder move, only folder move log data is collected. If a file or folder is overwritten during a move and then an Undo operation is performed, log data is output only for the deletion of the overwritten file. Following an Undo operation, if you perform a Redo operation in the **Redo Move** menu or using the **Ctrl** + **Y** keys, file deletion log data is collected. If a Redo operation is performed on a folder, folder move log data is collected.
- If an Undo operation is performed following a file move to Windows **Recycle Bin**, log data is collected for file deletions from **Recycle Bin** and for file creation at the restoration destination. In this case, a correct file name is not collected in the log data for file deletions from **Recycle Bin**.
- If multiple files or folders, or a folder containing multiple files or folders are selected and moved, log data might not be collected in some cases.

Notes on collecting name change operation log data

- If a file is overwritten by a name change operation, note the following points when you consolidate folders by clicking the **Yes** button in the Confirm File Replace dialog box:
    - If a folder before a name change contains several files, log data is output for file creation at the consolidation-destination folder and for file deletion prior to the name change. However, no log data is collected for the deletion of the pre-name-change folder. If a folder before a name change does not contain any file, log data is output only for the creation of a subfolder of the folder following the name change.
    - If a folder before a name change and the consolidation-destination folder contain subfolders that have the same name, subfolder creation log data is collected. In this case, no log data is collected for the deletion of the pre-name-change folder.
    - If a folder before a name change contains multiple files or subfolders, some log data might not be collected.

  - Log data might not be collected for the files that exist inside a subfolder of the pre-name-change folder.
- If multiple files or folders, or a folder containing multiple files or folders are selected and a batch name change operation is performed, log data might not be collected in some cases.

Notes on collecting deletion operation log data

- Following file deletion, if you perform an Undo operation or select the **Undo** menu, log data is collected for the file re-creation at the restoration destination and for file deletion from Windows **Recycle Bin**. However, a correct file name is not collected in the log for file deletion from Windows **Recycle Bin**.
- Following file deletion, if you move the file from Windows **Recycle Bin**, log data is collected for the movement of the deleted file to its original location.
- After multiple files or folders, or a folder containing multiple files or folders were selected and deleted, if you perform an Undo operation or select the **Undo** menu, or if you move the folder from Windows **Recycle Bin**, log data might not be collected in some cases.
- Following a file copy or move, if you delete the file within a certain amount of time and then perform an Undo operation, log data might be collected only for the file deletion from Windows **Recycle Bin**.

When you move a large number of files or folders, if you select **Move and replace** or **Move, but keep both files** during file replacement confirmation, file copy-and-deletion log data or file copy log data might be collected, instead of file move log data.

(8) Specifying the software operation history storage directory

Although a log's actual size is affected by the event data collected, operation logs tend to be large. Therefore, when you install JP1/Software Distribution Manager, you need to specify a drive with ample capacity for the directory that stores the operation history (software operation history storage directory).

When the size of the operation history stored in the software operation history storage directory exceeds a specified value, you can also save the operation history in another directory (operation history backup directory).

The drive containing the software operation history storage directory and operation history backup directory can be a local drive (including a shared disk in a cluster environment), but can also be a network drive, such as Windows Powered NAS. We recommend that you specify a local drive with ample capacity for the software operation history storage directory, which is frequently accessed, and a network drive for the operation history backup directory, which is accessed less frequently.

However, to specify a network drive, you need an environment in which a single piece of authentication information can be used to connect to the network drive. Provide authentication information (user ID and password) that has all of the following permissions:

- Permissions that allow login to the JP1/Software Distribution server and the domain group, as well as writing of data into a backup file storage directory
- Permissions that allow writing of data into the software operation history storage directory
- Permissions that allow writing of data into the operation history backup directory
- Permissions that allow writing of data into the network drive

We also recommend that, for the network drive, you specify a drive in the same domain or workgroup as the machine on which JP1/Software Distribution Manager is installed. If you specify any other drive, authentication might take a long time.

2.5.9 Collecting software operation time

You can collect the daily operation time for software executed on a client and report this information to the managing server as a monitoring result.

Once you have collected operation times, you can use the Software Operation Status window of Asset Information Manager Subset to check the operation rate for each software application. Such information is useful for locating and removing software that is used infrequently, for recommending use of certain software, and for other purposes.

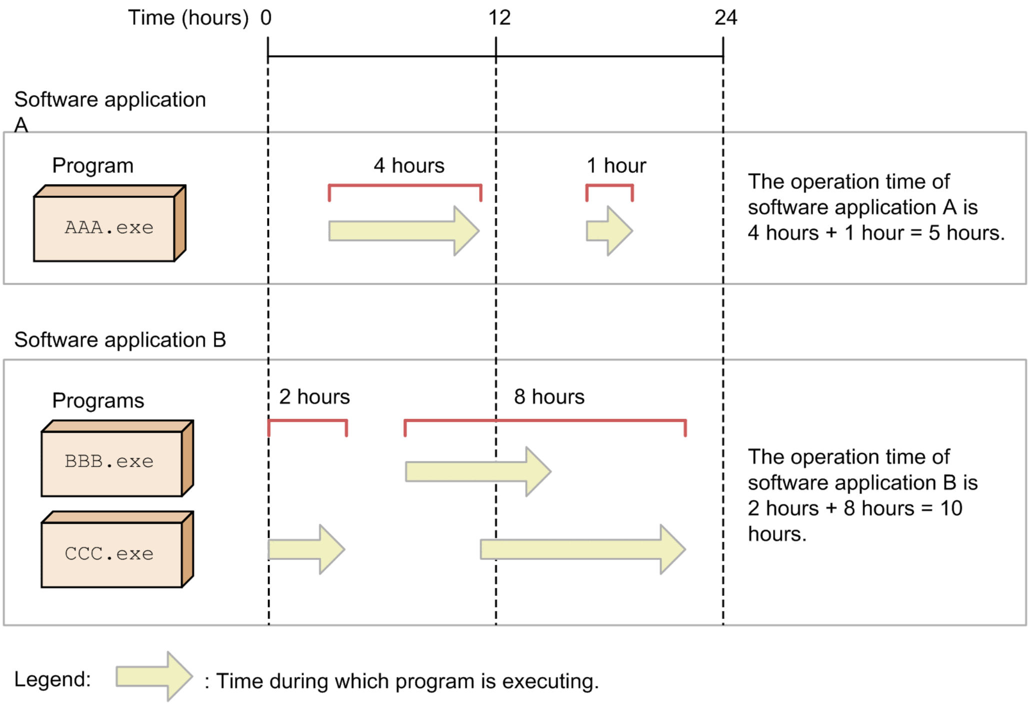
To collect operation times, you must specify the software applications to be monitored (monitoring target software) in the operation monitoring policy.

To collect the operation time for a software application, specify the program whose operation time you want to monitor. You can specify applications that have one of the following extensions as the software programs for which operation time is to be collected:

- `.exe`
- `.com`
- `.scr`

You can specify more than one program for a single software application. When you specify more than one program, the execution times of all those programs are acquired as the operation time for that software application. The following figure shows the relationship between the program execution times and the software operation time that is acquired.

Figure 2–26: Relationship between program execution times and the software operation time that is acquired


Time (hours)
0
12
24
Software application A
Program
AAA.exe
4 hours
1 hour
The operation time of software application A is 4 hours + 1 hour = 5 hours.
Software application B
Programs
BBB.exe
CCC.exe
2 hours
8 hours
The operation time of software application B is 2 hours + 8 hours = 10 hours.
Legend:
: Time during which program is executing.

Software operation time is totaled from 12:00 midnight (00:00) of the current day to 12:00 midnight (00:00) of the following day. Totaling of data for the following day begins at 12:00 midnight. Thus, the 12:00 midnight (00:00) operation time is included in both the current day and the following day.

If a date change occurs while a program is executing, the operation time until 00:00 is collected as the current day's data, and the operation time from 00:00 is collected as the following day's data. For the latter day, the data collected until 00:00 is then reported to the managing server as the previous day's operation time.

The following points should be noted about collecting software operation times:

- If suppression of software startup is specified in the operation monitoring policy, the operation times of the software applications whose startup is suppressed cannot be collected.
- Operation time is calculated based on the system time. This means that collected operation time might be incorrect if the system time is changed after collection of operation times has begun. If the operation time is a minus number, 0 hours is assumed to be the operation time.
- If the process that performs operation status monitoring is unable to determine the time a program terminated due to a machine failure or for some other reason, the operation time of that program is not collected.
- For a virtual environment, operation time is also collected for each software application. Operation time cannot be collected for each user who logged onto the virtual environment.

The operation time collected when multiple users concurrently perform operations on the same software application is the same as the operation time collected when the same user performs operations on multiple programs that are set in the software application.

For the notes on specifying a software application that collects operation time in an operation monitoring policy, see *6.2.7 Setup for obtaining the operation time* in the manual *Administrator's Guide Volume 1*.

2.5.10 Guidelines for the number of days to save operation information

Assuming one user per client, the amount of operation information generated in one day amounts to approximately 1,800 data items. A large amount of software operation information might overload the system. We recommend that you avoid overloading the system by taking appropriate measures, such as limiting the operation information items to be acquired, and adjusting the number of clients that are subject to information collection.

As a guideline for achieving system operation without overloading the system, you should use the operation monitoring facility within the scope determined by the following formula:

$n \mathbf{x}\ 1{,}800\ \mathbf{x}\ m\ \mathbf{x}\ x < 5{,}000{,}000$

n: Number of clients

m: Number of days operation log data is retained.

x: Coefficient of operation log data to be acquired.

Specify the total of the following values for the items you intend to acquire:

- `Start process`: 0.14
- `Stop process`: 0.14
- `Change caption`: 0.25
- `Change active window`: 0.25
- `File operations`: 0.08
- `Web access log`: 0.14

For the following operations, you need not calculate the log volume since the size of the logs collected is small.

- Machine startup/stop
- Logon/logoff
- Software startup suppression
- Print operation
- Print suppression
- Print suppression release
- External media operation
- Device operation
- USB media connection permission
- USB media connection suppression
- Device connection permission
- Device connection suppression

The following examples show the calculations assuming that all operation log data is acquired.

Determining the number of days operation log data can be retained for a medium-sized system consisting of 2,500 clients:

2,500 clients **x** 1,800 **x** m **x** 1 < 5,000,000

m = approximately 1 day

Determining the number of clients if operation information is to be retained for 5 days:

n **x** 1,800 **x** 5 **x** 1 < 5,000,000

n = approximately 500 clients

In this calculation example, 5,000,000 represents an estimated amount of data (number of log entries) that can be stored in the database for JP1/Software Distribution Manager. For the amount of Web access log data (number of log entries), it is assumed that 200 Web access log entries are generated per day using the filtering function for Web access log data.

2.5.11 Monitoring the operation status in a large-scale system

When monitoring client operation statuses in a large-scale system that uses relay managers, you can specify operation information management methods in detail. For instance, you can specify the method for managing the operation information of the clients under each relay manager, and the method for using the central manager to manage the operation information of the clients under multiple relay managers.

The following are examples of operation information management methods for monitoring the operation status in a large-scale system.

- Having the central manager centrally manage the operation information of the entire system

  When an operation monitoring policy is applied from a relay manager to a client, operation information reported by a lower system to the relay manager is not reported to the central manager in the default mode. If a relay manager is installed in each group and an operation monitoring policy is applied by each relay manager to its subordinate clients, the central manager cannot manage the operation information in each group.

  To enable the central manager to centrally manage the operation status of the entire system, set up the relay managers so that they report the received operation information to the central manager as well. Such a setup will enable the central manager to manage all operation information.

  For details about the items to set for the central manager and relay managers, see *4.2.14 Operation Monitoring page* and *4.3.2 Report To Higher System page* in the *Setup Guide*.

- Having each relay manager manage operation information

  If an operation monitoring policy is applied from the central manager to all clients, the operation information of all clients is reported to the central manager. In such an environment, if the volume of client operation information becomes very large, a disk capacity shortage might occur in the central manager, negatively impacting the system.

  To divide the operation information among the individual relay managers and manage it separately, set up the relay managers so that they will not report the operation information they receive to a higher system. Also, set up the relay managers so that they save the operation information that is reported to them.

  With such a setup, each relay manager manages the operation information of its subordinate clients, thus preventing a disk capacity shortage from occurring in the central manager.

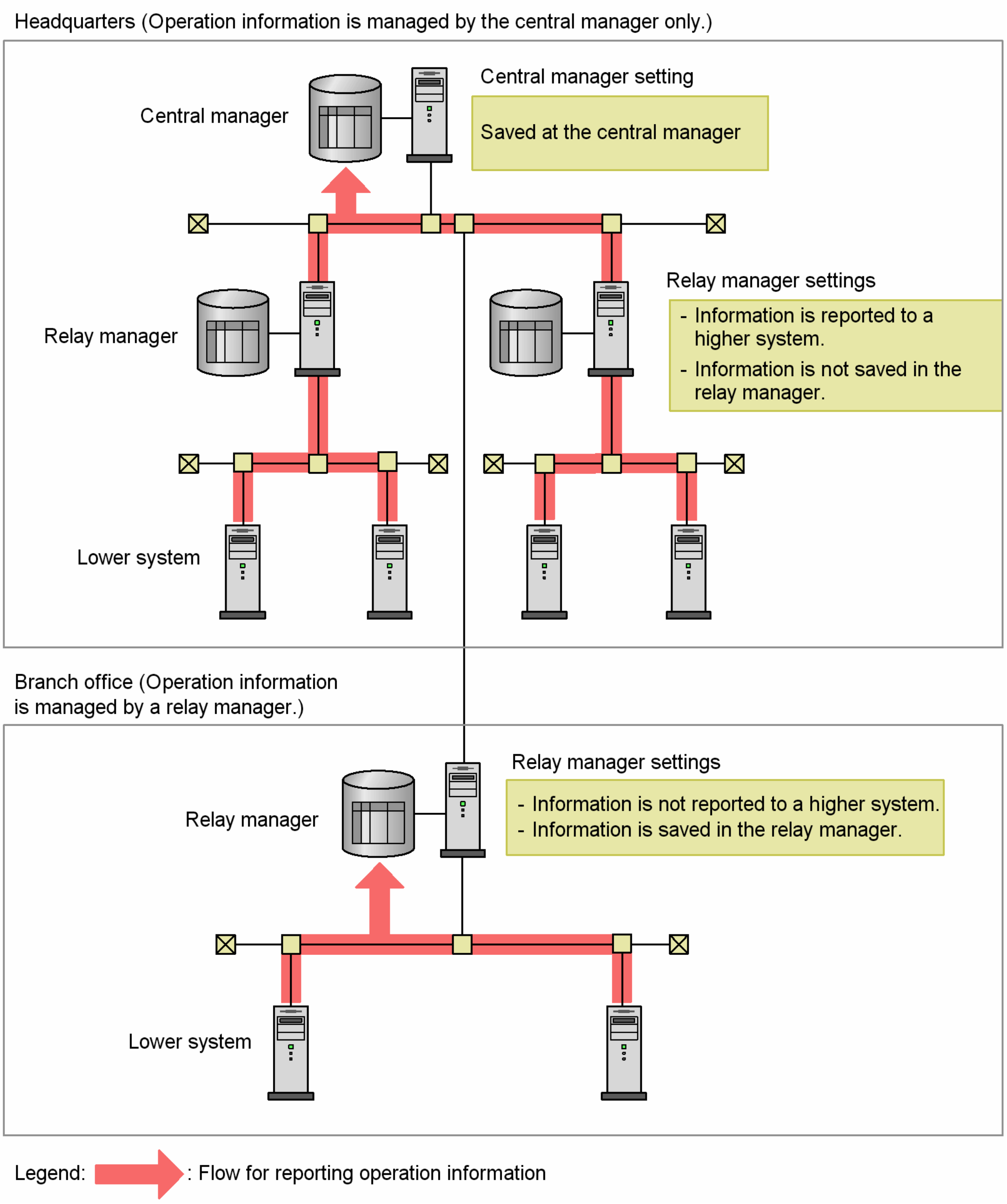
- Having the central manager and relay managers share an operation monitoring policy

  The central manager and relay managers can output a created operation monitoring policy to a file. By loading the output file, an operation monitoring policy can be created from the file. This operation mode is convenient when it is necessary to have multiple relay managers share a policy, or to customize an already-created operation monitoring policy on a different computer.

  For details on how to share an operation monitoring policy, see *6.9 Sharing operation monitoring policies* in the manual *Administrator's Guide Volume 1*.

Using an example in which the central manager manages the operation status of lower systems at the company headquarters while relay managers manage the operation status of lower systems at branch offices, the following figure shows how to manage operation information when the operation status of a large-scale system is to be monitored.

Figure 2–27: Managing operation information in a large-scale system


Headquarters (Operation information is managed by the central manager only.)
Central manager
Central manager setting
Saved at the central manager
Relay manager
Relay manager settings
- Information is reported to a higher system.
- Information is not saved in the relay manager.
Lower system
Branch office (Operation information is managed by a relay manager.)
Relay manager
Relay manager settings
- Information is not reported to a higher system.
- Information is saved in the relay manager.
Lower system
Legend:
: Flow for reporting operation information

2.5.12 Monitoring the operation status of stand-alone PCs

You can acquire operation information from clients that are not connected on the network (offline machines), in addition to the operation information you collect from networked clients. To acquire operation information from offline machines, you can use media such as floppy disks, CD-R discs, MO (magneto-optical) discs, or you can even email the information.

To acquire operation information from offline machines, the JP1/Software Distribution system must satisfy the following conditions:

Managing server

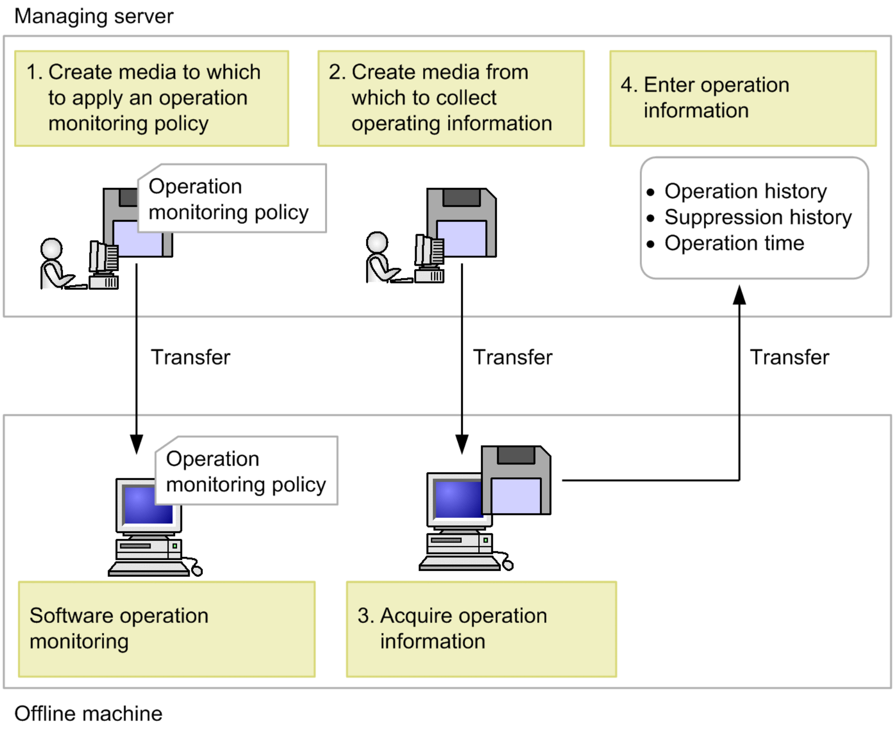
- JP1/Software Distribution Manager 09-00 or later (relational database edition) for Windows must be installed.
- Remote Installation Manager must be used on the same PC on which the above JP1/Software Distribution Manager is installed.

Offline machine

JP1/Software Distribution Client 09-00 or later for Windows must be installed.

The following figure shows the general procedure for acquiring operation information from an offline machine.

Figure 2–28: Acquiring operation information from an offline machine


Managing server
1. Create media to which to apply an operation monitoring policy
2. Create media from which to collect operating information
4. Enter operation information
Operation monitoring policy
• Operation history
• Suppression history
• Operation time
Transfer
Transfer
Transfer
Operation monitoring policy
Software operation monitoring
3. Acquire operation information
Offline machine

1. Create the media for applying the operation monitoring policy.
   In this step, you create the media for applying the operation monitoring policy. The operation monitoring policy is then applied to the offline machine from the media that you created.
2. Create media for acquiring operation information.
   In this step, you create the media for acquiring the operation information.
3. Acquire the operation information from the offline machine.
   In this step, you copy the operation information from the offline machine onto the media.
4. Enter the operation information onto the managing server.
   In this step, you enter the offline machine's operation information from the media to the managing server.

In addition to operation information, you can also acquire inventory information from offline machines. You use the same method to acquire each type of information.

For details about how to acquire inventory information and operation information from offline machines, see *7.7.2 Collecting inventory and operation information from offline machines* in the manual *Administrator's Guide Volume 1*.

2.6 Managing software operation information

Three windows are provided for managing the software operation information acquired from clients. The windows are listed below, with a brief description of the functionality available in each:

Operation Log List window

This window enables you to search suppression and operation log data, as well as to trace the operation history of specific files.

Operation Log Total window

This window enables you to check suppression and operation log totals for each search pattern that is specified in the Operation Log List window. Note that you must have first used the appropriate command to acquire totals.

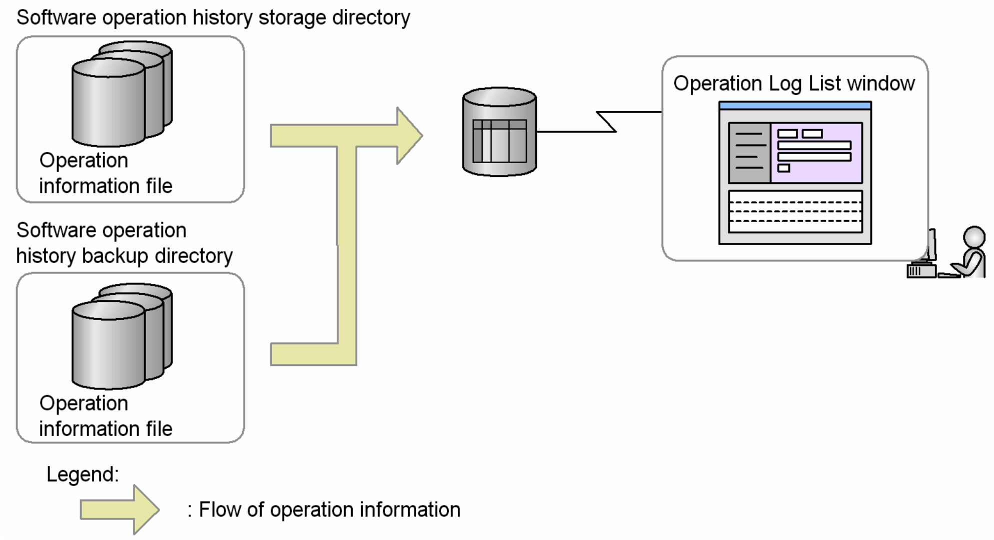
Software Operation Status window

This window enables you to check, for each software program, the software usage time and the number of copies that are being used in relation to a client's operation time.

To manage operation information in these windows, the operation information must be stored in a dedicated database. Storage of operation information in this database can either be configured at setup to be performed automatically or it can performed when needed by executing a command.

The following figure shows the framework for managing operation information, using the Operation Log List window as an example.

Figure 2–29: Framework for managing operation information (Operation Log List window)


Software operation history storage directory
Operation information file
Software operation history backup directory
Operation information file
Operation Log List window
Legend:
: Flow of operation information

The following subsections provide an overview of managing operation information using the Operation Log List window, Operation Log Total window, and the Software Operation Status window.

2.6.1 Preparations for managing operation logs

This subsection describes the preparations necessary for using the Operation Log List window, the Operation Log Total window, and the Software Operation Status window to manage operation logs acquired by JP1/Software Distribution.

(1) System configuration

To use any of these windows, the Asset Information Manager Subset component must be installed. The following table lists the programs required to use the Asset Information Manager Subset component, as well as the programs required to use the windows for managing operation information.

Table 2–31: Programs required to manage operation information

System configuration element	Required program
PC on which Asset Information Manager Subset is installed	Microsoft Internet Information Services 5.0, 5.1, 6.0, or 7.0
PC on which the Operation Log List window, Operation Log Total window, and Software Operation Status window are being used	Microsoft Internet Explorer 6.0 (Service Pack 2) or later

For details about the system configuration required for using Asset Information Manager Subset, see *5.2.1 System configuration in an environment where Asset Information Manager Subset is used*.

(2) Setup

To manage operation information in these windows, the following settings must be configured during managing server setup:

- Setting the timing for storing operation information in the database table

  If you want to automatically store operation information in JP1/Software Distribution's relational database, on the **Operation Monitoring** page in the setup, select both the **Save the operation monitoring history** and **Enable automatic storage** check boxes. When you execute a command, you can store operation information in the database regardless of these settings.

  Furthermore, when a virtual environment is being used, clear the **Enable automatic storage** check box. Execute the `dcmmonrst` command to back up the operation information to the operation history backup directory.
- The URL for Asset Information Manager Subset

  The URL for activating the windows from Remote Installation Manager must be set.

For details about the setup, see *4.2.14 Operation Monitoring page* and *4.2.19 AIM page* in the *Setup Guide*. For details about the `dcmmonrst` command, see *4.13 dcmmonrst.exe (storing operating information in a database)* in the manual *Administrator's Guide Volume 2*.

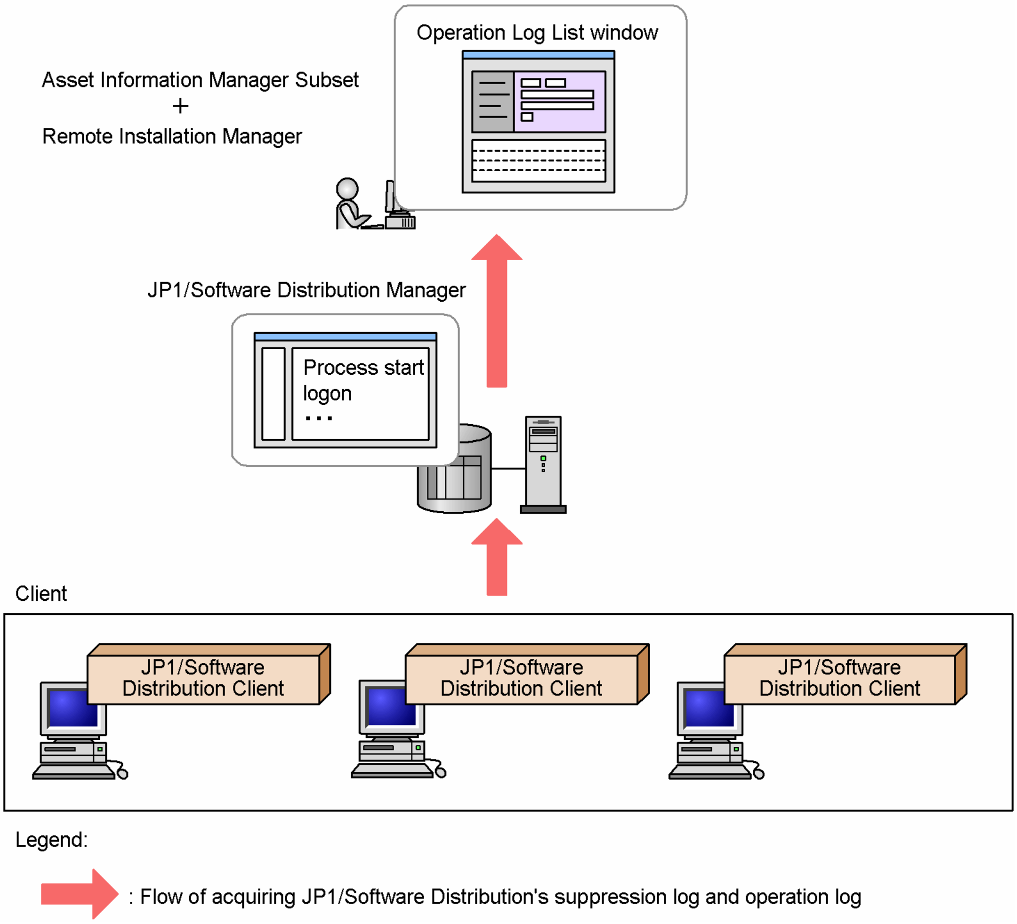
2.6.2 Viewing and tracing operation log data

In the Operation Log List window, you can search the suppression and operation log data acquired by JP1/Software Distribution and display only specific information. The data that can be managed in the Operation Log List window is called the *operation log* data. By using the Operation Log List window, you can integrate the management of operation log data throughout the entire system.

You can start the Operation Log List window if Asset Information Manager Subset (one of the JP1/Software Distribution Manager components) and Remote Installation Manager have been installed, or JP1/Asset Information Manager 08-00 or later is linked.

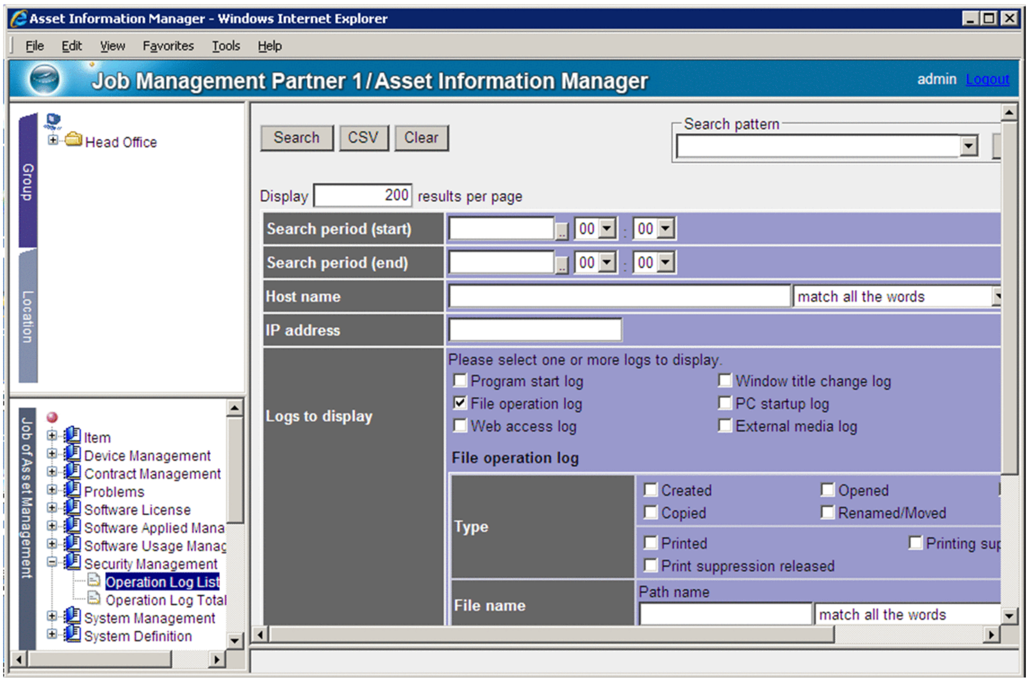
The following figure shows the concept of managing operation log data in the Operation Log List window.

Figure 2–30: Managing operation log data in the Operation Log List window


Operation Log List window
Asset Information Manager Subset
+
Remote Installation Manager
JP1/Software Distribution Manager
Process start
logon
・・・
Client
JP1/Software Distribution Client
JP1/Software Distribution Client
JP1/Software Distribution Client
Legend:
: Flow of acquiring JP1/Software Distribution's suppression log and operation log

You can start the Operation Log List window, shown in the following figure, from Remote Installation Manager.

Figure 2–31: Operation Log List window



Search pattern

Display 200 results per page

Search period (start) 00 : 00

Search period (end) 00 : 00

Host name match all the words

IP address

Logs to display: Please select one or more logs to display.

□ Program start log
□ Window title change log
☑ File operation log
□ PC startup log
□ Web access log
□ External media log

File operation log

Type:
□ Created
□ Opened
□ Copied
□ Renamed/Moved
□ Printed
□ Printing sup
□ Print suppression released

File name: Path name match all the words

For details about how to use the Operation Log List window, see *6.6 Using the Operation Log List window* in the manual *Administrator's Guide Volume 1*.

(1) Functions of the Operation Log List window

The following two functions are available in the Operation Log List window:

- Searching operation log data
- Tracing user operations

The following subsections explain these functions.

(a) Searching operation log data

You can use the following search functions in the Operation Log List window:

- Searching the operation log data acquired during a specific period
- Searching the operation log data by host name or IP address
- Searching the operation log data by type

You can also select a search pattern provided by JP1/Software Distribution and set the operation log search conditions in batch mode.

Using the above search functions, you can manage the following operation log data from the Operation Log List window:

- **Program start log**
  Log data on starting, stopping, and suppressing the programs being used
- **Window title change log**
  Titles of viewed Web sites
- **File operation log**
  Log data on creating, opening, deleting, copying, changing the name of, moving, and printing of folders and files
- **PC startup log**
  Log data related to the PC: starting, terminating, logging on, and logging off.
- **Web access log**
  Log data on Microsoft Internet Explorer accesses.
- **External media log**
  Log data on connecting or disconnecting a USB storage device, internal CD/DVD drive, etc.
  Log data on operations that permit or suppress connection to a USB storage device, internal CD/DVD drive, etc.

(b) Tracing user operations

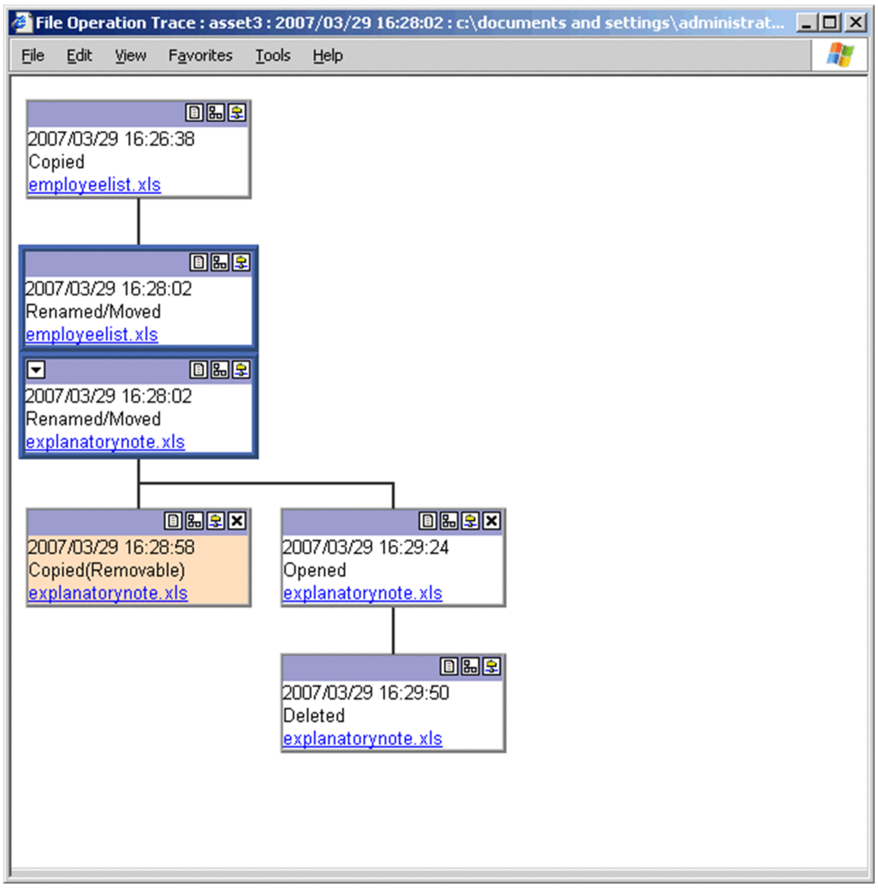
If you click the file name displayed in an operation log entry in the Operation Log List window, the File Operation Trace window opens.

In the File Operation Trace window, you can trace the user operations performed on the selected file based on its associated operation log data. If there is operation log data whose date and time is more recent than the operation log data displayed for the selected file, you can also trace subsequent operations on that file.

If you discover from operation log data that a confidential file was copied to a different location, you can determine the details of the unauthorized operation by tracing back to the user who copied the file as well as the route traversed by the copied file.

The following figure shows the File Operation Trace window.

Figure 2–32: File Operation Trace window


File Operation Trace : asset3 : 2007/03/29 16:28:02 : c:\documents and settings\administrat...
File Edit View Favorites Tools Help

2007/03/29 16:26:38
Copied
employeelist.xls

2007/03/29 16:28:02
Renamed/Moved
employeelist.xls

2007/03/29 16:28:02
Renamed/Moved
explanatorynote.xls

2007/03/29 16:28:58
Copied(Removable)
explanatorynote.xls

2007/03/29 16:29:24
Opened
explanatorynote.xls

2007/03/29 16:29:50
Deleted
explanatorynote.xls

For details about how to perform operations in the File Operation Trace window, see *6.6.4 Tracing operation logs* in the manual *Administrator's Guide Volume 1*.

2.6.3 Totaling operation log data

By totaling operation log data, you can check how many times a certain operation was executed in one day, and identify trends in the operation log data. For example, by totaling the number of times copy operations to removable disks were performed, you can identify clients where information is frequently copied to external media.

You use the `jamOperationLogAddUp.exe` command to total operation log data. You can also check the totals of operation log data in the Operation Log Total window. In order to use this window to check totals, you must first have executed the command and completed the totaling operation.

You can display the Operation Log Total window if the Asset Information Manager Subset and Remote Installation Manager components of JP1/Software Distribution Manager are installed, or if JP1/Software Distribution is linked to JP1/Asset Information Manager version 08-10 or later.

With Asset Information Manager Subset, you can assign clients to groups. Setting groups for clients enables you to check totals by group.

For details about how to total operation log data and how to perform operations in the Operation Log Total window, see *6.7 Using the Operation Log Total window* in the manual *Administrator's Guide Volume 1*.

(1) Prerequisites for totaling operation log data

Only operation log data displayed in the Operation Log List window is totaled.

This means that, before operation logs can be totaled, operation information must be stored in a dedicated database.

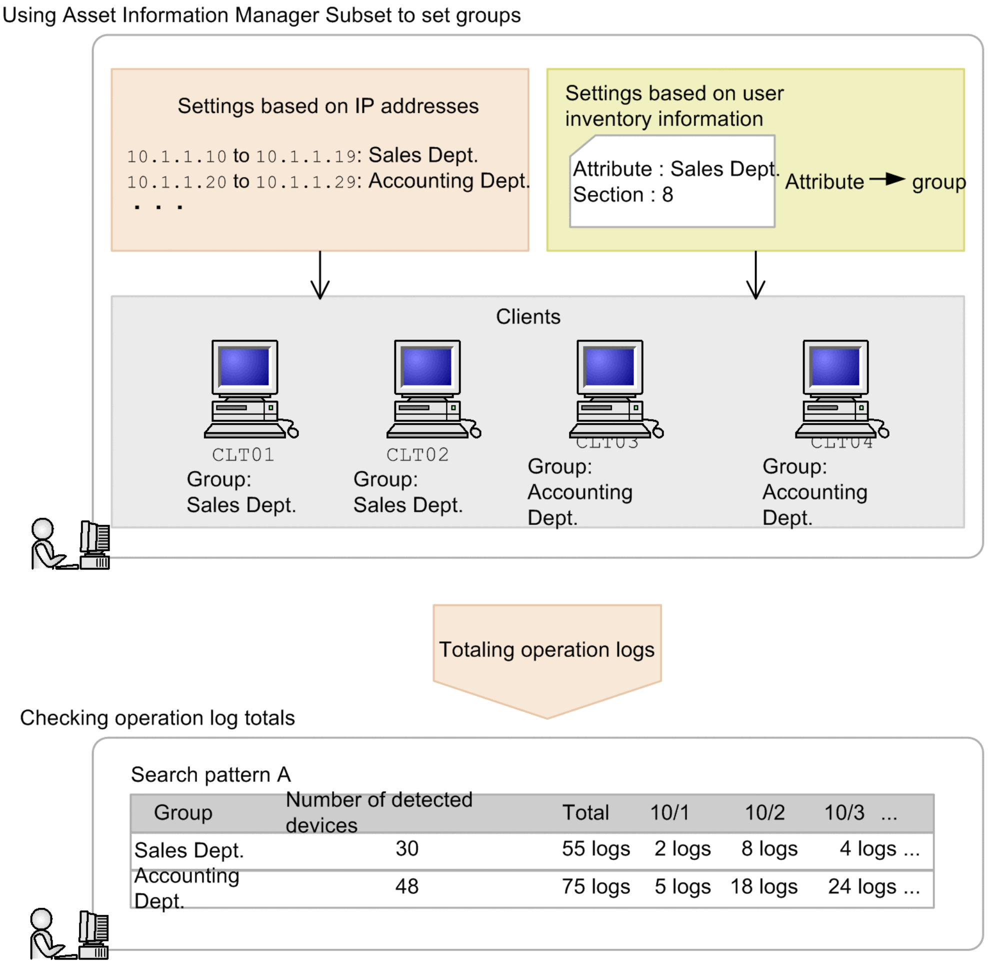
(2) Setting groups

Setting clients into groups before you total the operation log data enables you to check totals by group.

You set groups from Asset Information Manager Subset. The groups to which a client is to be assigned can be set automatically based on the client's IP address or user inventory information.

The following figure shows the concept of totaling operation log data by setting groups.

Figure 2–33: Totaling operation log data when groups are set


Using Asset Information Manager Subset to set groups
Settings based on IP addresses
10.1.1.10 to 10.1.1.19: Sales Dept.
10.1.1.20 to 10.1.1.29: Accounting Dept.
. . .
Settings based on user inventory information
Attribute : Sales Dept.
Section : 8
Attribute → group
Clients
CLT01
Group:
Sales Dept.
CLT02
Group:
Sales Dept.
CLT03
Group:
Accounting Dept.
CLT04
Group:
Accounting Dept.
Totaling operation logs
Checking operation log totals
Search pattern A

Group	Number of detected devices	Total	10/1	10/2	10/3 ...
Sales Dept.	30	55 logs	2 logs	8 logs	4 logs ...
Accounting Dept.	48	75 logs	5 logs	18 logs	24 logs ...

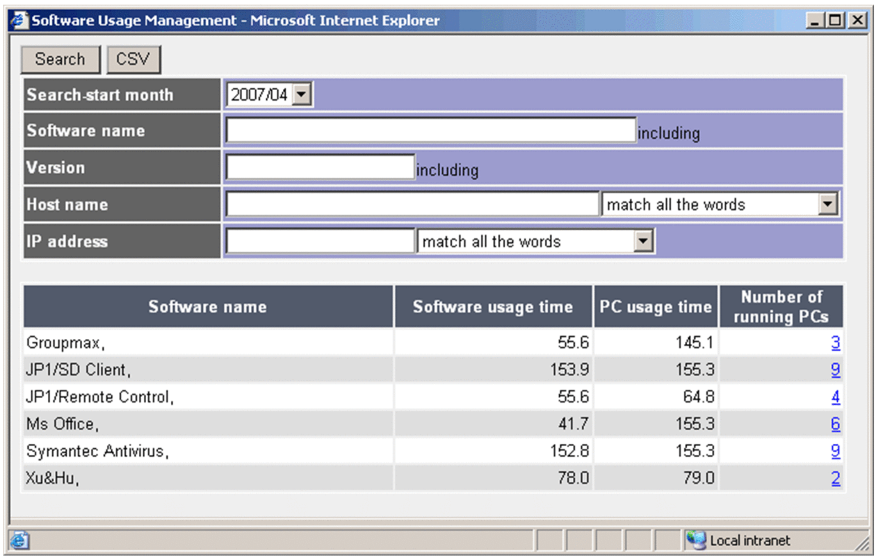
For details about how to set groups, see *10.8 Setting for summing the operation logs by group* in the *Setup Guide*.

2.6.4 Viewing software operation status

In the Software Operation Status window, you can total software operation times and operation rates by month, based on the operation times collected from the clients. From this information, you can determine how long a software application is being used and how much the operation rate varies from month to month.

The following figure shows the Software Operation Status window.

Figure 2–34: Software Operation Status window



Search start month	2007/04
Software name	including
Version	including
Host name	match all the words
IP address	match all the words

Software name	Software usage time	PC usage time	Number of running PCs
Groupmax,	55.6	145.1	3
JP1/SD Client,	153.9	155.3	9
JP1/Remote Control,	55.6	64.8	4
Ms Office,	41.7	155.3	6
Symantec Antivirus,	152.8	155.3	9
Xu&Hu,	78.0	79.0	2

Asset Information Manager Subset must be installed in order to use the Software Operation Status window. To view software operation times in the Software Operation Status window, you must first collect the software operation times from the clients.

For details about how to perform operations in the Software Operation Status window, see *6.8 Using the Software Operation Status window* in the manual *Administrator's Guide Volume 1*.

2.6.5 Examples of managing operation information

This section gives operation examples that show how to automatically store operation information in JP1/Software Distribution's relational database, and how to execute a command to store the information when necessary.

(1) Automated storage of operation information

By configuring JP1/Software Distribution for automated storage, you can ensure that the latest operation information is available any time a problem occurs. This setup is also useful in that it allows you to perform regular monitoring of the latest operation information. Even though automatically stored operation information is removed from the database after a specified retention period has elapsed, you can still execute a command to re-store the lost information for viewing.

The following explains the settings and user actions during JP1/Software Distribution operation in order to use automated storage.

Settings

Make the following settings on the **Operation Monitoring** page during setup.

- Select the **Save the operation monitoring history** check box.
- Select the **Store the operation monitoring history in the JP1/SD database** check box.
- Select the **Enable automatic storage** check box.

For details about setup, see *4.2.14 Operation Monitoring page* in the *Setup Guide*.

During operation

Operation information is automatically stored and deleted, so no user action is required during JP1/Software Distribution operation. If necessary, however, you can use the `dcmmonrst` command to store or delete operation information to or from the database.

For details about the `dcmmonrst` command, see *4.13 dcmmonrst.exe (storing operating information in a database)* in the manual *Administrator's Guide Volume 2*.

(2) Non-automated storage of operation information

Even if the monitoring timing and period have not been predetermined, you can still monitor operation information as needed over a desired period of time by means of command execution.

The following explains the settings and user actions during JP1/Software Distribution operation in order to use non-automated storage.

Settings

Make the following settings on the **Operation Monitoring** page in the setup.

- Select the **Save the operation monitoring history** check box.
- Select the **Store the operation monitoring history in the JP1/SD database** check box.
- Select the **Compress and move the operation history to the storage directory** radio button.
- Clear the **Enable automatic storage** check box.

For details about setup, see *4.2.14 Operation Monitoring page* in the *Setup Guide*.

During operation

You can use the `dcmmonrst` command to store or delete operation information to or from the database.

In the Embedded RDB environment, you must use the `netmdb_reclaim.bat` command to release the area after you delete operation information.

For details about the `dcmmonrst` command, see *4.13 dcmmonrst.exe (storing operating information in a database)* in the manual *Administrator's Guide Volume 2*.

(3) Using data partitions to store operation monitoring history

When you want to manually store operation information, you can use data partitioning, which is a facility of Microsoft SQL Server 2012, Microsoft SQL Server 2008 or Microsoft SQL Server 2005, to store operation monitoring history.

Large users

If the number of operation information items generated per day exceeds 10 million, we recommend that you create a data partition for each day to store the information.

Mid-size users

If the number of operation information items generated per month exceeds 10 million, we recommend that you create a data partition for each month to store the information.

Small users

Data partitions are not required in the following cases:

- The types of operation logs to be collected from the user are limited, and the number of operation logs to be managed is around several million.
- The number of users to be managed is small, and the number of operation logs to be managed is around several million per month.
- For users whose operation logs do not need to be managed, no data partitions are required.

Dividing a partition and locating the resulting partitions on multiple disks provides the following benefits:

- File input/output can be distributed.
- Index maintenance, database backup, and database restoration can be performed by partition.

Note that you need an operating procedure to reconfigure the partition to enable new data to be stored by stopping the system on a regular basis.

When you need to search for information in the operation monitoring history

Dividing a partition might weaken the search performance. Several cases are described below, using a search from the Operation Log List window as an example: one case in which search performance improves, and two cases in which search performance may deteriorate.

Case in which search performance improves

Search performance improves if a range within which the partition was divided (a range within a day if the partition was divided by day, or within a month if the partition was divided by month) is specified for the search period in the Operation Log List window.

Cases in which search performance may deteriorate

- When no search period is specified
- When the `jamTakeOperationLog.bat` command is executed to output all search results

When you need to delete unnecessary operation monitoring history

Using the `dcmmonrst` command for deletion purposes might take a long time. In this case, you can quickly delete data by converting all unnecessary monitoring history into tables to be deleted at once, and deleting those tables.

2.7 Managing clients

JP1/Software Distribution provides facilities for the following client management tasks:

- Obtaining patches to apply to clients
- Detecting client patch information
- Linking WSUS to manage security updates
- Monitoring client systems
- Sending messages to clients
- Using AMT to control clients

This section provides an overview of these client management facilities.

2.7.1 Obtaining patches to apply to clients

With JP1/Software Distribution, you can obtain patches provided by Microsoft, such as security updates and service packs. By then distributing these patches to clients, you can apply patches without having to directly implement security measures on the clients themselves.

You obtain patches by means of the Software Update Management dialog box. In this dialog box, you can also configure settings so that patches are obtained and packaged automatically according to specified conditions.

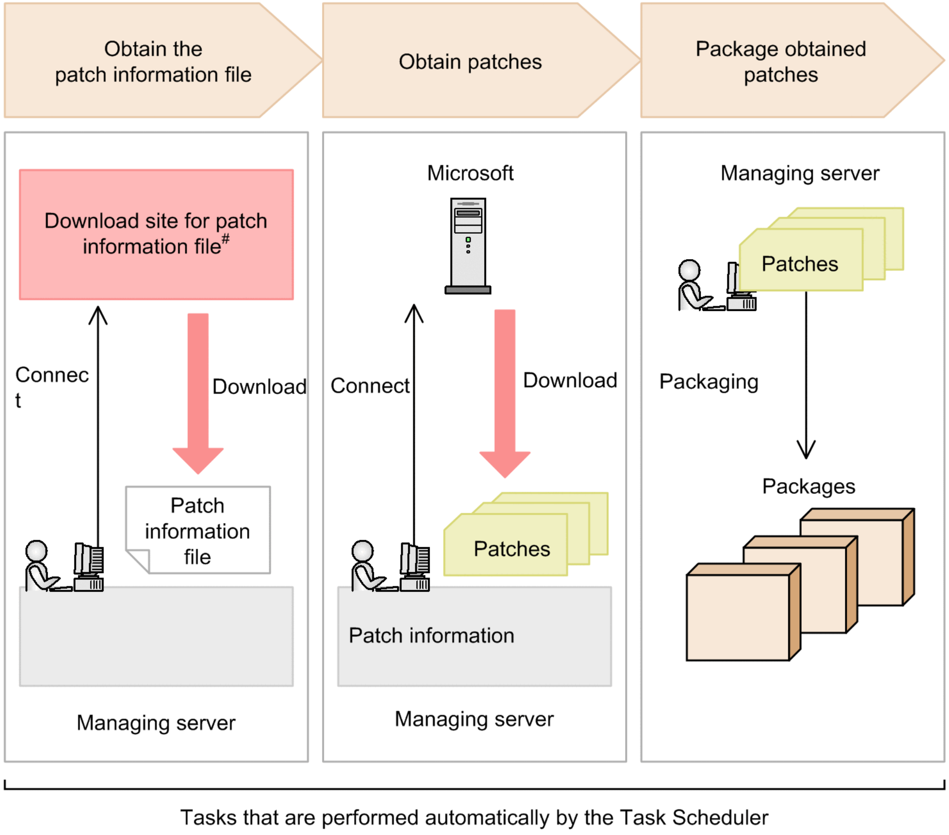
Before you obtain patches, you must obtain the *patch information file*. Obtaining the latest patch information file enables you to determine the list of patches that you wish to obtain. For details about how to obtain the patch information file, see the Readme file for JP1/Software Distribution Manager.

The patches you obtain are stored in a database. The Software Update Management dialog box is the only interface from which you can package the obtained patches.

You can also use Windows Task Scheduler to obtain patches automatically. Task Scheduler enables you to obtain the patch information file automatically and then to obtain and package the patches.

The following figure provides a conceptual overview of obtaining patches with JP1/Software Distribution.

Figure 2–35: Obtaining patches with JP1/Software Distribution



#: For the patch information file download site, see the Readme file for JP1/Software Distribution Manager.

For details about how to perform operations in the Software Update Management dialog box, and for details about how to use Task Scheduler to obtain patches, see *7.1 Acquiring patches to be installed at clients* in the manual *Administrator's Guide Volume 1*.

Note that the remote installation facility is used to apply the packages to the clients. For details about how to perform remote installation, see *2.3 Executing remote installation* in the manual *Administrator's Guide Volume 1*.

The following subsections explain the types of patches that you can obtain and the prerequisites and preparations for obtaining patches.

(1) Types of patches you can obtain

With JP1/Software Distribution, you can obtain patches for the programs listed in the following table. You can obtain OS patches for all OSs supported by JP1/Software Distribution Client.

Table 2–32: Programs for which you can obtain patches

Program	Type and version
Windows	Windows 8
	Windows Server 2012
	Windows 7
	Windows Server 2008
	Windows Vista
	Windows Server 2003

Program	Type and version
Windows	Windows XP
	Windows 2000
Windows Mail	6.0 or later#
Windows Media Player	7.1, 9.0, 10.0, 11.0 or later#
Microsoft .NET Framework	1.1, 2.0, 3.0 or later#
Microsoft Data Access Components	2.5, 2.7, 2.8 or later#
Microsoft Internet Explorer	6.0, 7.0 or later#
Microsoft Outlook Express	5.5, 6.0 or later#

#: Patches from the latest version can be obtained when they are released from Microsoft.

Of the patches that are provided for these programs, JP1/Software Distribution can obtain the following four types (or *classes*):

- Critical updates
- Security updates
- Service packs
- Security rollups

(2) Prerequisites for obtaining patches

The following prerequisites apply to obtaining patches with JP1/Software Distribution:

- JP1/Software Distribution Manager version must be 08-51 or later.
- MSXML 4.0 Service Pack 2 or MSXML 6.0 must be installed.
- The managing server that obtains the patches must be connected to the Internet

If you plan to package the patches yourself, the Packager component of JP1/Software Distribution Client 08-10 or later must be installed on the computer that obtains the patches.

(3) Notes on obtaining patches

- Before you distribute patches obtained with JP1/Software Distribution, make sure you can properly distribute and apply the patches to all the intended clients. Distribution or application of patches might fail in some client environments.
- The following types of patches cannot be obtained:
  - Patches provided by Microsoft before January 1, 2006
  - Patches provided with Microsoft security advisories
  - Patches for PC-98 series computers
- The patch information file is stored in the JP1/Software Distribution installation directory `\OSPATCH\XML`. The script file executed to install patches is stored in the JP1/Software Distribution installation directory `\OSPATCH\Script`. Do not modify these files. If they are modified, correct operation of JP1/Software Distribution cannot be guaranteed.

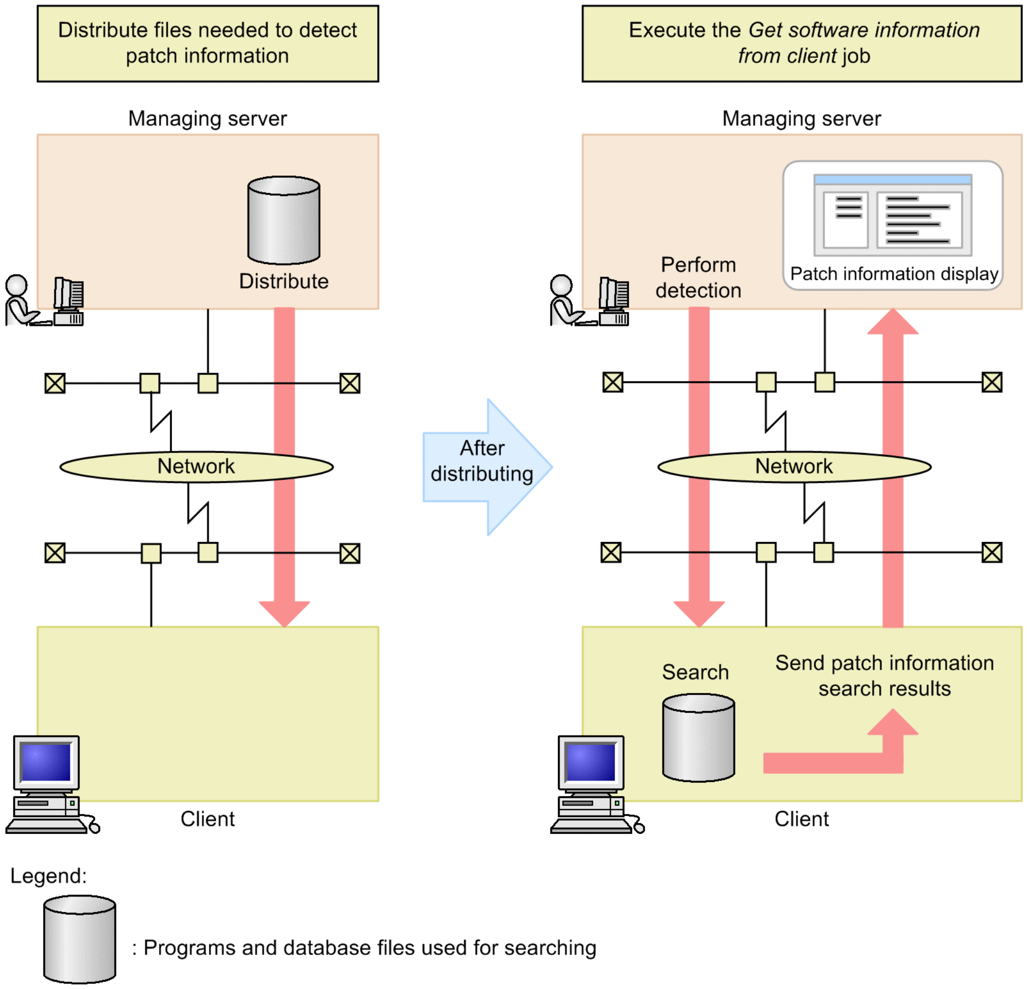
2.7.2 Detecting client patch information

JP1/Software Distribution can detect patches that have been installed at clients or have not been installed at clients and provide it as software information.

To detect clients' patch information, you must distribute a program for detecting patches and a detection database file to the clients and then execute a *Get software information from client* job.

The following figure shows the general procedure for detecting patch information.

Figure 2–36: General procedure for detecting patch information


Distribute files needed to detect patch information
Execute the *Get software information from client* job
Managing server
Distribute
Network
Client
After distributing
Managing server
Perform detection
Patch information display
Network
Search
Send patch information search results
Client
Legend:
: Programs and database files used for searching

JP1/Software Distribution supports two methods for detecting patch information:

- Using WUA to detect patch information
  This method detects information about patches that have been installed at clients as well as information about patches that have not been installed at the clients.
- Using MBSA 1.2.1 to detect patch information
  This method detects information only about patches that have not been installed at the clients.

You choose one of these detection methods, whichever is more suitable to the environment in which patch information is to be detected.

It is perhaps better to use WUA, because it detects not only OS patches but also software patches (such as for Microsoft Office).

If your system supports both WUA and MBSA 1.2.1, WUA will be used (and MBSA 1.2.1 will not be used).

For details about the methods used to detect patch information, see *7.2 Detecting client patch information* in the manual *Administrator's Guide Volume 1*.

The following subsections describe the patch information that can be acquired and the environment required for each detection method.

(1) Using WUA to detect patch information

You can detect patch information by installing WUA at a client, distributing the WUA database file to the client, and then executing a software information collection job.

(a) Detectable patch information

This method detects patch information for security updates provided by Microsoft Update. It can detect not only OS patches but also software patches (such as for Microsoft Office).

(b) JP1/Software Distribution Manager version and target environment required for detection

To detect patch information using WUA, Windows JP1/Software Distribution Manager 08-00 or later is required.

Additionally, the target clients must satisfy all the following conditions:

- The OS in use is Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, Windows Vista, Windows Server 2003, Windows Server 2003 (x64), or Windows 2000 (Service Pack 3 or later).
- Microsoft Internet Explorer 6.0 or later is installed.
- JP1/Software Distribution Client (client) 08-00 or later is installed.
- Windows Installer 3.0 or later is installed.
- WUA is installed.
- A database file for WUA has been stored.

There are no OS or version restrictions on the relay system that relays the *Get software information from client* job.

(2) Using MBSA 1.2.1 to detect patch information

You can detect uninstalled patch information by executing a *Get software information from client* job after distributing the MBSA 1.2.1 command line interface (`mbsacli.exe` file) and a database file for MBSA 1.2.1 to the clients.

(a) Detectable uninstalled patch information

From the results of the security update scan executed by `mbsacli.exe`, JP1/Software Distribution detects the latest patches that have not been installed (those that are displayed with **NOT Found** in the scanning results) as *unapplied patch information*. Note that unapplied patch information cannot be detected for Microsoft Office products because their security updates are not scanned by `mbsacli.exe`.

(b) JP1/Software Distribution Manager version and target environment required for detection

To detect uninstalled patch information using MBSA 1.2.1, Windows JP1/Software Distribution Manager 07-50 or later is required.

Additionally, the target computers must satisfy all the following conditions:

- The OS in use is Windows Server 2008, Windows Server 2003 (except Windows Server 2003 (x64)), Windows XP, Windows 2000, or Windows NT 4.0.
- JP1/Software Distribution SubManager 07-50 or later or JP1/Software Distribution Client 07-50 is installed.
- Microsoft Internet Explorer 6.0 or later is installed.
- The `mbsacli.exe` file for MBSA 1.2.1 and a database file for MBSA 1.2.1 are stored in the target computer.
- The Server service and Workstation service have been started.

There are no OS or version restrictions on the relay system that relays the *Get software information from client* job.

(3) Changing the detection method from MBSA 1.2.1 to WUA

In an environment in which MBSA 1.2.1 is used to detect uninstalled patches, only uninstalled OS patches (such as for Windows 2000 or Windows XP) can be detected. To detect not only OS patches but also uninstalled software patches (such as for Microsoft Office products and Microsoft SQL Server), you must change the detection method from MBSA 1.2.1 to WUA.

To change the detection method from MBSA 1.2.1 to WUA, the detection requirements for WUA must be satisfied by the JP1/Software Distribution Manager that will be used to execute the detection and by the target clients.

For details about the environment required for detection using WUA, see *(1)(b) JP1/Software Distribution Manager version and target environment required for detection*.

The `mbsacli.exe` file and database file for MBSA 1.2.1 can remain at the detection targets. In an environment in which WUA is used to detect uninstalled patches, MBSA 1.2.1 will not be used.

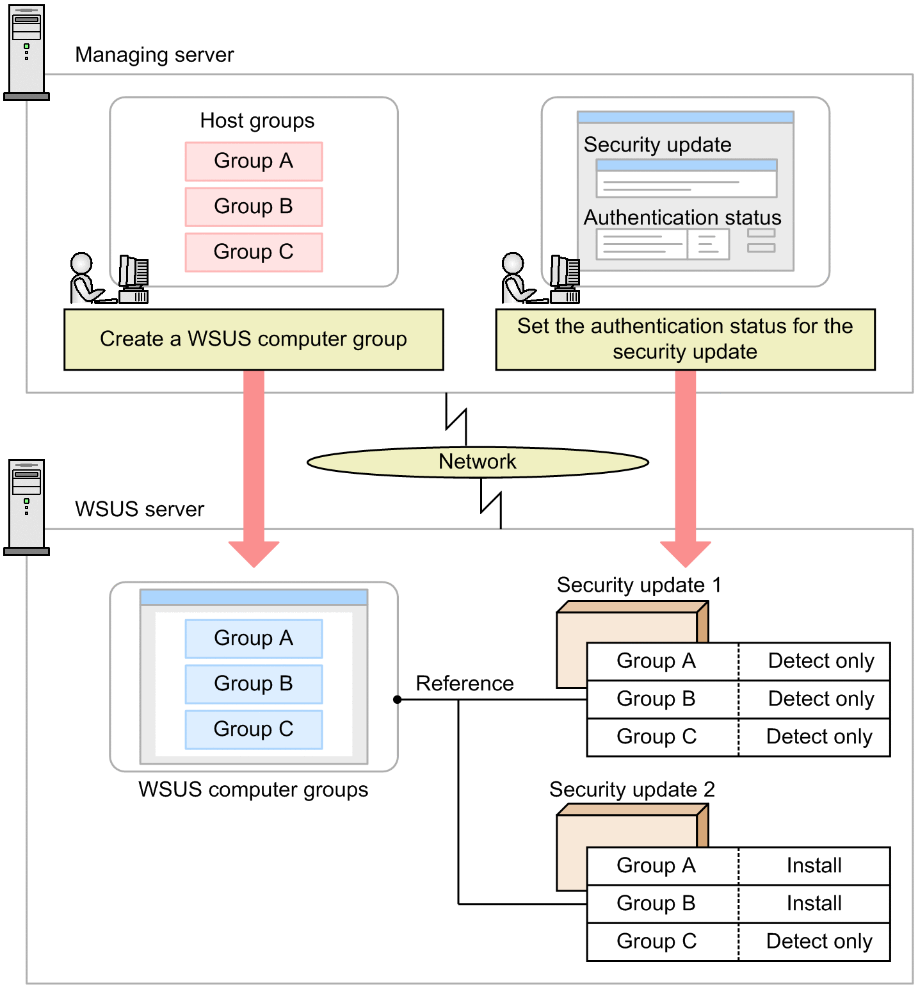
2.7.3 Linking with WSUS to manage security updates

If you link WSUS to your JP1/Software Distribution system, you can execute the following WSUS management tasks from JP1/Software Distribution:

- Creating a WSUS computer group
  You can use JP1/Software Distribution's host groups to create WSUS computer groups and to maintain them.
- Setting the authentication status of security updates
  You can change the authentication status of security updates for each WSUS computer group.

The following figure shows the concept of linking WSUS to manage security updates.

Figure 2–37: Concept of linking WSUS to manage security updates



Security update 1

Group A	Detect only
Group B	Detect only
Group C	Detect only

Security update 2

Group A	Install
Group B	Install
Group C	Detect only

JP1/Software Distribution also supports environments in which multiple WSUS servers are configured in a hierarchy. For details about the system configuration required for linking WSUS, see *5.2.4 System configuration for WSUS linkage*.

For details about how to link WSUS to manage security updates, see *7.3 Linking to WSUS to manage update programs* in the manual *Administrator's Guide Volume 1*.

(1) Prerequisites for linking with WSUS

In an environment where WSUS is linked, JP1/Software Distribution and WSUS must satisfy the following prerequisites.

Prerequisites for JP1/Software Distribution

- The center manager in use is JP1/Software Distribution Manager 08-51 or later.
- The relay system in use is JP1/Software Distribution SubManager 08-00 or later or JP1/Software Distribution Client (relay system) 08-00 or later.
- Each client in use is JP1/Software Distribution Client 08-00 or later.
- A relation database is used.

Prerequisites for WSUS

- WSUS 2.0 or WSUS 3.0 must be used.
- WSUS installed in a 32-bit version of the OS must be used.
- On WSUS's **Computer Options** page, **Use the Move computers task in Windows Server Update Services** is selected.
- WSUS Linkage, which is a component of JP1/Software Distribution version 08-00 and later, must be installed.

(2) Preparations for linking with WSUS

To link WSUS, you must set up an environment that supports WSUS linkage, and then complete the preparations shown below in both JP1/Software Distribution and WSUS.

For details about the system configuration that supports WSUS linkage, see *5.2.4 System configuration for WSUS linkage*.

Preparations in JP1/Software Distribution

- During server setup, on the **WSUS Linkage** page, specify the appropriate URL in **URL for WSUS Linkage**. For details about how to specify the URL for WSUS linkage, see *4.2.17 WSUS Linkage page* in the *Setup Guide*.
- You must execute in advance a *Get system information from client* job to obtain WSUS computer IDs from the clients. To obtain the WSUS computer IDs, select **Acquire all information** on the **Options** page when you create the job.

  Note that the WSUS computer ID is not normally displayed in a listing of system information.

Preparations in WSUS

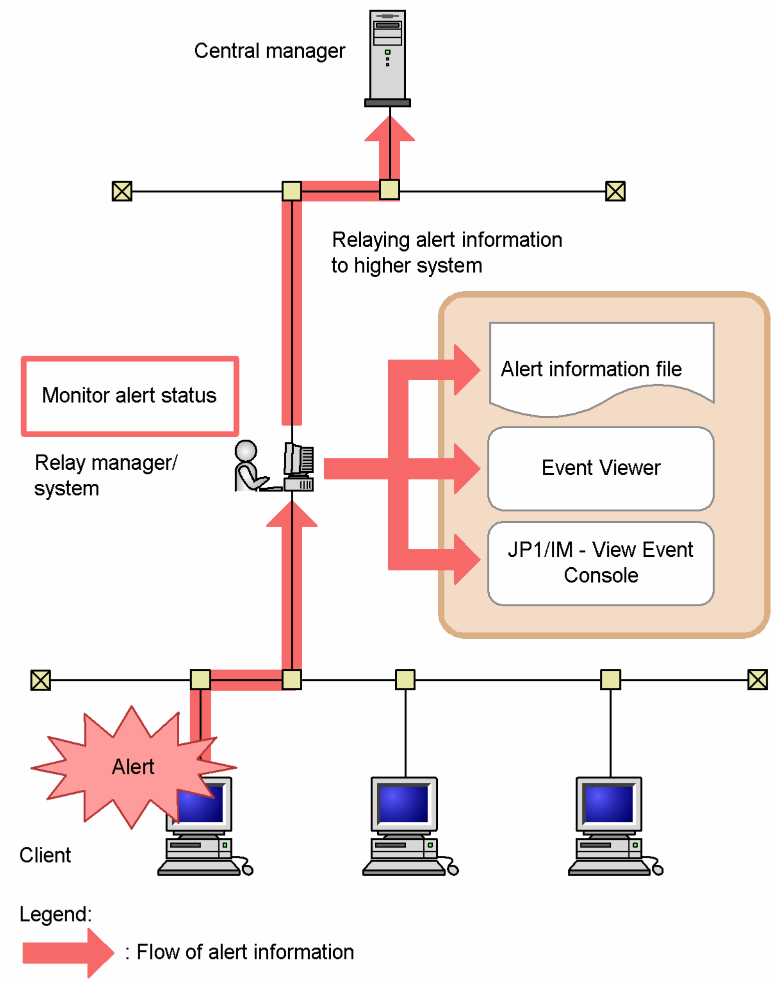
On WSUS's **Computer Options** page, select **Use the Move computers task in Windows Server Update Services**.

2.7.4 Monitoring client systems

A client has a facility for monitoring the hard disk and memory of the local machine and issuing an alert when an error is detected, such as when the amount of available space falls below a certain level. This facility is called the *system monitoring facility*. If clients are set to report alert information to a higher system, JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system) on a higher system can monitor the lower clients for alerts.

In a JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system), you can use a CSV alert information file, the Windows NT Event Viewer, or the Event Console window of JP1/IM - View to check the alert information from each client. The client's system information is sent with the alert information, so the cause of the alert can be investigated immediately. The alert information can also be relayed to a higher system. The following figure shows the flow of alert information reported by a client.

Figure 2–38: Flow of alert information reported by a client



For details about system monitoring at a client, see *11.8 Reporting an alert based on system monitoring* in the manual *Administrator's Guide Volume 1*. For details about how to report alert information from a client to a higher system, see *11.8.4(4) Reporting an alert to a higher system* in the manual *Administrator's Guide Volume 1*.

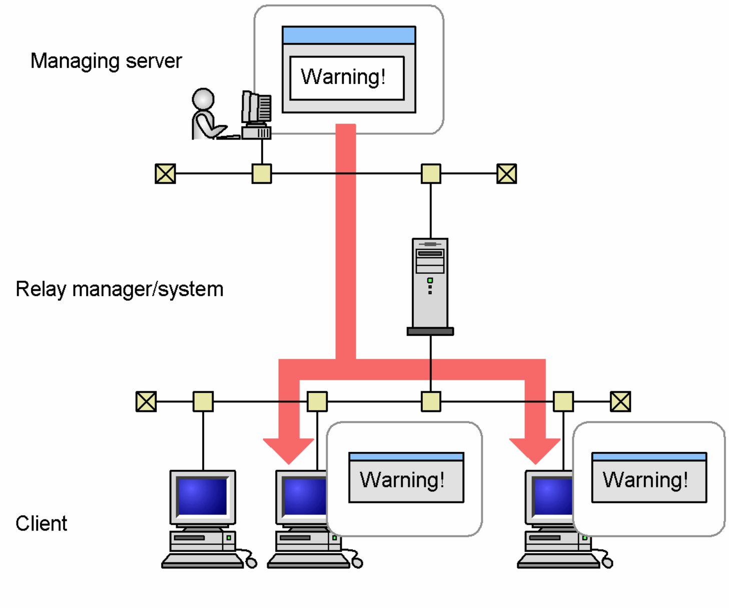
The output destination for alert information in JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system) is specified during each setup. For details about how to set and check the output destination of alert information, see *7.4 Checking alert information reported from clients* in the manual *Administrator's Guide Volume 1*.

2.7.5 Sending messages to clients

By executing a *Report message* job, you can send a message to the client at the job destination. You can specify any content for the message. This facility is useful for sending a warning message to a client that has poor security measures or for sending system maintenance information to all clients at once.

The following figure shows the concept of sending messages to clients.

Figure 2–39: Concept of sending messages to clients



For details about how to send messages to clients, see *7.5 Sending messages to clients* in the manual *Administrator's Guide Volume 1*.

This section explains for each of the elements comprising a JP1/Software Distribution system the programs required to send messages to clients.

■ Sending text messages to clients

The following table lists the programs required to send text messages to clients.

Table 2–33: Programs required to send text messages to clients

System configuration element	Required program
Central manager that will execute jobs	JP1/Software Distribution Manager 07-50 or later (relational database version) for Windows
System for relaying jobs	JP1/Software Distribution Manager 07-50 or later for Windows, JP1/Software Distribution Client (relay system) 08-00 or later for Windows, JP1/Software Distribution SubManager 07-50 or later for Windows, JP1/Software Distribution Client (relay system) 09-00 or later for UNIX, or JP1/Software Distribution SubManager 07-50 or later for UNIX
Client that will receive messages	JP1/Software Distribution SubManager 07-50 or later for Windows, JP1/Software Distribution Client 07-50 or later for Windows, or JP1/Software Distribution Client 09-00 or later for UNIX

■ Sending HTML messages to clients

The following table lists the programs required to send HTML messages to clients.

Table 2–34: Programs required to send HTML messages to clients

System configuration element	Required program
Central manager that will execute jobs	JP1/Software Distribution Manager 08-10 or later for Windows
System for relaying jobs	JP1/Software Distribution Manager 07-50 or later for Windows JP1/Software Distribution Client (relay system) 08-00 or later for Windows, JP1/Software Distribution SubManager 07-50 or later for Windows,JP1/Software Distribution Client (relay system) 08-00 or later for UNIX or JP1/Software Distribution SubManager 07-50 or later for UNIX

System configuration element	Required program
Client that will receive messages	JP1/Software Distribution Manager (relay manager) 08-10 or later for Windows or JP1/Software Distribution Client 08-10 or later for Windows

If you send an HTML message to a client running version 08-00 or earlier, the HTML tags will appear as text character strings. For this reason, you cannot send HTML messages to notify such clients.

In a security management system on which JP1/Client Security Control has been installed, you can use JP1/Software Distribution's *Report message* job to send messages to clients from the management server at which JP1/Client Security Control is installed.

2.7.6 Using AMT to control clients

If you use computers that support AMT, you can use AMT functionality to control clients by installing the AMT Linkage component on the clients and higher systems.

The following shows the prerequisites for using AMT to control clients.

Managing server:

- Microsoft .NET Framework 1.1, 2.0, 3.0, or 3.5 is installed
- `telnet.exe` is present inside the system folder (this is a prerequisite for using the remote control facility of AMT).
- imrsdk.dll is stored in a host on which the command is run (When the remote control function of AMT is used).
- JP1/Software Distribution version 08-10 or later is being used
- AMT Linkage is installed

Relay manager/system:

If you use AMT to control clients below a relay manager/system, the same prerequisites as those for the managing server apply to the relay manager/system.

To use the client functionality, the same prerequisites as those for the client system apply. However, for a relay system in the Windows 8, Windows Server 2012, Windows 7, Windows Server 2008 or Windows Vista Edition of JP1/Software Distribution Client, use version 08-51 or later.

Client:

- A computer that supports AMT is being used.
- Microsoft .NET Framework 1.1, 2.0, 3.0, or 3.5 is installed.
- An SOL driver is installed (this is a prerequisite for using the remote control functionality of AMT).
- DHCP is being used.
- The OS is Windows 7, Windows Vista, Windows Server 2003 (either without any service pack or with Service Pack 1), or Windows XP Professional (Service Pack 1 or later).
- One of the following versions of JP1/Software Distribution Client is being used:
    - 08-10 or later
    - 08-51 or later, and the OS is Windows Server 2008 or Windows Vista
    - 09-50 or later, and the OS is Windows 7
- AMT Linkage is installed.
- The host name is used as the ID key for operations.

For details about the system configuration needed to use AMT Linkage, see *5.2.5 System configuration when using AMT*.

(1) Using the client control facility

The client control facility enables you to control and execute jobs on clients that do not support Wake on LAN or on clients that are in standby or sleep mode.

Provided that the managing server and client environments support use of AMT Linkage, you can use AMT to control the client simply by enabling the client control facility for use when you execute the job. In an environment that supports use of Wake on LAN, you can also perform client control with Wake on LAN if AMT-based client control fails.

To determine whether a client supports use of AMT Linkage, check the value obtained for the AMT firmware version item in the system information. If there is no value, or if the value is `N/A`, AMT Linkage cannot be used on that client.

For details about the settings required to use this facility, see *6.3 Settings for using the client control facility*.

(2) Storing the client host ID

Normally, a new host ID is generated whenever a client is re-installed, so the higher systems recognize the new client as a different asset from when it existed before it was re-installed.

On a client that uses AMT Linkage, the host ID generated by the first installation can be stored by AMT in nonvolatile memory, so that the same host ID will be used after the client has been re-installed.

This means that the client can always be recognized as the same asset by higher systems, even if it must be re-installed due to a disk failure or some other problem.

For details about the settings required to use this functionality, see *6.5.1 Storing the client's host ID*.

(3) Remotely controlling a client on which a failure has occurred

Using the remote control facility of AMT, you can connect to a client whose power is off, and you can set up its BIOS. Additionally, if a floppy disk containing a diagnostic program is available in the managing server, from the managing server you can remotely execute the diagnostic program on a client.

If a failure occurs on a client, you can try to recover the client from the failure by checking its BIOS settings from the managing server, or by executing the diagnostic program to investigate the cause.

If you wish to use this functionality, the version of the managing server and the client must be 08-51 or later.

For details on how to use this functionality, see *7.6 Using AMT's remote control facility* in the manual *Administrator's Guide Volume 1*.

2.8 Controlling remote clients

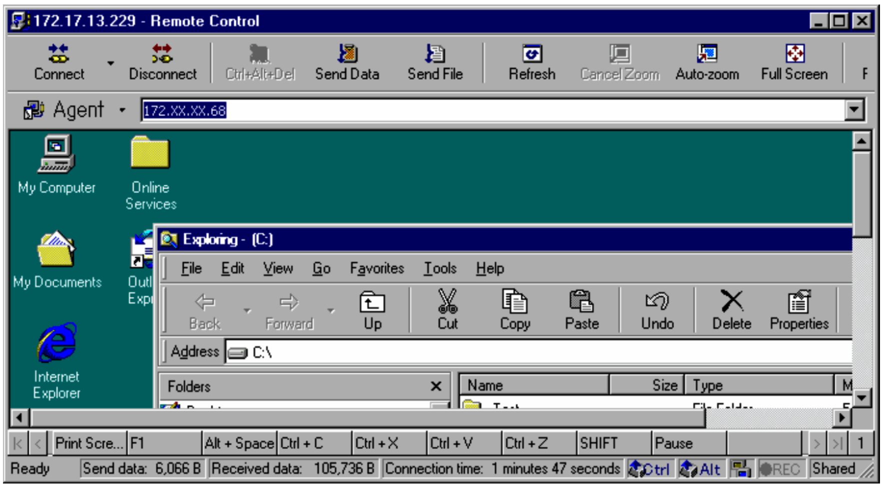
The managing server's Remote Control Manager enables you to control remote clients (a process called *remote control*). To control remote clients, Remote Control Agent must be running at the target clients.

This section provides an overview of remote control.

2.8.1 How to start Remote Control Manager

To control remote clients, you must start Remote Control Manager.

Figure 2–40: Remote Control window



Ready | Send data: 6,066 B | Received data: 105,736 B | Connection time: 1 minutes 47 seconds

To start Remote Control Manager, from the **Start** menu, choose **Remote Control Manager**, or use the following methods:

- Start Remote Control Manager from Remote Installation Manager
- Start Remote Control Manager from an inventory information counting result

(1) Starting Remote Control Manager from Remote Installation Manager

From Remote Installation Manager's System Configuration window, Destination window or Directory Information window, select a client, choose **Options**, and then choose **Start Remote Control Manager** to start Remote Control Manager.

Once Remote Control Manager starts, it connects automatically to the selected client.

(2) Starting Remote Control Manager from an inventory information counting result

From Inventory Viewer's counting result, select a client, choose **Tools**, and then choose **Start Remote Control Manager** to start Remote Control Manager.

You can select multiple clients, then select the client to be connected, and then start Remote Control Manager.

For details about how to start Remote Control Manager from Inventory Viewer, see *4.6 Using the remote control facility* in the manual *Administrator's Guide Volume 1*.

2.8.2 Functionality of Remote Control Manager

This subsection describes the functionality of Remote Control Manager.

For details about each function, see the manual *Job Management Partner 1/Remote Control Description and Operator's Guide*.

(1) Performing operations in client windows

You can connect to a client, display the client's windows, and perform operations in the windows. In addition to being able to perform keyboard and mouse operations, you can also transfer clipboard data.

(2) Transferring files

In Remote Control Manager's File Transfer window, you can use drag-and-drop operations to transfer files between the central manager and client or between clients. You can also compress data to transfer files efficiently.

(3) Recording and playing back a client's window information

You can record the information displayed in a client window and save it to a file. To play back the file, you can use Remote Control Player provided by the Remote Control Manager. You can also convert a saved file to AVI format so that it can be played back in an environment where the controller is not available.

(4) Chatting

You can use the chat facility to communicate with a client that is under remote control. The chat facility can also be used between central managers and between clients.

(5) Making connection requests from a client

A client can issue a connection request (that is, connect) to the central manager. Because the central manager that receives a connection request can check and connect to the requesting client, you can respond to client problems quickly.

2.9 Managing jobs

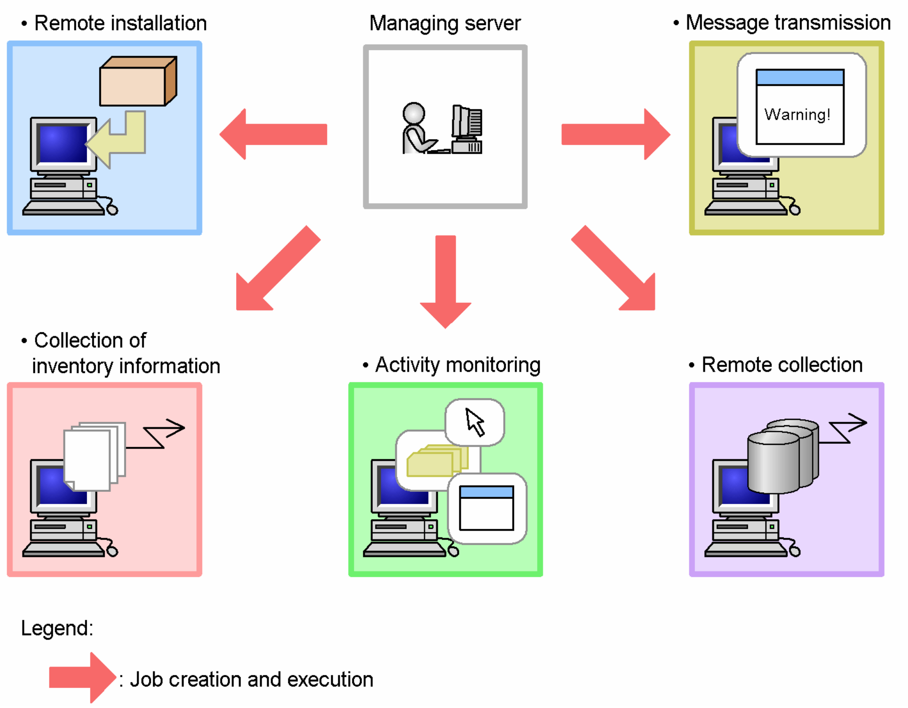
Many of the JP1/Software Distribution facilities, such as remote installation and acquisition of inventory information, implement their functions by executing jobs from the managing server to clients.

This section provides an overview of the jobs, including the concept and types of jobs and the tasks involved in job execution.

2.9.1 About jobs

A JP1/Software Distribution system implements various distribution and asset management tasks, such as remote installation of software and acquisition of client information, by creating and executing instructions called *jobs* from the managing server. The following figure shows the concept of job execution for implementation of distribution and asset management tasks.

Figure 2–41: Distribution and asset management tasks implemented by job execution



The basic tasks related to jobs, such as creating, executing, and storing jobs, are common to many JP1/Software Distribution facilities. To make the best use of JP1/Software Distribution in the distribution and asset management tasks, you must fully understand jobs.

For details about how to create and execute jobs, see *8.1 Job creation and execution procedures* in the manual *Administrator's Guide Volume 1*.

2.9.2 Types of jobs that can be created

The types of jobs (job types) that can be created depend on the type of managing server, that is, the central manager and relay managers or the relay systems. The following table lists and describes the types of jobs that can be created and the supported types of managing servers.

Table 2–35: Types of jobs that can be created in the managing server

No.	Job type	Description	Supported managing server	
			JP1/Software Distribution Manager	JP1/Software Distribution Client (relay system)
1	*Install package*	Installs a package at remote clients.	Y	Y
2	*Transfer package to relay system*	Transfers a package to a relay system.	Y	--
3	*Batch delete packages on relay system*	Deletes all packages from a relay system.	Y	--
4	*Collect files from client*	Collects files from client systems to the managing server.	Y	Y
5	*Collect files from client to relay system*	Collects files from clients to the relay manager/system (relay manager or relay system) directly under the managing server.	Y	--
6	*Acquire collected files from relay system*	Transfers files collected in a relay manager/system to the managing server.	Y	--
7	*Delete collected files from relay system*	Deletes all files collected in a relay manager/system.	Y	--
8	*Send package, allow client to choose*	Sends a package to clients who decide whether or not to install the software. A client uses Package Setup Manager to install software.	Y	Y
9	*Get system information from client*	Collects system information (system information and registry information) and user inventory from clients.	Y	Y
10	*Get software information from client*	Collects from clients information about the software that has been installed at the clients.	Y	Y
11	*Get user inventory information*	Collects user inventory information from clients.	Y	--
12	*Transfer registry collection definition*	Transfers settings for collecting registry information to clients.	Y	--
13	*Transfer user inventory schema to client*	Transfers the user inventory information items set in the managing server to clients.	Y	--
14	*Get system configuration information*	Collects system configuration information under relay managers or relay systems. This job can collect system configuration information for the following systems: • Relay systems and clients under each specified destination relay manager as well as the relay managers at the next level down • Relay systems and clients under the specified destination relay system	Y	--
15	*Hold report*	Instructs relay systems to temporarily hold reporting of job results.	Y	--

No.	Job type	Description	Supported managing server	
			JP1/Software Distribution Manager	JP1/Software Distribution Client (relay system)
16	*Hold-report release*	Instructs relay systems to stop holding reporting of job results.	Y	--
17	*Suspend file transfer*	Instructs relay systems to suspend file transfer to lower systems (relay systems and clients).	Y	--
18	*Resume file transfer*	Instructs relay systems to resume file transfer to lower systems.	Y	--
19	*Report message*	Sends a message, specified when the job was created, to a client.	Y	--
20	*Set the software monitoring policy*	Instructs a client to start or stop monitoring software operations.	Y	--
21	*Get software monitoring information from the client*	Collects the software suppression history and operation history from a client.	Y	--

Legend:

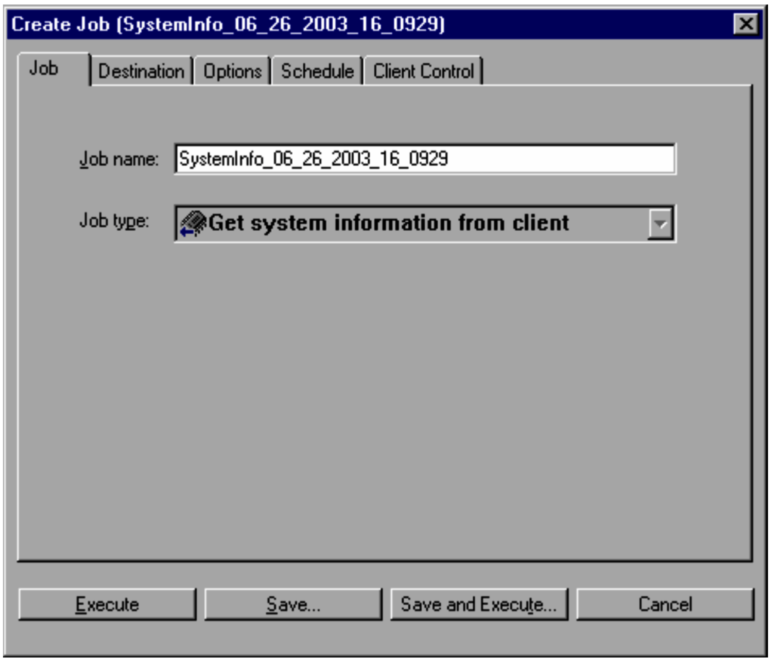
Y: Job can be created.

--: Job cannot be created.

2.9.3 Detailed job settings

You use Remote Installation Manager's Create Job dialog box to create a job.

Figure 2‒42: Create Job dialog box



Create Job (SystemInfo_06_26_2003_16_0929)

Job name: SystemInfo_06_26_2003_16_0929

Job type: Get system information from client

The Create Job dialog box displays the pages needed for the specified type of job so that you can set the details of the job, such as job name, destination, and execution conditions. For details about the pages that are displayed in the Create Job dialog box, see *8.2.2 Settings in the Create Job dialog box* in the manual *Administrator's Guide Volume 1*.

The following table lists the pages that are displayed in the Create Job dialog box and provides an overview of the information that is set on each page.

Table 2–36: Pages displayed in the Create Job dialog box

Page	Information to be set
Job page	Sets a name for the job.
Destination page	Sets the hosts that are targets of the executed job.
Package page	Sets options, such as the attributes of package to be installed remotely and the installation environment.
Job Distribution Attributes page	Sets information required for multicast distribution or split distribution of a package. These options are useful for large packages. Note that you can specify multicast distribution for an *Install package* job only.
Collect File page	Sets files to be collected remotely.
Options page	Specifies options for execution of jobs that acquire inventory information. The contents of this page depend on the job type specified.
Schedule page	Sets the job registration date and time, execution date and time, and execution time limit.
Client Control page	Enables you to start a PC at a job destination if it is not active. Also enables you to shut down such a PC after starting it.
Message Notification page	Enables you to set icons, titles, and text for messages to be displayed at the job destination.
Operation Monitoring Policy page	Enables you to specify start, change, and stop of operation monitoring at the job destination. To start or change operation monitoring, choose the operation monitoring policy to be applied.

2.9.4 Executing and saving jobs

You can execute a job as is after creating it in the Create Job dialog box, or you can save it first in the Job Definition window and then execute it. Once saved, a job can be used as a template, enabling you to execute a similar job easily as many times as needed.

To save a job, you must first create a folder to manage the created job in the Job Definition window.

For details about how to edit saved jobs and create folders, see *8.3.2 Managing saved jobs and folders* in the manual *Administrator's Guide Volume 1*.

2.9.5 Executing a job on grouped hosts

In the case of a large-scale system, it is simpler to specify a group of systems as a job execution target rather than specifying many systems individually. Examples of targets that are grouped include host groups, ID groups, and directory information. If the managing server is part of a hierarchical structure, the central manager can specify all its lower clients as the targets. The following describes the characteristics of the various groups.

Host groups:

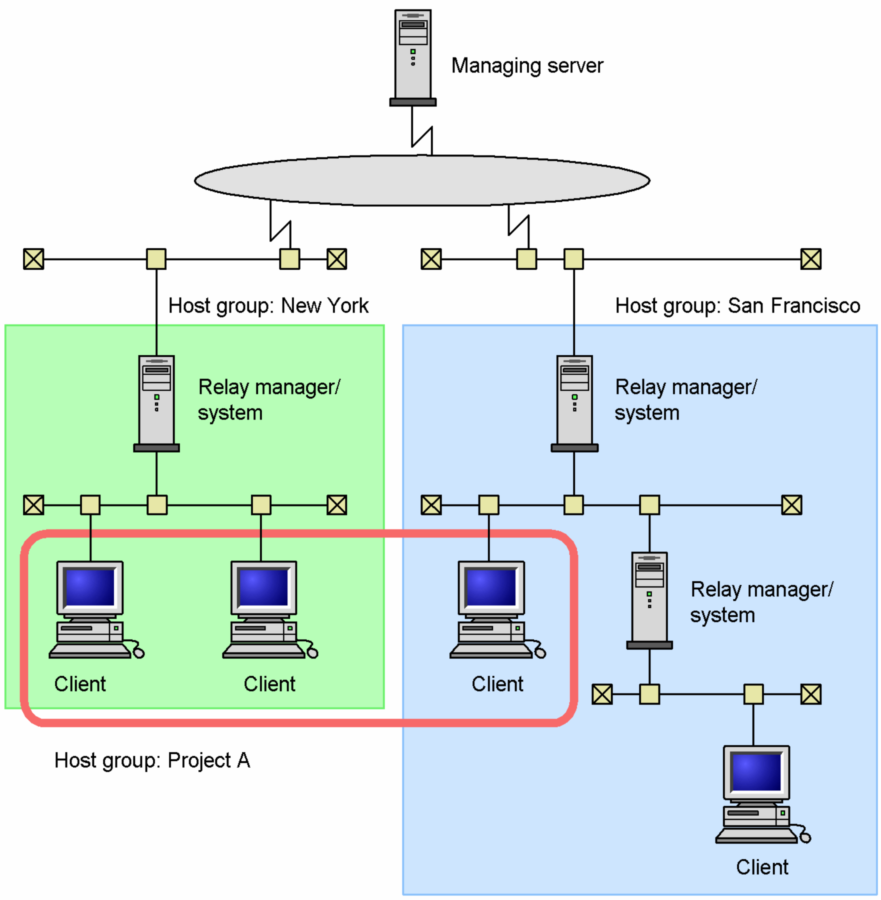
Host groups constitute destinations (targets) grouped by hierarchy, such as by department or by project. The managing server manages not only the group definitions but also the information about the clients that belong to each group. This type of grouping provides a logical hierarchical structure for job destinations. We recommend that you create host groups because such groups simplify management of job destinations.

If you specify that a host group is the destination of a job, the job will be executed on all the clients that belong to that group.

You can group clients by department as well as by project. This enables you to set the groups by department or by project when a project spans departments, as shown in the figure below.

The following figure shows the concept of host groups.

Figure 2–43: Concept of host group

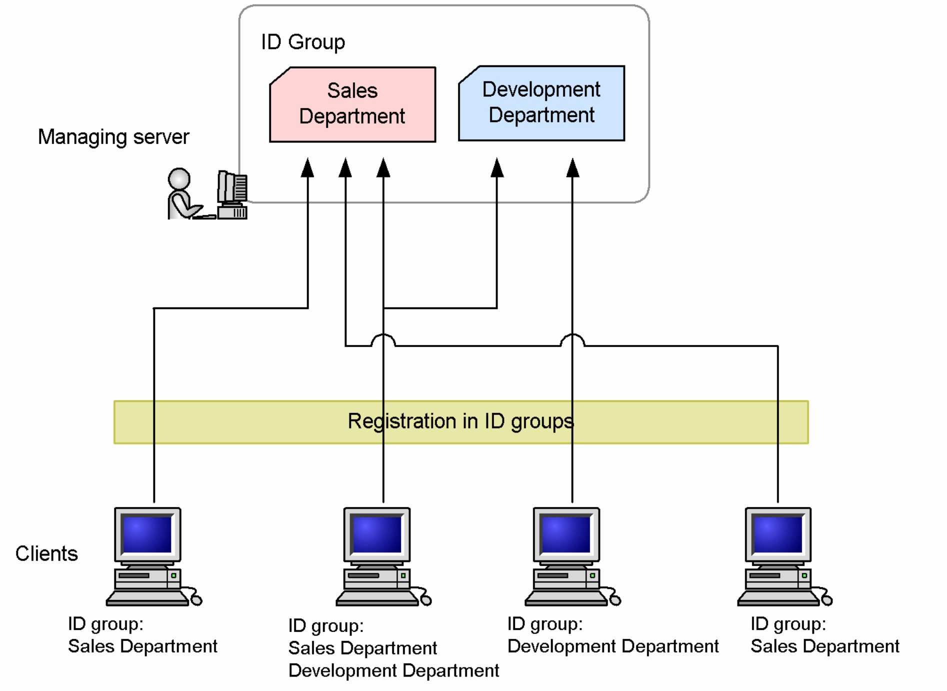


ID groups:

The use of ID groups not only allows registration of member clients, but also allows each client to select the ID groups to which it wishes to belong and to register into those groups. A job executed for an ID group is applied automatically to a new client that has added itself to the ID group; therefore, the managing server does not need to redistribute the corresponding software. Even when ID groups are based on information that is subject to change, such as groups for different OSs or types of machine usage, only the clients affected by a change need to change their ID group memberships. This reduces the system administrator's workload.

The following figure shows the concept of ID groups.

Figure 2–44: Concept of ID groups



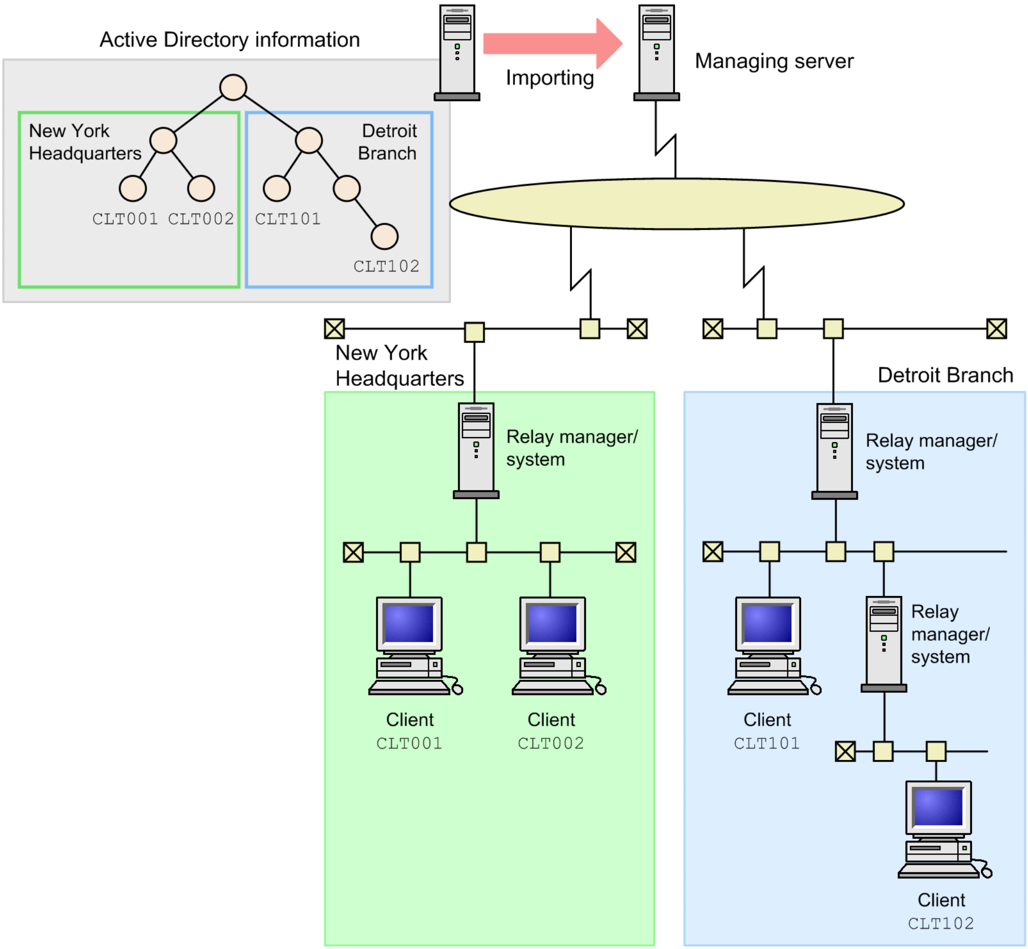
Directory information:

Directory information is information being managed in Active Directory that is imported into the managing server. Since the information being managed in Active Directory can be used as is, there is no need to create a new group. Using the directory information is convenient when you execute a job and specify a group as the target.

Furthermore, when a new computer is added, you can update the directory information simply by acquiring the latest information from Active Directory. This simplifies maintenance procedures.

The following figure shows the concept of directory information.

Figure 2–45: Concept of directory information



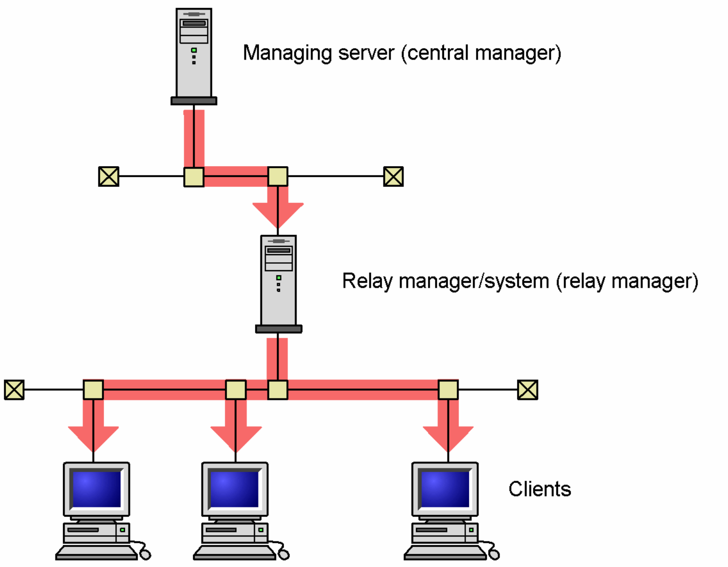
All lower clients:

This type of destination grouping can be selected for distributing software to be installed on all clients under a relay manager; no preparation of groups is required. The central manager can specify this destination grouping for managing servers that are structured in a hierarchy.

If you send a job specifying all lower clients from the central manager to a relay manager, the relay manager that receives the job executes it on all lower clients.

The following figure shows the concept of all lower clients.

Figure 2–46: Concept of all lower clients


Managing server (central manager)
Relay manager/system (relay manager)
Clients

2.9.6 Flow of job execution

This section describes the flow of job execution.

During setup of JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system), two of the items that can be specified are **Number of subsystems that can be connected at one time** and **Max. number of subsystems in which jobs can execute concurrently**.

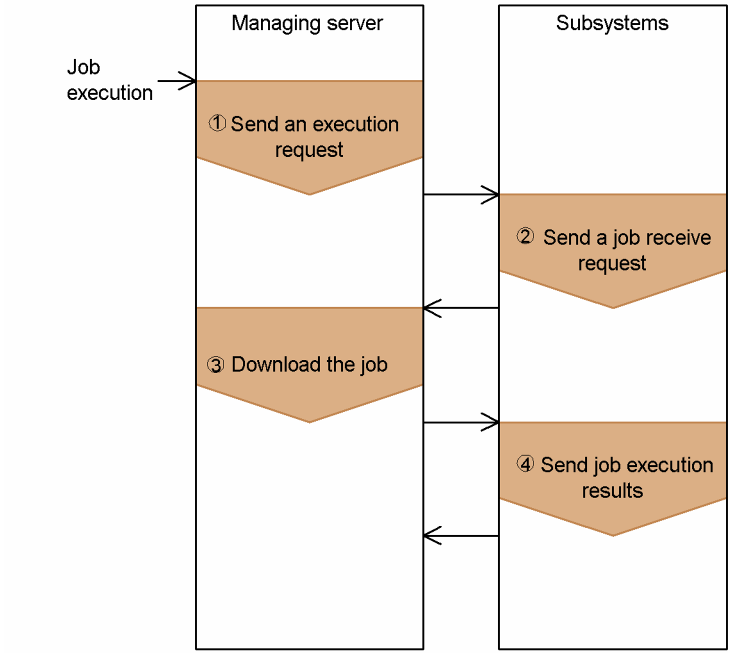
To execute a job:

1. Execute the job from the Remote Installation Manager.

   The managing server sends an execution request (notifying the subsystems that a job was executed) to the destinations (targets) specified during job execution.
2. The subsystems receive the execution request and request the job from the higher system.
3. The job is downloaded to the subsystems that request the job.
4. The execution results are sent from the subsystems to the managing server.

The following figure shows the flow of job execution.

Figure 2–47: Flow of job execution


Managing server
Subsystems
Job execution
① Send an execution request
② Send a job receive request
③ Download the job
④ Send job execution results

The managing server monitors jobs at one-minute intervals. If there are subsystems that need to be connected, the managing server sends an execution request to them. The maximum number of subsystems to which an execution request can be sent at one time is the value specified for **Max. number of subsystems in which jobs can execute concurrently**. However, if the number of currently connected subsystems is fewer than the value specified for **Number of subsystems that can be connected at one time**, the managing server sends only as many execution requests as there are subsystems that can still be connected.

Note that the number of subsystems for the destinations specified in a job refers to only the number of subsystems directly connected to the managing server that executed the job. Therefore, if the distribution route contains relay managers/systems (relay managers or relay systems), the number of relay managers/systems that are directly connected to the managing server is included in the number of subsystems. This number does not include any systems subordinate to the directly connected relay managers/systems.

(1) Job execution example

This section presents an example of job execution.

Conditions

Number of destinations specified for the job: 60

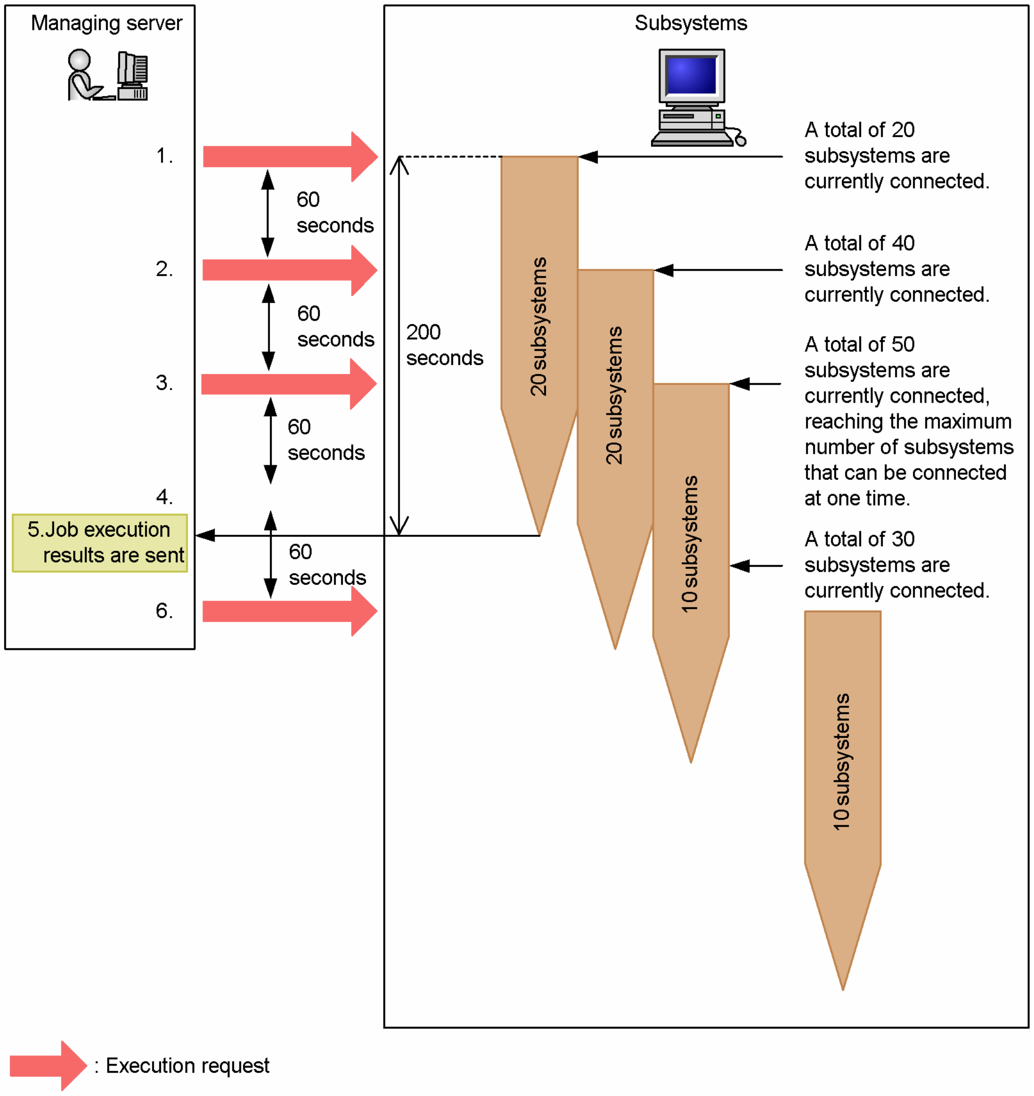
Max. number of subsystems in which jobs can execute concurrently: 20

Number of subsystems that can be connected at one time: 50

Job downloading time: 200 seconds

The following figure shows the flow of job execution under these conditions.

Figure 2–48: Example of the flow of job execution


Managing server
Subsystems
1.
2.
3.
4.
5.Job execution results are sent
6.
60 seconds
60 seconds
60 seconds
60 seconds
200 seconds
20 subsystems
20 subsystems
10 subsystems
10 subsystems
A total of 20 subsystems are currently connected.
A total of 40 subsystems are currently connected.
A total of 50 subsystems are currently connected, reaching the maximum number of subsystems that can be connected at one time.
A total of 30 subsystems are currently connected.
: Execution request

1. The execution request is sent to as many subsystems as the value specified for **Max. number of subsystems in which jobs can execute concurrently**, which is 20.

   Number of subsystems currently connected (20) < **Number of subsystems that can be connected at one time** (50)

2. The execution request is sent to as many subsystems as the value specified for **Max. number of subsystems in which jobs can execute concurrently**, which is 20.

   Number of subsystems currently connected (40) < **Number of subsystems that can be connected at one time** (50)

3. The execution request is sent to the remaining 10 subsystems that can still be connected concurrently.

   Number of subsystems currently connected (50) = **Number of subsystems that can be connected at one time** (50)

4. No execution request is sent because the number of subsystems currently connected equals the **Number of subsystems that can be connected at one time**.

5. Execution results are sent from the subsystems that were connected in step 1.

   Number of subsystems currently connected (30) < **Number of subsystems that can be connected at one time** (50)

6. Of the 60 destinations specified in the job, the execution request is sent to the remaining 10 subsystems.

2.9.7 Job execution order

Jobs for which an execution time (installation date/time) is specified are referred to in this section as *scheduled jobs* and other jobs are referred to as *real-time jobs*. When multiple jobs are to be run on a client at the same time, they are executed on the basis of the following rules:

- Scheduled jobs are executed according to their schedule; that is, they are executed in order based on the dates/ times specified for the jobs.
- Real-time jobs are executed in the order they are started by Remote Installation Manager.
- A real-time job that Remote Installation Manager starts before a scheduled job is executed before any scheduled job at the client.

(1) Using a schedule to execute packages

You might want to arrange packages into multiple jobs in order to execute the jobs so that the packages are installed in a specific order. In such a case, follow the above rules, and also keep in mind the following:

- Use the same route (via a relay manager/system) to execute the jobs.
- Specify the same installation mode (GUI or background) for all the packages.
- If you specify **Install when system starts** as the package installation timing, the package will not be installed until the client system is restarted. Therefore, if you want to schedule the installation of one package with **Normal installation** specified and another package with **Install when system starts** specified, be careful about the client restart timing.
- In a configuration consisting of a central manager, relay systems, and clients, if a relay system contains both a job created at the central manager and a job created at the relay system itself, the job created at the central manager is executed first.
- If multiple packages are included in the same job with the same installation time and installation mode, the packages are installed at a client in the order described below.

  Basic rule for installing packages:

  Packages are installed in the order determined by the character strings generated by combining a cabinet ID (two characters), package ID (up to 44 characters), version (six characters), and generation (four digits) specified in the Create Job dialog box of Remote Installation Manager. The packages are installed in ascending order of the generated character strings. If you distribute more than one package at the same time, you can specify the attributes such as a cabinet ID and package ID keeping to manage the installation order. The following shows an example for installing packages A and B with the following attributes:

Attribute	Package A	Package B
Cabinet ID	`'DD'`	`'AA'`
Package ID	`'AAA'`	`'CCCCC'`
Version	`'0100 '`	`'0100/A'`
Generation	`'0000'`	`'0001'`
String generated from the above attributes	`'DDAAA0100 0000'`	`'AACCCCC0100/A0001'`

  Because packages are installed in the ascending order of the generated strings, package B will be installed before package A.

  The **Package** page in the Job Creation dialog box lists package names in ascending order of the strings generated from the four attributes. The order in which the package names are displayed is the same as the order in which the packages will be installed, so you can use this page to check the package installation order.

  For user programs and data, and other companies' software:

  Assign a package ID that is alphanumerically lower in ASCII codes than that of packages you want to install earlier.

  For Hitachi program products:

  Hitachi program products have fixed package IDs. However, you can control the installation order by changing the cabinet IDs when packaging the products. Assign a cabinet ID that is alphanumerically lower in

ASCII codes than that of products you want to install earlier. Note that when you package products, you must create the cabinets keeping in mind the installation order.

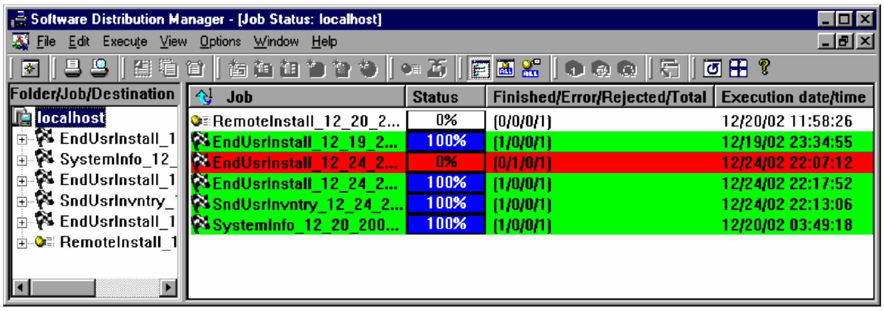
Also note the following points:

- If an installation date/time was specified as a schedule attribute of the package or if a job execution date/time was specified when the job was created, packages will not installed in the order in which Remote Installation Manager executes the jobs. Therefore, if you want to control the package installation order, do not specify an installation date/time or job execution date/time.
- A package in the background installation mode is installed before a package in the GUI installation mode. Therefore, if there are packages with different installation modes specified, execute different jobs to install the packages of the different installation modes separately. When you execute these jobs, execute one job first, and then execute the other job after the previous job has finished.
- If a job for which split distribution was specified was started and then a job was started by Remote Installation Manager, the latter job might be executed at the client before the split-distribution job.
- A job with **Distribute** specified is executed before a job that has been suspended.

2.9.8 Checking job execution status

You can check job execution status in the Remote Installation Manager's Job Status window. This window displays the status of executed jobs by folder or by job, in a hierarchical structure. The left-hand area displays the hierarchical structure of folders and jobs, while the right-hand area displays information about a selected item within the hierarchy.

Figure 2–49: Job Status window



Folder/Job/Destination

- localhost
  - EndUsrInstall_1
  - SystemInfo_12_
  - EndUsrInstall_1
  - SndUsrInvntry_
  - EndUsrInstall_1
  - RemoteInstall_1

Job	Status	Finished/Error/Rejected/Total	Execution date/time
RemoteInstall_12_20_2...	0%	(0/0/0/1)	12/20/02 11:58:26
EndUsrInstall_12_19_2...	100%	(1/0/0/1)	12/19/02 23:34:55
EndUsrInstall_12_24_2...	0%	(0/1/0/1)	12/24/02 22:07:12
EndUsrInstall_12_24_2...	100%	(1/0/0/1)	12/24/02 22:17:52
SndUsrInvntry_12_24_2...	100%	(1/0/0/1)	12/24/02 22:13:06
SystemInfo_12_20_200...	100%	(1/0/0/1)	12/20/02 03:49:18

Jobs displayed in colors can identify hosts that are targets of executed jobs and that are in statuses of concern. For example, if a job is displayed in red (indicating that an error has occurred), you can find the host in which the error occurred by tracing down its hierarchy level by level.

For details about how to check job execution status, see *8.4 Checking job execution status* in the manual *Administrator's Guide Volume 1*.

2.9.9 Handling after checking execution results

After checking job execution results in the Job Status window, you should delete the jobs that terminated normally. If you allow completed jobs to remain displayed, processing of jobs that are still executing might slow down or Remote Installation Manager might work slowly. If any jobs are waiting for transmission, or if there are jobs that resulted in a recoverable error, you can specify and re-execute those jobs. For details about handling after checking job execution results, see *8.5 Processing after checking job execution results* in the manual *Administrator's Guide Volume 1*.

If you are using a relational database, you can also view only the jobs that were completed successfully or only the jobs in which an error occurred. This allows efficient handling of jobs that require action. For details about how to display the jobs that require actions, see *8.4.7 Displaying jobs in a specified execution status* in the manual *Administrator's Guide Volume 1*.

2.10 Managing system configuration information

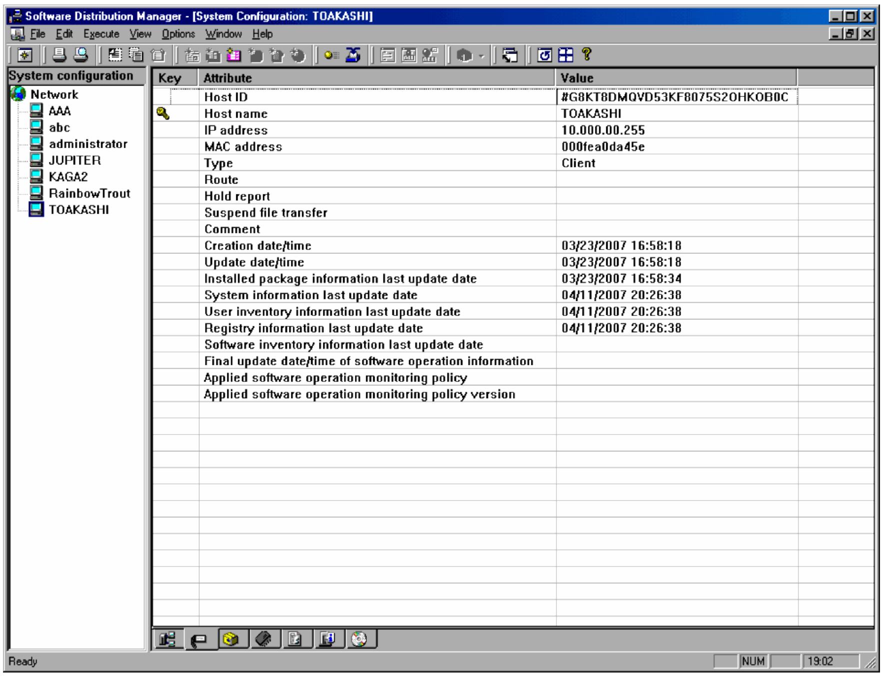
To use JP1/Software Distribution, at the managing server you must define the configuration of the distribution destinations (relay managers/systems and clients) and their addresses (host names and IP addresses). This information is called *system configuration information*. Once you set the system configuration information, the managing server will be able to identify each relay manager/system and client as a destination target of an executed job.

This section provides an overview of managing the system configuration information.

2.10.1 Creating system configuration information

You use Remote Installation Manager's System Configuration window to register and set system configuration information. The network hierarchy displayed in this window defines the actual routes used for job execution. The following shows the System Configuration window.

Figure 2–50: System Configuration window


Software Distribution Manager - [System Configuration: TOAKASHI]
File Edit Execute View Options Window Help
System configuration
Network
AAA
abc
administrator
JUPITER
KAGA2
RainbowTrout
TOAKASHI
Ready
NUM
19:02

Key	Attribute	Value
	Host ID	#G8KT8DMQVD53KF8075S20HKOB0C
🔍	Host name	TOAKASHI
	IP address	10.000.00.255
	MAC address	000fea0da45e
	Type	Client
	Route	
	Hold report	
	Suspend file transfer	
	Comment	
	Creation date/time	03/23/2007 16:58:18
	Update date/time	03/23/2007 16:58:18
	Installed package information last update date	03/23/2007 16:58:34
	System information last update date	04/11/2007 20:26:38
	User inventory information last update date	04/11/2007 20:26:38
	Registry information last update date	04/11/2007 20:26:38
	Software inventory information last update date	
	Final update date/time of software operation information	
	Applied software operation monitoring policy	
	Applied software operation monitoring policy version	

The hierarchical structure of the system is displayed in the left pane of the System Configuration window. The highest level of the hierarchy is indicated by the **Managing Server** icon (🌐). Double-clicking on a **Relay System** icon (▮) displays the hierarchy below the selected relay system and the respective **Client** icons (💻). In a system in which managing servers are configured in a hierarchy, **Relay Manager** icons (▮) are displayed under the managing server.

Host names or IP addresses are displayed next to the **Relay Manager**, **Relay System**, and **Client** icons.

If you select an item other than a client in the left pane, the right pane displays the configuration of the selected item's hierarchy.

For details about how to create system configuration information, see *8. Creating System Configuration Information and Destination Groups* in the *Setup Guide*.

2.10.2 Grouping clients

When you execute a job at the managing server, such as for remote installation, you specify the hosts that are the targets of the executed job (destinations). You can specify the individual destinations one by one from the system configuration information; however, this method is not efficient when there are many clients. JP1/Software

Distribution enables you to assemble clients into groups according to function regardless of the physical network configuration, and execute jobs for each group.

(1) Types of groups that can be created

You can create two types of groups, *host groups* and *ID groups*. Both types of groups can be created using any appropriate conditions, such as by department or by project. You can also register the same host into multiple host groups and/or ID groups so that the same PC belongs to multiple groups. For example, the same PC might belong to a department group and a project group. This enables you to manage destination hosts efficiently.

You can also use the groups being managed in Active Directory in the managing server as they are. In this case, there is no need to create a new group. When the directory information is acquired from Active Directory, groups are created automatically.

(a) Host group

Host groups constitute one of the methods for grouping hosts at the managing server. Because this method enables hosts to be grouped regardless of the system configuration, you can manage hosts by dividing them into hierarchical groups on the basis of appropriate conditions, such as by department or project. You can specify a name for each host group. Job execution is facilitated if you group hosts by section/department or by project and assign descriptive names to the groups.

When a host group is specified as the destination of a job, the job is executed on all clients that belong to that group.

(b) ID group

ID grouping is a method of setting in the managing server the group name and ID group managed by each relay manager/system (relay that manages the ID). Each client determines the group to which it belongs, and a client can belong to multiple ID groups.

You can also use a file at the managing server to register multiple clients in an ID group. Note that ID groups cannot be managed hierarchically.

When a job specifying an ID group as the destination (ID group job) is transferred to the relay that manages that ID, the relay executes the job on the clients that belong to the specified ID group.

When you create ID groups, the clients register themselves into appropriate ID groups; therefore, the administrator need not maintain individual clients at the job destinations. Even when additional clients are installed, if the clients register into ID groups, the jobs for the registered ID groups are executed automatically, thereby dynamically handling changes to the client configuration.

You can set passwords that allow clients to be registered into ID groups. This prevents a client from being registered into a restricted ID group.

(c) Directory information

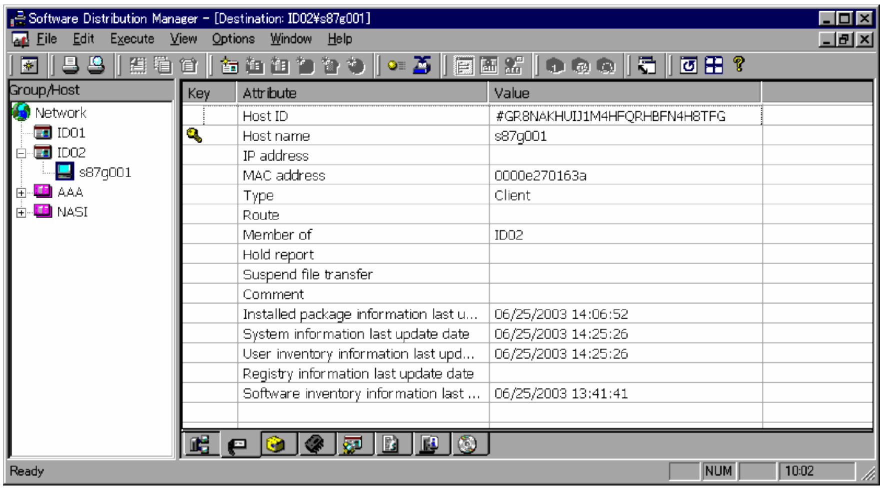
Directory information enables you to use the groups being managed in Active Directory in the managing server as they are. Consequently, you cannot create purpose-specific groups such as host groups or ID groups. However, directory information is convenient since you do not need to create a new group when you execute a job on a group being managed in Active Directory.

For details about the relationship between directory information and the system-configuration information on the managing server, see *2.10.3 Relationship between system configuration information and directory information*.

(2) How to group destinations

You use Remote Installation Manager's Destination window to set host groups and ID groups.

Figure 2–51: Destination window



Software Distribution Manager - [Destination: ID02¥s87g001]

Key	Attribute	Value
	Host ID	#GR8NAKHUIJ1M4HFQRHBFN4H8TFG
🔑	Host name	s87g001
	IP address	
	MAC address	0000e270163a
	Type	Client
	Route	
	Member of	ID02
	Hold report	
	Suspend file transfer	
	Comment	
	Installed package information last u...	06/25/2003 14:06:52
	System information last update date	06/25/2003 14:25:26
	User inventory information last upd...	06/25/2003 14:25:26
	Registry information last update date	
	Software inventory information last ...	06/25/2003 13:41:41

For details about how to create host groups, see *8.2 Creating host groups* in the *Setup Guide*.

For details about how to create ID groups, see *8.3 Creating ID groups* in the *Setup Guide*.

Reference note

> Since the directory information inherits the exact settings of Active Directory, there is no need to specify settings. You can view the directory information in the Directory Information window of Remote Installation Manager. For details on how to acquire directory information, see *3.4 Acquiring directory information* in the manual *Administrator's Guide Volume 1*.

The left pane of the Destination window displays the hierarchical structure of the groups. Double-clicking on an item in the left pane displays its lower hierarchies. The right pane displays information about a host that belongs to the group selected in the left pane.

The Destination window displays the following icons for groups:

- ▦ : Host group
- ▤ : ID group

In most cases, you use the Destination window to specify a client as a destination (target) of a job. You can also use the System Configuration window to specify this information, but it is not easy to identify hosts because this window displays hosts by their IP address or host name. In the Destination window, you can use groups to specify the hosts that are targets of executed jobs.

The system configuration information is used to manage the network configuration of clients, while host groups and ID groups are used to manage clients in groups. Evaluate the grouping criteria so that jobs will execute efficiently.

2.10.3 Relationship between system configuration information and directory information

Computer and user information collected from Active Directory is assigned to the managing server's system-configuration information and displayed in the Directory Information window. For the content displayed in the Directory Information window, see *1.4.7 Directory Information window* in the manual *Administrator's Guide Volume 1*.

How each information item is assigned is explained below.

- Computer information

  The DNS name in the computer information in Active Directory (or the computer name if there is no DNS name) is assigned to the host name in the managing server's system-configuration information.

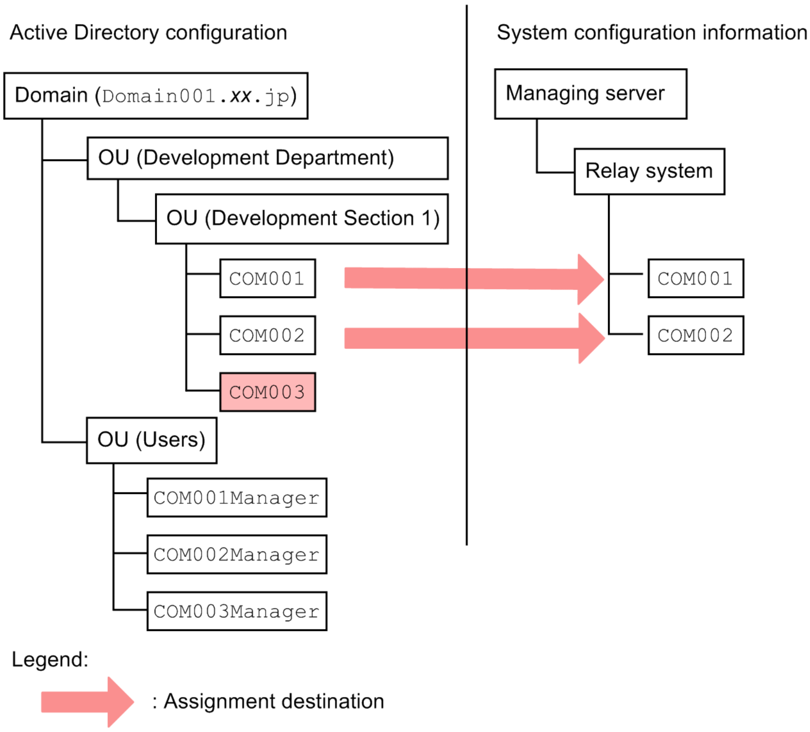
  Even when a DNS name is set up in Active Directory, computer information will not be assigned if there is no information that corresponds to the managing server's system-configuration information. Computer information that was not assigned will be reassigned if a change is made to the computer information in Active Directory, or to the managing server's system-configuration information the next time directory information is imported to the managing server.

- User information

  The user's LDAP indicator in Active Directory and the computer administrator's name in Active Directory are used for assignment. Note, however, that you can change the key information used for this assignment when you create a parameter file.

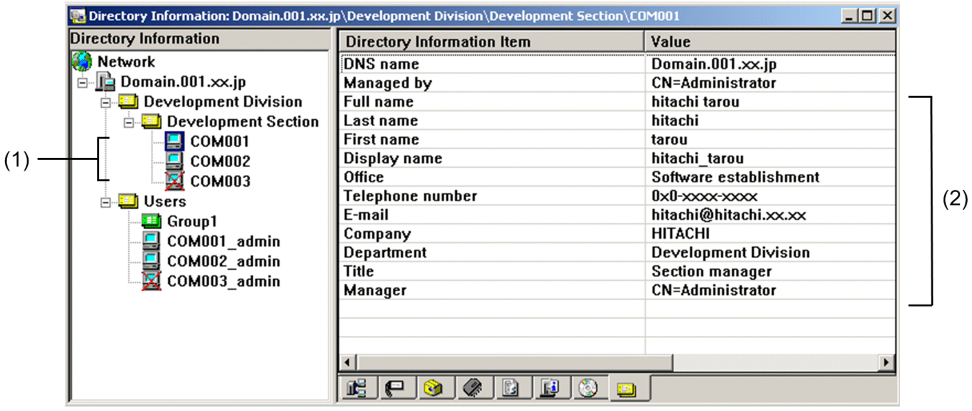
The following figure shows the relationship between Active Directory and the system-configuration information.

Figure 2–52: Relationship between the information managed in Active Directory and the system-configuration information



In this example, the COM001 and COM002 DNS names in the computer information collected from Active Directory match the host names in the system-configuration information, but there is no information that corresponds to COM003. Therefore, COM001 and COM002 are assigned, but COM003 is not. During this process, icons indicating whether or not items have been assigned to the system-configuration information are displayed in the Directory information window ((1) in Figure 2-52). Note that the user information is displayed as part of the computer information in the Directory information window ((2) in Figure 2-52), and is not displayed in the hierarchy information in the left pane. The following figure shows the Directory information window that corresponds to Figure 2-52.

Figure 2–53: Display example of the Directory information window



Directory Information: Domain.001.xx.jp\Development Division\Development Section\COM001

Directory Information

- Network
  - Domain.001.xx.jp
    - Development Division
      - Development Section
        - COM001
        - COM002
        - COM003
    - Users
      - Group1
      - COM001_admin
      - COM002_admin
      - COM003_admin

Directory Information Item	Value
DNS name	Domain.001.xx.jp
Managed by	CN=Administrator
Full name	hitachi tarou
Last name	hitachi
First name	tarou
Display name	hitachi_tarou
Office	Software establishment
Telephone number	0x0-xxxx-xxxx
E-mail	hitachi@hitachi.xx.xx
Company	HITACHI
Department	Development Division
Title	Section manager
Manager	CN=Administrator

(1): Icons indicating whether items have been assigned to the system-configuration information

(2): User information that is treated as part of the computer information

If multiple clients with the same name exist in the managing server's system-configuration information, and if that name matches the DNS name in the computer information in Active Directory (or the computer name if there is no DNS name), the first client found is assigned. If an unintended client is assigned, change it from the Directory information window. For details about how to change the assignment from the Directory information window, see *1.4.7 Directory information window* in the manual *Administrator's Guide Volume 1*.

Notes on assignment

- Directory information can be assigned to clients only. The relay manager and relay system are not assigned directory information.
- If you change the acquisition items or the key for assigning computers to users after the directory information has been imported, import all information again. If the assignment key has been changed, directory information is not imported until all information is imported.
- Offline machines and uninstalled hosts are not assigned to directory information.
- If the directory information collected from Active Directory contains computer information that has the same name as a UNIX client, it is assigned as follows:
  - When host ID is used as the working key for the entire JP1/Software Distribution system, the system identifies whether a client is using UNIX. Therefore, even if computer information with the same name is collected from the directory information, it is not assigned to a UNIX client.
  - When an IP address is used as the working key for the entire JP1/Software Distribution system, the system does not identify whether a client is using UNIX. Therefore, if computer information with the same name is collected from the directory information, it is assigned.
- If multiple users are available for assignment, the first user is assigned. If the user information was updated and another user was added to the new computer information available for assignment, the user information is overwritten with the updated information.

2.10.4 Maintaining system configuration information

In order to manage the system configuration, you must maintain the system configuration information. This subsection describes how to search for added hosts and register them into host groups, as well as how to search for hosts whose registration is duplicated and delete unneeded hosts. It also describes how to automatically delete hosts whose inventory information or software operation information has not been updated for a specified period of time, as well as hosts whose registration has been duplicated. Additionally, this subsection describes how to automatically assign new hosts added to the system configuration to appropriate host groups and ID groups on the basis of conditions created in advance.

(1) Manual maintenance of system configuration information

From the System Configuration window or Destination window of JP1/Software Distribution Manager, you can *search* for the destinations that satisfy a specified condition. There are three types of searches:

- Search using a name as the key value, such as a host group name or an ID group name
- Search using a date as the key value, such as a host registration date or the last update date for inventory information
- Search for *duplicate hosts* (hosts whose host IDs are different but their MAC address, IP address, or host names are the same)

You use these search functions to maintain the system configuration information, such as by copying the resulting hosts to the Destination window or deleting them from the system configuration information.

Note that you can execute searches by date and searches for duplicate hosts only from the System Configuration window.

For details about how to manually maintain the system configuration information using the search functions, see *9.1 Maintaining the system configuration information manually* in the *Setup Guide*.

(2) Automatic maintenance of system configuration information

You can maintain the system configuration information by automatically detecting unneeded hosts and deleting them from the system configuration information, host groups, and ID groups. This function is called *automatic system configuration maintenance*. There are two types of automatic system configuration maintenance:

- For a JP1/Software Distribution system that acquires inventory information periodically, there is a function that automatically deletes hosts whose inventory information has not been updated for a specified period time.
- For hosts whose host IDs are different but their MAC address, IP address, or host names are the same, there is a function that automatically deletes the hosts that have old update dates/times (retains only the host with the most recent update date/time).

The deletion processing occurs once a day starting at a specified time. Note that automatic system configuration maintenance does not delete the following hosts:

- Relay managers
- Relay systems
- Clients running on the same PC as a relay manager or relay system

The information that is automatically deleted when a client is deleted from the system configuration information is the same as in manual system configuration maintenance. For details, see *9.1.5 Deleting a host from the system configuration information* in the *Setup Guide*.

To use automatic system configuration maintenance, the JP1/Software Distribution system must satisfy the following conditions:

- During setup of JP1/Software Distribution Manager and JP1/Software Distribution Client (relay system), the **Link with system configuration modifications** check box is selected.
- Host IDs are used.

(3) Automatic maintenance of host groups

Methods of maintaining created host groups include editing them in the Destination window or importing data from a file. However, in a large-scale system with thousands of hosts, it is onerous for the system administrator to add and delete host groups frequently.

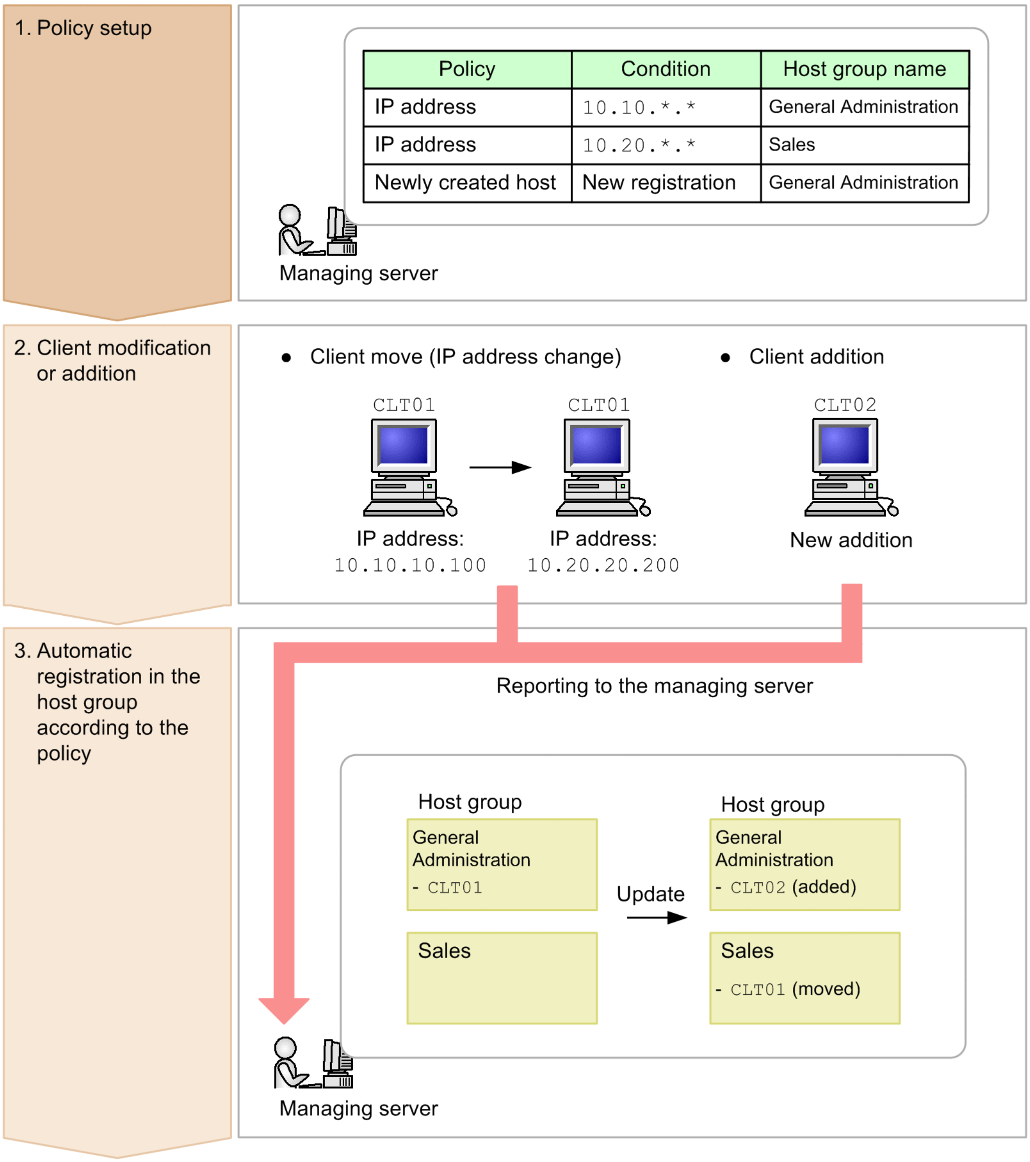
JP1/Software Distribution provides a facility that monitors the system configuration information to detect new hosts and moved hosts, and that adds the detected hosts to appropriate host groups on the basis of predefined grouping conditions (*policy*). This facility is called *automatic maintenance of host groups*. Such maintenance is performed at the following times:

- Upon notification of system configuration information from a client

- Upon notification of system information from a client
- Upon notification of user inventory information from a client

The following figure shows an overview of automatic maintenance of host groups.

Figure 2–54: Overview of automatic maintenance of host groups



Policy	Condition	Host group name
IP address	`10.10.*.*`	General Administration
IP address	`10.20.*.*`	Sales
Newly created host	New registration	General Administration

Maintenance of host groups can be performed at any time, not just upon notification of information from clients. Therefore, hosts registered in the system configuration information can be added to host groups in batches according to a created policy at any time (*Apply Policies to All Hosts*).

For details about how to apply policies to host groups, see *9.3.2 Applying policies to all host groups* in the *Setup Guide*.

You can also create policies from a file. By importing or exporting such files, you can back up or swap existing policies in and out. For details on creating a policy from a file, see *9.5 Creating a policy from a file* in the *Setup Guide*.

(4) Automatic maintenance of ID groups

As a rule, the client determines which created ID groups it will join. If you prefer that the managing server assign clients to groups, you can configure the system to register clients automatically based on whether they satisfy specified conditions. This is a more efficient and consistent way of registering clients into ID groups than performing such maintenance using the Destination window or by importing files.

The operations involved in setting conditions (a policy) for each ID group and automatically registering clients into ID groups is called *automatic maintenance of ID groups*.

The following two types of policies are available for automatic maintenance of ID groups:

- ID group registration associated with creation of a new client

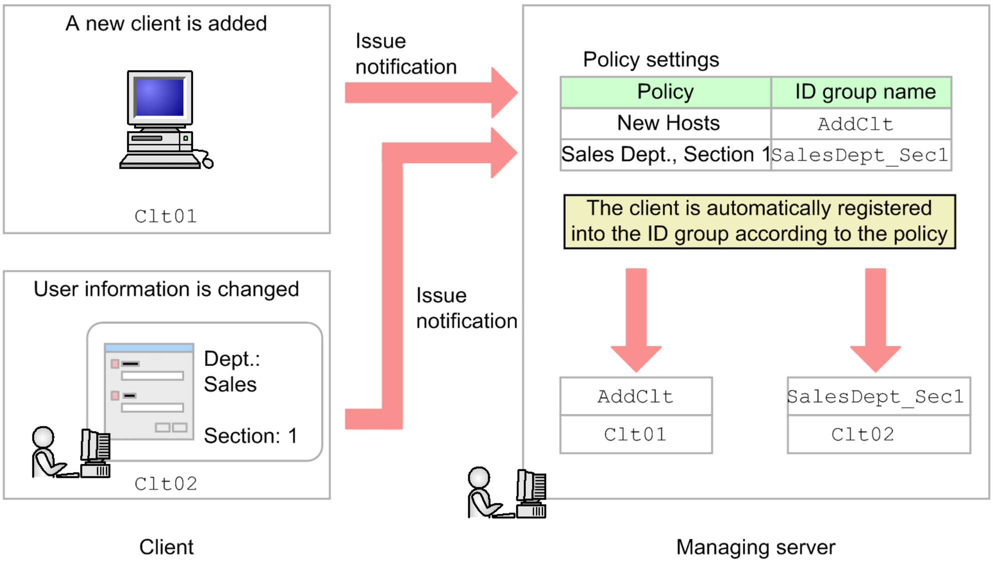
  This policy enables JP1/Software Distribution to automatically detect addition of a new client and then register it into appropriate ID groups.

  For JP1/Software Distribution to automatically register a newly added client, the **Automatically apply the system configuration** check box on the **System Configuration** page displayed during server setup must be selected.
- ID group registration based on user inventory information

  Whenever user inventory information is acquired, this policy enables JP1/Software Distribution to automatically register clients based on whether their user inventory information matches a policy.

The following figure provides an overview of automatic maintenance of ID groups.

Figure 2–55: Overview of automatic maintenance of ID groups



Policy	ID group name
New Hosts	AddClt
Sales Dept., Section 1	SalesDept_Sec1

For details about how to use automatic maintenance of ID groups, see *9.4 Automatic maintenance of ID groups* in the *Setup Guide*.

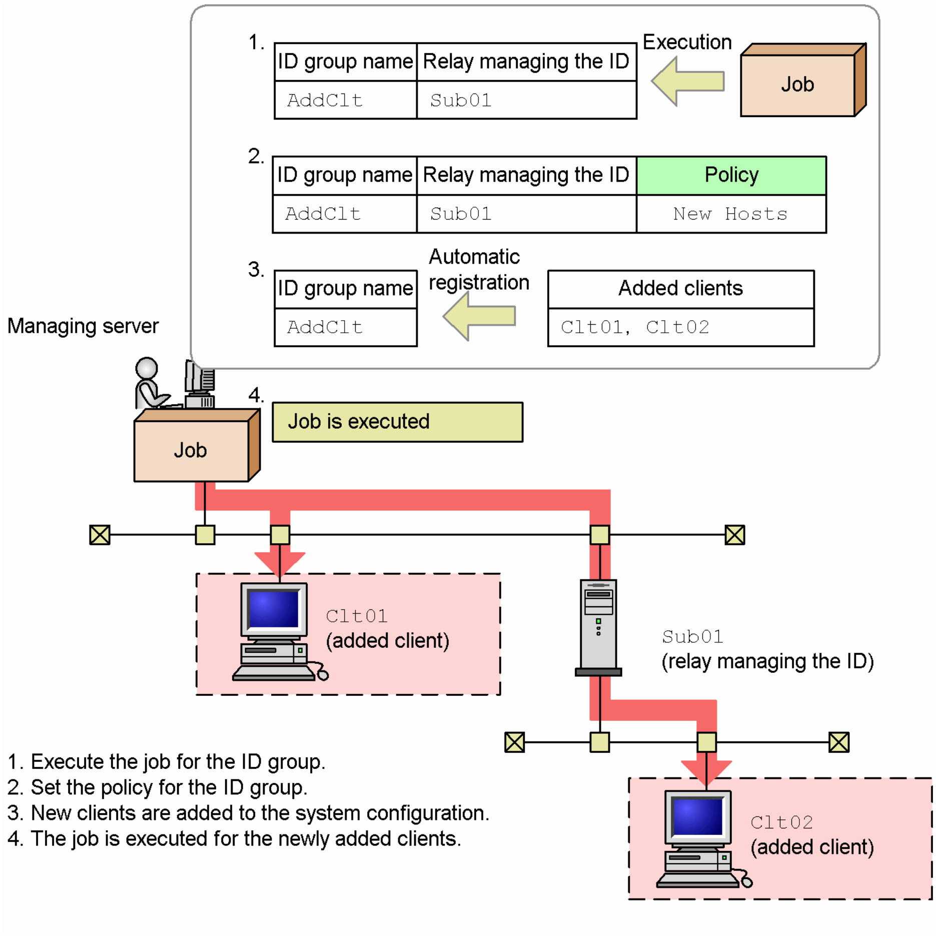
As with automatic maintenance of host groups, you can create a policy from a file (for details, see *9.5 Creating a policy from a file* in the *Setup Guide*).

Also note that before you use automatic maintenance of ID groups to execute a job, you must have already executed the job for that ID group.

For example, if there is a job that you always want to execute when you first install a client on a PC, by executing the job on that ID group beforehand, and then setting the newly added client to that ID group as a policy, you can configure JP1/Software Distribution so that it automatically executes the job for newly added clients.

The following figure shows the job flow when automatic maintenance of ID groups is used.

Figure 2–56: Job flow when automatic maintenance of ID groups is used



1. Execute the job for the ID group.
2. Set the policy for the ID group.
3. New clients are added to the system configuration.
4. The job is executed for the newly added clients.

(5) Automatic maintenance of directory information

To maintain directory information, acquire the latest information from Active Directory. Import the directory information whenever the Active Directory information is updated.

To acquire the directory information, execute the directory information acquisition command (`dcmadsync.exe`). By registering this command as a task in the Windows Task Scheduler, you can periodically import the latest information from Active Directory. You can also link with JP1/AJS to execute the command periodically.

2.10.5 Managing system configuration information deletion history

JP1/Software Distribution Manager can manage the deletion history so that you can determine when clients, relay systems, and relay managers were deleted from the system configuration information. Because the deletion history contains the system configuration information of deleted hosts, you can use the deletion history to restore hosts to the system configuration information.

To manage the system configuration information deletion history, the **Save deletion history** option must be selected at the time JP1/Software Distribution Manager is set up.

The host group, ID group, and inventory information of deleted hosts is not stored as historical data. Deletion history is not saved for hosts that were deleted in the batch mode when the system configuration information was created from a system configuration information file or for an offline folder.

For details about how to manage system configuration information deletion history, see *9.6 Managing the deletion history of system configuration information* in the *Setup Guide*.

2.10.6 Detecting hosts on which JP1/Software Distribution has not been installed

From the managing server, you can check the JP1/Software Distribution installation status by searching hosts in the network for those hosts on which JP1/Software Distribution is not installed.

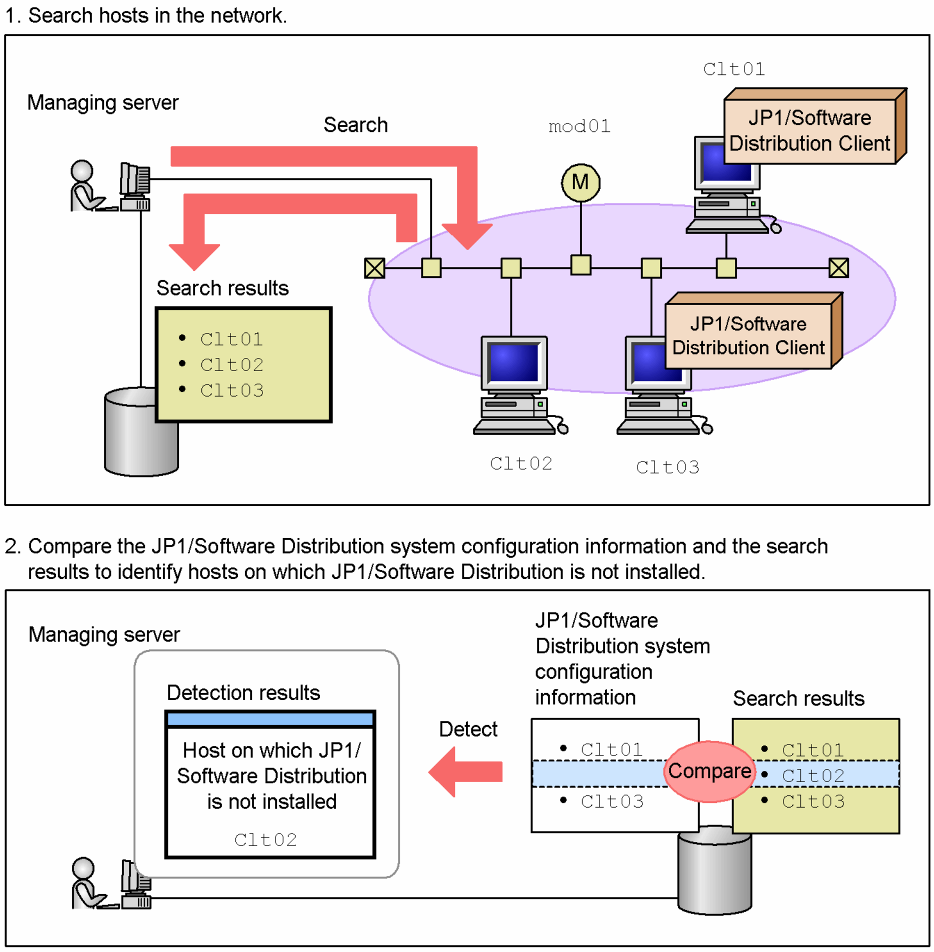
This function enables you to detect hosts in the local department network on which JP1/Software Distribution is not installed. By using the detection results to install JP1/Software Distribution on all hosts on which it is not already installed, you can place all computers in the local department network under the management of JP1/Software Distribution.

You can also use the detection results for the following purposes:

- To detect hosts that are not managed by JP1/Software Distribution, so that they can be disconnected from the network for security purposes
- To monitor hosts on which JP1/Software Distribution is not installed for a specified period of time, and then send them a warning email

The following figure provides an overview of the function for detecting hosts on which JP1/Software Distribution is not installed.

Figure 2–57: Overview of the function for detecting hosts on which JP1/Software Distribution is not installed


1. Search hosts in the network.

2. Compare the JP1/Software Distribution system configuration information and the search results to identify hosts on which JP1/Software Distribution is not installed.

Managing server
Search
mod01
M
Clt01
JP1/Software Distribution Client
Search results
• Clt01
• Clt02
• Clt03
JP1/Software Distribution Client
Clt02
Clt03
Managing server
Detection results
Host on which JP1/ Software Distribution is not installed
Clt02
Detect
JP1/Software Distribution system configuration information
• Clt01
• Clt03
Compare
Search results
• Clt01
• Clt02
• Clt03

A search for hosts (*host search*) uses SNMP (Simple Network Management Protocol). Therefore, in order to execute a host search and detect hosts on which JP1/Software Distribution is not installed, the router on the network must support SNMP.

As an alternative to executing a host search, you can also detect hosts on which JP1/Software Distribution is not installed by reading a *network configuration information file*, which is a CSV file containing information about the hosts in the network.

For details about how to detect hosts on which JP1/Software Distribution has not been installed, see *9.7 Detecting hosts on which JP1/Software Distribution is not installed* in the *Setup Guide*.

2.11 Outputting management information

You can output to a CSV file or to a printer the information managed by the managing server, such as inventory information, host attributes, package attributes, and job status.

This section provides an overview of how to output information managed by the managing server.

2.11.1 Outputting to a CSV file

You can output the information managed by the managing server (management information) to a CSV file. The CSV file can then be imported into another program, such as a spreadsheet. If you are using a relational database, you can specify an output range.

(1) How to output to a CSV file

There are two ways to output management information to a CSV file:

- CSV output utility

  The CSV output utility outputs management information in CSV format to a file. In the CSV Output Utility dialog box, you first set necessary information (such as output items and file destinations), and then execute the utility.

  For details about how to use the CSV output utility to output management information to a CSV file, see *9.1 Using the CSV output utility to output information to a file* in the manual *Administrator's Guide Volume 1*.

- `dcmcsvu` command

  The `dcmcsvu` command outputs inventory information to a CSV file or in parameter file format. You can execute this command on a managing server for which a relational database environment has been set.

  For details about the `dcmcsvu` command, see *4.5 dcmcsvu.exe (exporting to a CSV-formatted file)* in the manual *Administrator's Guide Volume 2*.

2.11.2 Outputting to a printer

You can print the information managed by the managing server. To do this, in the Print Setup dialog box, select the items that you want to print and then specify the necessary information.

For details about how to print management information, see *9.2 Printing managed information* in the manual *Administrator's Guide Volume 1*.

2.12 Totaling the inventory information according to work goals

To use inventory information collected by JP1/Software Distribution in actual work, you must total the information based on the work content, or create a list by filtering the collected information. With Asset Information Manager Subset, you can total the information or create a list according to your work goal.

By importing inventory information collected by JP1/Software Distribution into the database of Asset Information Manager Subset, you can obtain totals by linking to system information, software information, operation log data, and so on. Furthermore, you can also set up and manage information such as groups and installation locations for each client, separately from the inventory information. Moreover, a user who is assigned a division can manage the system information and software information of other groups.

Asset Information Manager Subset provides menu items matched to work goals. By using the totaling facility of Asset Information Manager Subset, you can use the information managed by JP1/Software Distribution in the following work:

- Managing devices

  You can register clients as devices and manage them.

  You can obtain the total numbers of various devices by using system information or software information as a condition, and you can obtain the total number of non-operating devices by obtaining the total number of devices on which inventory information has not been updated for a given period.

  You can use these total numbers to check the devices that are owned, and to check the network configuration.

- Managing software

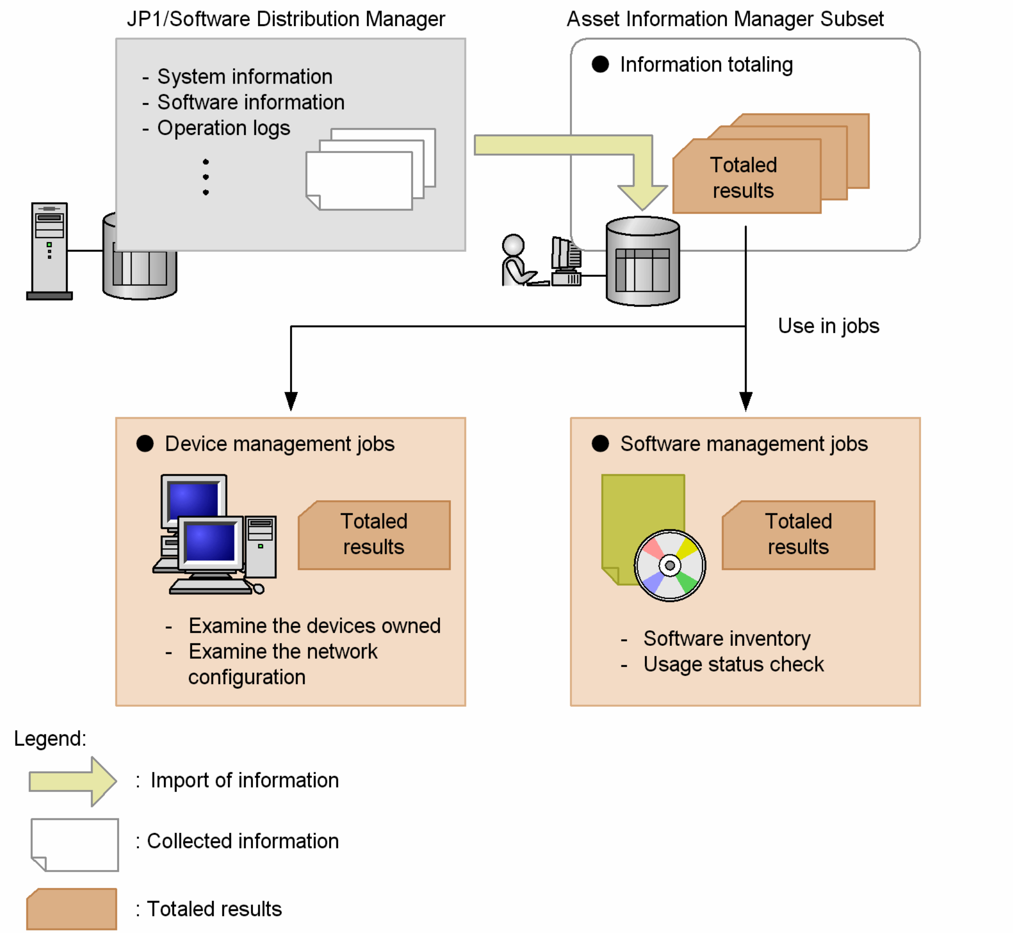
  You can search for devices in which a specific software product is installed, or examine whether software whose installation is prohibited has been installed. You can also examine the operation status of each software product.

  You can use these search results to check the software inventory and usage status.

The totaling and search operations that are executed from the individual operation windows of Asset Information Manager Subset can also be performed for each group and installation location.

The following figure provides an overview of totaling operations from Asset Information Manager Subset, according to work goals.

Figure 2–58: Overview of totaling operations according to work goals



For details about the operations that use Asset Information Manager Subset, see *10. Operating Asset Information Manager Subset* in the manual *Administrator's Guide Volume 1*.

2.13 Client facilities

A system equipped with facilities (that is, functionality) for receiving jobs executed at a managing server and for sending inventory information to the managing server is called a *client*. Clients include not only the PCs positioned at the bottom in the system configuration but also the relay managers and relay systems that relay jobs.

The following table lists the systems equipped with client facilities.

Table 2–37: Systems equipped with client facilities

System	Program
Relay manager#	JP1/Software Distribution Manager
Relay system	JP1/Software Distribution Client
Client	

#: The server component is installed. For details about the server component, see *1.1.2 Organization of components* in the *Setup Guide*.

This section describes the client facilities for the following tasks:

- Installing distributed software
- Reporting inventory information by job execution
- Displaying messages sent from the administrator
- Reporting inventory information from clients
- Displaying client information
- Reporting hardware failures

2.13.1 Installing distributed software

When an *Install package* job is executed on the managing server, the client automatically downloads the specified software and installs it on its own system. Because software downloading and installation are both executed automatically, the client normally does not control what is installed or when it is installed.

However, if automatic job execution is not appropriate for the operation of the client user, the two alternatives indicated below in (1) and (2) are available. In addition, alternative (3), in which the client's user selects and installs software manually, is also available.

(1) Stopping the client

Starting Windows automatically starts the client. By using *Client Manager*, you can also shut down the client manually. In addition, a JP1/Software Distribution Client can be set up to make the client non-resident.

A client that has not been started or is non-resident cannot receive jobs from the managing server. Therefore, in such a situation, software installation cannot be executed. However, a client's user can execute the installation job by choosing the **Execute Job Backlog** icon at a convenient time. For details about the handling when stopping of clients is involved, see *11.1.2 Client startup and job execution* in the manual *Administrator's Guide Volume 1*.

(2) Managing the job execution timing

The job execution time, such as for downloading or installing a package, is normally determined by the higher server (the managing server) and is transparent to the client. The client merely waits for the package to be transferred from the managing server or for automatic installation of the software.

In this mode, however, an installation job might activate suddenly in the midst of processing at the client and cause problems. The client user can forcibly prevent a job from being executed and specify that the job be executed at the user's convenience.

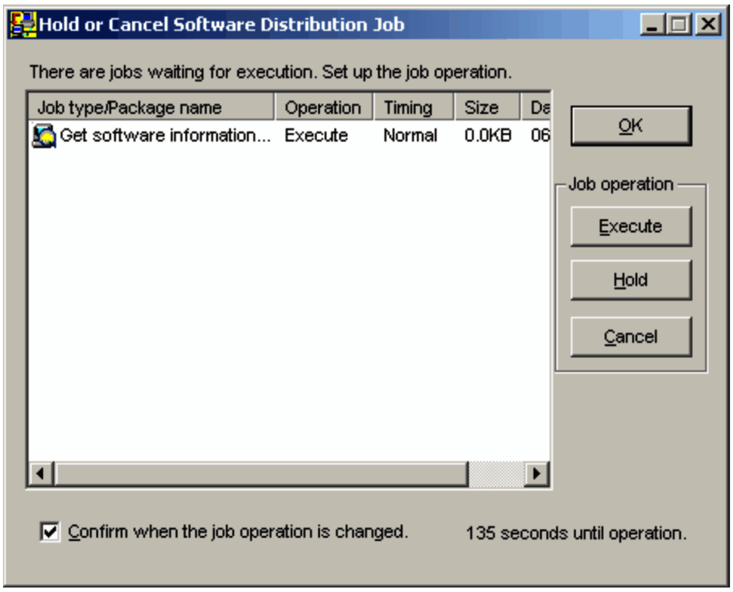
The client can use the following two methods to manage job execution timing:

- Using the job hold and cancellation facility
- Executing a job at an arbitrary time

(a) Using the job hold and cancellation facility

A method for preventing unilateral job execution by a higher server is the *job hold and cancellation facility*. When a job is transferred from a server, this facility displays the Hold or Cancel Software Distribution Job dialog box so that you can choose whether to execute the job. If you do not want to execute the job immediately, you can hold it for later execution or you can cancel it.

Figure 2–59: Hold or Cancel Software Distribution Job dialog box


Hold or Cancel Software Distribution Job

There are jobs waiting for execution. Set up the job operation.

Job type/Package name	Operation	Timing	Size	Da
Get software information...	Execute	Normal	0.0KB	06

☑ Confirm when the job operation is changed.

135 seconds until operation.

Use of the *job hold and cancellation facility* is specified in the setup process for the client by selecting the **Confirm jobs before execution** check box on the **Job Options** page.

The following two types of jobs can be held or canceled, provided that no execution date (package installation date or job execution date) is specified:

- *Install package* jobs in the GUI installation mode
- *Get software information from client* jobs with **While client is running** specified

For details about how to hold and cancel jobs, see *11.3.1 Holding or canceling a job* in the manual *Administrator's Guide Volume 1*.

(b) Executing a job at an arbitrary time

You can have JP1/Software Distribution Client (client) execute jobs at any time by choosing the **Execute Job Backlog** icon.

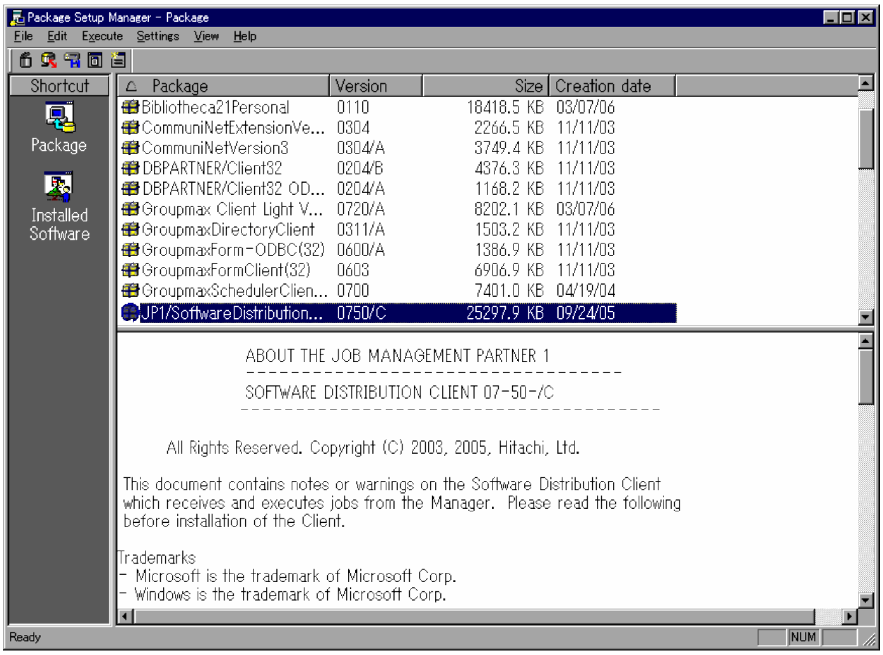
When the **Execute Job Backlog** icon is chosen, the client connects to the higher system to perform polling to determine if there are any unprocessed jobs. If such jobs exist, the client executes them. You can also use the **Execute Job Backlog** icon to execute jobs that were held temporarily by the job hold and cancellation facility.

You can also specify in the setup that the client is not to start automatically whenever the system starts. When this specification is in effect, the client user can execute a job at their convenience by choosing the **Execute Job Backlog** icon.

(3) Installing by selecting the software

Software distributed by the managing server in a *Send package, allow client to choose* job is not installed automatically. Instead, it arrives in a status in which its installation is permitted. The client user evaluates the need at the local system for the software items and decides whether to install them. To display a list of software programs that can be installed and then select and install the desired software, use Package Setup Manager, which is a client subcomponent.

Figure 2–60: Package Setup Manager window


Package Setup Manager - Package
File Edit Execute Settings View Help
Shortcut
Package
Installed Software
Ready
NUM

Package	Version	Size	Creation date
Bibliotheca21Personal	0110	18418.5 KB	03/07/06
CommuniNetExtensionVe...	0304	2266.5 KB	11/11/03
CommuniNetVersion3	0304/A	3749.4 KB	11/11/03
DBPARTNER/Client32	0204/B	4376.3 KB	11/11/03
DBPARTNER/Client32 OD...	0204/A	1168.2 KB	11/11/03
Groupmax Client Light V...	0720/A	8202.1 KB	03/07/06
GroupmaxDirectoryClient	0311/A	1503.2 KB	11/11/03
GroupmaxForm-ODBC(32)	0600/A	1386.9 KB	11/11/03
GroupmaxFormClient(32)	0603	6906.9 KB	11/11/03
GroupmaxSchedulerClien...	0700	7401.0 KB	04/19/04
JP1/SoftwareDistribution...	0750/C	25297.9 KB	09/24/05

```
                ABOUT THE JOB MANAGEMENT PARTNER 1
                ----------------------------------
                SOFTWARE DISTRIBUTION CLIENT 07-50-/C
               ---------------------------------------

       All Rights Reserved. Copyright (C) 2003, 2005, Hitachi, Ltd.

 This document contains notes or warnings on the Software Distribution Client
 which receives and executes jobs from the Manager.  Please read the following
 before installation of the Client.

Trademarks
- Microsoft is the trademark of Microsoft Corp.
- Windows is the trademark of Microsoft Corp.
```

A client for which no user information has been set might not be able to use Package Setup Manager depending on the server settings. Note that Package Setup Manager cannot be shared among multiple non-Administrator users.

For details about how to use Package Setup Manager, see *11.4 Using Package Setup Manager* in the manual *Administrator's Guide Volume 1*.

2.13.2 Reporting inventory information by job execution

To keep track of the status of clients, the managing server executes as necessary jobs that collect client information. The following is a description of the types of jobs that are executed to collect information from clients, and the action that each client takes in response to such a job.

Get system information from client job

Upon receipt of this job, the client automatically reports hardware-related information (the type of OS being used and the amount of available hard disk space) to the higher system.

Get software information from client job

Upon receipt of this job, the client searches for all the software programs that are installed on its system and reports the resulting information to the higher system.

This software-search process is executed automatically. During this processing, on the client's screen you can display a message dialog box that indicates that processing has started. When the client receives the job, you can use the Hold or Cancel Software Distribution Job dialog box to specify whether the job is to be executed immediately.

Get user inventory information job

When this job executes, the client screen displays dialog boxes containing input fields that were set up by the managing server. The client user enters information (user inventory information) into these fields. A dialog box for entering information is displayed automatically at set intervals specified during setup. The client user can specify display of this dialog box in order to modify entered values. For details about how to enter user inventory information, see *11.5 Entering user inventory information* in the manual *Administrator's Guide Volume 1*.

2.13.3 Displaying messages sent from the administrator

When a *Report message* job from the managing server is executed, the client system displays messages specified by the Administrator.

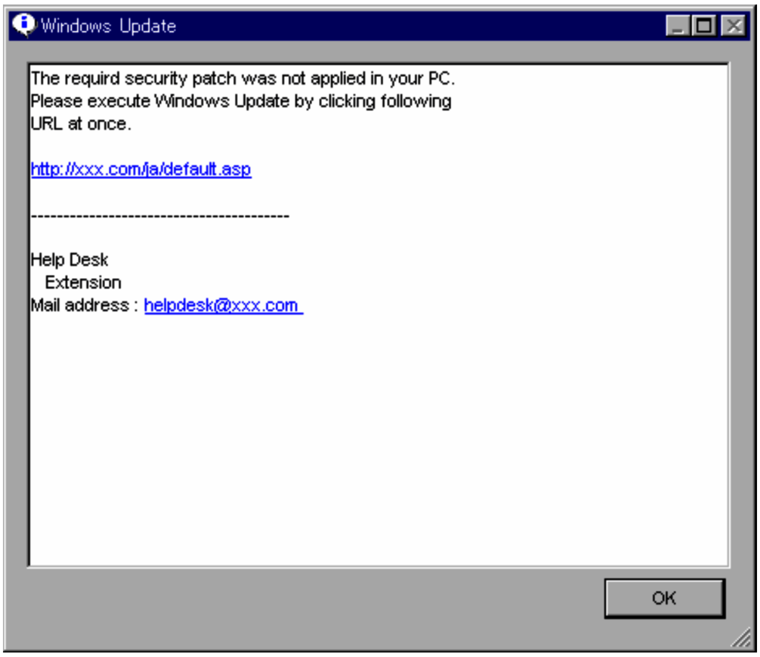
This section explains how to check the displayed messages and provides notes on displaying messages.

(1) Checking the displayed messages

Messages from the administrator are displayed in a message dialog box. Up to 10 message dialog boxes can be simultaneously displayed according to the order in which the client receives the messages.

The administrator can send messages in either text format or HTML format. Figure 2-61 shows how a text message is displayed, and Figure 2-62 shows how an HTML message is displayed.

Figure 2–61: Text message

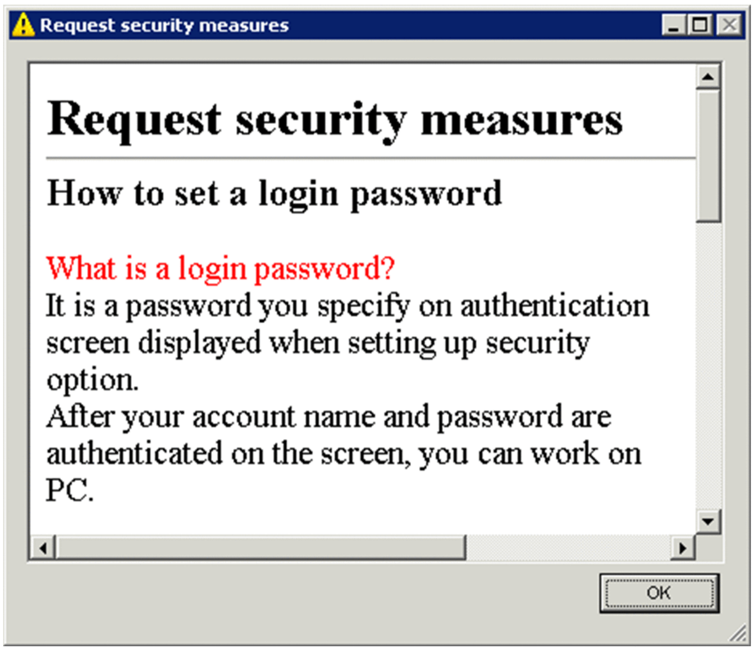


The requird security patch was not applied in your PC.
Please execute Windows Update by clicking following
URL at once.

http://xxx.com/ja/default.asp

Help Desk
  Extension
Mail address : helpdesk@xxx.com

Figure 2–62: HTML message



Request security measures

How to set a login password

What is a login password?
It is a password you specify on authentication screen displayed when setting up security option.
After your account name and password are authenticated on the screen, you can work on PC.

The title bar of the message dialog box displays an icon and a message title. The meaning of each icon is explained as follows.

- ⓘ : Information
- ⚠ : Caution (mildly critical information)
- ✖ : Warning (highly critical information)

If a URL is provided inside the message text, clicking the linked area starts the default browser, enabling you to browse the linked Web page. If an email address is provided, clicking it starts the default email program, enabling you to create email addressed to that address.

From the menu displayed by right-clicking the message text display area, you can copy a selected character string or select all character strings in the message text.

After you have checked the message, choose **OK** to close the message dialog box.

Note that clients running version 08-00 or earlier cannot display HTML messages. If you send an HTML message to such a client, the HTML tags will appear as text-format character strings.

For a client to display HTML messages, it also must have Microsoft Internet Explorer 4.0 or later installed.

(2) Notes on displaying messages

The following notes apply to displaying messages:

- Immediately after a client is installed or updated, the PC may have to be restarted in order to display messages.
- If you log off or shut down a client while it is displaying the message dialog box, the same message dialog box is displayed when you log onto the client the next time.
- If **Run the client with non-Administrator user permissions** is not selected on the **Security** page of the Client Setup dialog box, messages are displayed only while the user who installed the client is logged on.
- If the client's OS is Windows NT and the **Client starts automatically at system boot** check box is cleared on the **Default Running Status/Polling** page in the client setup, the message dialog box is displayed only immediately after a logon.

- For clients that use the Quick User Switching Feature of Windows 8, Windows Server 2012, Windows 7, Windows Server 2008 or Windows Vista, the following notes apply when a message is displayed by more than one user:
  - If a user who is viewing a message clicks the **OK** button, that message is not displayed for users who log in subsequently.
  - If a user who is viewing a message clicks the **OK** button, an error is displayed if a user who was already logged in clicks a link in the message.
- If the client's OS is Windows Server 2003 or Windows XP and similar taskbar buttons are grouped in the taskbar properties, executing an operation to close the group in the message dialog box does not close the message dialog box.
- The following elements are not supported in HTML messages:
  - MHTML
  - DHTML
  - Frames
  - Images, such as JPEG files and GIF files, that are stored as different files from the HTML file

2.13.4 Reporting inventory information from clients

To acquire inventory information, at the managing server you execute a *Get user inventory information* job. However, executing this job in a large-scale system places a heavy load on the network.

Instead of using this managing server-based approach, you can use a client-based notification method for reporting inventory information. The client-based method notifies the managing server whenever there is a change in the client's inventory information. This method means that the managing server acquires information only when necessary and only from the clients who have information to report, thus reducing the load on the network.

There are four methods of client-initiated reporting of inventory information.

Table 2–38: Methods of client-initiated reporting of inventory information

Type of change in the client	Means of notification	Timing of notification
Change in the user inventory information	Reporting from the Software Distribution - Update User Information dialog box	When the user chooses to report the information
Change in installed software	Package Setup Manager	When the user chooses to report the information
Update to the inventory information	When a connection is established with the managing server	Automatic reporting in the background
Addition of new clients to the JP1/Software Distribution system	When the system configuration is registered automatically	Automatic reporting in the background

The inventory information is reported only to the higher distribution manager to which the client is connected. If there are multiple higher destinations, the information is reported to the distribution manager only.

If a relay manager/system placed between the central manager (JP1/Software Distribution Manager) and clients uses JP1/Software Distribution Manager or JP1/Software Distribution SubManager for Windows 06-01 or an earlier version, the clients cannot report their inventory information to the central manager. Therefore, if you perform client-initiated reporting of inventory information, make sure that the version of the Windows relay manager/system is 06-51 or later. If the updated inventory information is to be reported automatically, make sure that the version of the relay manager/system is 07-00 or later.

(1) Reporting from the Software Distribution - Update User Information dialog box

If there is a change to the client's user inventory information, the user can report the change to the managing server at any time from the Software Distribution - Update User Information dialog box.

When user inventory information is reported, the system information (system information and registry information) is also reported to the managing server. The information that is reported from the Software Distribution - Update User Information dialog box is the same as when a *Get system information from client* job is executed.

Note that Software Distribution Workstation (relay system) of a version earlier than 03-00 does not manage user inventory information. Report files might accumulate on the disk, resulting in a space shortage. Therefore, if you use the Software Distribution - Update User Information dialog box to report inventory information to Software Distribution Workstation, make sure that the Software Distribution Workstation version in use is 03-00 or later.

For details about how to report inventory information from the Software Distribution - Update User Information dialog box, see *11.6.1 Using the Software Distribution - Update User Information dialog box to report inventory information* in the manual *Administrator's Guide Volume 1*.

(2) Using Package Setup Manager to report inventory information

If user software information changes, you can report the inventory information from the Installed Software window of Package Setup Manager.

The software information reported by Package Setup Manager includes all software information collected from the clients regardless of the software displayed in the Installed Software window.

For details about how to report software information from Package Setup Manager, see *11.6.2 Using Package Setup Manager to report inventory information* in the manual *Administrator's Guide Volume 1*.

(3) Automatic reporting of updated inventory information

If specific inventory information is updated (such as information about the installation of new software and application of patches), the inventory information can be reported automatically to the managing server when connection is established with the managing server by job execution or polling.

You can use this facility when the version of both the managing server and the client is 07-50 or later. If you are using a relay system, use one of version 07-00 or later.

For details about the settings for reporting updated inventory to the managing server, see *11.6.3 Automatic reporting of updated inventory information* in the manual *Administrator's Guide Volume 1*.

(a) Inventory information to be reported

This facility monitors inventory information that is useful for security management, such as OS information, patch information, and information on anti-virus products.

When inventory information being monitored is updated, system and software information, including the updated inventory information, is reported.

The table shows the types of inventory information that are monitored for updates and the inventory information that is reported.

Table 2–39: Inventory information monitored for updates and the inventory information that is reported

Inventory information monitored for updates	Inventory information that is reported
Host name	• System information • Registry inventory information monitored for updates and inventory information that is reported • Software information • Software listed in **Add/Remove Programs** or in **Add or Remove Programs**. • Hitachi program products • Applied patches#2 • Unapplied patches#2 • Information about Microsoft Office products • Information about anti-virus products • Standard search list • User inventory information
MAC address	
The following OS information: • OS version • OS sub-version • OS build number	
The following IE information: • Internet Explorer version • IE patch information	

Inventory information monitored for updates	Inventory information that is reported
The following security-related information: • Guest account • Days since password was last updated • Time-unlimited password • Automatic logon setting • Shared folders • Restriction on anonymous connections • Screensaver • Password protection for screensaver • Power-on password • Windows firewall setting • Windows automatic updates • Unnecessary services • BitLocker-based encryption information • HIBUN FDE-based encryption information	• System information • Registry inventory information monitored for updates and inventory information that is reported
Programs listed in **Add/Remove Programs**	• Programs listed in **Add/Remove Programs** • Hitachi program products • Installed patches#2 • Uninstalled patches#2
Hitachi program products#1	
Applied patches	
Database files for WUA	
Database files for MBSA 1.2.1	
Information about Microsoft Office products#3	Information about Microsoft Office products
Information about anti-virus products#3	Information about anti-virus products

#1

If a Hitachi program product is uninstalled, inventory information is not automatically reported. To check for uninstallation of Hitachi program products from a managing server, you must execute a job for collecting software information.

#2

To automatically report information about installed and uninstalled patches, various settings must be specified so that the clients can detect the patch information. For details about the settings for detecting patch information, see *7.2.2 Distributing the files necessary for detection using WUA* or *7.2.3 Distributing the files necessary for detection using MBSA 1.2.1* in the manual *Administrator's Guide Volume 1*.

#3

If the client's OS is Windows NT 4.0 or Windows 98, Windows Scripting Host must be installed on the client. If it is not installed, you can download Windows Script 5.6 from Microsoft Corporation's web site and install it.

Inventory information is also reported to the managing server whenever any of the following events occur. In this case, inventory information, including all of the inventory information listed on the right side of Table 2-39, in addition to the software information distributed by JP1/Software Distribution, is reported.

- A new client is installed.
- The connection destination is changed in client setup.
- A higher system switches from operation that is not based on host IDs to one that is based on host IDs.

(b) Notes

Note the following about automatic inventory information reporting:

- If inventory information is reported automatically, information is reported every time a client's inventory information is updated, and might place irregular burdens on the server or network environment. Therefore, if it is necessary to avoid irregular burdens on the server or network environment, do not select automatic reporting of inventory information. Instead, execute a job for collecting inventory information.

- If inventory information is reported automatically and JP1/Software Distribution SubManager for UNIX that is earlier than version 07-00 is used as a relay manager, unnecessary files might accumulate in JP1/Software Distribution SubManager for UNIX and might cause a disk space shortage.
- Software information about Hitachi program products collected and managed using a software search list might be different from the software information that is reported automatically. Therefore, to collect and manage software information about Hitachi program products, use either a software search list or automatic reporting of inventory information, but not both.
- If the version of a higher system is changed, execute both **Search for Microsoft Office products** and **Search for anti-virus products** in a *Get software information from client* job for the client from which inventory information is automatically reported. If you do not execute this job, information might not be correctly reported.
- If a client's connection destination was changed to another higher system and then switched back to the original connection destination, information about the software that was uninstalled while the client was connected to the other higher system might not be reported when the original connection is restored.
- If WUA is used to detect patch information, WUA checks for any change to the patch information when connection is established with the managing server. Because it might take some time for this detection by WUA, note the following:
    - If polling is enabled and the polling interval is set during client setup to be short, an excessive workload might affect the client. To avoid this, specify as large a value as possible for the polling interval on the **Default Running Status/Polling** page during client setup.
    - If polling is enabled and the first time polling is to be performed is set during client setup to **Before the client starts**, it might take some time to start the programs registered in the `Software Distribution Client Startup` folder.
    - If WUA is used to detect patch information, we recommend that you use a PC with high CPU performance, such as a PC with a processor having a clock speed of at least 2.0 GHz or a PC with multiple processors.

(4) Reporting during automatic registration of system configuration

Whenever clients are added to the JP1/Software Distribution system by adding machines, installing new clients, or moving clients within the network, the inventory information can be reported automatically to the managing server.

For details about the settings for reporting inventory information to the managing server when clients are added, see *11.6.4 Reporting inventory information at automatic registration of system configuration* in the manual *Administrator's Guide Volume 1*.

(a) Reporting timing

Inventory information is reported to the managing server at the following times:

- When a new client is installed.
- When the connection destination is changed in client setup.
- When the higher system switches from operation that is not based on host IDs to one that is based on host IDs.

(b) Inventory information that is reported

The following inventory information is reported:

- System information (system information and registry information)
- Software information listed in **Add/Remove Programs**

Note that Software Distribution Workstation (relay system) of a version earlier than 05-21 does not manage registry information. Due to reporting of registry information, unneeded files might accumulate on disk, resulting in a space shortage. Therefore, if you report inventory information to Software Distribution Workstation when the system configuration is registered, make sure that the Software Distribution Workstation version in use is 05-21 or later.

2.13.5 Displaying client information

A client user can use *Local System Viewer* to determine the local PC's status.

Using Local System Viewer, you can display the local PC's hardware and software information. For hard disks and memory, the total sizes and current usage statuses are graphically displayed, enabling you to determine whether they are running normally. The client user can view this information locally. For details about how to use Local System Viewer, see *11.7 Using Local System Viewer* in the manual *Administrator's Guide Volume 1*.

2.13.6 Reporting hardware failures

The client has a facility for monitoring hard disks and memory based on preset conditions and for reporting alerts when a failure is detected. This facility is called *system monitoring*. The information displayed on Local System Viewer is based on the settings specified here.

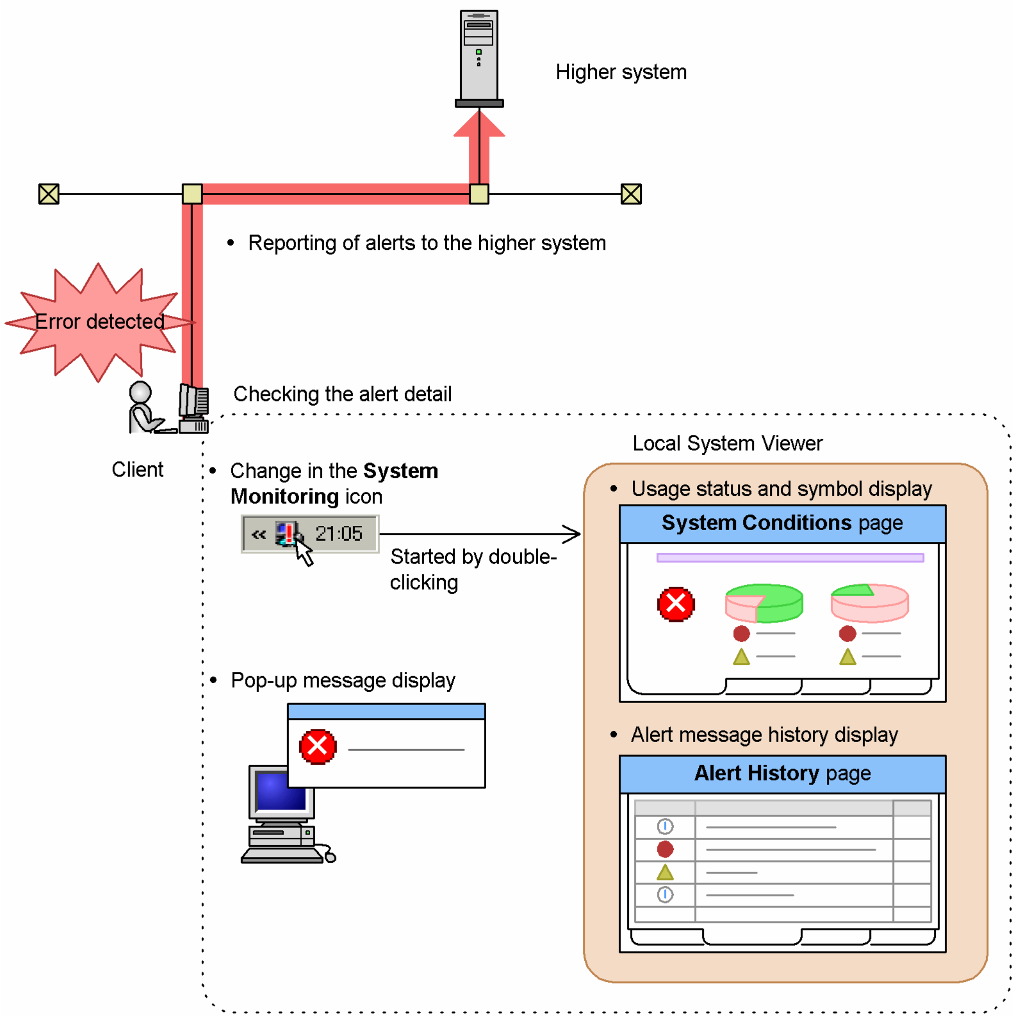
Alerts can be output using the following five methods:

1. Displaying the usage conditions on the **System Conditions** page of Local System Viewer (default)
2. Displaying alert messages on the **Alert History** page of Local System Viewer (default)
3. Reporting an alert by displaying a pop-up message
4. Reporting an alert to a higher system
5. Reporting an alert by changing the **System Monitoring** icon

If you use methods 1 and 2 only, you will miss any alert issued while Local System Viewer is not running. Therefore, to instantly recognize any alert issued, a client can use the **System Monitoring** icon ( ). This icon is displayed in the task bar notification area and acts as an interface for smoothly using the system monitoring facility. While this icon is displayed, changes to the icon inform you that an alert that has been issued. Double-click this icon to start Local System Viewer and check the alert details.

The following figure provides an overview of alert notifications.

Figure 2–63: Overview of alert notifications


Higher system
• Reporting of alerts to the higher system
Error detected
Checking the alert detail
Client
Local System Viewer
• Change in the **System Monitoring** icon
21:05
Started by double-clicking
• Usage status and symbol display
System Conditions page
• Pop-up message display
• Alert message history display
Alert History page

You can specify details for alert notification methods and system monitoring targets in advance. For example, you can choose to notify a higher system only and not to display a pop-up message, or you can choose to monitor only the hard disk and not to report any alerts about memory.

To use these facilities, you must change the default settings during client setup. For details about the mechanism of system monitoring and how to specify the settings, see *11.8 Reporting an alert based on system monitoring* in the manual *Administrator's Guide Volume 1*.

For details about how to check reported alerts at the higher system, see *7.4 Checking alert information reported from clients* in the manual *Administrator's Guide Volume 1*.

2.13.7 Notes on using a client

This section provides notes related to using a client.

If the client's OS is Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, or Windows Vista, also see *A.6. Notes on using the Windows 8/2012/7/2008/Vista Edition of JP1/Software Distribution Client* in the manual *Administrator's Guide Volume 2*.

- Notes on using a client in the terminal service environment

  To use a client in the terminal service environment of Windows Server 2003 or Windows 2000, use it on a local console. The terminal service is not supported. For limitations on using a client at a local console and how to perform remote installation, see *B. Using JP1/Software Distribution Client (Client) on a Terminal Server* in the *Setup Guide*.

- Notes on using other companies' software

  While other companies' software is being installed in a remote installation, you must not perform window operations on the active installer. If you do perform such an operation, the installer might freeze.

- Notes about password locking of clients

  If the client PC is locked by means of a logon password (a dialog box requesting entry of **Ctrl** + **Alt** + **Delete** keys is displayed), software that requires the user's intervention in the GUI installation mode is not installed remotely because no response can be made. Hitachi program products supporting remote installation are installed because they do not require user intervention during remote installation.

- Client cannot be started or takes too long to start

  In the following cases, the client (or relay system) might not be able to start or will take too long to start:

  1. The higher system to which the client is to be connected has not started.
  2. The client is transmitting the results of a job that it was unable to process during the previous startup.
  3. On the **Default Running Status/Polling** page in Setup, the **Start polling when the client program starts** option is selected and the system start polling frequency is specified as **Before the client starts**.

  In case 1, the client starts when the higher system to which it is to be connected starts.

  In case 2 or 3, the client starts when transmission of job results or polling of the higher system is completed.

- What to do when the installation process hangs

  If a user program that was started during remote installation processing freezes, or the user program termination code notification interface is incorrect in the GUI installation mode, the remote installation process also hangs. If this happens, restart the client PC.

- Notes on split distribution

  Split distribution in an environment where the client is nonresident and does not conduct polling:

  > If no client is resident, a job waiting for split distribution is run when you start **Execute Job Backlog**. After a split distribution job has been executed, if you choose **Execute Job Backlog** after the specified distribution interval, the next split distribution job is executed.
  >
  > If the client does not conduct polling, split distribution is only started by the server. If startup fails, you must use **Execute Job Backlog** to execute any waiting split distribution job as if no client were resident.
  >
  > In an environment where the client is nonresident and does not conduct polling, split distribution starts at the same time as **Execute Job Backlog**. Therefore, you should avoid split distribution in such an environment.

  Hold cancellation and split distribution:

  > In the case of split distribution, after all split jobs have been transferred, the Hold or Cancel Software Distribution Job dialog box is displayed asking the user whether to perform installation. Choosing **Execute** starts installation and choosing **Hold** delays installation. Installation is not performed until the user responds. Clicking **Cancel** deletes jobs without installation. When you retry canceled jobs, jobs are re-executed from the beginning of split distribution.

  Split distribution specified with an installation date/time:

  > If an installation date/time is specified for a split distribution and the installation time comes during a split distribution, installation will begin after all the split jobs for the split distribution have been transferred.

  Split distribution installation at startup time:

  > In the case of split distribution with installation specified at the time of system startup, installation begins when the system starts after all split jobs have been transferred.

- Limitations on using JP1/Software Distribution Client in a virtual environment

  Some limitations apply when you install or operate JP1/Software Distribution Client (client) in a virtual environment. Note also that depending on the OS type, JP1/Software Distribution Client (client) might not support a virtual environment. For more details about OS types, see *1.1.1 Supported OSs* in the *Setup Guide*.

  Limitations related to Remote Desktop

  - When you connect using Remote Desktop to install JP1/Software Distribution Client (client), you cannot use the installation set.
  - When you connect using Remote Desktop to install a package, you cannot use offline installation.
  - To connect using Remote Desktop to install or operate JP1/Software Distribution Client (client) when the OS is Windows Server 2003, connect to a console session.

To connect to a console session, specify the `/console` or `/admin` parameter as described below and execute Remote Desktop Connection Client.

- `/console` parameter

```
mstsc.exe /console
```

- `/admin` parameter

```
mstsc.exe /admin
```

The parameter required for connecting to the console session differs depending on the version of Remote Desktop Connection Client being used.

- When Remote Desktop is used to connect to and operate JP1/Software Distribution Client (client) when the OS is Windows Server 2012 or Windows Server 2008, multiple users cannot concurrently execute JP1/Software Distribution applications.

Limitations on the Quick User Switching Feature

- When the Quick User Switching Feature is used to connect to and operate JP1/Software Distribution Client (client) when the OS is Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, or Windows Vista, multiple users cannot concurrently execute JP1/Software Distribution applications.

Limitations related to terminal servers

- For the limitations applicable to using JP1/Software Distribution Client (client) on a terminal server, see *B. Using JP1/Software Distribution Client (Client) on a Terminal Server* in the *Setup Guide*. This appendix also explains limitations related to Citrix XenApp.

Limitations related to Windows XP Mode

- For the limitations applicable to using JP1/Software Distribution Client (client) in the Windows XP Mode environment, see *C. Using JP1/Software Distribution Client (Client) in a Windows XP Mode Environment* in the *Setup Guide*.

Limitations on Modern UI applications

- Software information cannot be collected for Modern UI applications.
- All the facilities for software operation monitoring do not support **Modern UI applications.**

2.14 Linking with other programs

When linked with other JP1 products, JP1/Software Distribution can integrate software distribution and management of clients' assets with management of the overall system.

This section provides an overview of operations that are achieved by linking JP1/Software Distribution with other programs.

2.14.1 Managing users when JP1/Software Distribution is linked to JP1/Base

By linking JP1/Software Distribution to JP1/Base, you can treat JP1 users managed by the JP1/Base user management functionality as JP1/Software Distribution users. In such a case, authentication of users to use JP1/Software Distribution is performed with the JP1/Base authentication server, rather than with the database.

You can set permissions for individual JP1 users. By creating JP1 users with permissions set for each type of administrator, you can do things like distribute the workload among administrators and specify that only certain administrators are able to change settings. In JP1/Software Distribution, you can configure six types of permissions based on the responsibilities of each administrator. The following table describes the types of permissions available in JP1/Software Distribution.

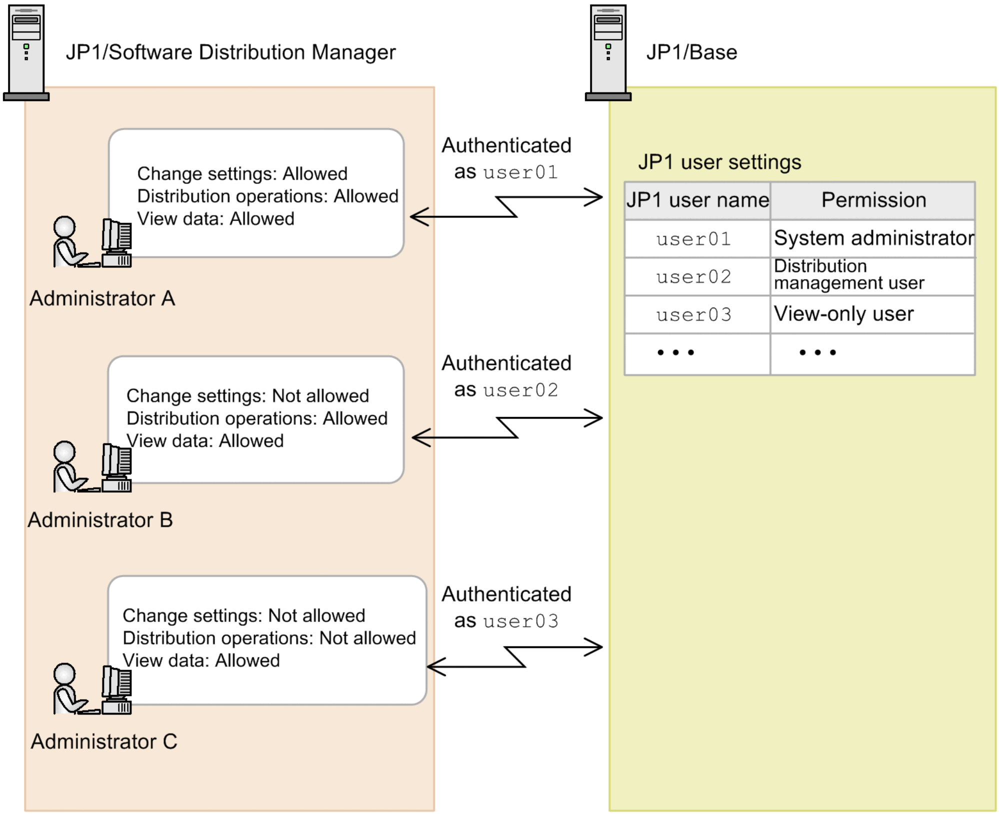
Table 2–40: Types of permissions provided by JP1/Software Distribution

No.	Permission	Overview
1	System administrator	This permission allows use of all JP1/Software Distribution functionality. It is assigned to administrators who manage the overall JP1/Software Distribution system.
2	Distribution management user	This permission allows distribution and packaging of software. It is assigned to administrators who manage distribution operations.
3	Asset management user	This permission allows collection, totaling, and printing of inventory information. It is assigned to administrators who manage assets.
4	Collection management user	This permission allows remote collection of client files. It is assigned to administrators who manage collection operations.
5	System-monitoring user	This permission allows monitoring of client operation status. It is assigned to administrators who monitor for unauthorized operations.
6	View-only user	This permission allows only viewing of data. It cannot be used to execute jobs or collect inventory information.

With the user management functionality, users must also be authenticated to use the unarchiver. The operations that can be used and the jobs that can be executed differ depending on the permissions. This enables you to prevent operations by unauthorized users and to strengthen security of the managing server.

The following figure provides a conceptual overview of user management when JP1/Software Distribution is linked to JP1/Base.

Figure 2–64: Conceptual overview of user management when JP1/Software Distribution is linked to JP1/ Base



JP1 user name	Permission
user01	System administrator
user02	Distribution management user
user03	View-only user
• • •	• • •

You select whether user management is to be available when you install JP1/Software Distribution Manager. To use the user management functionality, you must set up the JP1 users before you begin JP1/Software Distribution operations.

Note that if you use the user management functionality, you cannot use OpenView Linkage.

For details about user management when JP1/Software Distribution is linked to JP1/Base, see *1. Managing JP1/ Software Distribution Users by Linking with JP1/Base* in the manual *Administrator's Guide Volume 2*.

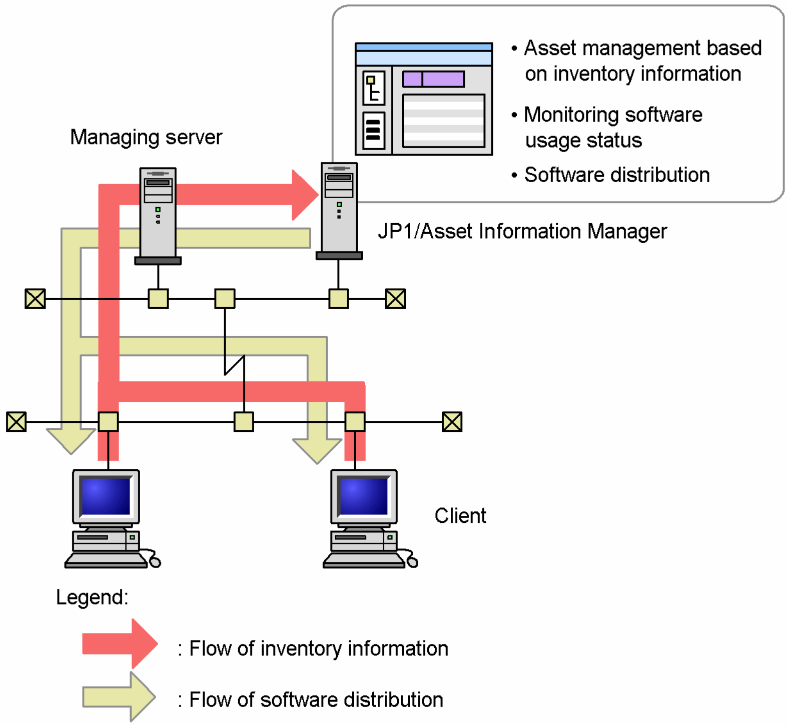
2.14.2 Managing application of software from JP1/Asset Information Manager

The JP1/Asset Information Manager program provides integrated management of corporate assets, such as software, hardware, and networks. You can manage the application of software by performing operations in the windows of JP1/Asset Information Manager.

You can use the information managed by JP1/Asset Information Manager to search devices on the basis of detailed conditions, and you can distribute software to identified devices. You can also check the distribution status of software. Note that the software to be distributed must have been packaged in advance by JP1/Software Distribution.

The following figure provides an overview of managing the application of software by linking JP1/Asset Information Manager.

Figure 2–65: Overview of managing the application of software by linking JP1/Asset Information Manager


• Asset management based on inventory information
• Monitoring software usage status
• Software distribution
Managing server
JP1/Asset Information Manager
Client
Legend:
: Flow of inventory information
: Flow of software distribution

From the operation window of JP1/Asset Information Manager, you can also view the operation history and software operation statuses collected by JP1/Software Distribution. In the operation window of JP1/Asset Information Manager, you can use the functions equivalent to those available in the Operation Log List window and the Software Operation Status window of JP1/Software Distribution.

For details about the JP1/Asset Information Manager functionality used to manage the application of software and the settings required for linkage, see the *Job Management Partner 1/Asset Information Manager Planning and Setup Guide*.

2.14.3 Managing security by linking with JP1/Client Security Control

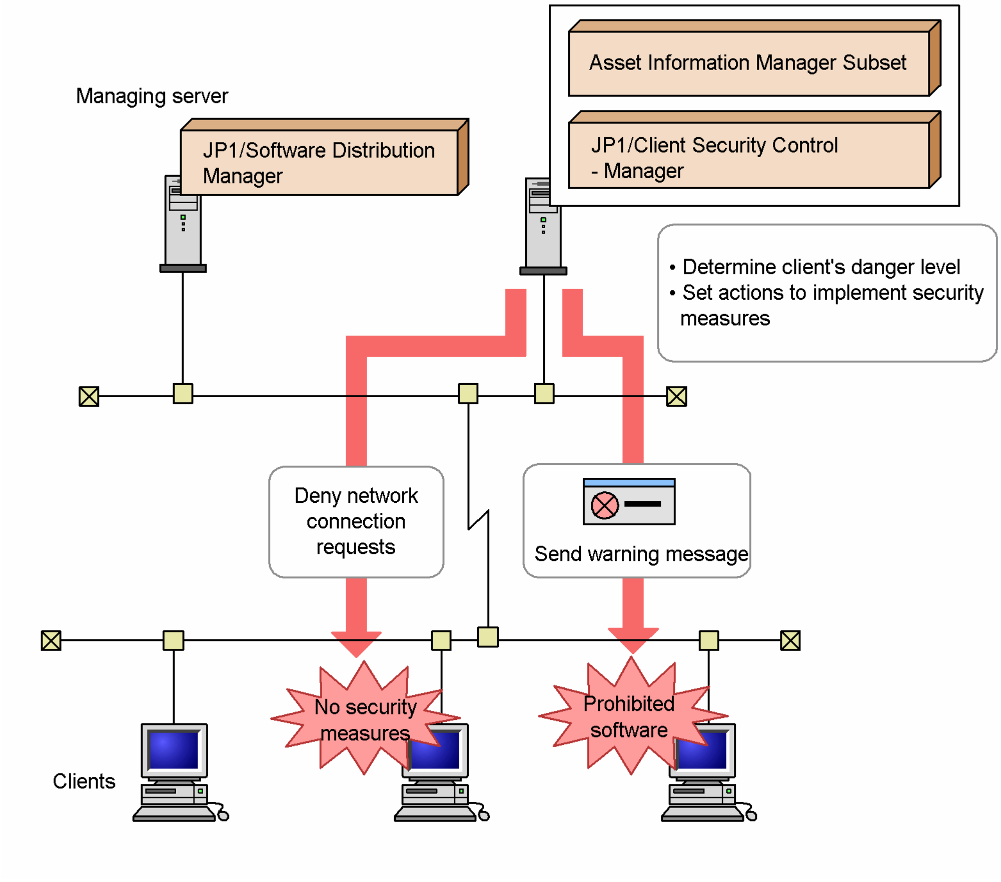
JP1/Client Security Control is a program that implements a series of operations management (*client security management*) tasks, from management of client asset information to client monitoring and handling of security risks. You can enhance your system's security by installing JP1/Client Security Control.

A client security management system employing JP1/Client Security Control uses inventory information collected by JP1/Software Distribution to monitor the client's security status. If there is any problem with security, the system can issue a warning message and take appropriate action for the risk level, such as denying network connection requests.

To link with JP1/Client Security Control, you must install Asset Information Manager Subset, which is a JP1/Software Distribution component.

The following figure provides an overview of managing security by linking with JP1/Client Security Control.

Figure 2–66: Overview of managing security by linking with JP1/Client Security Control


Managing server
JP1/Software Distribution Manager
Asset Information Manager Subset
JP1/Client Security Control - Manager
• Determine client's danger level
• Set actions to implement security measures
Deny network connection requests
Send warning message
No security measures
Prohibited software
Clients

For details about security management employing JP1/Client Security Control and the settings required for linkage, see the *Job Management Partner 1/Client Security Control Description, User's Guide and Operator's Guide*.

2.14.4 Managing JP1/Software Distribution from JP1/IM

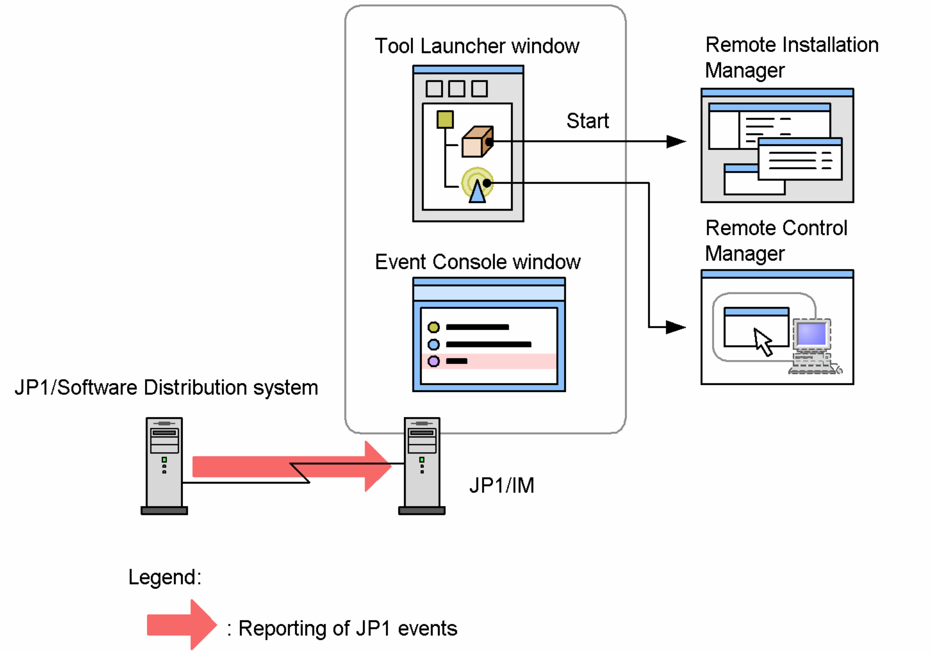
JP1/IM is a program that is linked with other JP1 products to achieve integrated management of the overall system.

JP1/IM's JP1/IM - View provides a window for selecting the programs that can be started from JP1/IM (*Tool Launcher window*). From this Tool Launcher window, you can start JP1/Software Distribution's Remote Installation Manager and Remote Control Manager.

JP1/Software Distribution can report information such as job execution results to JP1/IM. In JP1/IM's JP1/IM - View, you can view the reported information in the Event Console window that is used to monitor the system operation status.

The following figure provides an overview of managing JP1/Software Distribution by linking with JP1/IM.

Figure 2–67: Overview of managing JP1/Software Distribution by linking with JP1/IM


Tool Launcher window
Start
Remote Installation Manager
Remote Control Manager
Event Console window
JP1/Software Distribution system
JP1/IM
Legend:
: Reporting of JP1 events

For details about the facility for managing JP1/Software Distribution from JP1/IM, see *2. Managing JP1/Software Distribution from JP1/IM* in the manual *Administrator's Guide Volume 2*.

For details about the features of JP1/IM and operation methods, see the manual *Job Management Partner 1/Integrated Management - Manager User's Guide*.

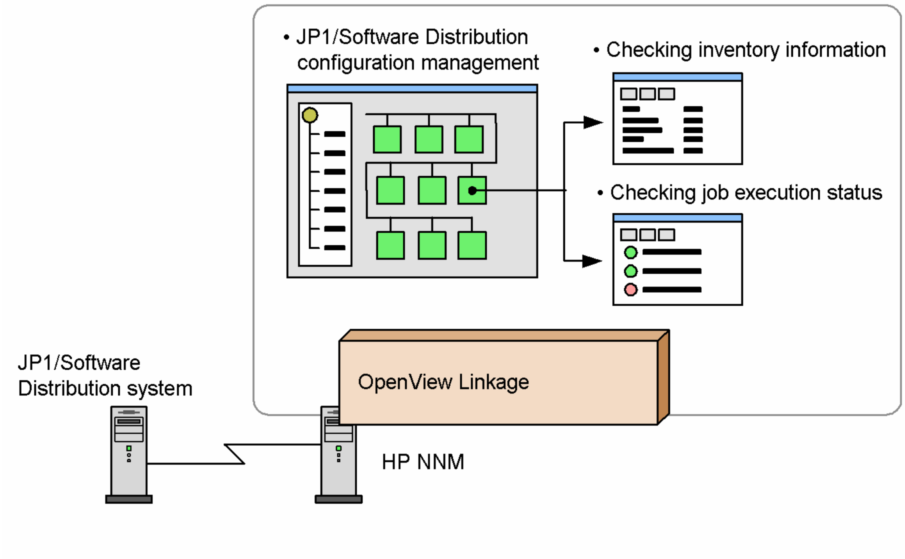
2.14.5 Managing JP1/Software Distribution from HP NNM

If you install the OpenView Linkage component of JP1/Software Distribution Manager on to HP NNM Network Node Manager, you can manage JP1/Software Distribution inventory information and job execution status from the monitoring window of HP NNM version 7.5 or earlier. This integrates network management by HP NNM and JP1/Software Distribution management.

The HP NNM Network Node Manager is a machine onto which HP NNM is installed that is used for managing the network configuration.

The following figure provides an overview of managing JP1/Software Distribution by linking with HP NNM.

Figure 2–68: Overview of managing JP1/Software Distribution by linking with HP NNM


• JP1/Software Distribution configuration management
• Checking inventory information
• Checking job execution status
OpenView Linkage
JP1/Software Distribution system
HP NNM

For details about how to install OpenView Linkage on HP Network Node Manager, see *2.5 Installing JP1/Software Distribution Manager in HP Network Node Manager* in the *Setup Guide*; for details about the facilities for managing JP1/Software Distribution from HP NNM, see *3. Managing JP1/Software Distribution from HP NNM* in the manual *Administrator's Guide Volume 2*.

If the OS being used is Windows Server 2012, Windows Server 2008 R2, Windows Server 2008 or Windows Server 2003 (x64), JP1/Software Distribution management from HP NNM is not supported.

(1) Managing the JP1/Software Distribution configuration

HP NNM is a program that manages the configuration of, and failures in, a TCP/IP network. It detects network configuration information automatically and represents it as a hierarchy diagram called a *node map*. A system being managed is represented by icons called *symbols*. JP1/Software Distribution configuration is also managed as symbols on the node map.

(2) Checking inventory information

Using symbols on the node map, you can check the following JP1/Software Distribution inventory information:

- System information
- Software information
- User inventory information
- Registry information

(3) Monitoring job execution status

If a JP1/Software Distribution job results in an error, it is reported to HP NNM. Therefore, you can monitor JP1/Software Distribution jobs from symbols on the node map. You can also check the execution status of the JP1/Software Distribution job.

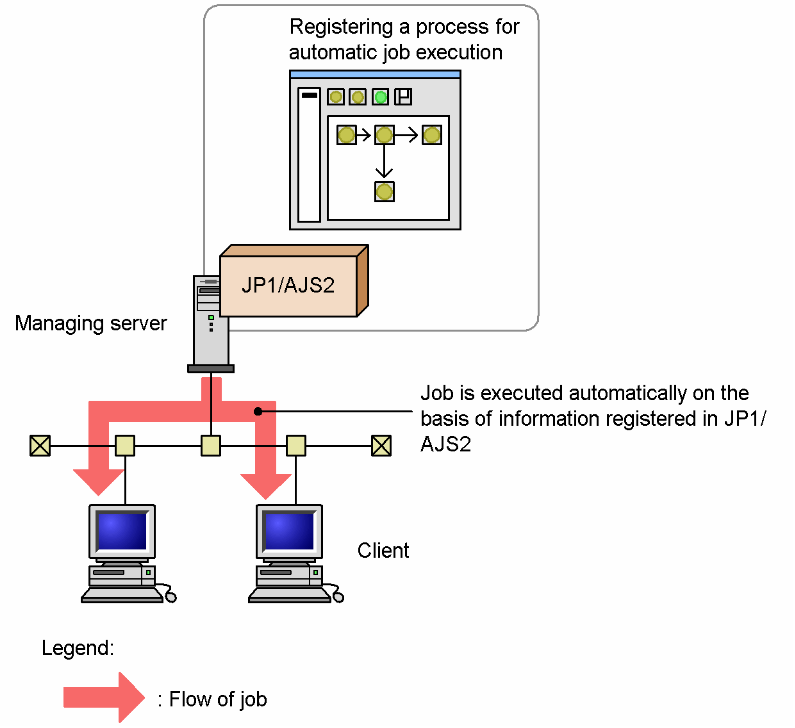
2.14.6 Executing jobs automatically by linking with JP1/AJS

JP1/AJS is a program used to automate jobs. It enables you to execute processing in sequence and at specific or regular times, and can start processing when a specific event occurs.

By using the command interface provided by JP1/Software Distribution for operations such as creating or executing jobs, you can register a command execution sequence in JP1/AJS in order to execute commands automatically or to execute JP1/Software Distribution commands when a specific event, such as a file update, occurs.

The following figure provides an overview of executing jobs automatically by linking with JP1/AJS.

Figure 2–69: Overview of executing jobs automatically by linking with JP1/AJS


Registering a process for automatic job execution
JP1/AJS2
Managing server
Job is executed automatically on the basis of information registered in JP1/AJS2
Client
Legend:
: Flow of job

For details about JP1/AJS functions and operation, see the JP1/AJS documentation.

For details about the commands provided with JP1/Software Distribution, see *4. Commands* in the manual *Administrator's Guide Volume 2*.

3 Flow of Tasks from Installation to Startup of Operations

This chapter provides an overview of the procedures from installation of JP1/Software Distribution to startup of operations.

3.1 Flow of tasks

When you install a new JP1/Software Distribution, there are tasks you must perform before you can start actual operations, such as designing the system configuration, installing programs, and setting up the environment.

The following figure shows the flow of tasks from installation of JP1/Software Distribution to startup of operations.

Figure 3–1: Flow of tasks

	Flow of operation	See
1	**Design the system configuration.** Before you install JP1/Software Distribution, design the configuration of the overall system.	Chapters 1 and 5
2	**Install JP1/Software Distribution.** Install the JP1/Software Distribution programs onto the PCs.	Setup Guide, Chapters 1 to 3
3	**Set up JP1/Software Distribution.** Set up the JP1/Software Distribution programs.	Setup Guide, Chapters 4 to 6
4	**Set up a relational database.** Use Database Manager to set up a relational database.	Setup Guide, Chapter 7
5	**Create the system configuration information.** Create the system configuration information needed to manage the relay systems and clients. This enables JP1/Software Distribution to recognize job destinations.	Setup Guide, Chapters 8 and 9
6	**Group job destinations.** Group clients for use as job destinations. This allows groups to be specified as job destinations.	Setup Guide, Chapters 8 and 9
7	**Start JP1/Software Distribution operations.** Start actual operations, such as remote installation of software, collection of inventory information, and linking to other JP1 products.	Administrator's Guide, Volumes 1 and 2

The following sections provide an overview of the tasks.

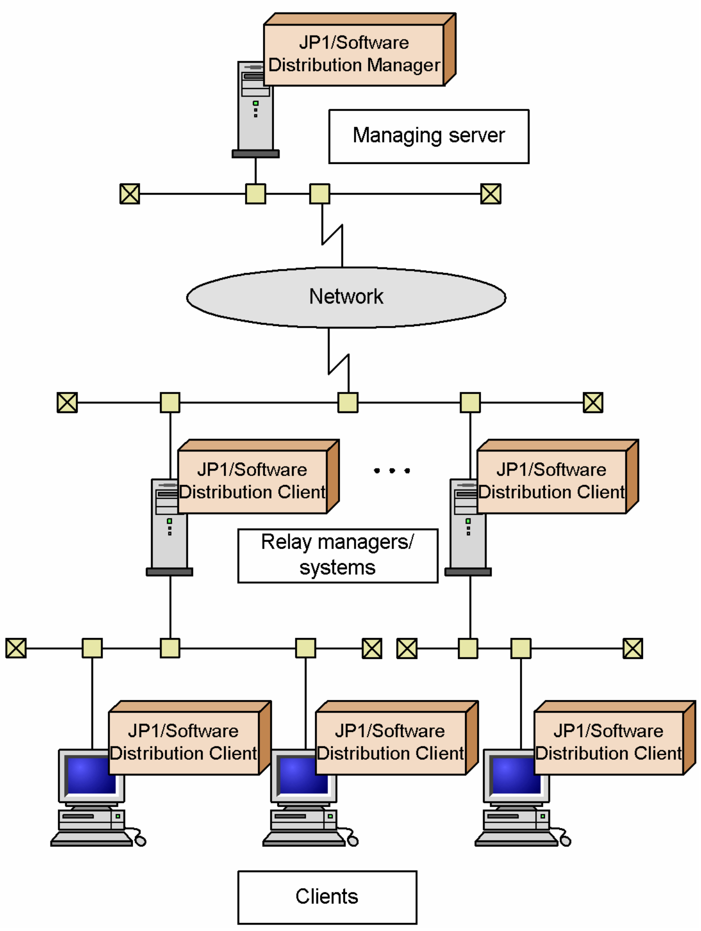
For details about each task, see the chapters and manuals indicated in Figure 3-1.

3.2 Designing the system configuration

In order to install JP1/Software Distribution, you must first design the system configuration, taking into account the structure of your organization, the size of the system, and the network environment.

The basic system configuration for JP1/Software Distribution consists of three hierarchical levels, a managing server, relay managers/systems, and clients. The following figure shows a basic system configuration.

Figure 3–2: Basic configuration of a JP1/Software Distribution system


JP1/Software Distribution Manager
Managing server
Network
JP1/Software Distribution Client
• • •
JP1/Software Distribution Client
Relay managers/ systems
JP1/Software Distribution Client
JP1/Software Distribution Client
JP1/Software Distribution Client
Clients

The following table describes the roles of the programs that are used as the system components.

Table 3–1: Components of a JP1/Software Distribution system

System component	Program used	Role
Managing server	JP1/Software Distribution Manager	Executes the jobs that perform tasks, such as distributing software and managing collected inventory information.
Relay manager/system	JP1/Software Distribution Manager or JP1/ Software Distribution Client#	Relays jobs between the managing server and clients.
Client	JP1/Software Distribution Client	Receives and executes jobs executed by the managing server and reports the execution results back to the managing server.

#: For details about the functional differences between JP1/Software Distribution Manager and JP1/Software Distribution Client, see *D.1 Functional differences between JP1/Software Distribution Manager and JP1/Software Distribution Client (relay system)*.

You should design a system configuration appropriate to your environment, taking into account the cost of hardware installation and network performance.

For details about the components of a JP1/Software Distribution system, see *1.3 System components of JP1/Software Distribution*; for details about designing the system configuration, see *5. Designing a JP1/Software Distribution System*.

3.3 Installing JP1/Software Distribution

After designing the system configuration, you must install the JP1/Software Distribution programs.

Each program includes components that can be selected for each facility. When installing each program, select the components to be used.

When installing each of the JP1/Software Distribution programs, install the programs sequentially from higher to lower systems.

To install JP1/Software Distribution for the first time:

1. Install JP1/Software Distribution Manager on the computer used as the managing server.
2. Install JP1/Software Distribution Manager or JP1/Software Distribution Client on each computer used as a relay manager/system.
3. Install JP1/Software Distribution Client on each computer used as a client.

When installing JP1/Software Distribution Client, which is usually installed on many machines, you can use the automatic installation facility to reduce the administrator's workload.

When you upgrade JP1/Software Distribution, you can use JP1/Software Distribution to upgrade the JP1/Software Distribution Clients by remote installation.

For details about the installation of each program, see the chapters and sections indicated in the following table:

Task	Manual	See	Chapter/section title
Overview of JP1/Software Distribution components and installation	*Setup Guide*	*Chapter 1*	*Overview of JP1/Software Distribution Installation*
Installation of JP1/Software Distribution Manager	*Setup Guide*	*Chapter 2*	*Installing JP1/Software Distribution Manager*
Installation of JP1/Software Distribution Client	*Setup Guide*	*Chapter 3*	*Installing JP1/Software Distribution Client*
Automatic installation of JP1/Software Distribution Client	*Setup Guide*	*Section 1.2.4*	*Using an installation set to install JP1/Software Distribution Client (client)*
Overwrite installation of JP1/Software Distribution	*Setup Guide*	*Section 1.2.2*	*Installing JP1/Software Distribution by overwriting*

3.4 Setting up JP1/Software Distribution

Once you install each JP1/Software Distribution program, you must set up the program.

To set up a program, the administrator uses the setup dialog box and specifies the settings on each page as necessary.

If you use the automatic installation facility for the JP1/Software Distribution Clients, JP1/Software Distribution Client is also set up automatically.

For details about the setup of each program, see the chapters indicated in the following table:

Task	Manual	See	Chapter title
Setting up JP1/Software Distribution Manager	*Setup Guide*	*Chapter 4*	*Setting Up JP1/Software Distribution Manager*
Setting up JP1/Software Distribution Client (relay system)	*Setup Guide*	*Chapter 5*	*Setting Up JP1/Software Distribution Client (relay system)*
Setting up JP1/Software Distribution Client (client)	*Setup Guide*	*Chapter 6*	*Setting Up JP1/Software Distribution Client (client)*

3.5 Setting up a relational database

JP1/Software Distribution uses a database to manage the various types of information, such as system information, software information, and user inventory information.

JP1/Software Distribution supports the following relational databases:

- Embedded RDB

  This relational database is embedded in JP1/Software Distribution Manager. You can install this database when you install JP1/Software Distribution Manager, which eliminates the need to provide a separate relational database.
- Microsoft SQL Server or Oracle

  You can use Microsoft SQL Server or Oracle as the relational database.

You select the relational database you will use when you install JP1/Software Distribution Manager.

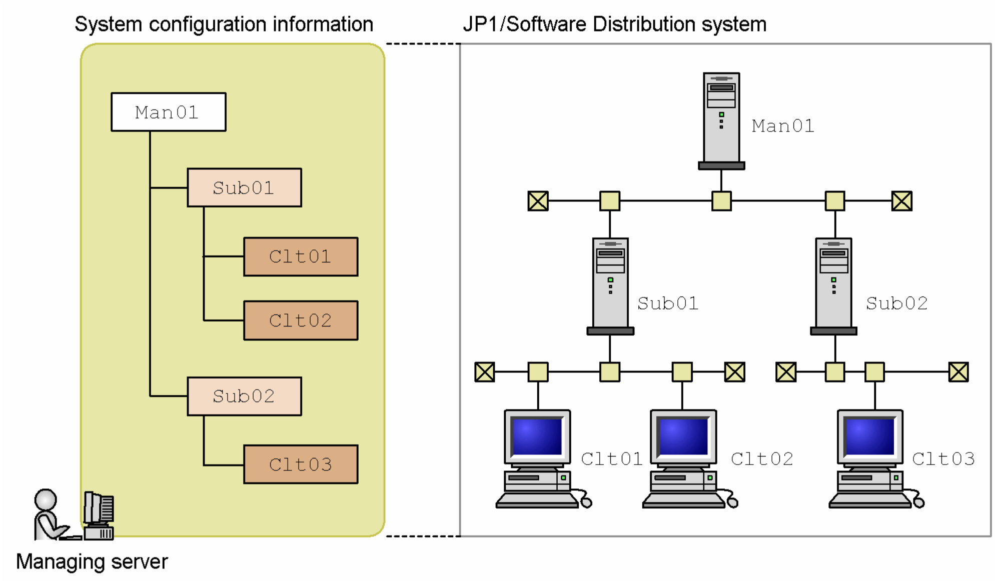
You use *Database Manager*, which is a JP1/Software Distribution Manager component, to create and maintain your relational database.

For details about setup of a relational database, see *7. Setting Up a Relational Database* in the *Setup Guide*.

3.6 Creating system configuration information

Before you can start JP1/Software Distribution operations, you must create system configuration information for managing the relay systems and clients. This system configuration information consists of system configuration settings and the address of each host. The managing server issues instructions for distributing software and collecting inventory information based on this system configuration information. The following figure provides a conceptual overview of system configuration information.

Figure 3–3: Conceptual overview of system configuration information



There are four ways to create the system configuration information:

- Use the facility for automatically registering the system configuration.
- Use a file that contains the system configuration information settings.
- Use the System Confirmation window.
- Acquire the system configuration information from the relay managers.

For details about creating and maintaining system configuration information, see the chapters indicated in the following table:

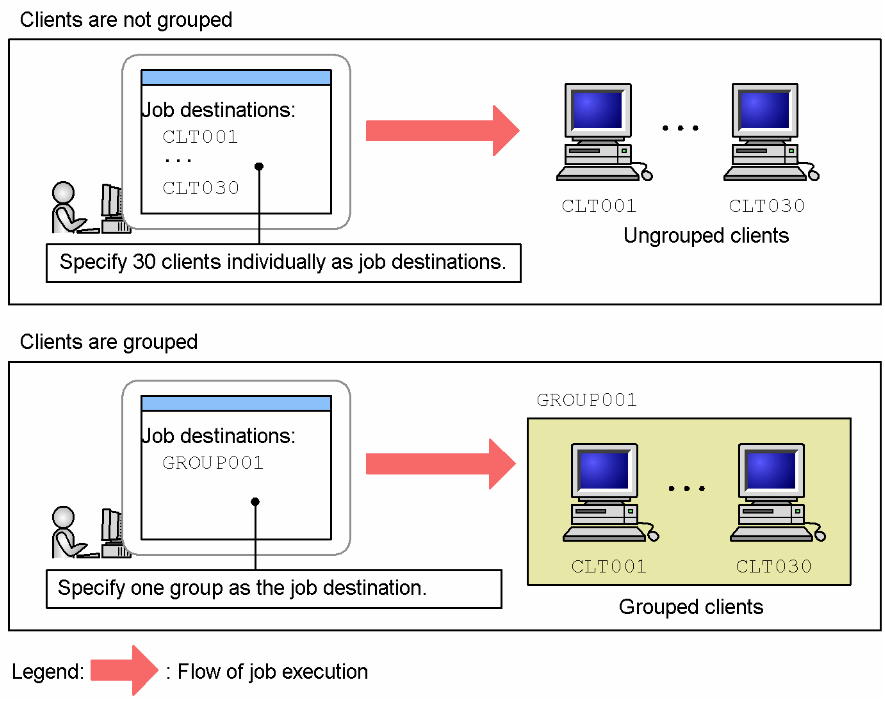
Task	Manual	See	Chapter title
Creating system configuration information	*Setup Guide*	*Chapter 8*	*Creating System Configuration Information and Destination Groups*
Maintaining system configuration information	*Setup Guide*	*Chapter 9*	*Maintaining System Configuration Information and Destination Groups*

3.7 Grouping job destinations

JP1/Software Distribution enables you to assign clients to groups and execute jobs by group, independently of the physical network configuration.

The following example shows the difference in job execution when 30 clients are grouped compared to when the same clients are not grouped.

Figure 3–4: Difference in job execution depending on whether clients are grouped



In the example in the figure, if the clients are not grouped, to execute a job you need to individually specify each of the 30 clients as job destinations. If the clients are grouped, to execute a job you need to specify only one group (containing the 30 clients) as the job destination.

You can execute jobs efficiently by grouping clients.

You can group job destinations by using any of the following methods:

- Grouping by host
  This method groups clients in the managing server. It classifies clients into hierarchical groups according to some criterion, such as by department, project, or OS. The groups are managed in the managing server.
- Grouping by ID
  This method enables each client to select the group it wishes to belong to. The ID groups are created in the managing server, then each client selects the ID group it wishes to belong to and registers itself into that ID group.
- Grouping by directory information
  This method groups clients by the organizational units managed in Active Directory. When computers and users are managed in Active Directory, you can execute jobs according to the organizational hierarchy used in Active Directory.

For details about creating and maintaining host groups, ID groups, and directory information, see the appropriate chapters indicated in the following table.

Task	Manual	See	Chapter title
Creating host groups and ID groups	*Setup Guide*	*Chapter 8*	*Creating System Configuration Information and Destination Groups*

Task	Manual	See	Chapter title
Maintaining host groups and ID groups	*Setup Guide*	*Chapter 9*	*Maintaining System Configuration Information and Destination Groups*
Acquiring and maintaining directory information	*Administrator's Guide Volume 1*	*3.4*	*Acquiring directory information*

3.8 Starting operation of JP1/Software Distribution

Finally, you start actual operations, such as remote installation of software and management of inventory information and clients.

For examples of typical JP1/Software Distribution operations, see *4. Examples of Typical System Construction and Operation*.

For details about each type of operation, see the manual *Administrator's Guide Volume 1* and the manual *Administrator's Guide Volume 2*.

4 Examples of Typical System Construction and Operation

This chapter provides examples of constructing and operating a basic JP1/Software Distribution system that uses the asset management and distribution management facilities. The chapter also discusses key points about system construction and operation.

4.1 Examples of construction and operation

The following table lists the examples of constructing and operating a typical system that uses JP1/Software Distribution:

Type	Example of constructing and operating a system	Section
Constructing	Installing a JP1/Software Distribution system	*4.2*
	Operating a remote JP1/Software Distribution system	*4.3*
Operating	Managing hardware assets	*4.4*
	Managing software assets	*4.5*
	Distributing software to sites	*4.6*
	Distributing software at specified distribution and installation dates/times	*4.7*
	Sending a warning message to clients on which the most recent virus definition file has not been installed	*4.8*
	Changing the power configuration for clients on which the power-save setting is not applied	*4.9*
	Shutting down clients at a specific date and time	*4.10*
	Distributing software to new clients automatically	*4.11*
	Using remote control to maintain a malfunctioning client from the managing server	*4.12*

This section uses the following format to describe each example of constructing and operating a system:

Title

Provides a simple description of the example.

Overview, prerequisites, operating procedure, and notes

Provides the necessary information appropriate to the example. Each item presents the key facility and operating procedure. For details about each facility and operating procedure, see the indicated section in the indicated manual.

In this manual, the manual *Job Management Partner 1/Software Distribution Setup Guide* is referred to as *Setup Guide* and the manual *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1* is referred to as *Administrator's Guide Volume 1*.

4.2 Installing a JP1/Software Distribution system

To install JP1/Software Distribution for the first time in the system, you must examine various aspects, such as the configuration of the JP1/Software Distribution system and the network environment to be employed. This section explains the steps required to build a basic JP1/Software Distribution system.

To install a JP1/Software Distribution system:

1. Evaluate the JP1/Software Distribution system to be installed.
2. Construct a database server.
3. Install JP1/Software Distribution Manager on the management server.
4. Install JP1/Software Distribution Client (relay system) on the relay servers.
5. Install JP1/Software Distribution Client (client) on the clients.

(1) Evaluating the JP1/Software Distribution system to be installed

You must first evaluate the system configuration and network environment for the JP1/Software Distribution system to be installed.

- For details on configuring the JP1/Software Distribution system, see *5.1.1 Designing a basic system configuration*.
- For details on evaluating the network environment, see *6.1 Evaluating the network environment*.
- For details on estimating the hardware requirements, see *5.3 Estimating the hardware requirements*.

(2) Constructing a database server

To use Microsoft SQL Server or Oracle as the relational database for the managing server, you must construct a database server before installing JP1/Software Distribution. If you use Embedded RDB, there is no need to construct a database server.

- For details on supported databases, see *5.1.5 Supported databases*.
- For details on configuring the system and setting up a relational database, see *7. Setting Up a Relational Database* in the *Setup Guide*.

(3) Installing JP1/Software Distribution Manager on the management server

Install the managing server (JP1/Software Distribution Manager) on the server that controls the JP1/Software Distribution system.

- For details on programs that can be installed, see *1.1 Supported OSs and organization of components* in the *Setup Guide*.
- For details on the installation method, see *2. Installing JP1/Software Distribution Manager* in the *Setup Guide*.

(4) Installing JP1/Software Distribution Client (relay system) on the relay servers

Install a relay system (JP1/Software Distribution Client) on the applicable servers, such as each department's management server.

- For details on programs that can be installed, see *1.1 Supported OSs and organization of components* in the *Setup Guide*.
- For details on the installation method, see *3. Installing JP1/Software Distribution Client* in the *Setup Guide*.

You can also construct a JP1/Software Distribution system using JP1/Software Distribution Manager as the relay manager.

- For an example of system construction using a relay manager, see *5.1.2 Designing a large-scale system configuration*.
- For details on the installation method, see *2. Installing JP1/Software Distribution Manager* in the *Setup Guide*.

- For details on functional differences between JP1/Software Distribution Manager and JP1/Software Distribution Client (relay system), see *D.1 Functional differences between JP1/Software Distribution Manager and JP1/Software Distribution Client (relay system)*.

(5) Installing JP1/Software Distribution Client on the clients.

Install JP1/Software Distribution Client on the clients that are to be managed by the JP1/Software Distribution system.

- For details on installable programs, see *1.1 Supported OSs and organization of components* in the *Setup Guide*.
- For details on the installation method, see *3. Installing JP1/Software Distribution Client* in the *Setup Guide*.

Installing JP1/Software Distribution Client individually on each client from storage media requires a lot of time and labor. JP1/Software Distribution lets you create a JP1/Software Distribution Client *installation set* to automate the installation job. To create an installation set, you must have JP1/Software Distribution Administrator Kit.

- For an overview of automatic installation, see *1.2.4 Using an installation set to install JP1/Software Distribution Client (client)* in the *Setup Guide*.
- For details on how to create an installation set and how to use it for installation, see the manual *Job Management Partner 1/Software Distribution Administrator Kit Description and Operator's Guide*.

(6) Notes

- For notes on using relational databases, see *7.2 Notes on using a relational database* in the *Setup Guide*.

4.3 Operating a remote JP1/Software Distribution system

You can construct a system that lets you perform operations on a JP1/Software Distribution system at a remote location.

For example, you can install JP1/Software Distribution on the management server at an office, and then use the administrator's PC to perform JP1/Software Distribution operations.

There are two ways to perform operations on a remote JP1/Software Distribution system:

- Install the JP1/Software Distribution server facilities on one computer and the GUI for performing operations on those server facilities on a separate computer
- Remotely control the computer on which a managing server has been installed

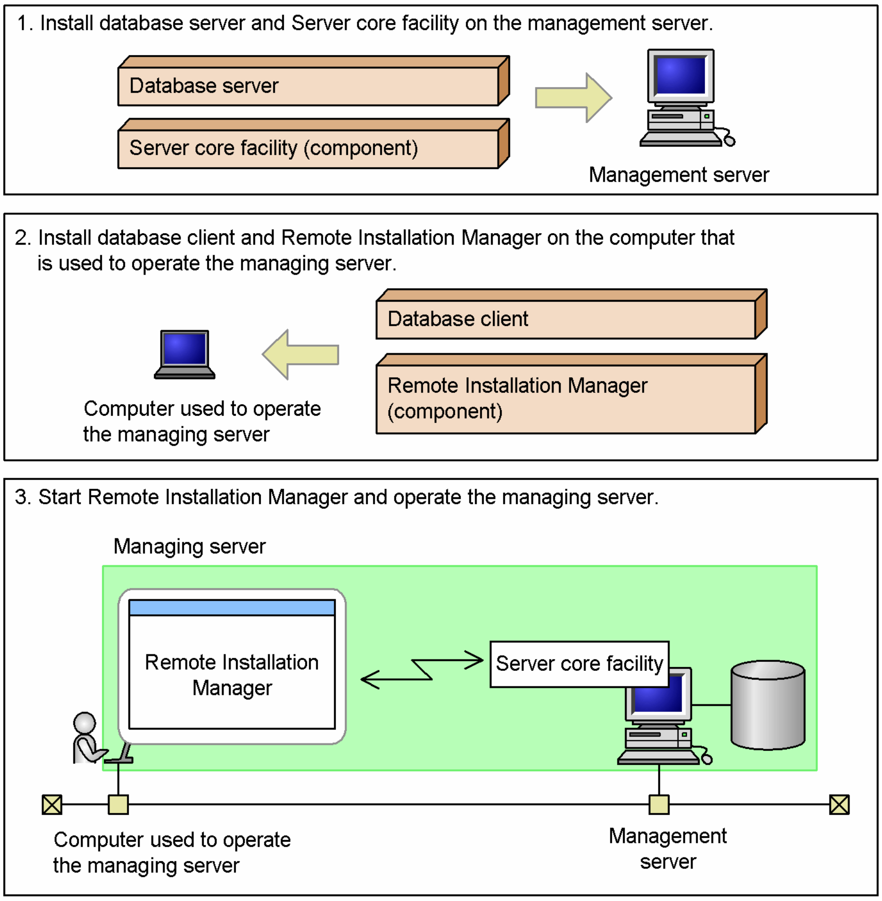
4.3.1 Installing JP1/Software Distribution's server facilities and the GUI on separate computers

■ Overview

Install, on separate computers, the Server core facility and Remote Installation Manager, which are installation components of JP1/Software Distribution Manager, and then run the managing server.

The following figure shows the flow for installing the JP1/Software Distribution server facilities and GUI on separate computers.

Figure 4–1: Flow for installing JP1/Software Distribution server facilities and GUI on separate computers


1. Install database server and Server core facility on the management server.
Database server
Server core facility (component)
Management server
2. Install database client and Remote Installation Manager on the computer that is used to operate the managing server.
Database client
Remote Installation Manager (component)
Computer used to operate the managing server
3. Start Remote Installation Manager and operate the managing server.
Managing server
Remote Installation Manager
Server core facility
Computer used to operate the managing server
Management server

■ Operating procedure

To install JP1/Software Distribution's server facility and the GUI on separate computers:

1. Install the database server on the management server.
   If you use Embedded RDB as the database, there is no need to install a database server.
   - For details on placement of the relational database server, see *7.1.2 System configuration* in the *Setup Guide*.
   - For details on setup of the relational database, see *7.3 Setting up the relational database environment* in the *Setup Guide*.
2. Install JP1/Software Distribution's Server core facility onto the management server.
   - For details on the installation method, see *2. Installing JP1/Software Distribution Manager* in the *Setup Guide*.
3. Install a database client on the computer that is used to perform operations on the managing server.
   If you use Embedded RDB as the database, there is no need to install a database client.
   - For details on placement of the relational database client, see *7.1.2 System configuration* in the *Setup Guide*.
4. Install Remote Installation Manager on the computer that is used to perform operations on the managing server.
   - For details on the installation method, see *2.2 Installing Remote Installation Manager* in the *Setup Guide*.
   - For details on setup of the server connection (during installation), see *2.1.18 Specifying the connection destination (Remote Installation Manager)* in the *Setup Guide*.
5. Start Remote Installation Manager and perform operations on the managing server.
   - For details on how to start Remote Installation Manager, see *1.3 Starting and terminating Remote Installation Manager* in the manual *Administrator's Guide Volume 1*.

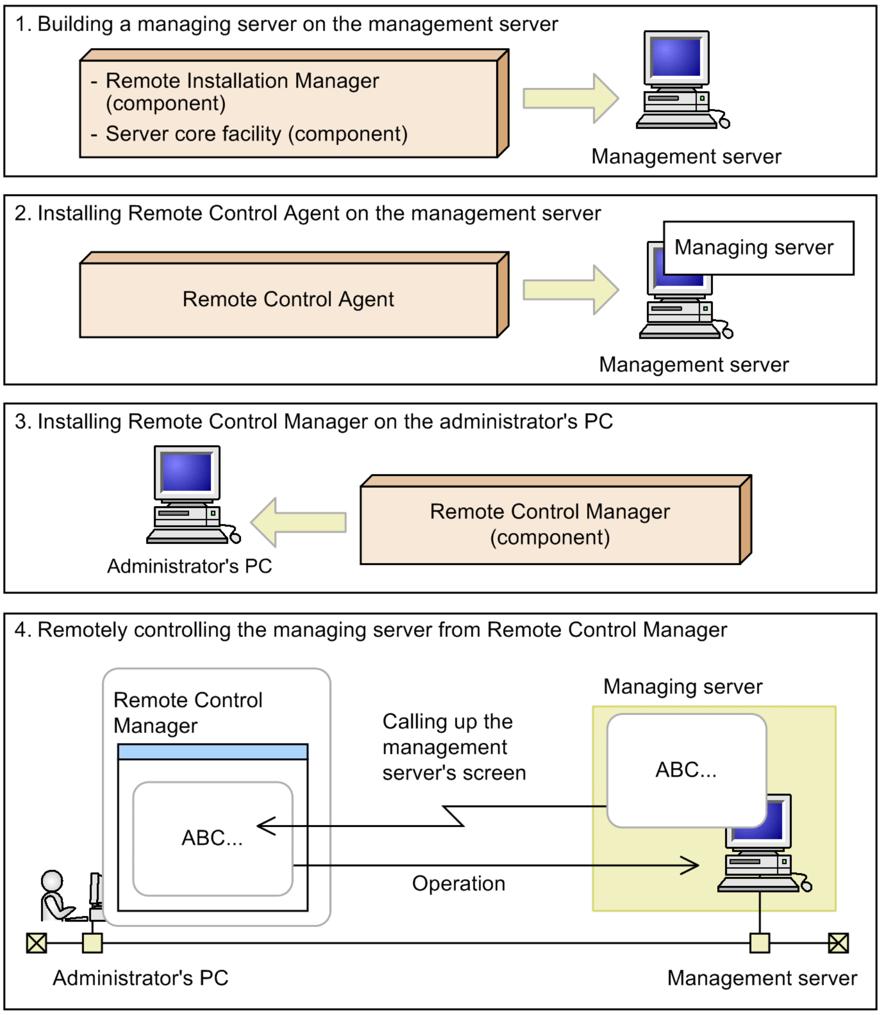
4.3.2 Controlling the remote computer where JP1/Software Distribution is installed

■ Overview

You can remotely control a managing server by installing Remote Control Agent on the *management* server on which the *managing* server has been constructed, and installing Remote Control Manager on the Administrator's PC.

The following figure shows the general procedure for remote control of a managing server.

Figure 4–2: General procedure for remote control of a managing server


1. Building a managing server on the management server
- Remote Installation Manager (component)
- Server core facility (component)
Management server
2. Installing Remote Control Agent on the management server
Remote Control Agent
Managing server
Management server
3. Installing Remote Control Manager on the administrator's PC
Administrator's PC
Remote Control Manager (component)
4. Remotely controlling the managing server from Remote Control Manager
Remote Control Manager
ABC...
Calling up the management server's screen
Operation
Managing server
ABC...
Administrator's PC
Management server

■ Prerequisites

Remote Control Agent, which is an installation component of JP1/Software Distribution Manager, cannot be installed on the managing server (central manager). Therefore, provide Remote Control Agent separately from JP1/Software Distribution Manager.

■ Operating procedure

To control a remote computer where JP1/Software Distribution is installed:

1. Build a managing server on the management server.
    - For details on how to install JP1/Software Distribution Manager, see *2.1 How to install JP1/Software Distribution Manager* in the *Setup Guide*.
2. Install Remote Control Agent on the management server.
    - For details on how to install Remote Control Agent, see the manual *Job Management Partner 1/Remote Control Description and Operator's Guide*.

    On the relay manager, you can install Remote Control Agent, which is an installation component.
3. Install Remote Control Manager on the Administrator's PC.
    - For details on how to install Remote Control Manager, see *2. Installing JP1/Software Distribution Manager* in the *Setup Guide*.

      Select **Remote Control Manager** as the component to be installed.

4. Control the remote managing server from Remote Control Manager.

    - For details on how to operate Remote Control Manager, see the manual *Job Management Partner 1/Remote Control Description and Operator's Guide*.

4.4 Managing hardware assets

■ Overview

You can use JP1/Software Distribution's inventory management facility to manage the client system information that is registered in the managing server.

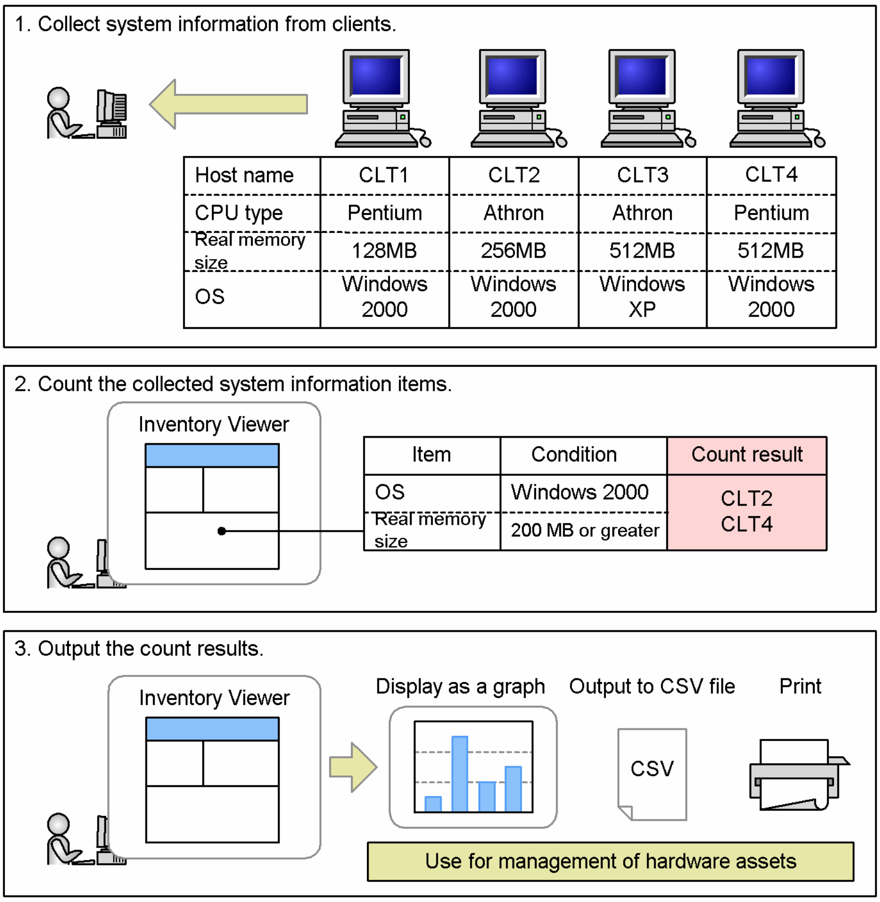
- For details on system information that can be managed by JP1/Software Distribution, see *2.2.1 Acquiring system information*.

By using the managing server's Inventory Viewer, you can use system information collected from clients: for example, to count the clients that satisfy specific hardware conditions or to display count results as a graph.

If you output count results to a CSV file or a printer, you can use the results as a ledger for managing hardware assets.

The following figure illustrates the general procedure for managing clients' hardware assets.

Figure 4–3: General procedure for managing clients' hardware assets


1. Collect system information from clients.

Host name	CLT1	CLT2	CLT3	CLT4
CPU type	Pentium	Athron	Athron	Pentium
Real memory size	128MB	256MB	512MB	512MB
OS	Windows 2000	Windows 2000	Windows XP	Windows 2000

2. Count the collected system information items.
Inventory Viewer

Item	Condition	Count result
OS	Windows 2000	CLT2 CLT4
Real memory size	200 MB or greater	

3. Output the count results.
Inventory Viewer
Display as a graph
Output to CSV file
Print
CSV
Use for management of hardware assets

■ Operating procedure

To manage the hardware assets:

1. Collect system information from clients.
    - For details on collecting system information, see *3.1.1 System information collection procedure* in the manual *Administrator's Guide Volume 1*.
2. Count the collected system information items.
    - For details on starting Inventory Viewer, see *4.1.1 Starting Inventory Viewer* in the manual *Administrator's Guide Volume 1*.

- For details on using inventory information to count clients, see *4.2.1 Counting procedure* in the manual *Administrator's Guide Volume 1*.
- For details on displaying count results, see *4.2.3(6) Counting hosts by system information items* in the manual *Administrator's Guide Volume 1*.

3. Output the count results.

   Display the count results as a graph.

   - For details on displaying the count results as a graph, see *4.2.6 Displaying count results as a graph* in the manual *Administrator's Guide Volume 1*.

   Export the count results to a CSV file.

   - For details on exporting the count results to a CSV file, see *4.5.2 Exporting to a CSV-formatted file* in the manual *Administrator's Guide Volume 1*.

   Print the count results.

   - For details on printing the count results, see *4.5.3 Printing* in the manual *Administrator's Guide Volume 1*.

■ Notes

- For notes on collecting system information, see *3.1.4 Notes on collecting system information* in the manual *Administrator's Guide Volume 1*.

4.5 Managing software assets

This section describes how to check which clients have specific software installed and manage the number of licenses for software installed on clients.

4.5.1 Checking which clients have specific software installed

■ Overview

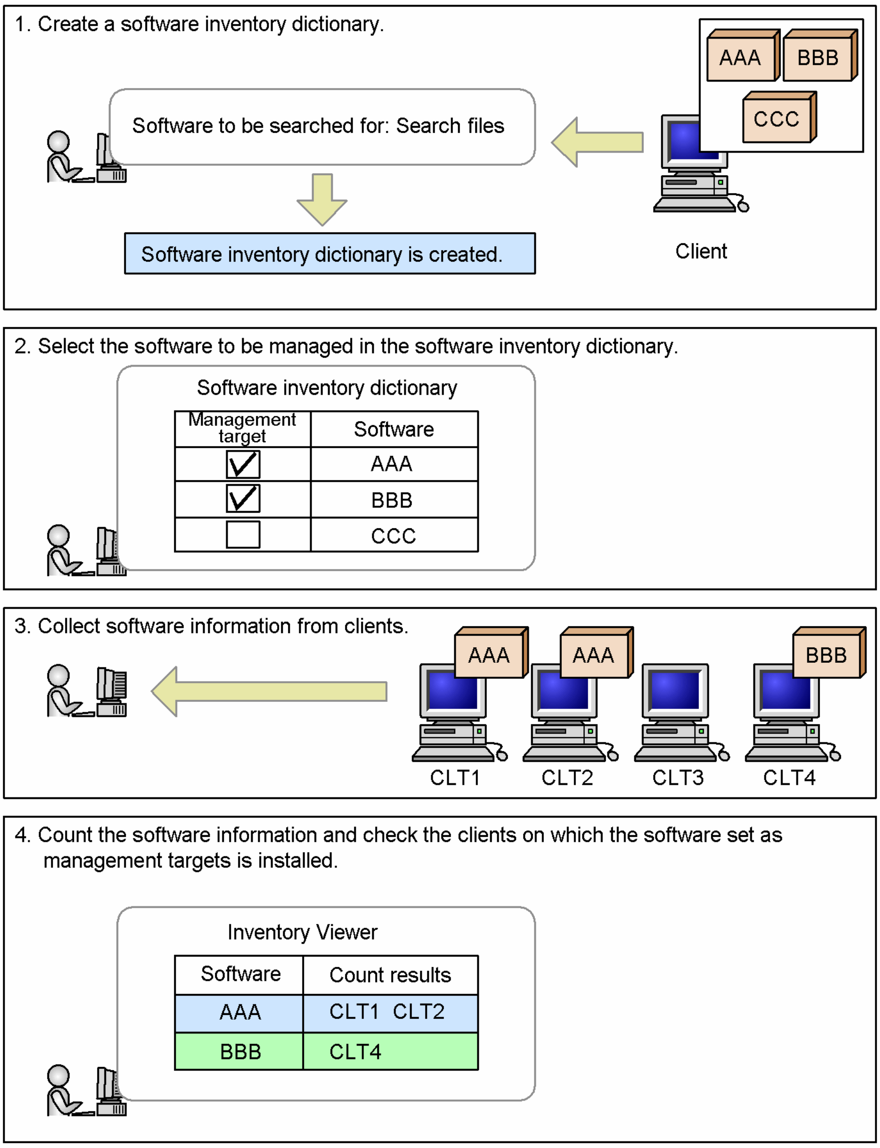
You can use software information collected from clients to determine which clients have specific software installed.

To manage information about items of software that are not managed by default by JP1/Software Distribution, such as user-specific programs, you must set those software items as management targets in the *software inventory dictionary* that is created when software information is collected.

Once a software item has been set as a management target, you can count the clients that have that software item installed by totaling the values in the collected software information.

The following figure shows the general procedure for checking which clients have specific software installed.

Figure 4–4: General procedure for checking which clients have specific software installed



1. Create a software inventory dictionary.

2. Select the software to be managed in the software inventory dictionary.

Software inventory dictionary

Management target	Software
☑	AAA
☑	BBB
□	CCC

3. Collect software information from clients.

4. Count the software information and check the clients on which the software set as management targets is installed.

Inventory Viewer

Software	Count results
AAA	CLT1 CLT2
BBB	CLT4

Software to be searched for: Search files
Software inventory dictionary is created.
AAA
BBB
CCC
Client
AAA
AAA
BBB
CLT1
CLT2
CLT3
CLT4

■ Operating procedure

1. Create a software inventory dictionary.

   To create a software inventory dictionary, collect software information from a small number of clients (1 to several) on which the software to be managed has been installed.

   - For details on how to collect software information, see *3.2.1 Procedure for collecting software information* in the manual *Administrator's Guide Volume 1*.

   On the **Options** page that is displayed when a *Get software information from client* job is created, specify **Search for a file** in **Software to be searched**, and then execute the job. Execute the job for which **Search for a file** is specified on only a small number of clients (1 to several) in order to minimize the workload on the database.

   A software inventory dictionary is created on the basis of the collected software information.

2. Select the software to be managed in the software inventory dictionary.

   - For details on specifying the software to be managed, see *3.2.5(1) Setting the software inventory information to be displayed* in the manual *Administrator's Guide Volume 1*.

3. Collect software information from clients.

- For details on how to collect software information, see *3.2.1 Procedure for collecting software information* in the manual *Administrator's Guide Volume 1*.

4. Count the software information and check the clients on which the software set as management targets is installed.
    - For details on how to start Inventory Viewer, see *4.1.1 Starting Inventory Viewer* in the manual *Administrator's Guide Volume 1*.
    - For details on how to count items of inventory information, see *4.2.1 Counting procedure* in the manual *Administrator's Guide Volume 1*.

■ Notes

- For notes about collecting software information, see *3.2.3 Notes on collecting software information* in the manual *Administrator's Guide Volume 1*.

4.5.2 Managing the number of software licenses

■ Overview

By collecting information about the software programs installed on the clients, you can check for software programs whose licenses are close to expiration or whose licenses have already expired.

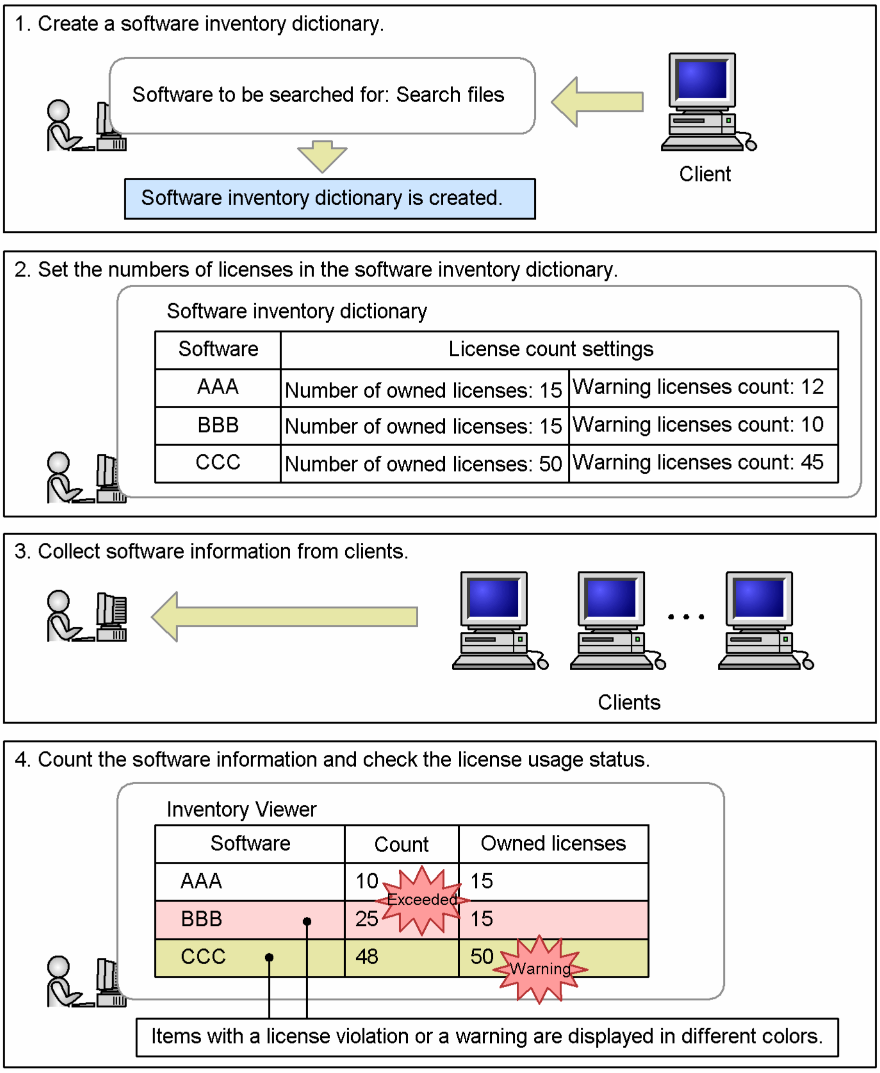
- For details on software information that can be collected by JP1/Software Distribution, see *2.2.2 Acquiring software information*.

To manage the number of software licenses, use the software inventory dictionary (created when software information is collected) to set the number of software licenses to be managed by JP1/Software Distribution.

By setting the number of licenses and counting the relevant items of software information, you can determine the software whose number of users is close to the specified number of licenses or whose number of users exceeds the specified number of licenses.

The following figure shows the general procedure for managing the number of software licenses.

Figure 4–5: General procedure for managing the number of software licenses



1. Create a software inventory dictionary.

Software to be searched for: Search files

Software inventory dictionary is created.

2. Set the numbers of licenses in the software inventory dictionary.

Software inventory dictionary

Software	License count settings	
AAA	Number of owned licenses: 15	Warning licenses count: 12
BBB	Number of owned licenses: 15	Warning licenses count: 10
CCC	Number of owned licenses: 50	Warning licenses count: 45

3. Collect software information from clients.

4. Count the software information and check the license usage status.

Inventory Viewer

Software	Count	Owned licenses
AAA	10	15
BBB	25	15
CCC	48	50

Items with a license violation or a warning are displayed in different colors.

■ Operating procedure

To manage the number of software licenses:

1. Create a software inventory dictionary.

   To create a software inventory dictionary, collect software information from a small number of clients (1 to several).

   - For details on how to collect software information, see *3.2.1 Procedure for collecting software information* in the manual *Administrator's Guide Volume 1*.

   On the **Options** page that is displayed when a *Get software information from client* job is created, specify **Search for a file** in **Software to be searched**, and then execute the job. Execute the job for which **Search for a file** is specified on only a small number of clients (1 to several) in order to minimize the workload on the database.

   A software inventory dictionary is created on the basis of the collected software information.

2. Set the numbers of licenses in the software inventory dictionary.

   - For details on setting the software to be managed, see *3.2.5(1) Setting the software inventory information to be displayed* in the manual *Administrator's Guide Volume 1*.
   - For details on setting the numbers of licenses, see *3.2.5(3) Setting license counts* in the manual *Administrator's Guide Volume 1*.

3. Collect software information from clients.

- For details on how to collect software information, see *3.2.1 Procedure for collecting software information* in the manual *Administrator's Guide Volume 1*.

4. Use the software information to count clients and check license information.
    - For details on starting Inventory Viewer, see *4.1.1 Starting Inventory Viewer* in the manual *Administrator's Guide Volume 1*.
    - For details on how to use inventory information to count clients, see *4.2.1 Counting procedure* in the manual *Administrator's Guide Volume 1*.
    - For details on displaying license information, see *4.2.3(2) Counting hosts by software inventory* in the manual *Administrator's Guide Volume 1*.

■ Notes

- For notes on collecting system information, see *3.2.3 Notes on collecting software information* in the manual *Administrator's Guide Volume 1*.

4.5.3 Managing Microsoft Office and anti-virus software

■ Overview

By collecting information about the Microsoft Office and anti-virus software installed on the clients, you can determine which software is installed on the clients. The following explains the general procedure for determining which Microsoft Office and anti-virus software is installed on the clients.

1. Execute a *Get software information from client* job with the following options to obtain the latest software information from the clients.
    - Search for anti-virus products
    - Search for Microsoft Office products

    How information on Microsoft Office and anti-virus products is collected from clients

    (1)The managing server executes a *Get software information from client* job and sends the search information files for Microsoft Office and anti-virus products to the client.

    (2)The client searches for the products installed on the client computer based on the received search information files for Microsoft Office and anti-virus products.

    (3)The client sends the search results back to the managing server.

2. The managing server collects the Microsoft Office and anti-virus products information so that you can determine which product is installed on the clients.

■ Operating procedure

1. Collect software information from clients.
    - For details on how to collect software information, see *3.2.1 Procedure for collecting software information* in the manual *Administrator's Guide Volume 1*.
2. Use the collected information and determine which Microsoft Office and anti-virus products are installed on the clients.
    - For details on starting Inventory Viewer, see *4.1.1 Starting Inventory Viewer* in the manual *Administrator's Guide Volume 1*.
    - For details on how to use inventory information to count clients, *see 4.2.1 Counting procedure* in the manual *Administrator's Guide Volume 1*.

■ Notes

- For notes on collecting system information, *see 3.2.3 Notes on collecting software information* in the manual *Administrator's Guide Volume 1*.

4.6 Distributing software to sites

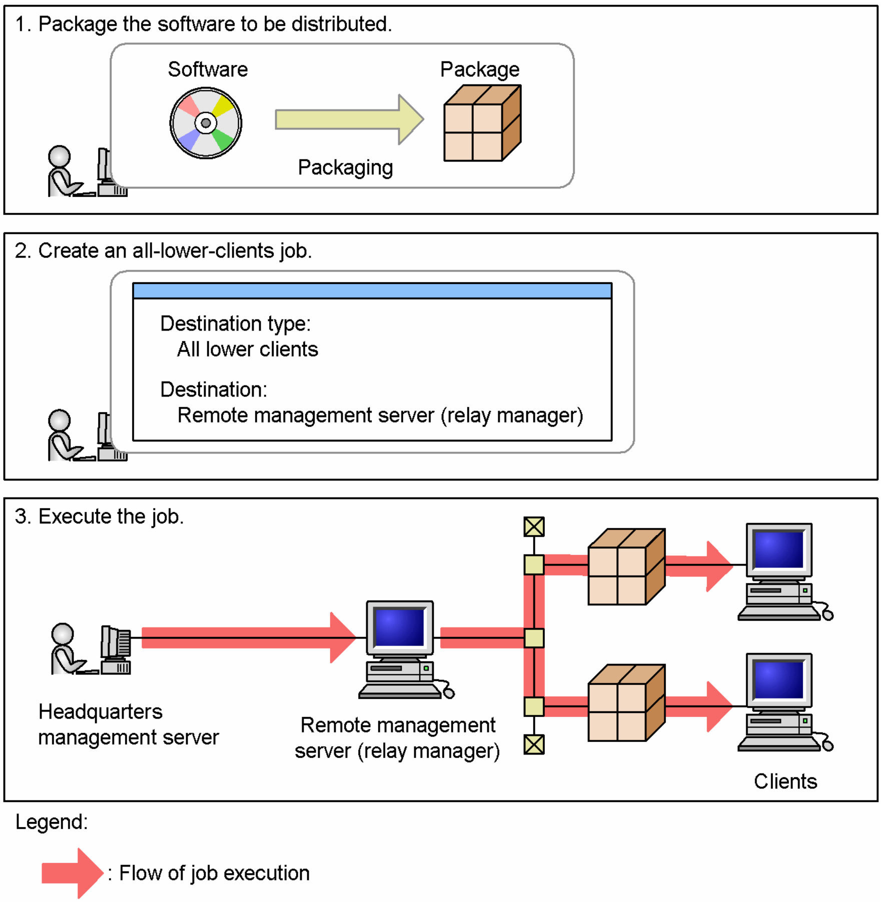
■ Overview

In a JP1/Software Distribution system configuration where the management server at the headquarters centrally manages the management servers at individual sites, by executing a job that targets the management servers at individual sites you can distribute software to all clients under the control of those servers. This type of job is referred to as an *all-lower-clients job*.

- For an overview of all-lower-clients jobs, see *5.1.2(3) Executing a job from the central manager*.

The following figure shows the general procedure for distributing software to clients under a remote management server by using an all-lower-clients job.

Figure 4–6: General procedure for distributing software to clients under a remote management server



1. Package the software to be distributed.
Software
Package
Packaging
2. Create an all-lower-clients job.
Destination type:
All lower clients
Destination:
Remote management server (relay manager)
3. Execute the job.
Headquarters management server
Remote management server (relay manager)
Clients
Legend:
: Flow of job execution

■ Operating procedure

To distribute software to each site:

1. Package the software to be distributed.
   - For details on how to package, see *2.1 Packaging procedure* in the manual *Administrator's Guide Volume 1*.
2. Create an all-lower-clients job.
   - For details on how to create the job, see *2.3.1 Remote installation execution procedure* in the manual *Administrator's Guide Volume 1*.

   On the **Destination** page, specify **All lower clients** in **Destination type**.

- For details on the settings on the **Destination** page, see *8.2.4 Setting up the Destination page* in the manual *Administrator's Guide Volume 1*.

Select the target relay manager as the destination.

3. Execute the job.

- For details on how to execute a job, see *8.3 Executing and saving a job* in the manual *Administrator's Guide Volume 1*.

Check the job execution status.

- For details on displaying the execution status, see *8.4.3 Items displayed in the Job Status window* in the manual *Administrator's Guide Volume 1*.
- For details on how to check the execution status, see *8.4.6 Displaying the execution status of all-lower-clients jobs* in the manual *Administrator's Guide Volume 1*.

Re-execute a job that resulted in an error.

- For details on how to re-execute a job, see *8.5.2 Re-executing a job* in the manual *Administrator's Guide Volume 1*.

■ Notes

- For notes on packaging, see *2.1.4 Notes on packaging* in the manual *Administrator's Guide Volume 1*.
- For notes on specifying a job destination, see *8.2.4(4) Notes on specifying destinations* in the manual *Administrator's Guide Volume 1*.
- For notes on checking the job execution status, see *8.4.2 Notes on checking the job execution status* in the manual *Administrator's Guide Volume 1*.

4.7 Distributing software at specified distribution and installation dates/times

■ Overview

You can set a schedule for distribution of software. You can also specify the date and time software is to be installed at the destination, as well as the installation timing, such as when the system starts or terminates.

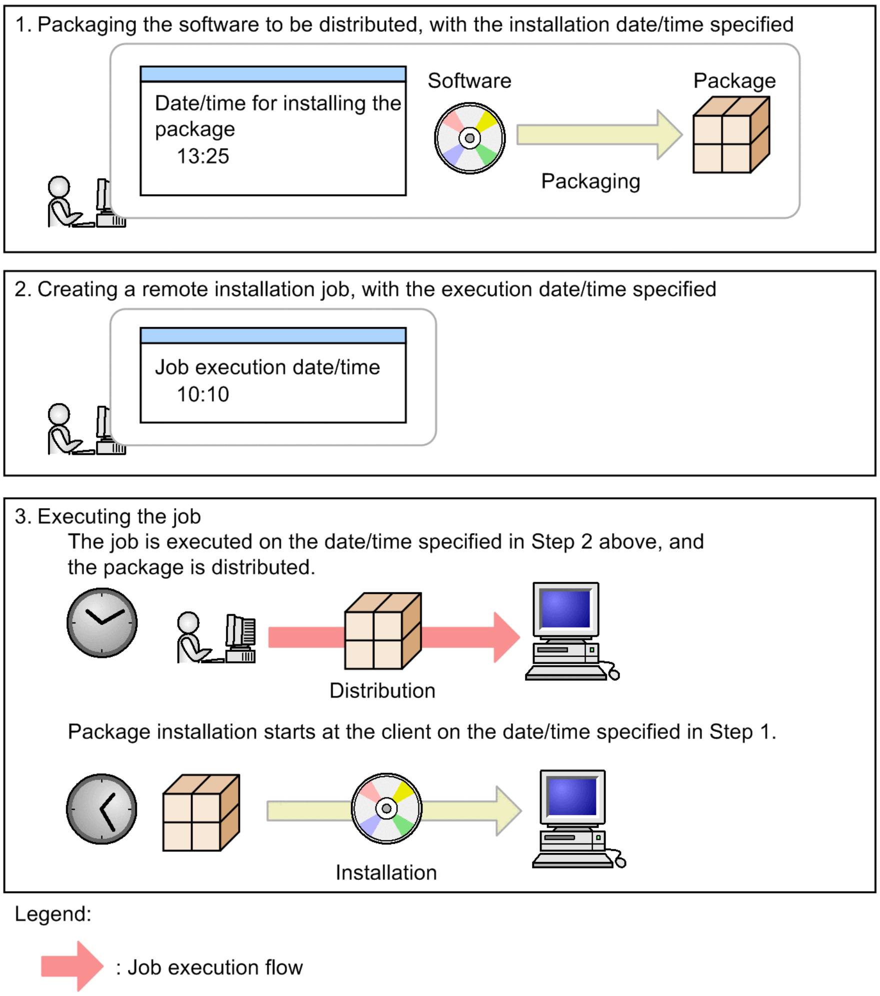
For example, if you distribute a package for which the same installation date and time is specified for multiple clients, the software can be installed on all the clients at exactly the same time.

When you package software, you can specify the date and time the software is to be installed at the clients, as well as the installation timing. You can specify the job execution date and time when you create the job.

- For an example of executing jobs at a specified date and time, see *2.5.5 Installing at a specified time* in the manual *Administrator's Guide Volume 1*.

The following figure shows the general procedure for distributing software with the dates and times of distribution and installation specified.

Figure 4–7: General procedure for distributing software with the dates and times of distribution and installation specified


1. Packaging the software to be distributed, with the installation date/time specified
Date/time for installing the package
13:25
Software
Package
Packaging
2. Creating a remote installation job, with the execution date/time specified
Job execution date/time
10:10
3. Executing the job
The job is executed on the date/time specified in Step 2 above, and the package is distributed.
Distribution
Package installation starts at the client on the date/time specified in Step 1.
Installation
Legend:
: Job execution flow

■ Operating procedure

To distribute software with the dates and times of distribution and installation specified:

1. Package the software to be distributed with the installation date/time specified.
    - For details on the packaging procedure, see *2.1 Packaging procedure* in the manual *Administrator's Guide Volume 1*.
    - For details on how to specify the package installation date/time, see *2.2.6 Schedule page* in the manual *Administrator's Guide Volume 1*.
2. Create a remote installation job with the execution date/time specified.
    - For details on how to create a job, see *2.3.1 Remote installation execution procedure* in the manual *Administrator's Guide Volume 1*.
    - For details on specifying the job execution date and time (when the job is created), see *8.2.5 Setting up the Schedule page* in the manual *Administrator's Guide Volume 1*.
3. Execute the job.
    - For details on executing a job, see *8.3 Executing and saving a job* in the manual *Administrator's Guide Volume 1*.
    - For details on the execution order of jobs, see *2.9.7 Job execution order*.

    The job is executed according to the schedule that was specified when the job was created. The package distributed to the clients is installed according to the schedule that was specified when the package was created.

    Check the job execution status.

    - For details on how to check the execution status, see *8.4.3 Items displayed in the Job Status window* in the manual *Administrator's Guide Volume 1*.

    Re-execute a job that resulted in an error.

    - For details on how to re-execute a job, see *8.5.2 Re-executing a job* in the manual *Administrator's Guide Volume 1*.

■ Notes

- For notes on packaging, see *2.1.4 Notes on packaging* in the manual *Administrator's Guide Volume 1*.
- For notes on checking the job execution status, see *8.4.2 Notes on checking the job execution status* in the manual *Administrator's Guide Volume 1*.

4.8 Sending a warning message to clients on which the most recent virus definition file has not been installed

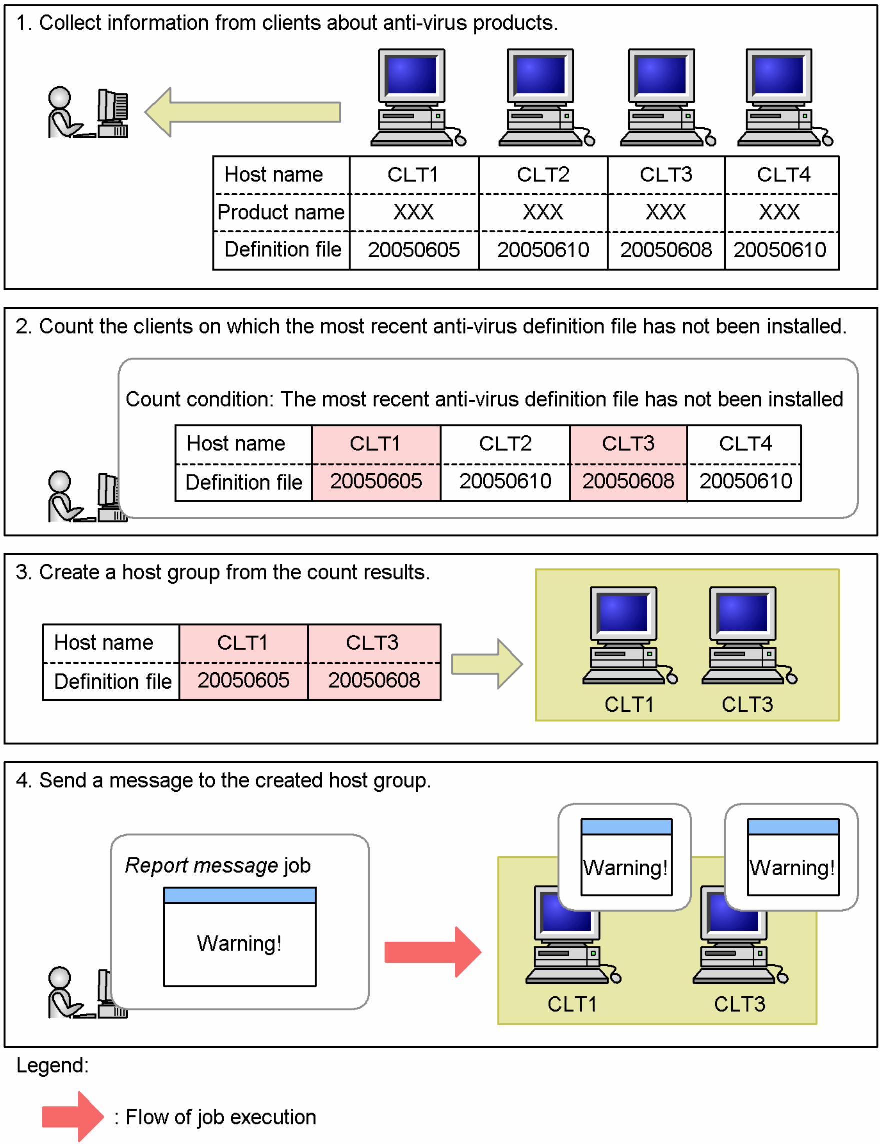
■ Overview

You can count items of inventory information collected from clients to determine whether or not the most recent anti-virus definition file has been installed. You can also group clients on the basis of the count results and send a warning message in batch mode to clients where the most recent anti-virus definition file has not been installed.

- For details on the anti-virus products for which information can be acquired by JP1/Software Distribution, see *2.2.2(1) Available software information*.

The following figure shows the general procedure for sending a warning message to clients if the most recent anti-virus definition file has not been installed.

Figure 4–8: General procedure for sending a warning message to clients if the most recent anti-virus definition file has not been installed



1. Collect information from clients about anti-virus products.

Host name	CLT1	CLT2	CLT3	CLT4
Product name	XXX	XXX	XXX	XXX
Definition file	20050605	20050610	20050608	20050610

2. Count the clients on which the most recent anti-virus definition file has not been installed.

Count condition: The most recent anti-virus definition file has not been installed

Host name	CLT1	CLT2	CLT3	CLT4
Definition file	20050605	20050610	20050608	20050610

3. Create a host group from the count results.

Host name	CLT1	CLT3
Definition file	20050605	20050608

4. Send a message to the created host group.

Legend:

🟥 : Flow of job execution

■ Operating procedure

To send a warning message to the clients on which the most recent virus definition file has not been installed:

1. Acquire information about the anti-virus products from the clients.
   - For details on how to execute the *Get software information from client* job, see *3.2.1 Procedure for collecting software information* in the manual *Administrator's Guide Volume 1*.
2. Count the clients where the most recent virus definition file has not been installed.
   - For details on starting Inventory Viewer, see *4.1.1 Starting Inventory Viewer* in the manual *Administrator's Guide Volume 1*.
   - For details on how to use inventory information to count clients, see *4.2.1 Counting procedure* in the manual *Administrator's Guide Volume 1*.
   - For details on displaying the virus-definition files, see *4.2.3(3)(a) Counting by virus definition files* in the manual *Administrator's Guide Volume 1*.

   Count the clients where the most recent virus definition file has not been installed.
3. Create a host group from the count results.
   - For details on how to create a host group from count results, see *4.2.7 Creating a host group from count results* in the manual *Administrator's Guide Volume 1*.
4. Send a message to the created host group.
   - For details on sending messages, see *7.5 Sending messages to clients* in the manual *Administrator's Guide Volume 1*.

■ Notes

- For notes on collecting software information, see *3.2.3 Notes on collecting software information* in the manual *Administrator's Guide Volume 1*.
- For notes on executing the *Report message* job, see *7.5.2 Notes on sending messages to clients* in the manual *Administrator's Guide Volume 1*.

4.9 Changing the power configuration for clients on which the power-save setting is not applied

■ Overview

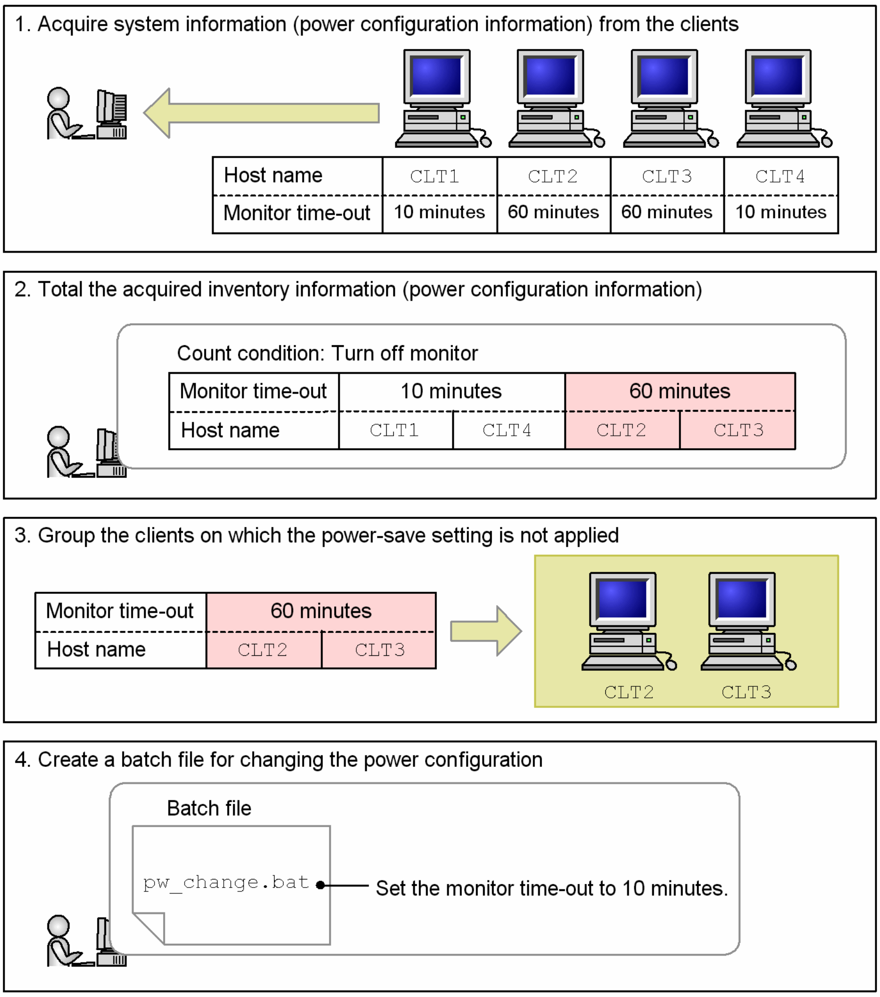
You can acquire information about the power configuration of a PC as part of the client's system information. By then totaling the power configuration information acquired from the clients, you can gain an understanding of the overall power configuration status.

- For details on the system information that can be managed by JP1/Software Distribution, see *2.2.1 Acquiring system information*.

For an environment in which the power-save settings of the PCs in the system are standardized, you can ensure that uniform power-save settings are applied throughout the system by remotely installing a batch file that changes the power configuration of clients on which the power-save setting has not been applied.

The following figure shows the general procedure for changing the power configuration of clients on which the power-save setting is not applied.

Figure 4–9: General procedure for changing the power configuration of clients on which the power-save setting is not applied (1/2)



1. Acquire system information (power configuration information) from the clients

Host name	CLT1	CLT2	CLT3	CLT4
Monitor time-out	10 minutes	60 minutes	60 minutes	10 minutes

2. Total the acquired inventory information (power configuration information)

Count condition: Turn off monitor

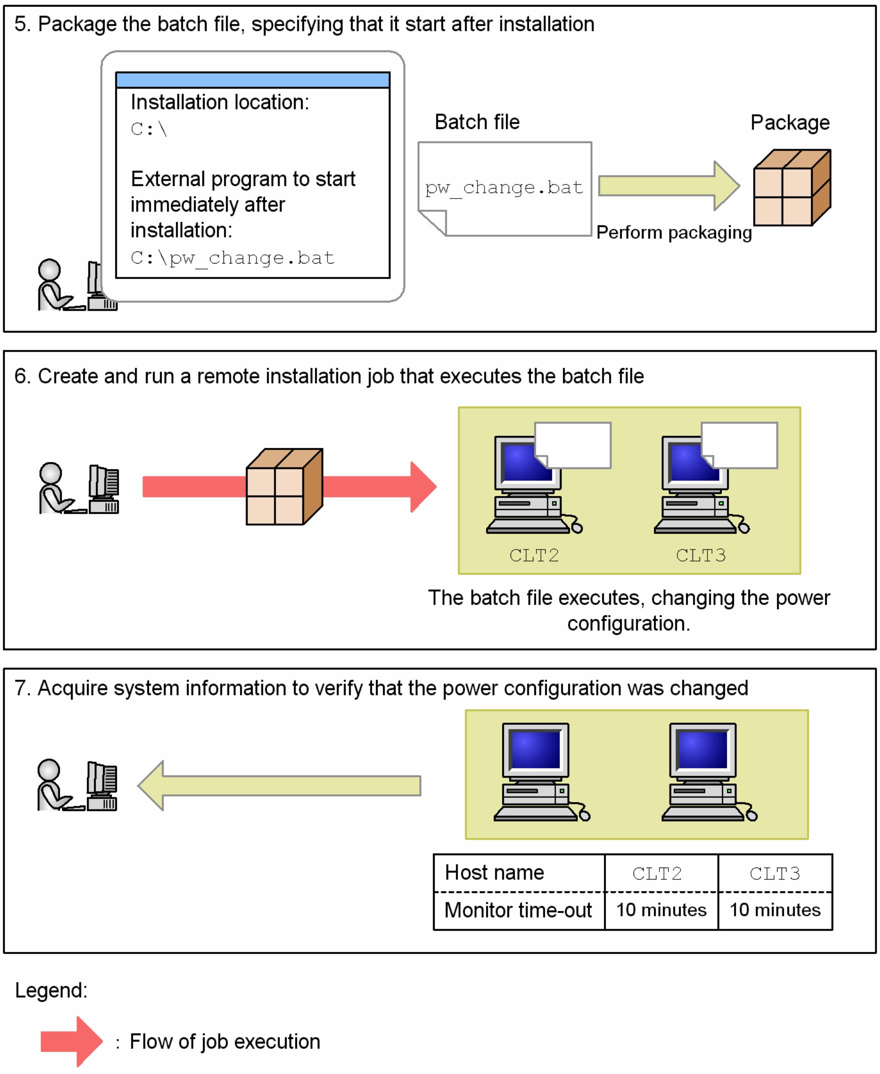
Monitor time-out	10 minutes		60 minutes	
Host name	CLT1	CLT4	CLT2	CLT3

3. Group the clients on which the power-save setting is not applied

Monitor time-out	60 minutes	
Host name	CLT2	CLT3

4. Create a batch file for changing the power configuration

Figure 4–10: General procedure for changing the power configuration of clients on which the power-save setting is not applied (2/2)


5. Package the batch file, specifying that it start after installation
Installation location:
C:\
External program to start immediately after installation:
C:\pw_change.bat
Batch file
pw_change.bat
Package
Perform packaging
6. Create and run a remote installation job that executes the batch file
CLT2
CLT3
The batch file executes, changing the power configuration.
7. Acquire system information to verify that the power configuration was changed
Legend:
: Flow of job execution

Host name	CLT2	CLT3
Monitor time-out	10 minutes	10 minutes

■ Operating procedure

To change the power configuration of clients on which the power-save setting is not applied:

1. Acquire system information (power configuration information) from the clients.
   - For details on how to acquire system information, see *3.1.1 System information collection procedure* in the manual *Administrator's Guide Volume 1*.
2. Total the acquired inventory information (power configuration information).
   - For details on how to start Inventory Viewer, see *4.1.1 Starting Inventory Viewer* in the manual *Administrator's Guide Volume 1*.
   - For details on how to total inventory information, see *4.2.1 Counting procedure* in the manual *Administrator's Guide Volume 1*.

   Count clients using a power setting such as **Turn off monitor (AC)** as the condition.
3. Group the clients on which the power-save setting is not applied.
   - For details on how to create a host group from totaled results, see *4.2.7 Creating a host group from count results* in the manual *Administrator's Guide Volume 1*.
4. Create a batch file for changing the power configuration.

You can change the power configuration by using the Windows `powercfg` command. For example, for a Windows XP client, create a batch file with the following content to set 10 minutes as the time from when a monitor is activated by AC power to the time power is turned off, and to set 20 minutes as the time until the system is set to standby:

```
powercfg /change home-or-company-desk /monitor-timeout-ac 10
powercfg /change home-or-company-desk /standby-timeout-ac 20
```

5. Package the batch file, specifying that it start after installation.

   In this step, you package the batch file. You also set the batch file you created as an external program that starts after remote installation.

   - For details on the packaging procedure, see *2.1 Packaging procedure* in the manual *Administrator's Guide Volume 1*.
   - For details on how to start a batch file, see *2.2.10 External Program page* in the manual *Administrator's Guide Volume 1*.

6. Create and run a remote installation job that executes the batch file.

   - For details on how to create a job, see *2.3.1 Remote installation execution procedure* in the manual *Administrator's Guide Volume 1*.
   - For details on how to execute a job, see *8.3 Executing and saving a job* in the manual *Administrator's Guide Volume 1*.

7. Acquire system information to verify that the power configuration was changed.

   - For details on how to acquire system information, see *3.1.1 System information collection procedure* in the manual *Administrator's Guide Volume 1*.

■ Notes

For notes on the inventory information that can be acquired, see *2.2.1(1) System information that can be obtained from a Windows client*.

4.10 Shutting down clients at a specific date and time

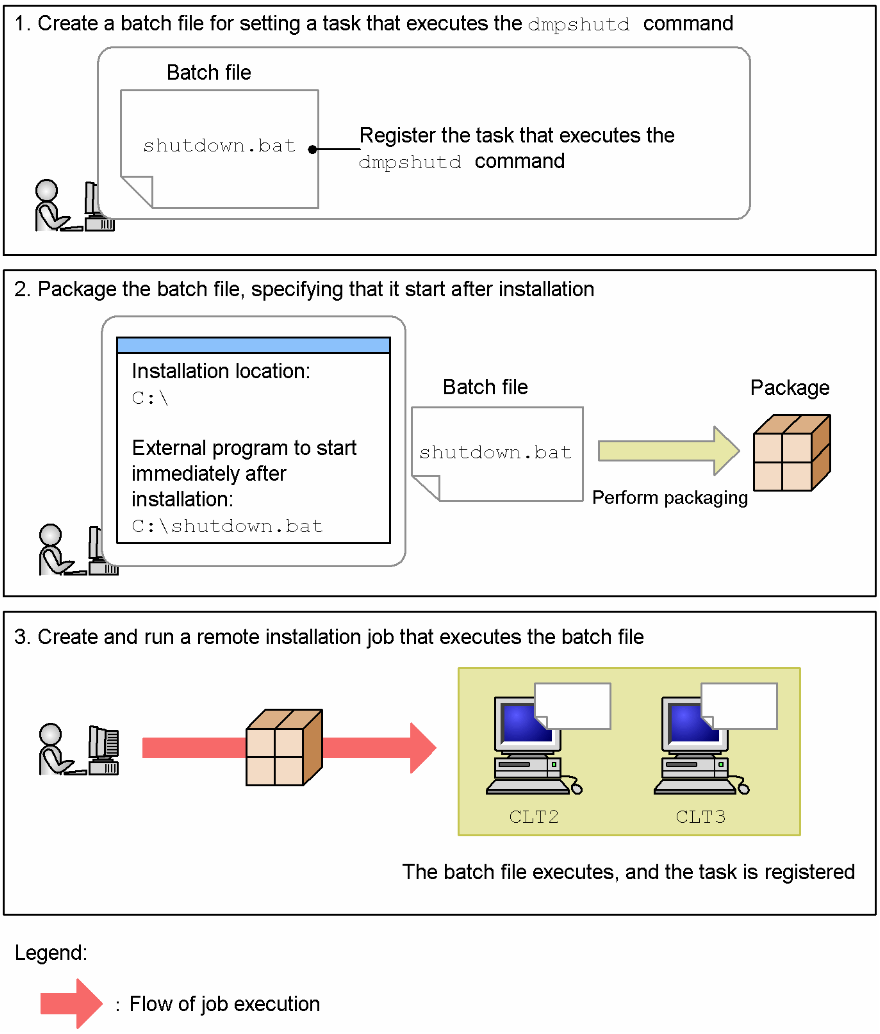
■ Overview

You can shut down a computer by executing the `dmpshutd` command on a client. By using the `dmpshutd` command with a Windows task, you can reduce power consumption by configuring the client to shut down at a specific time on specific days as a measure against the user forgetting to turn off the power.

This subsection describes how to shut down a client at 8:00 PM on Mondays through Fridays.

The following figure shows the general procedure for shutting down a client at a specific time on specific days.

Figure 4–11: General procedure for shutting down a client at a specific time on specific days


1. Create a batch file for setting a task that executes the dmpshutd command
Batch file
shutdown.bat
Register the task that executes the dmpshutd command
2. Package the batch file, specifying that it start after installation
Installation location:
C:\
External program to start immediately after installation:
C:\shutdown.bat
Batch file
shutdown.bat
Package
Perform packaging
3. Create and run a remote installation job that executes the batch file
CLT2
CLT3
The batch file executes, and the task is registered
Legend:
: Flow of job execution

■ Operating procedure

1. Create a batch file for setting a task that executes the `dmpshutd` command.

   Create a batch file that sets a task for executing the `dmpshutd` command on a client at 8:00 PM on Monday through Friday. The content of the batch file to create is as follows:

```
AT 20:00 /interactive /every:M,T,W,Th,F
"C:\Program Files\Hitachi\NETMDMP\BIN\dmpshutd.exe" /USER,8 > C:\at.txt
```

   The execution results of the batch file are output to `C:\at.txt`.

   Whenever you execute the `dmpshutd` command, make sure to specify the `/USER,8` option.

2. Package the batch file, specifying that it start after installation.

   In this step, you package the batch file. You also set the batch file you created as an external program that starts after remote installation.

   - For details about the packaging procedure, see *2.1 Packaging procedure* in the manual *Administrator's Guide Volume 1*.
   - For details on how to start a batch file, see *2.2.10 External Program page* in the manual *Administrator's Guide Volume 1*.

3. Create and run a remote installation job that executes the batch file.

   - For details on how to create a job, see *2.3.1 Remote installation execution procedure* in the manual *Administrator's Guide Volume 1*.
   - For details on how to execute a job, see *8.3 Executing and saving a job* in the manual *Administrator's Guide Volume 1*.

To cancel the shutdown setting, use the same procedure to remotely install a batch file with the following content on the client:

```
@echo off
FOR /F "tokens=4" %%i in (C:\at.txt) do set atdel=%%i
at %atdel% /DELETE
exit
```

■ Notes

When you cancel a shutdown setting, remote installation cannot be used to delete the batch file execution results (`C:\at.txt` in the above procedure). You must manually delete the file using a task registered on the client.

4.11 Distributing software to new clients automatically

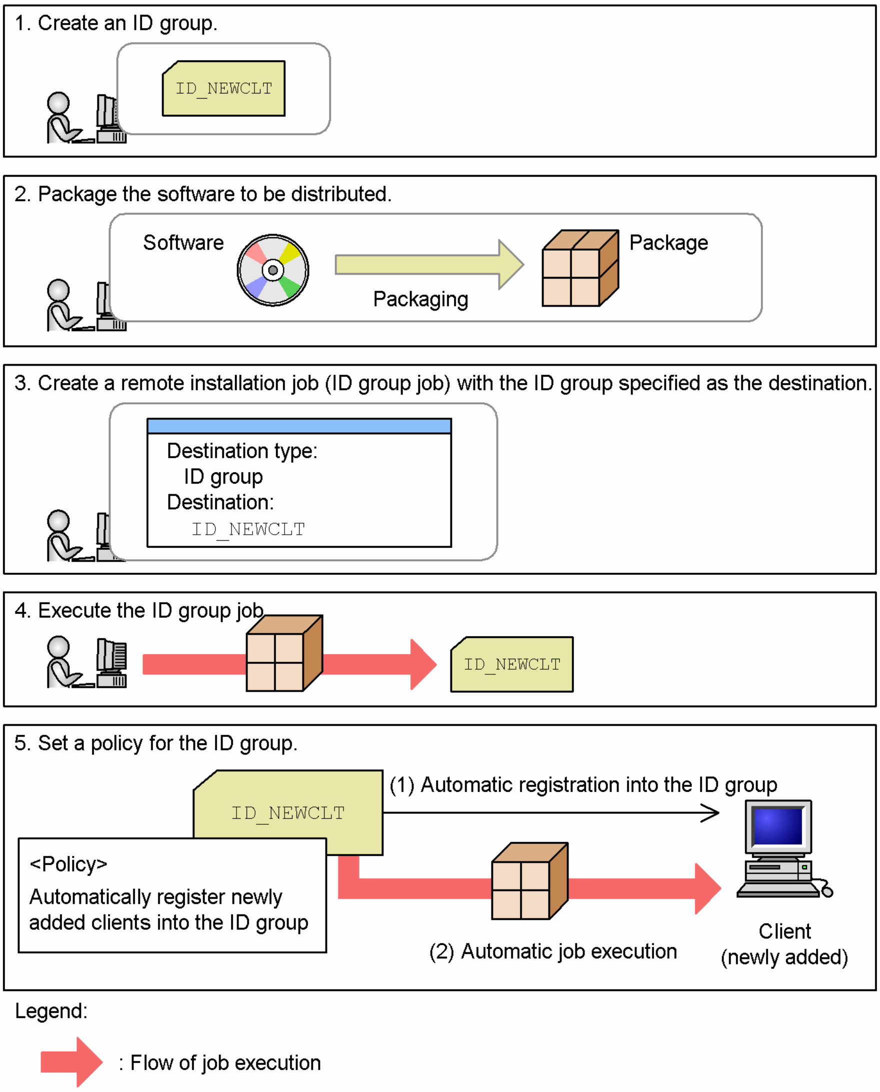
■ Overview

If you set conditions (a *policy*) for an ID group, new clients that are added to a system managed by JP1/Software Distribution can be automatically registered into that ID group.

By executing a software distribution job for the ID group in advance, you can have that software distributed automatically to new clients whenever they are added to the ID group. This is useful for security because it allows you to distribute necessary software, such as anti-virus products, whenever a new computer is added.

The following figure shows the general procedure for creating the ID group `ID_NEWCLT` and then automatically distributing software to clients who are added to that ID group.

Figure 4–12: General procedure for automatically distributing software to newly added clients


1. Create an ID group.
ID_NEWCLT
2. Package the software to be distributed.
Software
Packaging
Package
3. Create a remote installation job (ID group job) with the ID group specified as the destination.
Destination type:
ID group
Destination:
ID_NEWCLT
4. Execute the ID group job.
ID_NEWCLT
5. Set a policy for the ID group.
ID_NEWCLT
<Policy>
Automatically register newly added clients into the ID group
(1) Automatic registration into the ID group
(2) Automatic job execution
Client
(newly added)
Legend:
: Flow of job execution

■ Operating procedure

To automatically distribute software to new clients:

1. Create an ID group.
   - For details on how to create ID groups, see *8.3.2 Creating an ID group* in the *Setup Guide*.
2. Package the software to be distributed.

- For details on software packaging, see *2.1 Packaging procedure* in the manual *Administrator's Guide Volume 1*.

3. Create a remote installation job (ID group job) with the ID group specified as the destination.
    - For details on how to create a remote installation job, see *2.3.1 Remote installation execution procedure* in the manual *Administrator's Guide Volume 1*.
    - For details on how to specify a destination during job creation, see *8.2.4 Setting up the Destination page* in the manual *Administrator's Guide Volume 1*.
4. Execute the job.
5. Set policies for the ID group.

    New clients will be registered automatically into the ID group.

    Once a new client is registered into the ID group, the next time that client establishes connection with the higher system, the job executed for the ID group is executed automatically at the client.
    - For details on how to set a policy for an ID group, see *9.4 Automatic maintenance of ID groups* in the *Setup Guide*.

    Check the job execution status.
    - For details on displaying the execution status, see *8.4.3 Items displayed in the Job Status window* in the manual *Administrator's Guide Volume 1*.
    - For details on how to check the execution status, see *8.4.5 Displaying the execution status of ID group jobs* in the manual *Administrator's Guide Volume 1*.

    Re-execute a job that resulted in an error.
    - For details on re-execution settings, see *8.5.2(1)(b) Re-executing an ID group job* in the manual *Administrator's Guide Volume 1*.
    - For details on how to re-execute jobs, see *8.5.2(2) Re-executing a job that resulted in an error* in the manual *Administrator's Guide Volume 1*.

■ Notes

- For notes on packaging, see *2.1.4 Notes on packaging* in the manual *Administrator's Guide Volume 1*.
- For notes on using ID groups, see *8.3.5 Notes on using ID groups* in the *Setup Guide*.
- For notes on linking system configuration information and ID groups, see *8.4.3 Notes on linking system configuration information and ID groups* in the *Setup Guide*.
- For notes on checking the execution status of ID group jobs, see *8.4.5(4) Notes on checking the execution status of an ID group job* in the manual *Administrator's Guide Volume 1*.
- For notes on automatically adding clients to ID groups, see *9.4.2 Notes on using automatic maintenance of ID groups* in the *Setup Guide*.

4.12 Using remote control to maintain a malfunctioning client from the managing server

If an error occurs at a client, JP1/Software Distribution can notify the server automatically (report an alert). By controlling a malfunctioning remote client from the server, (remote control), the system administrator can directly check the problem and recover from the malfunction (error).

This section describes how an error is reported from a client to the server, how the server checks the malfunctioning client, and how a remote client can be controlled from the server.

4.12.1 Notifying the server of errors

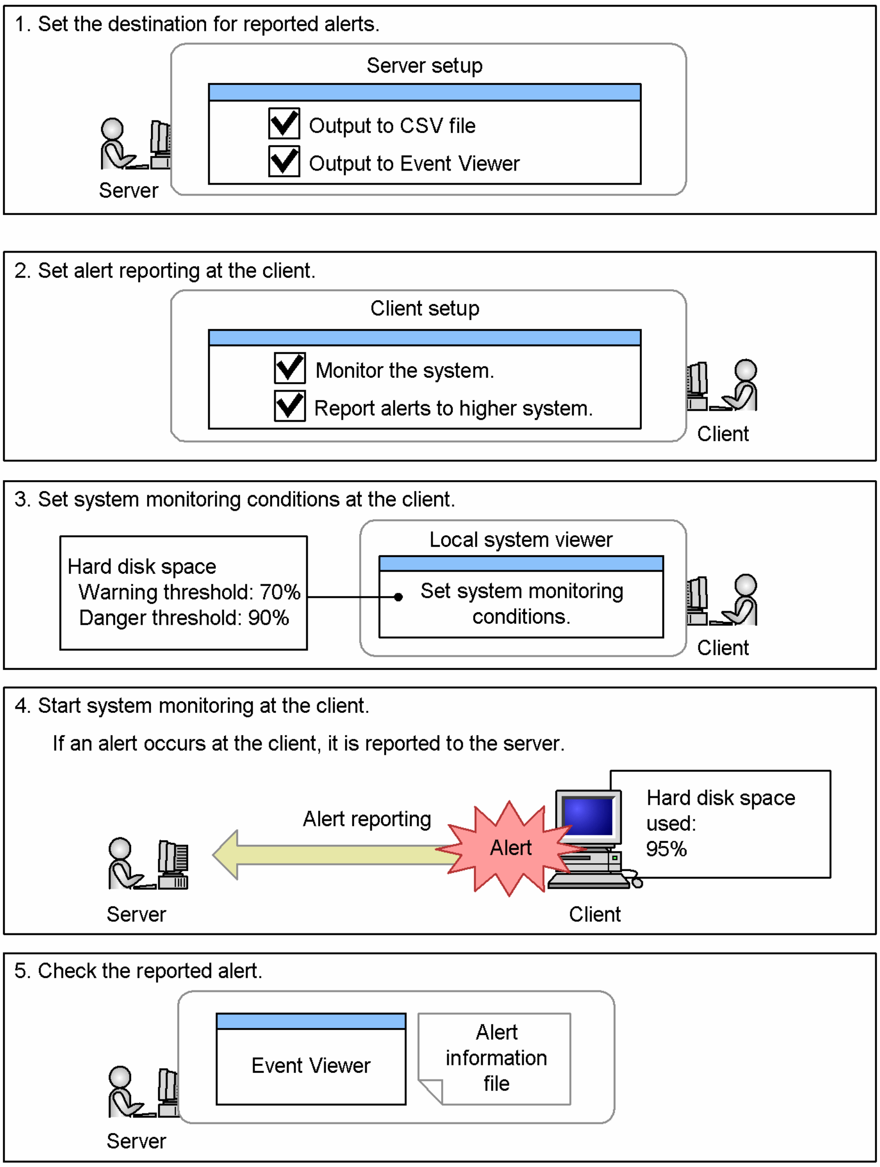
■ Overview

When system monitoring conditions set at the client are satisfied, an alert is sent from a client to the server. The server uses the output alert information to check the client that reported the alert.

- For an overview of alert reporting, see *1.2.5(3) Monitoring a client system*.

The following figure shows the general procedure for reporting errors that occurred at a client to the server.

Figure 4–13: General procedure for reporting errors at a client to the server


1. Set the destination for reported alerts.
Server setup
☑ Output to CSV file
☑ Output to Event Viewer
Server
2. Set alert reporting at the client.
Client setup
☑ Monitor the system.
☑ Report alerts to higher system.
Client
3. Set system monitoring conditions at the client.
Hard disk space
Warning threshold: 70%
Danger threshold: 90%
Local system viewer
Set system monitoring conditions.
Client
4. Start system monitoring at the client.
If an alert occurs at the client, it is reported to the server.
Alert reporting
Alert
Hard disk space used: 95%
Server
Client
5. Check the reported alert.
Event Viewer
Alert information file
Server

■ Operating procedure

To report errors at a client to the server:

1. Set the destination for reported alerts.
    - For details on server settings, see *4.2.13 Client Alert page* in the *Setup Guide*.
    - For details on settings for relaying alerts, see *7.4.2 Relaying alert information* in the manual *Administrator's Guide Volume 1*.
2. Set alert reporting at the client.
    - For details on the client settings, see *11.8.4(4) Reporting an alert to a higher system* in the manual *Administrator's Guide Volume 1*.
    - For details on the client settings, see *6.2.9 System Monitoring page* in the *Setup Guide*.
3. Set system monitoring conditions at the client.
    - For details on setting up the system monitoring conditions, see *11.8.2 Specifying system monitoring conditions* in the manual *Administrator's Guide Volume 1*.

4. Start system monitoring at the client.
    - For details on how to start system monitoring, see *11.8.1 Starting or stopping system monitoring* in the manual *Administrator's Guide Volume 1*.
5. Check the alert reported from the client.
    - For details on how to check a reported alert, see *7.4.1 Checking alert information* in the manual *Administrator's Guide Volume 1*.

■ Notes

- For notes on checking alerts, see *7.4.1(1)(c) Notes on using the alert information file* in the manual *Administrator's Guide Volume 1*.

4.12.2 Controlling a remote client

■ Overview

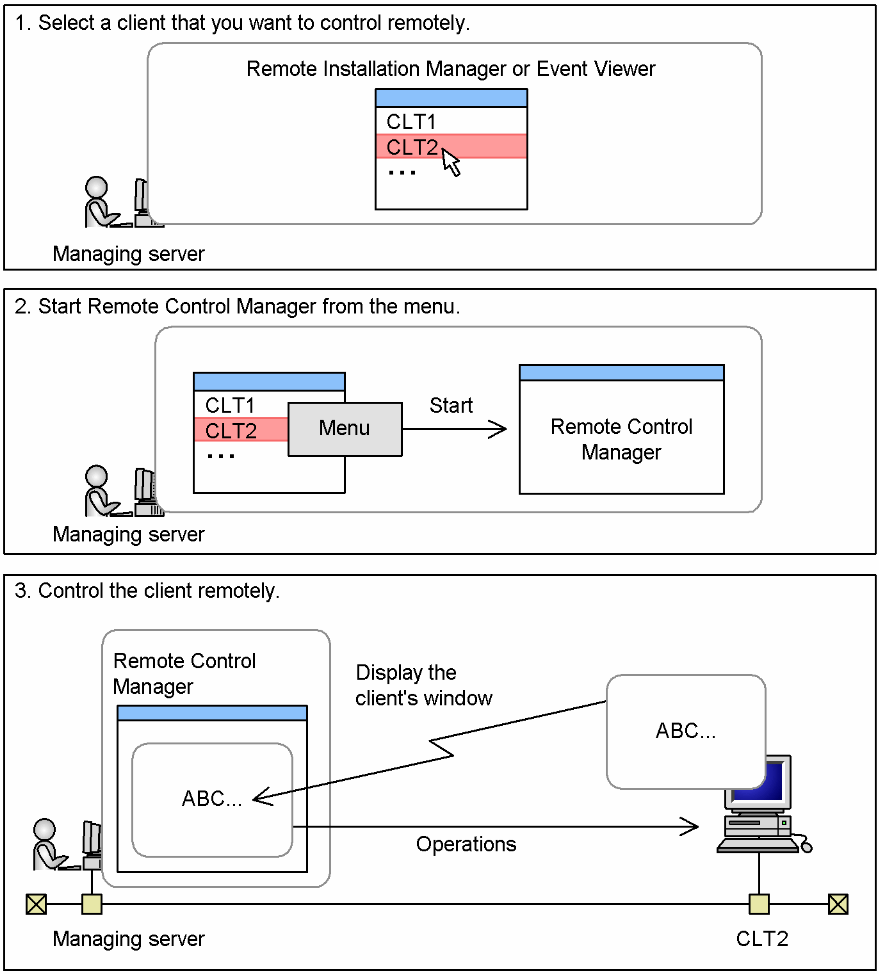
You can control a selected client remotely by selecting the client from the JP1/Software Distribution system configuration displayed in the Remote Installation Manager's System Configuration window, Destination window, or Directory Information window and then starting Remote Control Manager.

You can also start Remote Control Manager by selecting a client displayed in inventory information count results.

- For an overview of remote control, see *2.8 Controlling remote clients*.

The following figure shows the general procedure for controlling a client remotely.

Figure 4–14: General procedure for controlling a client remotely


1. Select a client that you want to control remotely.
Remote Installation Manager or Event Viewer
CLT1
CLT2
...
Managing server
2. Start Remote Control Manager from the menu.
CLT1
CLT2
...
Menu
Start
Remote Control Manager
Managing server
3. Control the client remotely.
Remote Control Manager
ABC...
Display the client's window
ABC...
Operations
Managing server
CLT2

■ Prerequisites

- For details on the required system configuration, see *1.3.6 System components required for using the remote control facility*.

■ Operating procedure

To control a remote client when using the JP1/Software Distribution system configuration:

1. From the Remote Installation Manager's System Configuration window, Destination window, or Directory Information window select the remote client that you want to control.
2. From **Options**, choose **Start Remote Control Manager** to start Remote Control Manager.
3. Control the remote client.
    - For details on how to operate Remote Control Manager, see the manual *Job Management Partner 1/Remote Control Description and Operator's Guide*.

To control a remote client when using inventory information count results:

1. Count the relevant items in the inventory.
    - For details on how to start Inventory Viewer, see *4.1.1 Starting Inventory Viewer* in the manual *Administrator's Guide Volume 1*.
    - For details on how to count items in the inventory, see *4.2.1 Counting procedure* in the manual *Administrator's Guide Volume 1*.

2. From the count results, select the remote client that you want to control.
3. From the menu, start Remote Control Manager.
    - For details on how to start Remote Control Manager by using the count results, see *4.6 Using the remote control facility* in the manual *Administrator's Guide Volume 1*.
4. Control the remote client.
    - For details on how to operate Remote Control Manager, see the manual *Job Management Partner 1/Remote Control Description and Operator's Guide*.

5 Designing a JP1/Software Distribution System

Before you install JP1/Software Distribution programs, it is important to review the configuration of the overall system, taking into account various elements such as the structure of your organization, the number of computers, and their performance characteristics.

This chapter describes the items to be evaluated before you install JP1/Software Distribution and provides guidelines for designing the system configuration and determining the hardware requirements.

5.1 Designing the system configuration

JP1/Software Distribution supports systems of any size, from small and medium systems (with several dozen to several hundred clients) to large systems (with several thousand or more clients).

This section describes the design of a system configuration tailored to the size of your system and your environment.

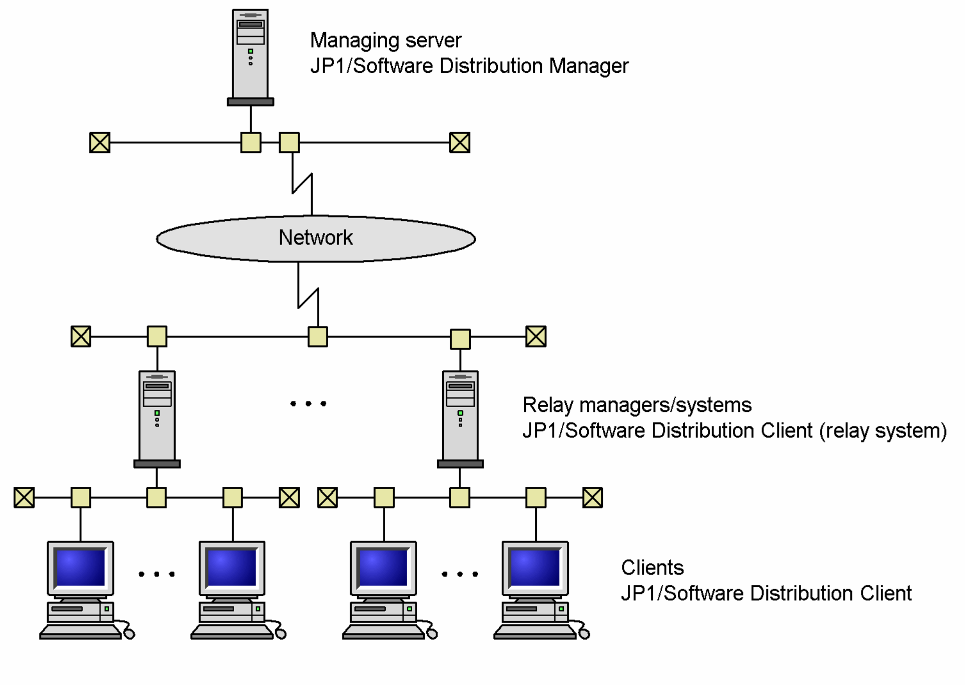
5.1.1 Designing a basic system configuration

In a network in which several dozen to several hundred clients are connected via a LAN in each building or workplace and the workplaces are connected via a WAN, a basic configuration is a multi-level hierarchy in which JP1/Software Distribution Manager handles distribution management and asset management for the entire system and JP1/Software Distribution Client (relay system) acts as a relay at each site.

JP1/Software Distribution Client (relay system) can function not only as a relay system but also as a managing server for the clients in the same LAN.

The following figure shows a basic configuration of JP1/Software Distribution.

Figure 5–1: Basic system configuration


Managing server
JP1/Software Distribution Manager
Network
Relay managers/systems
JP1/Software Distribution Client (relay system)
Clients
JP1/Software Distribution Client

We recommend that, in general, a maximum of 200 clients be connected directly to a managing server, although the number depends on the hardware environment. If more than 200 clients are to be managed, consider installing relay systems, taking into account the way in which the system is used and the network configuration.

For details about the placement of relay systems and other points that need to be checked, see *5.1.4 Evaluating a system configuration that uses relay managers/systems*.

5.1.2 Designing a large-scale system configuration

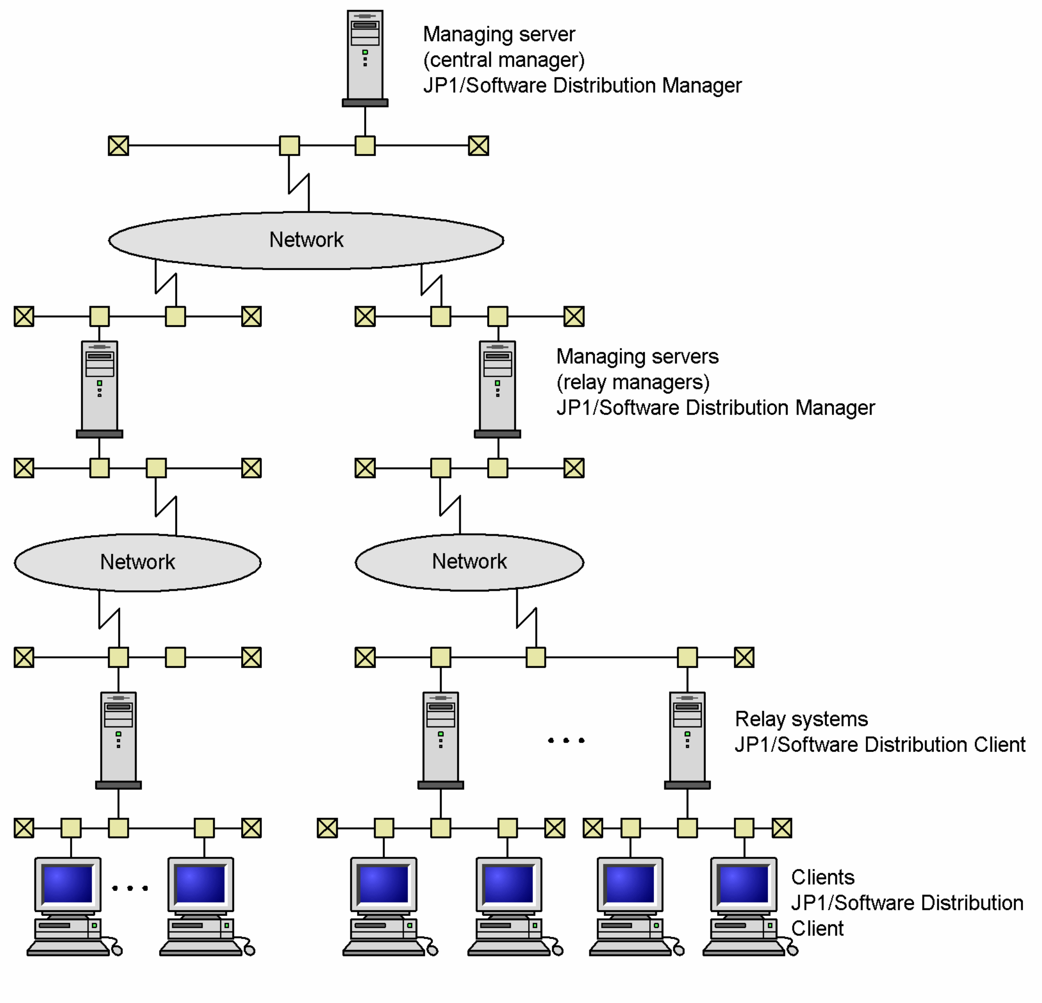
In a large-scale, nationwide system consisting of several thousand clients or more, it is difficult for a single JP1/Software Distribution Manager to handle all management tasks. In such a case, JP1/Software Distribution Client (relay system) can be used as a managing server for each department. However, such a configuration has limitations: for example, jobs can be executed on the next lower hierarchical level only, and fewer job types can be executed.

We recommend that you configure JP1/Software Distribution Manager in a hierarchy. Under the JP1/Software Distribution Manager (central manager) that manages the entire system, you should place JP1/Software Distribution

Managers (relay managers) with relay facilities to handle operations at the various departments. Such a configuration greatly reduces the workload of the managing server that manages the overall system.

The following figure shows an example of a JP1/Software Distribution system configuration for a large-scale network.

Figure 5–2: Configuration of a large-scale system


Managing server
(central manager)
JP1/Software Distribution Manager
Network
Managing servers
(relay managers)
JP1/Software Distribution Manager
Network
Network
Relay systems
JP1/Software Distribution Client
Clients
JP1/Software Distribution
Client

To operate a large JP1/Software Distribution system, you must be familiar with the following, in addition to the operation of the basic system configuration:

- Advantages of managing servers in a hierarchical configuration
- Managing system configuration information under relay managers
- Executing a job from the central manager

These topics discussed below.

(1) Advantages of managing servers in a hierarchical configuration

When JP1/Software Distribution Managers are used in a hierarchical configuration, a hierarchy with the relay manager of each department at its apex is treated as one of the JP1/Software Distribution systems. This provides the following benefits:

- Different client identification keys can be used for departments

  In a JP1/Software Distribution system, individual hosts must be identified using standardized host names or IP addresses. When JP1/Software Distribution Managers are configured in a hierarchy, the choice of host names or IP addresses can be made for each relay manager instead of at the system level.

- Each department can have unique management items

  JP1/Software Distribution has a facility that enables the system administrator to create unique management items for collecting needed information, such as user inventory and registry information. These management items can be set separately for the central manager and for the relay managers. In a large network, it may be desirable to manage some information on a system-wide basis and other information by department. Information appropriate to each level can be collected in this way.

  For details about managing registry information, see *2.2.1 Acquiring system information*. For details about managing user inventory information, see *2.2.3 Acquiring user inventory information*.

(2) Managing system configuration information under relay managers

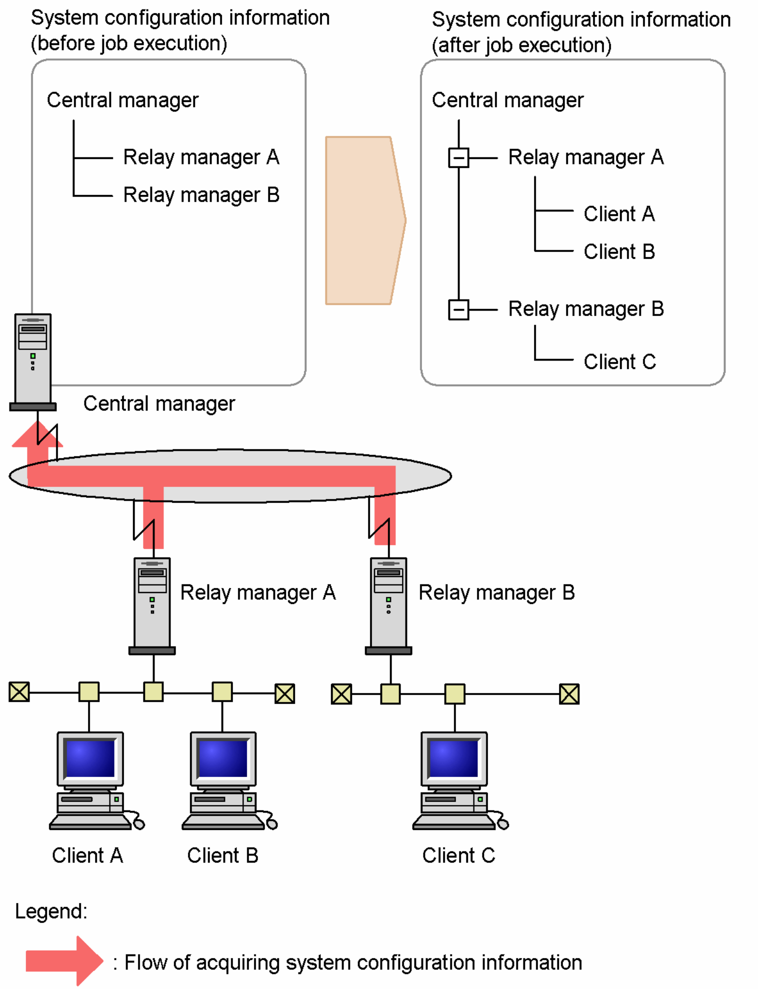
If a relay manager is placed under the central manager, the central manager cannot perform operations on system configuration components under the relay manager (for example, it cannot add, move, or remove lower relay systems or clients). Only the relay manager can perform operations on the system configuration components below it.

Consequently, if you build a large-scale JP1/Software Distribution system in which JP1/Software Distribution Managers are configured in a hierarchy, at each main site you should first build a basic system that has a relay manager at its apex, and then create system configuration information at each of those relay managers. After that, you can install the central manager and define the managing servers at all the main sites as relay managers.

After you set up, at the central manager, a JP1/Software Distribution Manager at each main site as a relay manager, you must collect information on the system configuration under each relay manager. To perform a batch operation that collects all this information from one relay manager, execute a *Get system configuration information* job with the relay manager as the job destination. The system configuration information managed by that relay manager is then transferred and displayed in the System Configuration window of the central manager. To collect, from a higher relay manager in a multiple-level hierarchy, the system configuration information of a lower relay manager, specify the lower relay manager as the destination.

The following figure shows the general procedure for collecting system configuration information from relay managers by executing a *Get system configuration information* job.

Figure 5–3: Collecting system configuration information from relay managers



After the information has been collected, all relay managers, relay systems, and clients within the network can be handled as normal destinations. Also, if you use the central manager to create IDs, you can set up all relay managers and relay systems within the network as relays that can manage the IDs.

To keep the information in the System Configuration window up to date, when you set up the central manager and relay managers you should specify the option that automatically registers and applies system configuration information. Changes to the system configuration under a relay manager will then be relayed automatically to the central manager.

(3) Executing a job from the central manager

From a managing server, you can normally specify any of three types of job destinations: a host group, an ID group, or a single client. However, if JP1/Software Distribution Managers are arrayed in a hierarchical configuration, the highest manager (the central manager) can execute a job specifying all lower clients (all-lower-clients job) as the destination. All lower clients means all hosts under the relay managers. If you execute an all-lower-clients job for a specific relay manager, the relay manager that received the job executes it for all its lower clients.

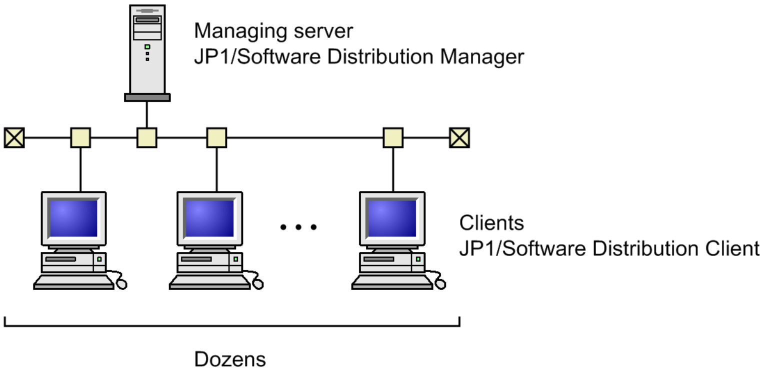
The central manager can check the execution results of an all-lower-clients job based on the number of clients (total count and count per set of execution results). You can also check the execution status of each client if you specify, during relay manager setup, that the execution results of all-lower-clients jobs are to be recorded.

If you re-execute an all-lower-clients job from the central manager, the relay manager automatically detects and re-executes the job for only those clients whose job status is **Waiting for transmission** or **Error**.

5.1.3 Designing a small-scale system configuration

For a system in which the number of clients connected via a LAN is in the dozens, you can manage the clients by using JP1/Software Distribution Manager only, and do not need to use relay managers/systems. The following figure shows the configuration of a small-scale JP1/Software Distribution system.

Figure 5–4: Configuration of JP1/Software Distribution in a small-scale system


Managing server
JP1/Software Distribution Manager
Clients
JP1/Software Distribution Client
Dozens

5.1.4 Evaluating a system configuration that uses relay managers/ systems

Relay systems can be used to reduce the workload on the managing server and the network in a JP1/Software Distribution system. Using relay systems enables you to manage a large number of clients in a hierarchical configuration. Relay systems can also reduce the number of clients that are connected directly to the managing server and the volume of data to be handled by the network.

For clients in a virtual environment, the number of operation logs collected increases in proportion to the number of login users. Therefore, we recommend that you use an operation mode in which clients are directly connected to the managing server.

(1) Guidelines for placing relay systems

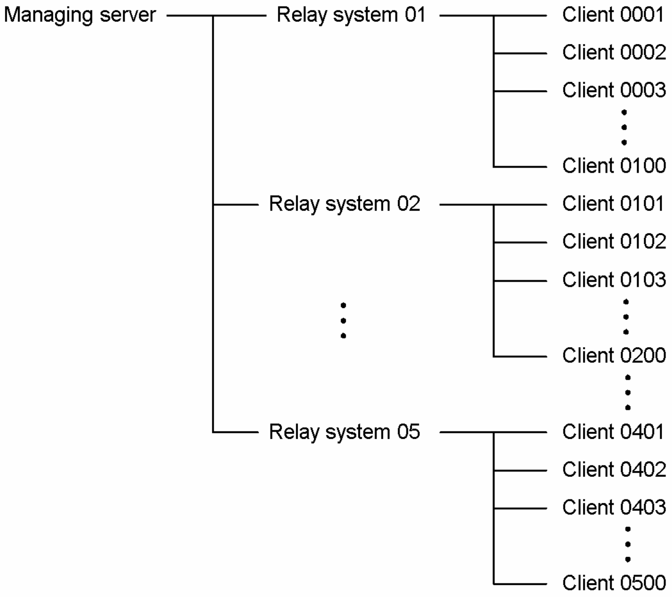
We recommend that, in general, a maximum of 200 clients be connected directly to a managing server, although the number depends on the hardware environment. If more than 200 clients are to be managed, we recommend installing relay manager/systems between the managing server and the clients

If you are using the managing server functions on a relay system, we recommend that you connect no more than 1,000 machines directly to that relay system.

If you are not using the managing server functions on a relay system, we recommend that you connect no more than 200 clients directly to that relay system. Once the number of managed clients exceeds 200, you should consider installing another relay manager.

For example, in a configuration in which JP1/Software Distribution is installed in a medium-sized network of 500 clients and managing server functions are used to manage the clients, the following figure depicts a system configuration that could be considered.

Figure 5–5: Guidelines for installing relay managers/systems



You can manage a larger number of clients by increasing the number of relay system hierarchies. However, if there are too many hierarchies, processes such as software distribution may slow down. You should determine an appropriate number of hierarchies by considering hardware acquisition costs as well as network performance.

During setup of a managing server, you can set **Number of subsystems that can be connected at one time** to limit the number of subsystems that can be connected simultaneously. Similarly, during setup of a relay system, you can set **Number of clients that can be connected at one time** to limit the number of clients that can be connected simultaneously. You should tune these settings based on data such as the network's workload and server CPU usage factors.

(2) Determining the appropriate number of relay system hierarchies

An extremely large number of clients can be managed by setting up an appropriate number of relay system hierarchies. However, hardware costs increase as the number of relay systems increases, because relay systems require better hardware performance than clients. Moreover, if a software package must pass through many relay systems before reaching clients, it may take too long to distribute software. Therefore, you must determine an appropriate number of relay system hierarchies by taking into consideration hardware implementation costs and network performance.

(3) Limits on the number of relay system hierarchies

The number of relay systems must be within the following limits:

- The maximum number of hierarchies is seven.
- The combined total length of all host names in the system (excluding the managing server, which is at the top of the hierarchies) must not exceed 255 bytes.

The following explains the limit on the number of hierarchies based on the host name length.

To execute a job from a managing server, you specify processing-target clients. The route from the managing server to the clients is managed by an address that consists of the host names of all the relay systems and clients involved in the processing. The address format is as follows.

If DNS is not used:

host-name ! *host-name...*

If DNS is used:

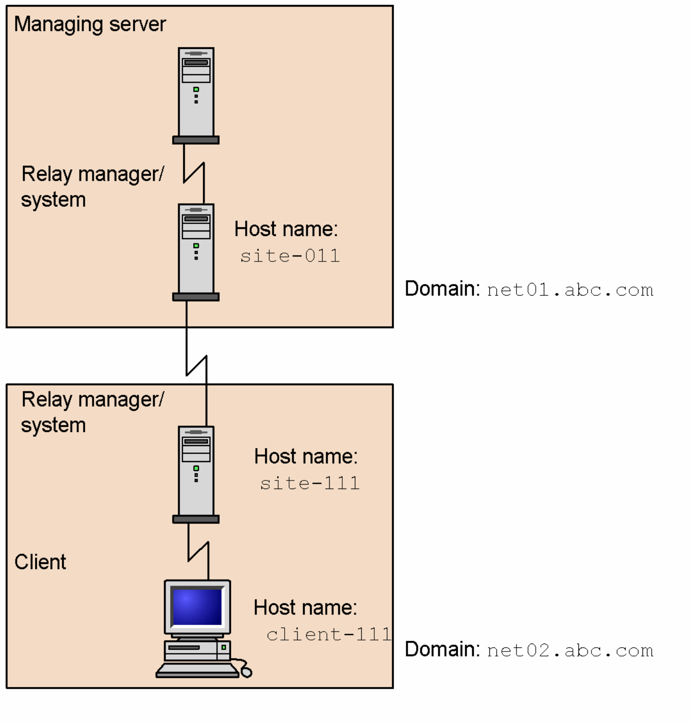
host-name **.** *domain-name* ! *host-name* **.** *domain-name...*

Host names are delimited by an exclamation point (`!`). If DNS is used, specify a host in the format *host-name*`.`*domain-name*. The maximum address length is 255 bytes, including the delimiters (`!` and `.`). You can specify up to 64 bytes for a single host name.

Relay systems must observe these limits. Therefore, very long host names or long DNS domain names will limit the number of relay system hierarchies.

The following figure shows an example of a relay manager/system hierarchy.

Figure 5–6: Example of relay manager/system hierarchy



In this example, the managing server manages the following addresses:

If DNS is not used:

- Address of the relay manager/system: `site-111`
  `site-011!site-111` (17 bytes)
- Address of the client: `client-111`
  `site-011!site-111!client-111` (28 bytes)

If DNS is used:

- Address of the relay manager/system: `site-111`
  `site-011.net01.abc.com!site-111.net02.abc.com` (49 bytes)
- Address of the client: `client-111`
  `site-011.net01.abc.com!site-111.net02.abc.com!client-111.net02.abc.com` (76 bytes)

5.1.5 Supported databases

The managing server uses a relational database to manage various information, such as packages, job execution results, and inventory information.

JP1/Software Distribution supports the following relational databases:

- Embedded RDB

The standard embedded relational database provided by JP1/Software Distribution Manager. If you are using Embedded RDB, there is no need to provide another relational database program.

- Microsoft SQL Server

  Microsoft Corporation's relational database. To use this database, you must provide programs in addition to JP1/ Software Distribution.
- Oracle

  Oracle Corporation's relational database. To use this database, you must provide programs in addition to JP1/ Software Distribution.

  If the OS is Windows Server 2012, Windows Server 2008 R2, or Windows Server 2008, Oracle cannot be used.

Full JP1/Software Distribution functionality is available no matter which of these databases you use. Choose the relational database that best suits your environment.

(1) Programs required for the relational database

If you use Embedded RDB, there is no need to provide additional programs, because the relational database is included.

If you use Microsoft SQL Server or Oracle, you must provide the following programs:

- Relational database server

  The server program that manages database information. You can use Microsoft SQL or Oracle.
- Relational database client

  The client functionality for gaining access to database information.

For notes on and details about the system configuration for using a relational database, see *7. Setting Up a Relational Database* in the *Setup Guide*.

(2) Selecting the storage destination for package data

JP1/Software Distribution uses the relational database to manage various types of management information, but you can specify settings such that the package data to be distributed will be stored in a file system.

To specify the storage destination for package data, you use the Select Database for Saving Packages dialog box when you install JP1/Software Distribution Manager.

Listed below are operational differences that depend on where package data is stored. Select the storage destination that matches your purpose.

If you store package data in the relational database:

  Backing up administration information for JP1/Software Distribution is easier.

If you store package data in a file system:

  Package transfer performance during remote installation is improved compared with when package data is stored in the relational database.

5.1.6 Compatibility between versions

JP1/Software Distribution Manager and JP1/Software Distribution Client are compatible between all versions. So, for example, you can connect any version of JP1/Software Distribution SubManager and JP1/Software Distribution Client to a specific version of JP1/Software Distribution Manager. If you use an early version of a program, you can use only the facilities supported by that version.

For details about compatibility between versions of Remote Control Manager and Remote Control Agent, see the manual *Job Management Partner 1/Remote Control Description and Operator's Guide*.

5.1.7 System date/time and time zone settings

This subsection describes the system date/time and time zone settings in the JP1/Software Distribution system.

(1) System date/time settings

You must set the correct date/time in all computers comprising a JP1/Software Distribution system so that, for example, they will all execute a date/time-specified job simultaneously. If the date/time settings are ahead of or behind the actual date/time, the execution results of *Get system configuration information* jobs, *Hold report* jobs, and *Hold-report release* jobs, or automatic registration of the system configuration information, might not be committed to the managing server.

If necessary, change the system time only during system startup or shutdown. If a job is being processed, change the system time after the job finishes. If you change the system time while a job is being processed, the following problems might occur:

- A job specified to be executed at a certain date/time might be executed at a different time.
- If you set the system time back, a job specified to be executed at a certain date/time might be executed twice.

  If you set the system time forward, a job specified to be executed at a certain date/time might not be executed until that time is reached the next day.
- The log output time will shift, making it difficult to analyze the cause of errors.

In the case of JP1/Software Distribution Manager and JP1/Software Distribution Client (relay system), if you set the system time back and then create a job, an existing job might be overwritten. Therefore, wait until the set back period elapses before creating a job. If a previously-executed job has been overwritten, re-execute it.

(2) Time zone settings

The same time zone as is set in **Date/Time** on the **Control Panel** must be set for the `TZ` system environment variable. The following are the procedures for setting the time zone to `<GMT-05:00> Eastern Time (in the eastern U.S. and Canada).`

For Windows NT:

From **Control Panel**, choose **System**, set `TZ=EST+5` for the System Environment variable, and then restart the system.

For Windows Me or Windows 98:

To `AUTOEXEC.BAT`, add `SET TZ=EST+5` and then restart the system.

In JP1/Software Distribution, the date and time in the time zone set on a client are used as the date and time displayed for information collected from the client. This means that, if the time zone of a client is changed, the information collected after the change is recognized as being different.

The date and time of jobs run on a client also rely on the client's time zone. If a job is specified to execute at 10:00, it executes at 10:00 in the client's time zone. If you want to collect all information at 10:00 according to the managing server's time zone, you must determine the differences in dates and times compared to the time zones of the clients, and execute the jobs that are scheduled for the appropriate dates and times.

5.2 Designing a system configuration appropriate to the environment

This section describes the design of a system configuration that is appropriate to the environment in which the JP1/Software Distribution system is used.

5.2.1 System configuration in an environment where Asset Information Manager Subset is used

Asset Information Manager Subset uses a dedicated relational database that is separate from the managing server's database.

If you use Embedded RDB as the relational database and install JP1/Software Distribution's server core facility and Asset Information Manager Subset on the same computer, two databases are created, requiring a large amount of machine resources. Therefore, we recommend that you install Asset Information Manager Subset on a separate computer from JP1/Software Distribution's server core facility.

For details about how to install Asset Information Manager Subset, see *2.3 Installing Asset Information Manager Subset* in the *Setup Guide*.

The following figures show, for each type of relational database, the configuration of the JP1/Software Distribution system in an environment in which Asset Information Manager Subset is used.

Figure 5–7: Configuration of JP1/Software Distribution system when Asset Information Manager Subset is used (Embedded RDB is used)

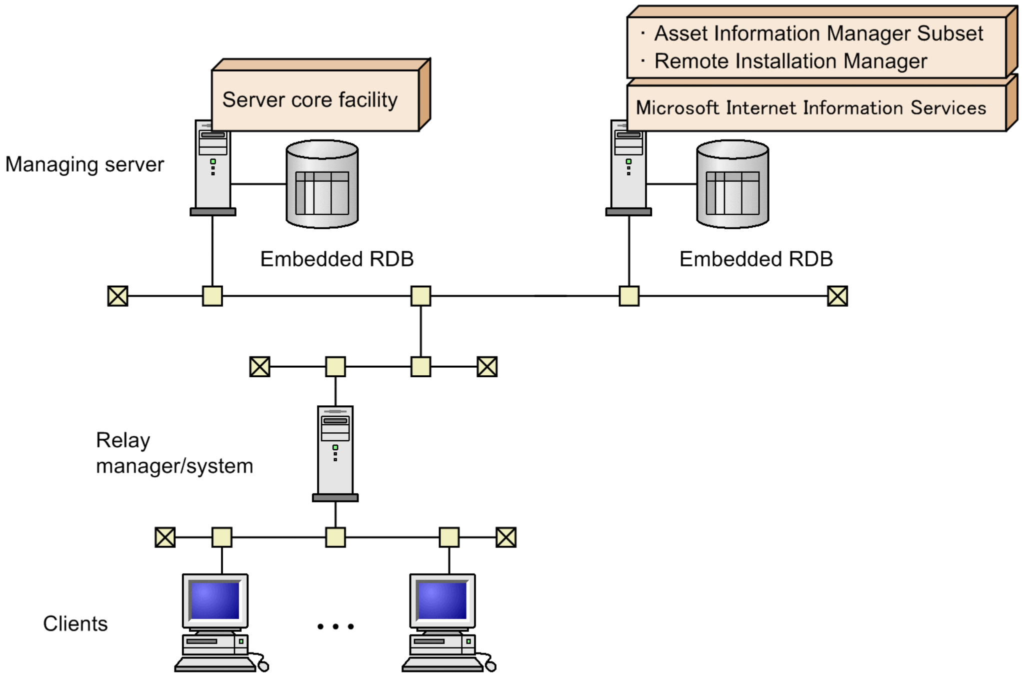
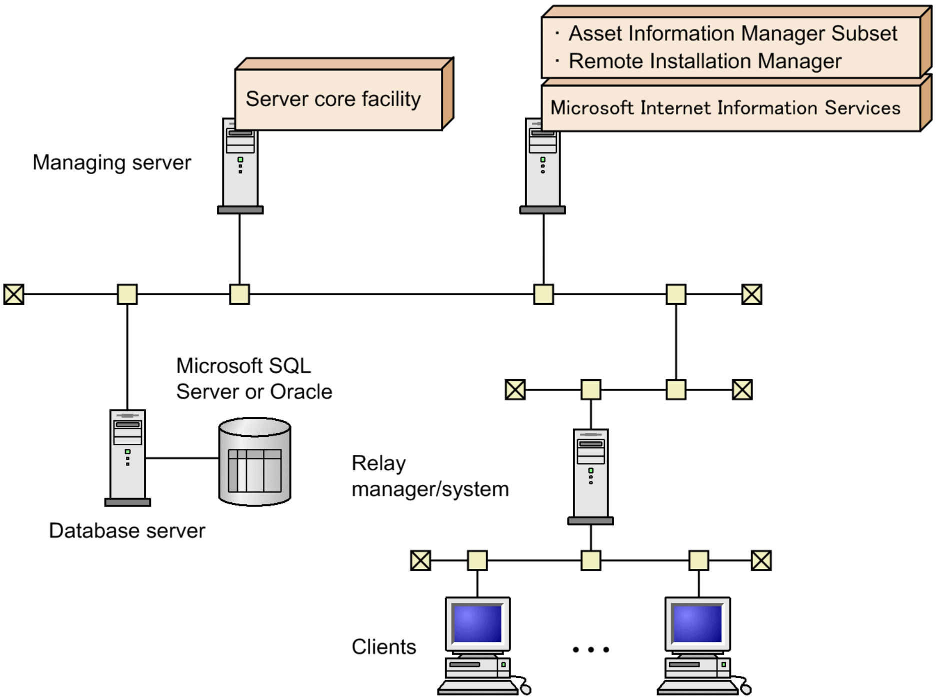

· Asset Information Manager Subset
· Remote Installation Manager
Server core facility
Microsoft Internet Information Services
Managing server
Embedded RDB
Embedded RDB
Relay manager/system
Clients
• • •

Figure 5–8: Configuration of JP1/Software Distribution system when Asset Information Manager Subset is used (Microsoft SQL Server or Oracle is used)

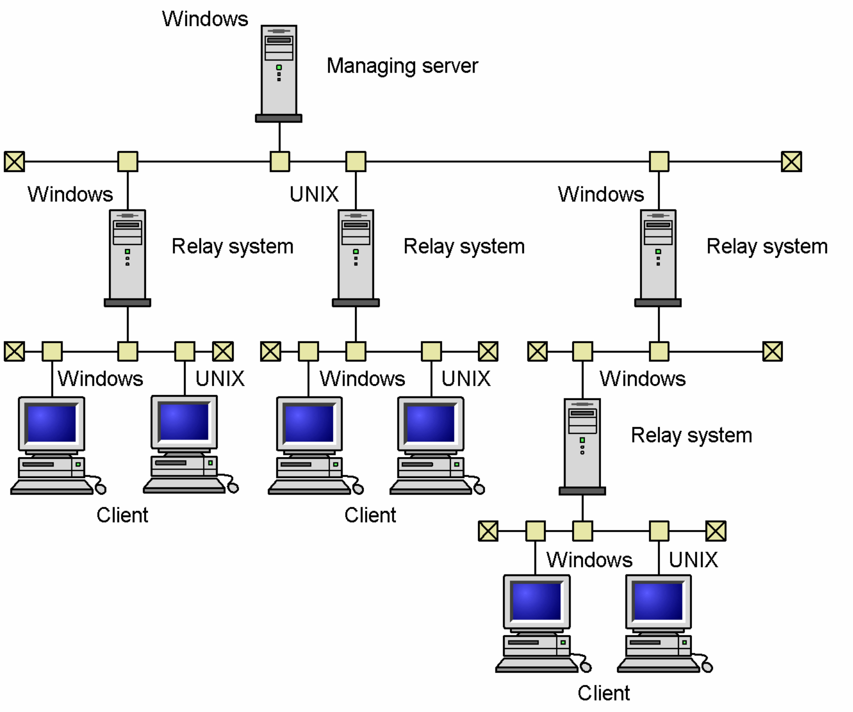


Note that Asset Information Manager Subset cannot be installed on the computer where JP1/Asset Information Manager is installed.

5.2.2 System configuration in an environment that includes UNIX systems

The following figure shows a JP1/Software Distribution configuration in an environment that includes UNIX systems.

Figure 5–9: JP1/Software Distribution configuration in an environment that includes UNIX systems



Three JP1/Software Distribution products are available for UNIX:

JP1/Software Distribution Manager

Provides the facilities of a managing server. You can connect JP1/Software Distribution Client for Windows under JP1/Software Distribution Manager.

JP1/Software Distribution Client

Provides the relay system, client, and Packager facilities. You can use the Packager facility to register software for distribution in the managing server for Windows.

! Important note

JP1/Software Distribution Client for UNIX (relay system) cannot be placed under JP1/Software Distribution Client (relay system) for Windows.

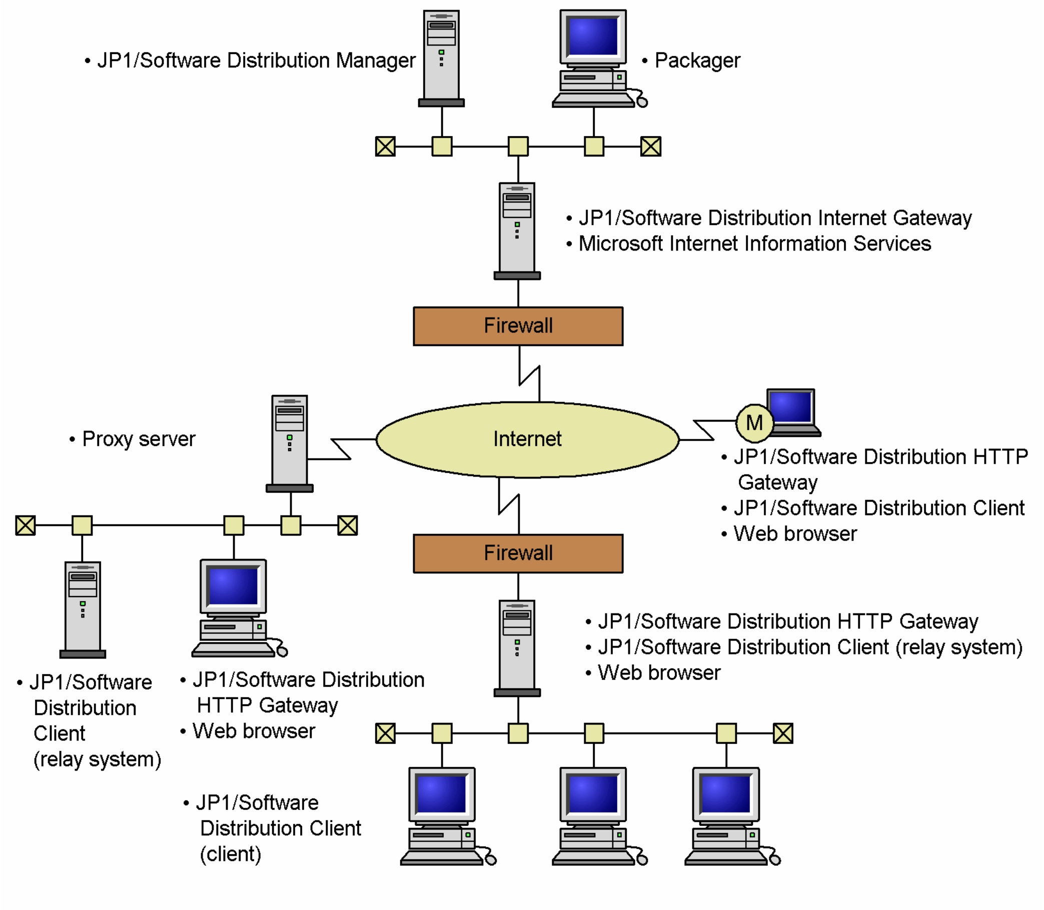
5.2.3 System configuration in an Internet environment

By using *Internet Options*, you can easily install JP1/Software Distribution in an environment in which nodes are connected via the Internet. Internet Options is the generic name for facilities consisting of JP1/Software Distribution Internet Gateway and JP1/Software Distribution HTTP Gateway.

When JP1/Software Distribution Internet Gateway and JP1/Software Distribution HTTP Gateway are installed between JP1/Software Distribution nodes that are connected via the Internet, the communications protocol between these nodes is converted from the JP1/Software Distribution protocol to HTTP. Therefore, in a Web-enabled system environment, you can avoid complex settings. For details about the Internet Options, see *E. Using Internet Options to Install JP1/Software Distribution* in the *Setup Guide*.

The following figure shows an overview of a system configuration using the Internet Options.

Figure 5–10: Overview of a system configuration using the Internet Options


• JP1/Software Distribution Manager
• Packager
• JP1/Software Distribution Internet Gateway
• Microsoft Internet Information Services
Firewall
• Proxy server
Internet
M
• JP1/Software Distribution HTTP Gateway
• JP1/Software Distribution Client
• Web browser
Firewall
• JP1/Software Distribution HTTP Gateway
• JP1/Software Distribution Client (relay system)
• Web browser
• JP1/Software Distribution Client (relay system)
• JP1/Software Distribution HTTP Gateway
• Web browser
• JP1/Software Distribution Client (client)

5.2.4 System configuration for WSUS linkage

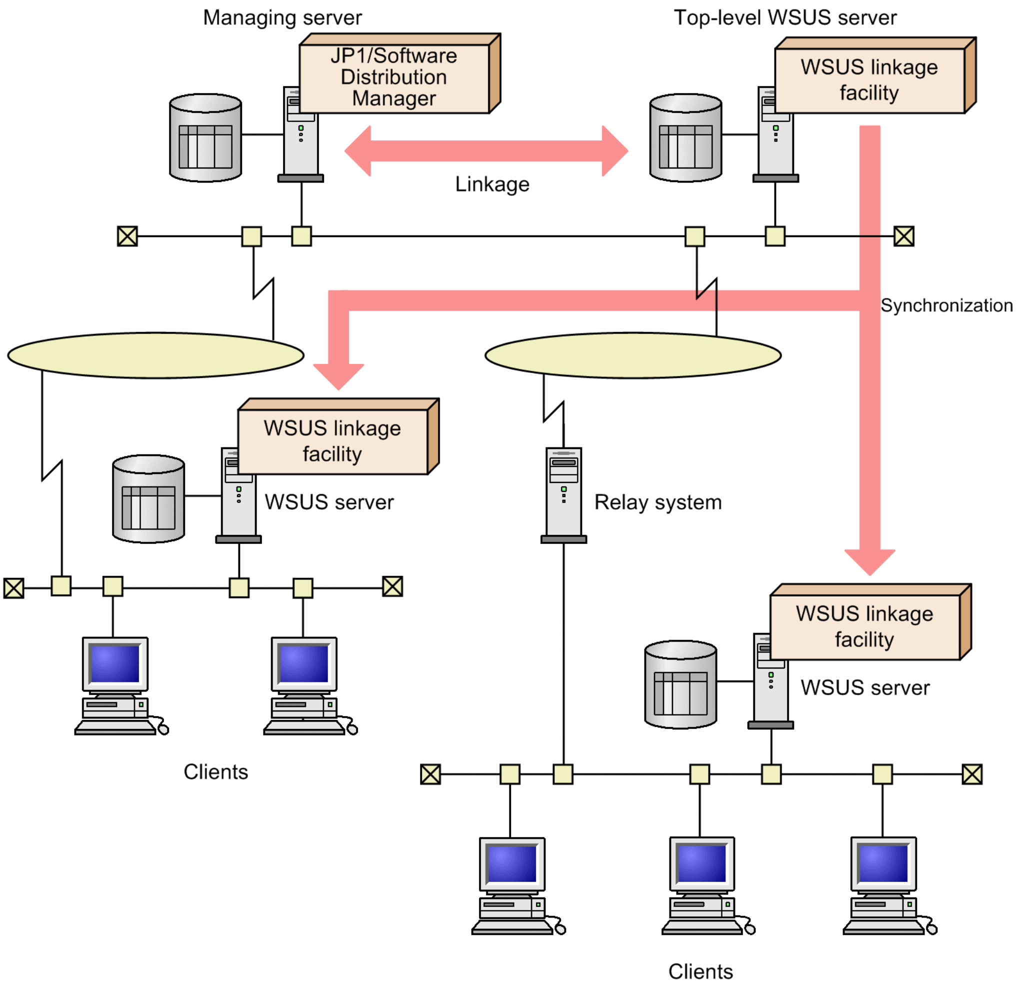
In a system in which JP1/Software Distribution links with WSUS, only one WSUS can be linked. If there are multiple WSUS servers, you must link your JP1/Software Distribution to only one of them. If the WSUS servers are configured in a hierarchy, link your JP1/Software Distribution with the WSUS server at the top of the hierarchy.

To synchronize the WSUS server linked to JP1/Software Distribution with lower WSUS servers, you use a command provided by JP1/Software Distribution.

To link JP1/Software Distribution to WSUS, you must install WSUS Linkage, which is a JP1/Software Distribution component, on all WSUS servers within the system. For details about how to install WSUS Linkage, see *2.4 Installing JP1/Software Distribution on a WSUS server* in the *Setup Guide*.

The following figure shows the configuration of a JP1/Software Distribution system when WSUS is linked.

Figure 5–11: Configuration of a JP1/Software Distribution system when WSUS is linked



You can install JP1/Software Distribution and WSUS on the same computer. In this case, for JP1/Software Distribution and WSUS to use different versions of Microsoft SQL Server, one of the Microsoft SQL Server versions must be on a separate computer.

Note, however, that when you install JP1/Software Distribution in a 64-bit version of the OS, you cannot use the WSUS that is installed on the same computer. In this case, use a WSUS configured on a computer that is running a 32-bit version of the OS.

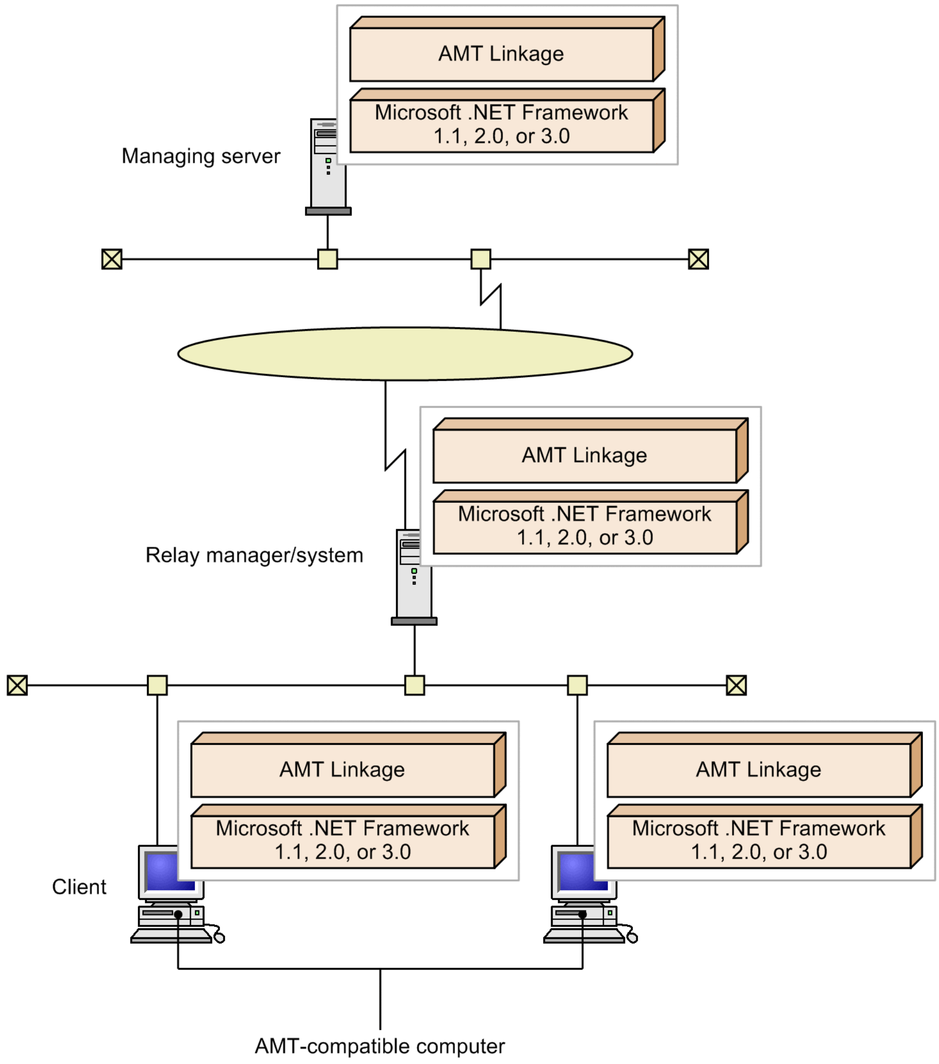
After you have finished configuring an environment to be linked to WSUS, in the settings of the managing server you must specify the URL of WSUS Linkage to which you plan to connect. For details about how to specify the URL, see *4.2.17 WSUS Linkage page* in the *Setup Guide*.

5.2.5 System configuration when using AMT

To use AMT Linkage functionality, Microsoft .NET Framework 1.1, 2.0, 3.0, or 3.5 must be installed, and a computer that supports AMT must be used as the client.

The following figure shows a system configuration in which AMT is used from JP1/Software Distribution.

Figure 5–12: System configuration when AMT is used


AMT Linkage
Microsoft .NET Framework 1.1, 2.0, or 3.0
Managing server
AMT Linkage
Microsoft .NET Framework 1.1, 2.0, or 3.0
Relay manager/system
AMT Linkage
Microsoft .NET Framework 1.1, 2.0, or 3.0
AMT Linkage
Microsoft .NET Framework 1.1, 2.0, or 3.0
Client
AMT-compatible computer

Note that you do not need to install AMT Linkage on the same computer as the Server core facility; you can install it on the computer on which Remote Installation Manager is installed.

(1) Settings required before JP1/Software Distribution is installed

Before you install AMT Linkage, on the client you must specify settings for AMT. The following describes how to set up AMT.

To set up AMT:

1. Enable the AMT functionality.
2. Specify `Small Business` as the Provision model.
3. Perform the AMT network and other settings.

Note that you cannot specify `Enterprise` as the AMT Provision model.

(2) Notes on system configurations that use AMT Linkage

- The user name and password that you set in the AMT user information (AMT management user) when you install JP1/Software Distribution must match the user name and password set in the system.
- You use the host name as the ID key for operations.

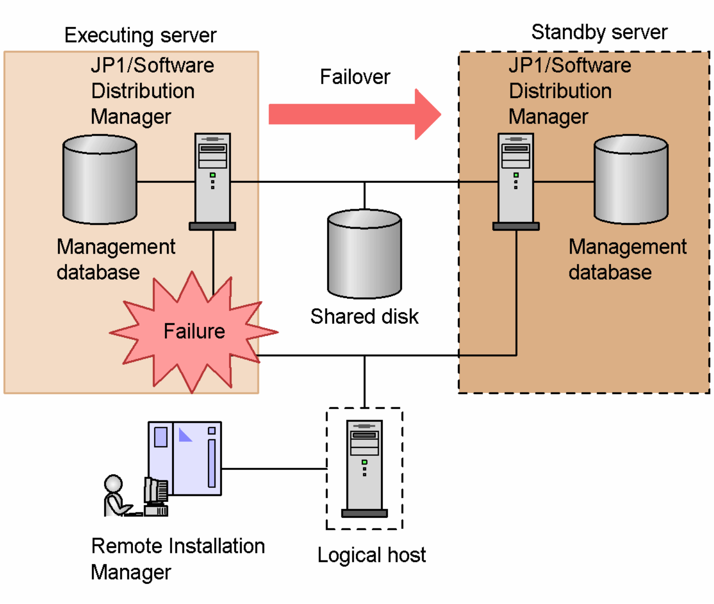
5.2.6 Using JP1/Software Distribution in a cluster system

You can also install JP1/Software Distribution in a cluster system that uses Microsoft Cluster Service or Windows Server Failover Cluster. A cluster system consists of more than one server operated as a single system. A cluster system provides higher system availability because if one server fails, another server can continue processing (failover), thereby avoiding shutdown of the entire system. A cluster system's failover functionality is available only to JP1/Software Distribution Manager (central manager).

JP1/Software Distribution Manager supports the *active/standby* configuration, which is one of the operation modes of cluster systems. The active/standby configuration is a two-node cluster system in which one node is defined as the active system (usually called an *executing system* in JP1/Software Distribution documentation) and the other as the standby system.

The following figure shows an overview of a cluster system that uses JP1/Software Distribution.

Figure 5–13: Overview of a cluster system that uses JP1/Software Distribution



In addition to the physical host names and IP addresses of the multiple JP1/Software Distribution Managers in a cluster system, a logical host name or logical IP address is used to connect to the logical manager. This makes it possible for the standby machine to establish connection without having to know which manager is being used for processing.

If you use a relational database as the management database, you can use the failover facility of Microsoft Cluster Service or Windows Server Failover Cluster. When this failover functionality is used, the cluster software monitors:

- Shared disk
- Logical IP addresses
- Remote Install Server, which is one of the services provided by JP1/Software Distribution Manager

You can also use the servers that constitute the cluster system as individual nodes (not as logical hosts) by using their physical host names or IP addresses.

For details about how to construct a cluster system and set up its environment, see *11.1 Constructing a JP1/Software Distribution Cluster System* in the *Setup Guide*.

(1) System configuration examples

Examples of a cluster system for JP1/Software Distribution are described below.

(a) Configuration examples in which JP1/Software Distribution is failed over

This section presents examples of configurations in which JP1/Software Distribution is failed over. The following types of system configurations are supported:

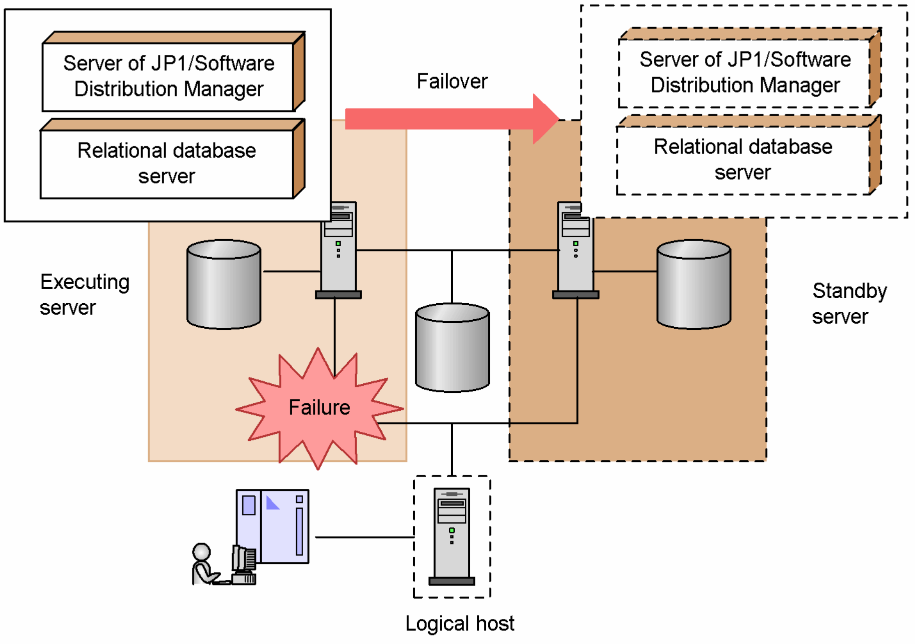
- Two-node cluster system configuration in which one JP1/Software Distribution Manager is paired with another

  In a cluster environment implemented with Microsoft Cluster Service or Windows Server Failover Cluster, if you set the JP1/Software Distribution Manager service to use the failover facility, hardware problems and errors in the JP1/Software Distribution Manager service are detected automatically. In such cases, processing is automatically switched from the active server to the standby server.

  The relational database server to be used after failover can be set up in the same cluster group or in another cluster group.

  The following figure shows an example of a system configuration for using the failover functionality to monitor the services of JP1/Software Distribution Manager.

  Figure 5–14: Example of a system configuration for using the failover functionality to monitor the services of JP1/Software Distribution Manager


Server of JP1/Software Distribution Manager
Relational database server
Failover
Server of JP1/Software Distribution Manager
Relational database server
Executing server
Standby server
Failure
Logical host

  If you use this configuration, you must set the logical host names for the higher connection destinations when you set up the following programs:

  - Connection destination of the Remote Installation Manager that is connected to JP1/Software Distribution Manager
  - JP1/Software Distribution Manager (Relay Manager)
  - JP1/Software Distribution Client (relay system)
  - JP1/Software Distribution Client (client)

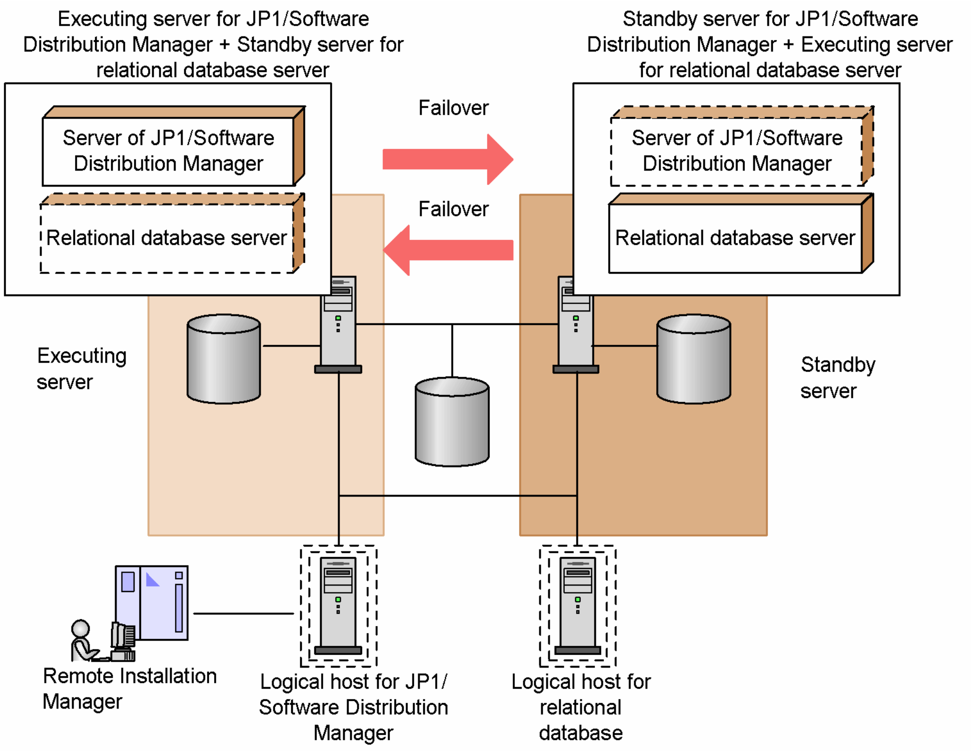
  When a failover occurs, an error occurs at the connection-source system; however, you can recover the system by re-connecting from the Remote Installation Manager and the lower systems.

- Two-node cluster system configuration in which JP1/Software Distribution Manager is paired with a relational database server

  If you create a two-node cluster system by placing JP1/Software Distribution Manager and its relational database server on different server machines, you can use the two machines as mutual standby servers. This configuration supports load distribution between the two machines, as well as the failover functionality.

  The following figure shows an example of a system configuration for mutually monitoring JP1/Software Distribution Manager and a relational database between two servers.

Figure 5–15: Example of a system configuration for mutually monitoring JP1/Software Distribution Manager and a relational database between two servers


Executing server for JP1/Software Distribution Manager + Standby server for relational database server
Standby server for JP1/Software Distribution Manager + Executing server for relational database server
Server of JP1/Software Distribution Manager
Relational database server
Failover
Failover
Server of JP1/Software Distribution Manager
Relational database server
Executing server
Standby server
Remote Installation Manager
Logical host for JP1/ Software Distribution Manager
Logical host for relational database

If you create this configuration, you must include the following configuration settings:

- In the JP1/Software Distribution Manager settings, set the logical host for the relational database as the connection destination of the relational database server
- In JP1/Software Distribution Manager (relay manager), Remote Installation Manager, and JP1/Software Distribution Client to be connected to JP1/Software Distribution Manager, set the logical host for JP1/ Software Distribution Manager as the higher connection destination.

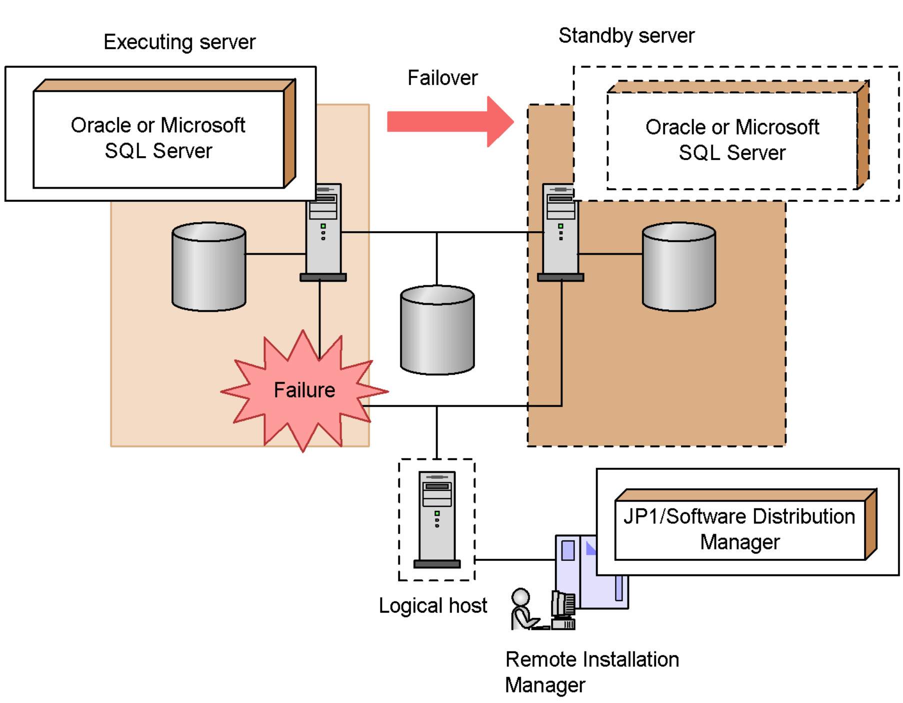
- Two-node cluster system configuration in which only a relational database server is duplicated

In a cluster environment implemented with Microsoft Cluster Service or Windows Server Failover Cluster, if you construct an environment that uses the failover facility of Microsoft SQL Server or Oracle, hardware problems and errors in the relational database server service are detected automatically. In such cases, processing is automatically switched from the active server to the standby server.

When JP1/Software Distribution and other applications share a relational database server in this configuration, an error in JP1/Software Distribution does not affect the processing of other applications. Also with this configuration, you can link JP1/Software Distribution with a clustered Oracle 8i system running on Solaris 7.

The following figure shows an example of a two-node cluster system configuration in which a relational database server is duplicated.

Figure 5–16: Example of a two-node cluster system configuration in which a relational database server is duplicated


Executing server
Standby server
Failover
Oracle or Microsoft SQL Server
Oracle or Microsoft SQL Server
Failure
Logical host
JP1/Software Distribution Manager
Remote Installation Manager

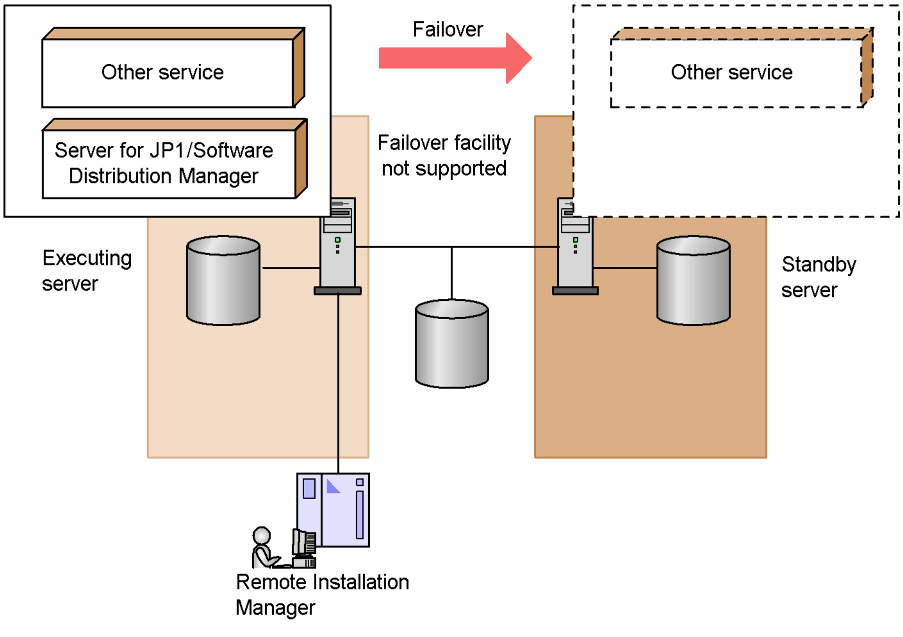
In the JP1/Software Distribution Manager setup, you must set the logical host for the relational databases as the connection destination of the relational database server.

(b) Configuration example in which JP1/Software Distribution is not failed over

You can use the executing (i.e., active) and standby computers as different systems without registering JP1/Software Distribution Manager in a cluster group and without using the failover functionality. In this configuration, while another program is using the logical host, JP1/Software Distribution can access the physical hosts that constitute the logical host by using their physical host names or IP addresses. If JP1/Software Distribution is not to be failed over, you can install a relay manager (JP1/Software Distribution Manager) or JP1/Software Distribution Client on the physical host that constitutes the cluster system.

The following figure shows an example configuration in which JP1/Software Distribution is not failed over.

Figure 5–17: Example of configuration in which JP1/Software Distribution is not failed over


Other service
Server for JP1/Software Distribution Manager
Failover
Other service
Failover facility not supported
Executing server
Standby server
Remote Installation Manager

(2) JP1/Software Distribution facilities supported in a cluster system

The following table lists the JP1/Software Distribution facilities and whether they are supported in a cluster system.

Table 5–1: JP1/Software Distribution facilities and whether they are supported in a cluster system

Item		Supported?
Supported cluster	Microsoft Cluster Service	Y
	Windows Server Failover Cluster	Y
Supported cluster system configuration	Active/standby configuration	Y
	Active/active configuration	--
ID key for operations	By host name	Y
	By IP address	Y
	By host identifier	Y
Network-related items	Operation in environment of multiple LAN connections	--
Database for JP1/Software Distribution Manager	Embedded RDB	Y
	Microsoft SQL Server 7.0	Y
	Microsoft SQL Server 2000	Y
	Microsoft SQL Server 2005	Y
	Microsoft SQL Server 2008	Y
	Microsoft SQL Server 2012	Y
	Oracle8i (Windows NT)	Y
	Oracle8i (Solaris)	Y
	Oracle9i (Windows NT)	Y
JP1/Software Distribution Manager facilities	Ordinary distribution	Y

Item		Supported?
JP1/Software Distribution Manager facilities	Distribution using ID group	Y
	Split distribution	Y
	Remote collection	Y
	Inventory collection	Y
	Automatic registration of system configuration	Y
	Sending events to JP1/IM	Y
	Automatic dialing	--
	OpenView Linkage	Y (no FF)
	Packager	Y (no FF)
	Relay manager	Y (no FF)
JP1/Software Distribution Client (relay system)	Relay system	Y (no FF)
JP1/Software Distribution Client (client)		Y (no FF)
Asset Information Manager Subset		Y
Remote Control Manager		Y (no FF)
Remote Control Agent		Y (no FF)

Legend:

Y: Facility is supported.

--: Facility is not supported.

Y (no FF): Facility is supported within the range where failover does not occur.

5.3 Estimating the hardware requirements

This section describes the CPU performance required in order to run JP1/Software Distribution and the procedure for calculating the required disk and memory space. For the disk space required for the remote control facility, see the manual *Job Management Partner 1/Remote Control Description and Operator's Guide*.

5.3.1 CPU performance

The following table shows the CPU performance necessary for running the various components of JP1/Software Distribution.

Table 5–2: CPU performance required by JP1/Software Distribution

Facility	Minimum	Recommended
Server	1-gigaherz processor	2-gigaherz or faster processor
Relay system#	1-gigaherz processor	2-gigaherz or faster processor
Client#	300-megaherz processor	1-gigaherz or faster processor
Asset Information Manager Subset	700-megaherz processor	If there are fewer than 5,000 clients: 1.5-gigaherz or faster processor If there are 5,000 or more clients: 3-gigaherz or faster dual processors
Packager	300-megaherz processor	1-gigaherz or faster processor
Automatic Installation Tool	300-megaherz processor	1-gigaherz or faster processor
OpenView gateway server	1-gigaherz processor	2-gigaherz or faster processor
OpenView Linkage	1-gigaherz processor	2-gigaherz or faster processor

#

When you monitor operations in a virtual environment, the minimum required CPU performance varies. It also varies depending on the number of users connected.

30 or fewer users: 3-gigaherz dual-core processor

60 or fewer users: 3-gigaherz quad-core processor

5.3.2 Memory requirements

(1) Memory required for a managing server

The following table shows the memory requirements of JP1/Software Distribution Manager as a managing server.

Table 5–3: Memory requirements of JP1/Software Distribution Manager

Facility	Memory requirements (in megabytes)
JP1/Software Distribution server	34 + 0.020 **x** *a* *a*: Number of concurrently connected servers#2
JP1/Software Distribution server (relay manager)#1	71 + 0.020 **x** (*a* + 25) *a*: Number of concurrently connected servers#2
Remote Installation Manager	20 + 0.002 **x** *b*

Facility	Memory requirements (in megabytes)
Remote Installation Manager	*b*: Number of displayed data items#3
Inventory Viewer	7.5 + 0.007 **x** *c* *c*: Number of computers displaying inventory
Relational database (when Embedded RDB is used)	300 + (*a* **x** 2) **x** 10 *a*: Number of concurrently connected computers#2

#1

When you monitor operations in a virtual environment, the minimum memory requirement varies. It also varies depending on the number of users connected.

30 or fewer users: 4 gigabytes

60 or fewer users: 8 gigabytes

#2

Number of concurrently connected computers is the value specified for the number of lower systems that can be concurrently connected on the **Server Customization** page in the Server Setup dialog box.

#3

Number of displayed data items is the total number of items displayed in the following windows of Remote Installation Manager:

- System Configuration window:
  Relay managers, relay systems, clients, system information items, and inventory items such as software inventory
- Destination window:
  ID groups, destination groups, clients, system information items and inventory items such as software inventory
- Job Definition:
  Job definitions
- Package window:
  Cabinets and packages
- Job Status window:
  Jobs and job destinations
- List of Software Information window:
  Search lists
- Directory Information window:
  Organizational units (OUs), groups, computers, system information items, and inventory items such as software inventory items

If you display the same window more than once, count all the items displayed in all instances of that window.

(2) Memory required for a relay system

The following table shows the memory requirements of JP1/Software Distribution Client (relay system).

Table 5–4: Memory requirements of a relay system

Facility	Memory requirements (in megabytes)
Relay system#1	28 + 0.018 **x** (*a* + 8) + (*b* **x** 0.001) *a*: Number of concurrently connected computers#2 *b*: Size of the management file cache#3

#1

When you monitor operations in a virtual environment, the minimum memory requirement varies. It also varies depending on the number of users connected.

30 or fewer users: 4 gigabytes

60 or fewer users: 8 gigabytes

#2

Number of concurrently connected computers is the value specified for the number of clients that can be concurrently connected on the **Relay System Customization** page in the relay system basic settings.

#3

Use the following formula to calculate the size of the management file cache:

Size of the management file cache (kilobytes) =

number of jobs retained on the relay system that were executed on the relay system or by the higher system
x *number of lower clients per job*
x *number of packages per job (for remote installation jobs)*
x 1 kilobyte

(3) Memory required for a client

The following table shows the memory requirements of the client facility.

Table 5–5: Memory requirements of a client

Facility		Memory requirements (in megabytes)
Client#	When resident	18
	Remote installation of package	24
	Installation by client user	28
Startup Kit Support Tool		4

#

When you monitor operations in a virtual environment, the minimum memory requirement varies. It also varies depending on the number of users connected.

30 or fewer users: 4 gigabytes

60 or fewer users: 8 gigabytes

(4) Memory required for Asset Information Manager Subset

The following table shows the memory requirements of Asset Information Manager Subset:

Table 5–6: Memory requirements of Asset Information Manager Subset

Facility	Memory requirements
Asset Information Manager Subset	If there are fewer than 5,000 clients: 1.0 gigabyte or more If there are 5,000 or more clients: 1.5 gigabytes or more

(5) Memory required for the Packager

The following table shows the memory requirements of the Packager.

Table 5–7: Memory requirements of the Packager

Facility	Memory requirements (in megabytes)
Packager	9

(6) Memory required for the Automatic Installation Tool

The following table shows the memory requirements of the Automatic Installation Tool.

Table 5–8: Memory requirements of the Automatic Installation Tool

Facility	Memory requirements (in megabytes)
Automatic Installation Tool	4

(7) Memory required for the OpenView Linkage

The following table shows the memory required for the OpenView Linkage.

Table 5–9: Memory required for the OpenView Linkage

Facility	Memory requirements (in megabytes)
OpenView Linkage	7
OpenView gateway server	1

5.3.3 Disk space requirements

(1) Disk space required for JP1/Software Distribution Manager

Tables 5-10 and *5-11* show the disk space required for JP1/Software Distribution Manager.

Table 5–10: Disk space required for JP1/Software Distribution Manager (central manager)

Facility		Disk space requirements
JP1/Software Distribution server	For Embedded RDB	120 MB + space allocated during database operations The amount of space allocated automatically during database operations depends on the scale selected when the database was created: Small scale: 300 MB Medium scale: 500 MB Large scale: 1,100 MB
	For Microsoft SQL Server or Oracle	12 MB
Remote Installation Manager	For Embedded RDB	24 MB
	For Microsoft SQL Server or Oracle	22 MB
Asset Information Manager Subset	For Embedded RDB	140 MB + space allocated during database operations The amount of space allocated automatically during database operations depends on the size of the database: 100 MB or less: 300 MB 101 to 500 MB: 1 GB 501 MB or more: 1 GB
	For Microsoft SQL Server or Oracle	45MB
AMT Linkage		1 MB
WSUS Linkage		1 MB
OpenView Linkage		9 MB
OpenView Gateway Server		4 MB

Facility	Disk space requirements
Common area of JP1/Software Distribution Manager	36 MB
Packaging by the Packager	1 KB + package size
Package storage	Number of packages ∑ (package size after compression + 2 KB) (KB)
Storing operation history	See *(3) Disk space required for storing operation log files*.
Backing up operation history	Number of clients **x** ∑ (size of compressed operation history that is to be backed up) (MB)
Remote installation	1.0 **x** number of packages **x** number of clients + number of packages **x** 0.3 (KB)

Table 5–11: Disk space required for JP1/Software Distribution Manager (relay manager)

Facility		Disk space requirements
JP1/Software Distribution server	For Embedded RDB	142 MB
	For Microsoft SQL Server or Oracle	34 MB
Remote Installation Manager	For Embedded RDB	24 MB
	For Microsoft SQL Server or Oracle	22MB
AMT Linkage		1 MB
WSUS Linkage		1 MB
OpenView Linkage		9 MB
OpenView Gateway Server		4 MB
Common area of JP1/Software Distribution Manager		43 MB
Packaging by the Packager		1 KB + package size
Package storage		Number of packages ∑ (package size after compression + 2 KB) (KB)
Storing operation history		See *(3) Disk space required for storing operation log files*.
Backing up operation history		Number of clients **x** ∑ (size of compressed operation history that is to be backed up) (MB)
Remote installation		1.0 **x** number of packages **x** number of clients + number of packages **x** 0.3 (KB)
Storage of packages distributed from the central manager		Number of packages ∑ (package size after compression + 2 KB) (KB)
Storage of management information about the package distributed from the central manager		Number of clients ∑ (number of packages within client **x** 2 KB) (KB)
Package installation		See *(4) Disk space required for package installation* below.

(2) Disk space required for JP1/Software Distribution Client

Tables 5-12 and *5-13* show the disk space required for JP1/Software Distribution Client.

Table 5–12: Disk space required for JP1/Software Distribution Client (relay system)

Facility	Disk space requirements
Relay system	30 MB

Facility	Disk space requirements
Remote Installation Manager	4 MB
Common area of JP1/Software Distribution SubManager	39 MB
AMT Linkage	1 MB
Storage of packages at relay system	Number of packages ∑ (package size after compression + 2 KB) (KB)
Storage of relay system management information	Number of clients ∑ (number of packages within client **x** 2 KB) (KB)
Package distribution	1.0 **x** number of packages **x** number of clients + number of packages **x** 0.3 (KB)
Package installation	See *(4) Disk space required for package installation* below.

Table 5–13: Disk space required for JP1/Software Distribution Client (client)

Facility		Disk space requirements
Client	Client core	24 MB
	Package Setup Manager	2 MB
	Additional facility	5 MB
	Distribution facility by Visual Test 6.0	2 MB
	Distribution facility by Visual Test 6.5	2 MB
	AMT Linkage	1 MB
Storage of client management information		Number of packages within client **x** 1.0 (KB)
Packaging information display		Number of packages to be packaged **x** 1.0 (KB)
Package installation		See *(4) Disk space required for package installation* below.
Startup Kit Support Tool		4 MB
Help		4 MB
Common area for JP1/Software Distribution Client		11 MB

(3) Disk space required for storing operation log files

This subsection explains the formula for calculating the disk space required for storing operation log files. Calculate the required capacity according to the operation log data you plan to collect.

Size of the operation log data for each item for one day

The following gives the formula for calculating the size of each item that can be collected as operation log data in one day.

- Process start = *number of events expected per day* (*a*) **x** 335 = *A*
- Process stop = *number of events expected per day* (*b*) **x** 335 = *B*
- Caption change = *number of events expected per day* (*c*) **x** 335 = *C*
- Active window change = *number of events expected per day* (*d*) **x** 590 = *D*
- Machine start = *number of events expected per day* (*e*) **x** 15 = *E*
- Machine stop = *number of events expected per day* (*f*) **x** 15 = *F*
- Logon = *number of events expected per day* (*g*) **x** 35 = *G*
- Logoff = *number of events expected per day* (*h*) **x** 35 = *H*
- File operation = *number of events expected per day* (*i*) **x** 837 = *I*
- Web access = *number of events expected per day* (*j*) **x** (621) = *J*

- Print operation = *number of events expected per day* (*k*) **x** 890 = *K*
- Printing suppression = *number of events expected per day* (*l*) **x** 890 = *L*
- Print suppression released = *number of events expected per day* (*m*) **x** 147 = *M*
- Operations to or from external media = *number of events expected per day* (*n*) **x** 150 = *N*
- USB media connection permission = *number of events expected per day* (*o*) **x** 300 = *O*
- USB media connection suppression = *number of events expected per day* (*p*) **x** 300 = *P*
- Device connection = *number of events expected per day* (*q*) **x** 350 = *Q*
- Device disconnection = *number of events expected per day* (*r*) **x** 350 = *R*
- Device connection permission = *number of events expected per day* (*s*) **x** 350 = *S*
- Device connection suppression = *number of events expected per day* (*t*) **x** 350 = *T*

For any item that will not be collected as an operation log, substitute `0` for the number of events. The units for all items is bytes.

For *a* - *t*, substitute the number of events expected per day for the corresponding item. *A* - *T* indicate the size of the operation log data for one day for individual items. The number of events expected per day is the number of operation-target events that occur in one day on a client PC. For Web accesses, multiple log entries are collected for any Web page that is divided into frames. Note, therefore, that multiple log entries might be collected even for a single Web access. For Web accesses, choose whether the maximum value (2,484 bytes) or effective log size (621 bytes) will be used for calculating the size of each event.

Additionally, to collect operation logs from a virtual environment, add the following size:

size of operation logs per day **x** *number of logon users*

Size of operation log data for a single client and JP1/Software Distribution Manager

Determine the size of the operation log data for a single client as described below based on the size of each item per day. *DAY*, *WEEK*, and *MONTH* indicate the size for 1 day, 1 week, and 1 month, respectively.

- Size of operation log data on a single client = *A* + *B* + *C* + *D* + *E* + *F* + *G* + *H* + *I* + *J* + *K* + *L* + *M* + *N* + *O* + *P* + *Q* + *R* + *S* + *T* = *DAY*
- Size of operation log data on a single client in 1 week (5 days) = *DAY* **x** 5 = *WEEK*
- Size of operation log data on a single client in 1 month (20 days) = *DAY* **x** 20 = *MONTH*

Based on the size of operation log data for a single client as determined using the above formulas, determine the disk space required for JP1/Software Distribution Manager. For example, if *X* clients are being managed, the following formula is used to calculate the disk space required for 1 month:

- Disk space required for 1 month when *X* clients are being managed = *MONTH* **x** *X*

(4) Disk space required for package installation

The required disk space depends on the type of package to be installed. The value to be used in the calculation formula should be rounded up for each cluster size.

- Hitachi program product or another company's software

  Disk space requirement (bytes) =

  PCn **x** 944 + Σ (size of installation script + size of AIT or recorder file) + Σ (RPSz) + MAX(PPSz) + Σ (APSz) + PCn **x** 300

  The sizes of the installation script, AIT file, and recorder file are as follows:

  For a Hitachi program product:

  The size of the installation script is 2,700 bytes and the size of the AIT and recorder files is 0.

  For another company's software (when the standard AIT or recorder file is used):

  The maximum total size of the installation script and the AIT or recorder file is 43 kilobytes.

  For another company's software (when a user-created AIT or recorder file is used):

  The maximum total size of the installation script and the AIT or recorder file is the total size of the files created by the user.

- For user data and user programs

  Disk space requirement (bytes) =

PCn **x** (944 + 2500) + Σ (RPSz) + MAX(RPSz) + Σ (APSz) + PCn **x** 300

- For user data and user programs with optional facilities specified

  Disk space requirement (bytes) =

  PCn **x** (944 + 2500) + Σ (RPSz) + MAX(RPSz) + MAX(size of installation destination directory) + Σ (APSz) + PCn **x** 300

- When the background installation mode is used for data and user programs and when normal installation is specified

  Using the background installation mode and specifying normal installation can reduce the disk space required for a client during remote installation.

  Disk space requirement (bytes) =

  PCn **x** (944 + 2500) + MAX(RPSz) + Σ (APSz) + PCn **x** 300

Legend:

PCn

Number of packages to be installed concurrently

RPSz

Size of the package, which can be obtained from the following formula:

(Number of files to be packaged + number of directories) 80 + size of the program product to be remote-installed on the storage media)

PPSz

Size of the program product to be installed on the storage media

APSz

Size of the program product after installation (if a new version is being distributed, use the difference in size from the previous version)

Σ ( )

Sum of the values

MAX( )

Maximum value

(5) Disk space required for the Packager

The following table shows the disk space required for the Packager.

Table 5–14: Disk space required for the Packager

Facility	Disk space requirements (in megabytes)
Packager	7

(6) Disk space required for packaging

The required disk space depends on the type of package. The value to be used in the calculation formula should be rounded up for each cluster size.

- Packing user data or user programs

  Disk space requirement (bytes) = RPSz

- Packing compressed user data or user programs

  Disk space requirement (bytes) = RPSz **x** 2

- Packaging of Hitachi program product or another company's software on FD

  Disk space requirement (bytes) = RPSz + RDs

- Compressed packaging of Hitachi program product or another company's software on FD

  Disk space requirement (bytes) = RPSz **x** 2 + RDs

- Packaging of Hitachi program product or another company's software on CD-ROM

Disk space requirement (bytes) = RPSz

- Compressed packaging of Hitachi program product or another company's software on CD-ROM
  Disk space requirement (bytes) = RPSz **x** 2

Legend:

RPSz

(Number of files to be packaged + number of directories) **x** 80 + total size of the files to be packaged

RDs

Data size of the target storage media

(7) Disk space required for the Automatic Installation Tool

The following table shows the disk space required for the Automatic Installation Tool.

Table 5–15: Disk space required for the Automatic Installation Tool

Facility	Disk space requirements (in megabytes)
Automatic Installation Tool	6

(8) Disk space required for files that depend on the user environment

For JP1/Software Distribution Manager (central manager), there are no files that depend on the user environment. For details about the database files for JP1/Software Distribution Manager, see *5.4 Estimating disk space requirements for the database*.

The following files depend on the user environment of JP1/Software Distribution Manager (relay manager) and JP1/ Software Distribution Client.

Files for managing higher systems:

Files for managing higher systems are created in `\Master\Db\HOSTSYS` in the installation directory of JP1/ Software Distribution. One of these files is created for each higher system, and each file uses 400 bytes. A file is created when the higher system is changed or when the local system is accessed by the higher system. When multi-polling is used, a file is required for each of the specified higher systems.

File for managing installed-package information:

The installed-package information management file `UPLISTD.BON` is created in `\Master\Db\` in the installation directory of JP1/Software Distribution. As many information items as there are software programs are added to this file at the following times:

- When software is found by **Search software installed by Software Distribution**, **Search all software**, or **Search software listed in "Add/Remove Programs"** of a *Get software information from client* job
- When software is installed by a *Install package* or *Send package, allow client to choose* job.

Each software item requires one kilobyte of space.

Note that all software packages installed by JP1/Software Distribution that have the same package ID are treated as the same package. Therefore, there is only one software information item for a software program with the same package ID even if multiple different versions are installed.

File for managing file search information:

The file search information management file `VIFLIST.BON` is created in `\Master\Db` in the installation directory of JP1/Software Distribution. As many information items are added to this file as there are files found by **Search for a file** of a *Get software information from client* job.

Each file uses 300 bytes of disk space.

File for managing Microsoft Office product information:

The Microsoft Office product information management file `INFSCT`*x*`0.BON` (*x*: internal management number) is created in `\Master\Db\` in the installation directory of JP1/Software Distribution. As many information items are added to this file as there are software programs found by **Search for Microsoft Office products** of a *Get software information from client* job. Although the size depends on the product, approximately 300 bytes of disk space are required for each software item.

File for managing anti-virus product information:

The anti-virus product information management file `INFSCT`*x*`1.BON` (*x*: internal management number) is created in `\Master\Db\` in the installation directory of JP1/Software Distribution. As many information items are added to this file as there are software programs found by **Search for anti-virus products** of a *Get software information from client* job. Although the size depends on the product, approximately 300 bytes of disk space are required for each software item.

For details about the user environment-dependent files for JP1/Remote Control, see the manual *Job Management Partner 1/Remote Control Description and Operator's Guide*.

5.4 Estimating disk space requirements for the database

This section provides formulas for determining the disk space required for the different types of database that can be used in the JP1/Software Distribution system.

5.4.1 Estimating disk space required for Embedded RDB

This subsection provides formulas for determining the disk space required when using Embedded RDB as the database. If a calculation results in a decimal fraction, round it up to the next integer.

In the formulas, *remote installation-related job* and *remote collection-related job* mean one of the jobs listed below.

Remote installation-related jobs:

- *Install package* job
- *Transfer package to relay system* job
- *Send package, allow client to choose* job

Remote collection-related jobs:

- *Collect files from client* job
- *Collect files from client to relay system* job

(1) Disk space required for work table files

Out of the disk space requirements described below, use the maximum value as the estimate for the worktable area.

- Disk space required by the basic functions
- Disk space required by Inventory Viewer
- Disk space required by the CSV output utility
- Disk space required by the operation log list

The following gives the formulas for calculating these disk space requirements.

(a) Disk space required for the basic functions

Disk space required for the basic functions (bytes) =
[(*average number of clients per job* ÷ 2) **x** 4096 **x** 2 **x** 2]
+ [(*average number of clients per job* ÷ 3) **x** 4096 **x** 2 **x** 2]
+ [(*average number of clients per job* ÷ 3) **x** 4096 **x** 2 **x** 2]

(b) Disk space required for Inventory Viewer

Disk space required for Inventory Viewer (bytes) =
((*average number of system information items to be acquired by system* + *number of user inventory items* + *number of registry items to be acquired*) **x** *number of clients* ÷ 4) **x** 4096 **x** 2 **x** 9

(c) Disk space required for the CSV output utility

For the disk space required for the CSV output utility, choose the maximum value from the results obtained from the formulas shown below.

Destination attribute (bytes) =
[(*number of clients belonging to host group* ÷ 7) **x** 4096 **x** 2 **x** 2]
+ [(*number of clients belonging to ID group* ÷ 32) **x** 4096 **x** 2 **x** 2]
+ [(*number of clients* ÷ 51 **x** 4096 **x** 2 **x** 2)]

Package attribute (bytes) =
(*number of packages* ÷ 57) **x** 4096 **x** 2 **x** 5

Inventory (bytes) =

[(*number of user inventory items* ÷ 255) **x** 4096 **x** 2 **x** 5]

+ [(*number of user inventory items* ÷ 11) **x** 4096 **x** 2 **x** 2]

Registry information (bytes) =

(*number of registry items to be acquired* **x** *number of clients* ÷ 5) **x** 4096 **x** 2 **x** 2

Installed package information (bytes) =

(*average number of software information items to be acquired* **x** *number of clients* ÷ 19) **x** 4096 **x** 2 **x** 2

Job execution status (bytes) =

(*average number of clients per job* **x** *average number of packages per job* (use `1` in all cases except for remote installation-related jobs) ÷ 6) **x** 4096 **x** 2 **x** 2

User management information (bytes) =

(*number of user inventory items* **x** *number of clients* ÷ 14) **x** 4096 **x** 2 **x** 2

Software inventory (bytes) =

(*number of files to be managed by software inventory dictionary* **x** *number of clients* ÷ 12) **x** 4096 **x** 2 **x** 2

Package content (bytes) =

((*number of packages* + 1) ÷ 184) **x** 4096 **x** 2 **x** 2

Microsoft Office product information (bytes) =

(*number of Microsoft Office products to be managed* **x** *number of clients* ÷ 8) **x** 4096 **x** 2 **x** 2

Anti-virus product information (bytes) =

(*number of anti-virus products to be managed* **x** *number of clients* ÷ 19) **x** 4096 **x** 2 **x** 2

Startup suppression logs (bytes) =

[(*number of clients* + *number of clients with startup suppression logs* ÷ 19) **x** 4096 **x** 2 **x** 2]

+ [(*number of clients* + *number of clients with startup suppression logs* ÷ 56) **x** 4096 **x** 2 **x** 2]

(d) Disk space required for the operation log list

For the disk space required for the operation log list, choose the maximum value from the results obtained from the formulas shown below.

Operation log list (bytes) =

(*total number of operation information items* (suppression logs and operation logs) ÷ 1) **x** 4096 **x** 2 **x** 2

Operation log details (bytes) =

(*total number of operation information items* (suppression logs and operation logs) ÷ 1) **x** 4096 **x** 2 **x** 2

Disk space required for the operation log total (bytes) =

[(*total number of operation information items* (suppression logs and operation logs) ÷ 1) **x** 4096 **x** 2 **x** 2]

+ [(*total number of operation information items* (suppression logs and operation logs ÷ 184) **x** 4096 **x** 2 **x** 2]

(2) Disk space required for the resident table file

Size of a resident table file (bytes) =

(1048576 **x** 2)

+ {[135 **x** (*number of cabinets* + 2)]

+ [421 **x** (*number of remote collection-related jobs* **x** *average number of clients per job*)]

+ [1028 **x** (*number of remote installation-related jobs* **x** *average number of packages per job* **x** *average number of clients per job*)

+ (*number of jobs other than remote installation-related jobs* **x** *average number of clients per job*)]

+ [972 **x** (*number of remote installation-related ID group jobs managed by the relay managing the ID* **x** *average number of packages per job* **x** *average number of clients per ID group*)

+ (*number of ID group jobs other than remote installation-related jobs* **x** *average number of clients per ID group*)]

+ [96 **x** *number of ID groups*]

+ [654 **x** (*number of ID groups* **x** *average number of relays per ID group* **x** *average number of clients registered per ID group*)]

+ [360 **x** (*number of clients* **x** *average number of files to be acquired by searching software inventory*)]

+ [488 **x** (*number of clients* **x** *average number of system information items to be acquired*)]

+ [600 **x** (*number of jobs defined* + *number of folders*)]

+ [1256 **x** (*number of remote collection-related jobs defined* **x** *number of folders*)]

+ [802 **x** ((*number of jobs defined* **x** *average number of clients per job*) + *number of folders*)]

+ [1798 **x** ((*number of remote installation-related jobs defined* **x** *average number of packages per job*) + *number of folders*)]

+ [348 **x** (*number of Get software information from client jobs defined* + *number of folders*)]

+ [206 **x** (*number of Transfer user inventory schema to client jobs defined* + *number of folders*)]

+ [352 **x** (*number of jobs* + *number of folders*)]

+ [406 **x** (*number of ID groups managed by the relay managing the ID* **x** *total number of ID groups specified by ID group jobs*)]

+ [114 **x** (*number of remote installation-related jobs* **x** *average number of packages per job*)]

+ [76 **x** (*number of items in the software search list* + 1)]

+ [234 **x** (*number of hosts in the system configuration when OpenView Linkage is used*)]

+ [634 **x** (*number of clients* + *number of host groups*)]

+ [122 **x** *number of packages*]

+ [918 **x** (*number of packages* + *number of cabinets*)]

+ [148 **x** *number of jobs scheduled and executed*]

+ [194 **x** (*number of remote installation-related jobs* **x** *average number of packages per job* **x** *average number of clients per job*) + (*number of jobs other than remote installation-related jobs* **x** *average number of clients per job*)]

+ [346 **x** *number of clients* **x** *number of user inventory items*]

+ [768 **x** *number of user inventory items*]

+ [1204 **x** (*number of clients* **x** *average number of software information items to be acquired*)]

+ [464 **x** (*number of all-lower-clients jobs defined* **x** *total number of relay managers specified by all-lower-clients jobs*)]

+ [610 **x** *number of hosts from which registry information is to be collected* **x** *number of registry items to be acquired*]

+ [358 **x** *number of registry acquisition entries to be created*]

+ [1514 **x** *number of hosts in the system configuration*]

+ [918 **x** *number of files to be managed in the software inventory dictionary*]

+ [126 **x** *number of files whose licenses are to be managed*]

+ [406 **x** *number of files whose deletion is to be managed in the software inventory dictionary*]

+ [1970 **x** (*number of clients for which Microsoft Office products are to be obtained* + *number of Microsoft Office products to be managed*)]

+ [1950 **x** (*number of clients for which anti-virus products are to be obtained* + *number of anti-virus products to be managed*)]

+ [806 **x** *number of automatic host group maintenance policies*]

+ [2780 **x** *number of automatic ID group maintenance policies*]

+ [1156 **x** *number of system configuration information deletion entries*]

+ [452 **x** *number of uninstalled JP1/Software Distribution hosts*]

+ [208 **x** *number of conditions set in search host*]

+ [276 **x** *number of communities specified in the search host settings*]

+ [440 **x** *number of hosts found by search host*]

+ [266 **x** *number of Report message jobs defined*]

+ [175 **x** *number of software operation monitoring policies*]

+ [77 **x** (*number of software operation monitoring policies* **x** 7[#1])]

+ [770 **x** *number of programs to be monitored*]

+ [473 **x** *number of programs for which operation time is to be acquired*]

+ [176 **x** *number of permitted software monitoring information entries*]

+ [556 **x** 10000$^{\#2}$]

+ [254 **x** *number of Set the software monitoring policy jobs defined*]

+ [342 **x** *number of filtering conditions specified in operation monitoring policies*]

+ [138 **x** *number of USB media access suppression exclusion conditions*]

+ [939 **x** *number of patch information items*]

+ [22 **x** 3]$^{\#3}$

+ [14]$^{\#4}$

+ [280]$^{\#5}$

+ [64]

+ [2731 **x** (*number of domains* + *number of OUs* + *number of groups* + *number of computers* + *number of users*)]

+ [2305 **x** (*number of OUs* **x** *number of items to be collected from OUs*) + (*number of groups* **x** *number of items to be collected from groups*) + (*number of computers* **x** *number of items to be collected from computers*) + (*number of users* **x** *number of items to be collected from users*)]

+ [2024 **x** (*number of items to be collected from OUs* + *number of items to be collected from groups* + *number of items to be collected from computers* + *number of items to be collected from users*)]

+ [3157 **x** *number of domains*]

+ [66 **x** *number of members belonging to groups*]

+ [165 **x** *number of Web access log filtering conditions*]}

#1: Number of device types

#2: Maximum number of suppression history events to be saved

#3: Number of management items at the last modification date for system configuration information, system configuration information deletion history, and uninstalled host information

#4: Valid period setting for search hosts results

#5: Patch management information

(3) Disk space required for the index file

Size of the index file (bytes) =

(1048576 **x** 2)

+ {[8 **x** (*number of cabinets* + 2)]

+ [28 **x** (*number of remote collection-related jobs* **x** *average number of clients per job*)]

+ [672 **x** (*number of remote installation-related jobs* **x** *average number of packages per job* **x** *average number of clients per job*)

+ (*number of jobs other than remote installation-related jobs* **x** *average number of clients per job*)]

+ [368 **x** (*number of remote installation-related ID group jobs managed by the relay managing the ID* **x** *average number of packages per job* **x** *average number of clients per ID group*)

+ (*number of ID group jobs other than remote installation-related jobs* **x** *average number of clients per ID group*)]

+ [36 **x** *number of ID groups*]

+ [328 **x** (*number of ID groups* **x** *average number of relays per ID group* **x** *average number of clients registered per ID group*)]

+ [360 **x** (*number of clients* **x** *average number of files to be acquired by searching software inventory*)]

+ [280 **x** (*number of clients* **x** *average number of system information items to be acquired*)]

+ [208 **x** (*number of jobs defined* + *number of folders*)]

+ [208 **x** (*number of remote collection-related jobs defined* **x** *number of folders*)]

+ [172 **x** (*number of ID groups* **x** *average number of relays per ID group* **x** *average number of clients registered per ID group*)]

+ [548 **x** ((*number of jobs defined* **x** *average number of clients per job*) + *number of folders*)]

+ [276 **x** ((*number of remote installation-related jobs defined* **x** *average number of packages per job*) + *number of folders*)]

+ [208 **x** (*number of Get software information from client jobs defined* + *number of folders*)]

+ [36 **x** (*number of Get user inventory information jobs defined* + *number of folders*)]

+ [272 **x** (*number of jobs* + *number of folders*)]

+ [276 **x** (*number of ID groups managed by the relay managing the ID* **x** *total number of ID groups specified by ID group jobs*)]

+ [28 **x** (*number of remote installation-related jobs* **x** *average number of packages per job*)]

+ [40 **x** (*number of software search list items* + 1)]

+ [76 **x** (*number of hosts in the system configuration when OpenView Linkage is used*)]

+ [144 **x** (*number of clients* + *number of host groups*)]

+ [8 **x** *number of packages*]

+ [72 **x** (*number of packages* + *number of cabinets*)]

+ [144 **x** *number of jobs scheduled and executed*]

+ [120 **x** (*number of remote installation-related jobs* **x** *average number of packages per job* **x** *average number of clients per job*)] + [*number of jobs other than remote installation-related jobs* **x** *average number of clients per job*]

+ [136 **x** *number of clients* **x** *number of user inventory items*]

+ [136 **x** *number of user inventory items*]

+ [116 **x** (*number of clients* **x** *average number of software information items to be acquired*)]

+ [320 **x** (*total number of all-lower-clients jobs* **x** *total number of relay managers specified by all-lower-clients jobs*)]

+ [328 **x** *number of hosts from which registry information is acquired* **x** *number of registry items to be acquired*]

+ [260 **x** *number of registry acquisition entries created*]

+ [168 **x** *number of hosts in the system configuration*]

+ [408 **x** *number of files managed in software inventory dictionary*]

+ [108 **x** *number of files whose licenses are to be managed*]

+ [296 **x** *number of files whose deletion is to be managed*]

+ [328 **x** (*number of clients* + *number of Office products to be managed*)]

+ [588 **x** (*number of clients* + *number of anti-virus products to be managed*)]

+ [12 **x** *number of automatic destination maintenance policies*]

+ [72 **x** *number of system configuration information deletion history entries*]

+ [36 **x** *number of hosts in which JP1/Software Distribution has not been installed*]

+ [20 **x** *number of conditions set in search host*]

+ [12 **x** *number of communities specified in search host settings*]

+ [24 **x** *number of hosts found in host search*]

+ [208 **x** *number of Report message jobs defined*]

+ [68 **x** *number of software operation monitoring policies*]

+ [72 **x** (*number of software operation monitoring policies* **x** 7[#1])]

+ [76 **x** n*umber of programs to be monitored*]

+ [340 **x** *number of programs for which operation time is to be acquired*]

+ [473 **x** *number of operation time information items to be acquired*][#2]

+ [348 **x** *number of permitted information items for software operation monitoring*]

+ [68 **x** 10000[#3]]

+ [208 **x** *number of Set the software monitoring policy jobs defined*]

+ [336 **x** *number of filtering conditions specified in operation monitoring policies*]

+ [160 **x** *number of software operation monitoring log information items*][#4]

+ [68 **x** *number of USB media access suppression exclusion conditions*]

+ [304 **x** (*number of domains* + *number of OUs* + *number of groups* + *number of computers* + *number of users*)]

+ [36 **x** (*number of OUs* **x** *number of items to be collected from OUs*) + (*number of groups* **x** *number of items to be collected from groups*) + (*number of computers* **x** *number of items to be collected from computers*) + (*number of users* **x** *number of items to be collected from users*)]

+ [12 **x** (*number of items to be collected from OUs* + *number of items to be collected from groups* + *number of items to be collected from computers* + *number of items to be collected from users*)]

+ [260 **x** *number of domains*]

+ [72 **x** *number of members belonging to groups*]

+ [68 **x** *number of Web access log filtering conditions*]

#1: Number of device types

#2: Number of operation time information items acquired =
220 **x** *number of clients* **x** *number of programs for which operation time is to be acquired*

#3: Maximum number of suppression history events to be saved

#4: Number of software operation monitoring log information items =
number of clients to be subject to software operation monitoring
x *size of operation information acquired for 1 client per day*
x *number of days operation information is to be retained*

(4) Disk space required for the job-related binary object file

Size of the job-related binary object file (bytes) =
{32000
+ [*number of remote installation-related ID group jobs managed by the relay managing the ID* **x** *average number of packages per job* **x** *average number of clients per ID group*]
+ [8 **x** (*number of remote installation-related jobs* **x** *average number of packages per job* **x** *average number of clients per remote installation-related job*)]
+ [*number of jobs other than remote installation-related jobs* **x** *average number of clients per job*]
+ [13 **x** (*number of Get software information from client jobs defined* + *number of folders*)]
+ [*number of Collect files from client jobs* + *number of Collect files from client to relay system jobs* + *number of Acquire collected files from relay system jobs* + *number of Delete collected files from relay system jobs*]
+ [(*number of software search lists* + 1)]
+ [*number of scheduled and executed jobs*]
+ [8 **x** (*number of Report message jobs defined*)]}
x 8192

(5) Disk space required for the asset information-related binary object file

Size of an asset information-related binary object file (bytes) =
{12800
+ [7 **x** (*number of packages*)]
+ [28 **x** (*number of user inventory items*)]}
x 8192

(6) Disk space required for the software operation monitoring log file

Size of a software operation monitoring log file (bytes) =
4194304
+ (1363 **x** *number of software operation monitoring log entries*)$^{\#1}$
+ [80 **x** *number of operation time information items acquired*]$^{\#2}$

#1: To determine the number of software operation monitoring log entries, use the following formula:

Number of software operation monitoring log entries =
number of clients subject to software operation monitoring
x *size of operation information acquired for 1 client per day*
x *number of days operation information is to be retained*

#2: Number of operation time information items acquired =
220 **x** *number of clients* **x** *number of programs for which operation time is to be acquired*

For clients in a virtual environment, the number of information items collected increases in proportion to the number of login users. Therefore, add the number of expected login users to *number of clients*.

If you use the `dcmmonrst` command provided by JP1/Software Distribution, you can also store in the database the operation information whose retention days specified at setup have expired. When you determine the number of days operation information is to be retained, take into account the number of days operation information is stored in the database by the `dcmmonrst` command.

(7) Disk space required for the updated program management file

Updated program management file (bytes) =

[4024433 **x** *number of downloaded patches*#]

+ [3403 **x** *number of installed scripts*]

#: Excludes OS service packs.

(8) Disk space required for the temporary table file

Temporary table file size (bytes) =

713031680

+ [(*resident table file size* + *index file size*) **x** 0.6]

(9) Notes on differences between sizes for version 08-00 and earlier and version 08-10 and later

When you upgrade from version 08-00 or earlier to version 08-10 or later, the database structure is different so the disk space required by the database is also different. This means that an error may occur during upgrading due to insufficient disk space.

Before you upgrade, re-estimate the amount of disk space required for the database. You can change the size of the database when you upgrade.

The formulas provided below are applicable if, after upgrading, you use only the functions supported in version 08-00 or earlier. To use the new functions supported in version 08-10 and later, you must use the formulas in subsections (1) through (8) above to calculate the database size of the additional functions.

The following subsections provide the formulas for calculating the database size needed in version 08-10 and later, based on the database size in version 08-00 and earlier.

(a) Resident table file

Size of resident table files (bytes) =

size of version 08-00 or earlier resident table files

+ [73 **x** (*number of cabinets* + 2)]

+ [233 **x** (*number of remote collection-related jobs* **x** *average number of clients per job*)]

+ [1008 **x** (*number of remote collection-related jobs defined* **x** *number of folders*)]

+ [736 **x** ((*number of remote installation-related jobs defined* **x** *average number of packages per job*) + *number of folders*)]

+ [746 **x** (*number of packages* + *number of cabinets*)]

+ [908 **x** (*number of clients* **x** *average number of software information items to be acquired*)]

(b) Index file

No changes have been made to index files.

(c) Job-related binary object file

Size of job-related binary object file (bytes) =

size of version 08-00 or earlier job-related binary object file

- {[7 **x** (*number of remote collection-related jobs* **x** *average number of clients per job*)]

+ [15 **x** (*number of remote collection-related jobs* **x** *number of folders*)]

+ [20 **x** ((*number of remote installation-related jobs* **x** *average number of packages per job*) + *number of folders*)]}

x 8192

(d) Asset information-related binary object file

Size of asset information-related binary object file (bytes) =

size of version 08-00 or earlier asset information-related binary object file

- {[7 **x** (*number of cabinets* + 2)]

+ [7 **x** (*number of packages*)]

+ [7 **x** (*number of clients* **x** *average number of asset information items per client*)]}

x 8192

(e) Software operation monitoring log file

No changes have been made to the software operation monitoring log file.

(f) Temporary table file

No changes have been made to the temporary table file.

5.4.2 Estimating disk space required for Microsoft SQL Server

This subsection provides formulas for determining the disk space required for using Microsoft SQL Server as the database. If a calculation results in a decimal fraction, round it up to the next integer.

In the formulas, *remote installation-related job* means one of the jobs listed below.

Remote installation-related jobs:

- *Install package* job
- *Transfer package to relay system* job
- *Send package, allow client to choose* job

(1) Disk space required for the database device

Size of the database device (bytes) =

{(*number of cabinets* **x** 1.021 + 1)

+ ((*number of remote installation-related jobs* **x** *average number of packages per job* **x** *average number of clients per job* + *number of jobs other than remote installation-related jobs* **x** *average number of clients per job*) **x** 1.111 + 1000)

+ (*number of hosts specified as job destination* **x** 0.083 + 1450)

+ (*number of jobs registered* **x** (*number of hosts directly under the managing server through which the job is routed* + *number of hosts directly under the managing server targeted by the job*) **x** 0.045 + 200)

+ (*number of clients* **x** *average number of software information items to be acquired* **x** 1.1 + 1050)

+ (*number of clients* **x** 0.254 + 32)

+ (*number of jobs defined* **x** 0.067 + 2)

+ ((*number of Collect files from client jobs defined* + *number of Collect files from client to relay system jobs defined*) **x** 2.071 + 2)

+ (*number of packages targeted by Install package jobs and Transfer package to relay system jobs* **x** 0.25 + 2)

+ (*number of Get software information from client jobs defined* **x** 0.048 + 2)

+ (*number of jobs registered* **x** 0.1 + 2)

+ ((*number of packages targeted by Install package jobs and Transfer package to relay system jobs* + *number of Collect files from client jobs and Collect files from client to relay system jobs defined*) **x** 0.039 + 2)

+ (*number of host groups* **x** 0.1 + 3)

+ (*number of packages to be stored* **x** 1.094 + 4)

+ (*number of jobs scheduled* **x** 1.053 + 2)
+ (*number of ID groups* **x** 0.037 + 2)
+ ((*number of clients registered to ID groups* + *number of relays managing the ID*) **x** 0.037 + 2)
+ (2816 **x** *number of automatic ID group maintenance policies*)
+ (*number of software search lists stored* **x** 0.11 + 2)
+ (*total size of software search lists* ÷ 1800 + 6)
+ ((0.111 **x** *number of hosts in the system configuration when OpenView Linkage is used*) + 36)}
x 2048
+ (*size of software inventory*[#1])
+ (466 **x** *number of clients* **x** *average number of system information items collected*)
+ (328 **x** *number of clients* **x** *number of user inventory items*)
+ (64963 **x** *number of user inventory items*)
+ (580 **x** *number of hosts from which to acquire registry information* **x** *number of registry items to acquire*)
+ (332 **x** *number of registry collection items created*)
+ (1126 **x** *number of system configuration information deletion entries*)
+ (420 **x** *number of uninstalled JP1/Software Distribution hosts*)
+ (175 **x** *number of conditions set in search host*)
+ (260 **x** *number of community names specified in search host settings* **x** *number of conditions set in search host*)
+ (412 **x** *number of hosts found by search host*)
+ (144 **x** *number of software operation monitoring policies*)
+ [336 **x** (*number of software operation monitoring policies* **x** 7[#2])]
+ (733 **x** *number of programs to be monitored by each policy*)
+ (364 **x** *number of programs for which operation time is to be acquired*)
+ (331 **x** *number of permitted information items for software operation monitoring*)
+ (140 **x** *number of filtering conditions specified in operation monitoring policies*)
+ (160 **x** *number of Web access log filtering conditions*)
+ (282 **x** *number of access suppression exclusion conditions for USB media*)
+ (521 **x** 10000[#3])
+ (939 **x** *number of patch information items*)
+ (4024433 **x** *number of downloaded patches*[#4])
+ (3403 **x** *number of installed scripts*)
+ 280[#5]
+ 3
+ (4706 **x** (*number of domains* + *number of OUs* + *number of groups* + *number of computers* + *number of users*))
+ (4287 **x** ((*number of OUs* **x** *number of items to be collected from OUs*) + (*number of groups* **x** *number of items to be collected from groups*) + (*number of computers* **x** *number of items to be collected from computers*) + (*number of users* **x** *number of items to be collected from users*)))
+ (4020 **x** (*number of items to be collected from OUs* + *number of items to be collected from groups* + *number of items to be collected from computers* + *number of items to be collected from users*))
+ (6319 **x** *number of domains*)
+ (64 **x** *number of members belonging to groups*)

#1: Software inventory size
= (*size of the software inventory dictionary*)
+ (*size when the client software inventory is obtained*)
+ (*size of the number-of-clients table*)
+ (*size of deleted software management table*)

#2: Number of device types

#3: Maximum number of suppression history events to be saved

#4: Excludes OS service packs.

#5: Patch management information

Guidelines for calculating the amount of data usage are provided below.

(a) Size of the software inventory dictionary

887 **x** *number of files to be collected from the hosts when searching software inventory* (bytes)

Example: When files with `*.exe` or `*.dll` extensions are collected

Suppose that the number of `*.exe` and `*.dll` files in a client is 1,000.

887 **x** 1000 = 887000 bytes (about 0.85MB)

(b) Size when client software inventory is obtained

342 bytes (size of one table) **x** *number of destinations to be searched* **x** *number of search result files*

Example: When the number of destination clients is 1,000 and each client has 1,000 files

342 **x** 1000 **x** 1000 = 342000000 bytes (about 326MB)

(c) Size of the number-of-clients table

108 bytes (size of one table) **x** *number of files to be processed by license management*

Example: When 100 of the 1,000 files are to be processed by license management

108 **x** 100 = 10800 bytes (about 0.01MB)

(d) Size of deleted software management table

384 bytes (size of one table) **x** *number of files to be processed by deletion management*

Example: When 100 software programs are not added to the software inventory dictionary

384 **x** 100 = 38400 bytes (about 0.04MB)

Note that no software program is duplicated between the software inventory dictionary and deleted software management table.

(2) Disk space required for the transaction log device

Microsoft SQL Server recommends that you set the size of the transaction log device to about 20% of the size of the entire relational database. Also, we recommend that you configure the automatic expansion of transaction log files. For details, see the Microsoft SQL Server documentation.

For details about the transaction log settings, see *(8) Setting the transaction log in 7.3.2 Setting up an environment for Microsoft SQL Server* in the manual *Setup Guide*.

(3) Disk space required for the software package database device

Size of software package database device (bytes) =

((*size of managed packages*/1800 (if less than 1, round up it to 1))

+ 2 **x** *number packages to be stored*

+ 2 **x** *number of packages for which installation attributes were changed at job definition registration*

+ 2 **x** *number of packages at job registration*

+ 2 **x** *number of Collect files from client job registrations*)

x 2048

(4) Disk space required for the software operation monitoring log database device

Size of a software operation monitoring log database device (bytes) =

(1861[#1] **x** *number of software operation monitoring log information entries*)[#2]

+ (80 **x** *number of operation time information items acquired*)[#3]

#1: If you want to specify a maximum value for the operation log information size, specify 1861 (bytes). If you want to specify a typical size for software operation monitoring logs, specify the total of the column *size per entry* (bytes) **x** *coefficient* for items 1 through 6 in the table shown below, which is 543 (bytes).

Item	Item	Size per entry (bytes)	Coefficient	Size per entry (bytes) **x** coefficient
1	Process start	335	0.14	46.9
2	Process stop	335	0.14	46.9
3	Caption change	590	0.25	147.5
4	Active window switching	590	0.25	147.5
5	File operation	837	0.08	66.96
6	Web access log	621	0.14	86.94

For details about coefficients, see *2.5.10 Guidelines for the number of days to save operation information*.

#2: To determine the number of software operation monitoring log entries, use the following formula:

number of software operation monitoring log information entries =
number of clients subject to software operation monitoring
x *size of operation information acquired for 1 client per day*
x *number of days operation information is to be retained*

#3: *number of operation time information items acquired* =
220 **x** *number of clients* **x** *number of programs for which operation time is to be acquired*

For clients in a virtual environment, the number of information items collected increases in proportion to the number of login users. Therefore, add the number of expected login users to *number of clients*.

If you use the `dcmmonrst` command provided by JP1/Software Distribution, you can also store in the database the operation information whose retention days specified at setup have expired. When you determine the number of days operation information is to be retained, take into account the number of days operation information is stored in the database by the `dcmmonrst` command.

Furthermore, if you want to use the following data partitioning facility to store the operation monitoring logs, you must create either a new regular relational database using Database Manager, or a different data partition after an upgrade:

- Data partitioning facility of Microsoft SQL Server 2012
- Data partitioning facility of Microsoft SQL Server 2008
- Data partitioning facility of Microsoft SQL Server 2005

To create data partitions, use SQL Server Management Studio. For details, see *7.6 Using data partitions to store operation monitoring history* in the *Setup Guide*.

(5) Disk space required for the temporary database (tempdb)

Among the formulas for determining the temporary database size, use the maximum value as the size of `tempdb`. If multiple facilities execute in parallel, use the sum of their temporary database sizes as the value of `tempdb`.

- Size of temporary database required for the basic facilities

  Size of temporary database (bytes) =
  (1.14 **x** *total number of hosts targeted by jobs to be registered*
  + 1.17 **x** *total number of packages targeted by jobs to be registered*
  + 3.20 **x** *total number of hosts targeted by jobs to be registered* **x** *total number of packages targeted by jobs to be registered*)
  x 2048

- Size of temporary database required for Inventory Viewer

Size of temporary database (bytes) =

466 bytes **x** *number of items of system information to display per node* **x** *number of nodes for displaying the inventory* + 328 bytes **x** *number of user inventory items to display per node* **x** *number of nodes for displaying the inventory* + 586 bytes **x** *number of items of registry information to display per node* **x** *number of nodes for displaying the inventory*

- Size of temporary database required for the CSV output utility
    - Host attributes

      Size of temporary database (bytes) =

      500 bytes **x** *number of hosts belonging to the host group* + 1000 bytes **x** *total number of hosts* + 70 bytes **x** *number of clients belonging to the ID group*
    - Package attributes

      Size of temporary database (bytes) =

      950 bytes **x** *total number of packages*
    - User inventory information

      Size of temporary database (bytes) =

      70 bytes **x** *number of items managed on local server and items managed on higher and local servers (user inventory items)* + 450 bytes **x** *number of items managed on local server and items managed on higher and local servers* (user inventory items) **x** *number of clients from which information has been acquired*
    - Registry information

      Size of temporary database (bytes) =

      550 bytes **x** *number of items managed on local server and items managed on higher and local servers (registry collection items)* **x** *number of clients from which information has been acquired*
    - Installed package information

      Size of temporary database (bytes) =

      400 bytes **x** *number of packages installed per node* **x** *number of clients from which information has been acquired*
    - Job status

      Size of temporary database (bytes) = *sum of the size for each job*#

      #: Size for each job = 2250 bytes **x** *number of destinations per job* **x** *number of packages per job* (for jobs other than distribution jobs, this value is 1)
    - User management information

      Size of temporary database (bytes) =

      70 bytes **x** *number of items managed on local server and items managed on higher and local servers (user inventory items)* + 70 bytes **x** *total number of clients* + 1100 bytes
    - System information

      Size of temporary database (bytes) =

      600 bytes **x** *number of inventory items per node* **x** *number of clients from which information has been acquired*
    - Software inventory

      Size of temporary database (bytes) =

      1100 bytes **x** *number of managed programs* **x** *number of clients from which information has been acquired*
    - License information

      Size of temporary database (bytes) =

      150 bytes **x** *number of licensed programs* + 100 bytes **x** *number of managed programs*
    - Package contents

      Size of temporary database (bytes) =

      300 bytes **x** *total number of files for all the packages whose package type is User programs and data*

(6) Disk space required for the database table for storing obtained patches

Size of database table for storing patches (bytes) =

5468 **x** *number of patch information items* + *average size of patch* **x** *number of patches obtained*

5.4.3 Estimating disk space required for Oracle

This subsection provides formulas for determining the disk space required for using Oracle as the database. If a calculation results in a decimal fraction, round it up to the next integer.

In the formulas, *remote installation-related job* and *remote collection-related job* mean one of the jobs listed below.

Remote installation-related jobs:

- *Install package* job
- *Transfer package to relay system* job
- *Send package, allow client to choose* job

Remote collection-related jobs:

- *Collect files from client* job
- *Collect files from client to relay system* job

(1) Disk space required for the user table area

- Initial size = *total size of all tables* + (*total size of all tables* **x** 20%)
- Table size = *line size* **x** *number of lines*
- Line size = *line header* **x** (3 **x** *UB1*) + *total column size including byte length*
  (*UB1* is a variable for an unsigned byte; the system obtains the value from `V$type_size`.)
- Row header = 3 + *number of short columns* + (3 **x** *number of long columns*)
  (A short column has up to 255 bytes; a long column has 256 bytes or more.)

Size of user table area (bytes) =

{[156 (*number of cabinets* + 2)]

+ [460 **x** (*number of remote collection-related jobs* **x** *average number of clients per job*)]

+ [1729 **x** (*number of remote installation-related jobs* **x** *average number of packages per job* **x** *average number of clients per job*)

+ (*number of jobs other than remote installation-related jobs* **x** *average number of clients per job*)]

+ [1708 **x** (*number of remote installation-related ID group jobs managed by the relay managing the ID* **x** *average number of packages per job* **x** *average number of clients per ID group*)

+ (*number of jobs other than remote installation-related ID group jobs* **x** *average number of clients per ID group*)]

+ [96 **x** *number of ID groups*]

+ [202 **x** (*number of ID groups* **x** *average number of relays per ID group* **x** *average number of clients registered per ID group*)]

+ [763 **x** (*number of clients* **x** *average number of files to be acquired by searching software inventory*)]

+ [496 **x** (*number of clients* **x** *average number of system information items to be acquired*)]

+ [306 **x** (*number of jobs* + *number of folders*)]

+ [3265 **x** (*number of remote collection-related jobs* **x** *number of folders*)]

+ [337 **x** (*number of ID group jobs* **x** *number of folders*)]

+ [585 **x** ((*number of jobs* **x** *average number of clients per job*) + *number of folders*)]

+ [2390 **x** ((*number of remote installation-related jobs* **x** *average number of packages per job*) + *number of folders*)]

+ [359 **x** (*number of Get software information from client jobs defined* + *number of folders*)]

+ [206 **x** (*number of Transfer user inventory schema to client jobs defined* + *number of folders*)]

+ [355 **x** (*number of jobs* + *number of folders*)]

+ [468 **x** (*number of ID groups managed by the relay managing the ID* **x** *total number of ID groups specified in ID group jobs*)]

+ [2792 **x** *number of automatic ID group maintenance policies*]

+ [1145 **x** (*number of Collect files from client jobs* + *number of Collect files from client to relay system jobs* + *number of Acquire collected files from relay system jobs* + *number of Delete collected files from relay system jobs*)]

+ [65622 **x** (*number of software search list items* + 1)]

+ [244 **x** *number of hosts in the system configuration when the OpenView Linkage is used*]

+ [583 **x** (*number of clients* + *number of host groups*)]

+ [65669 **x** *number of packages*]

+ [979 **x** (*number of packages* + *number of cabinets*)]

+ [458 **x** *number of jobs scheduled and executed*]

+ [232 **x** (*number of remote installation-related jobs* **x** *average number of packages per job* **x** *average number of clients per job*)]

+ [232 **x** (*number of jobs other than remote installation-related jobs* **x** *average number of clients per job*)]

+ [1031 **x** *number of clients*]

+ [56]

+ [1577 **x** (*number of ID groups* **x** *average number of relays per ID group* **x** *average number of clients registered per ID group*)]

+ [328 **x** *number of clients* **x** *number of user inventory items*]

+ [64962 **x** *number of user inventory items*]

+ [370 **x** (*number of clients* **x** *average number of software information items to be acquired*)]

+ [438 **x** (*number of all-lower-clients jobs defined* **x** *total number of relay managers specified by all-lower-clients jobs*)]

+ [273 **x** *number of relay managers/systems in system configuration*]

+ [632 **x** *number of hosts* **x** *number of registry items to be acquired*]

+ [378 **x** *number of registry acquisition items created*]

+ [864 **x** *number of hosts in the system configuration*]

+ [*size of software inventory*$^{\#1}$]

+ [1141 **x** *number of system configuration information deletion logs*]

+ [465 **x** *number of uninstalled JP1/Software Distribution hosts*]

+ [260 **x** *number of conditions set in search host*]

+ [286 **x** *number of community names specified in search host settings* **x** *number of conditions set in search host*]

+ [12]

+ [446 **x** *number of hosts found by search host*]

+ [237 **x** *number of software operation monitoring policies*]

+ [361 **x** (*number of software operation monitoring policies* **x** 7$^{\#2}$)]

+ [735 **x** *number of programs to be monitored*]

+ [370 **x** *number of programs for which operation time is to be acquired*]

+ [337 **x** *number of permitted information items for software operation monitoring*]

+ [340 **x** *number of filtering conditions specified in operation monitoring policies*]

+ [419 **x** *number of Web access log filtering conditions*]

+ [397 **x** *number of access suppression exclusion conditions for USB media*]

+ [520 **x** 10000$^{\#3}$]

+ [4713 **x** (*number of domains* + *number of OUs* + *number of groups* + *number of computers* + *number of users*)]

+ [4287 **x** ((*number of OUs* **x** *number of items to be collected from OUs*) + (*number of groups* **x** *number of items to be collected from groups*) + (*number of computers* **x** *number of items to be collected from computers*) + (*number of users* **x** *number of items to be collected from users*))]

+ [4008 **x** (*number of items to be collected from OUs* + *number of items to be collected from groups* + *number of items to be collected from computers* + *number of items to be collected from users*)]

+ [6319 **x** *number of domains*]}

+ [64 **x** *number of members belonging to groups*]}

#1: Software inventory size
= (*size of the software inventory dictionary*)
+ (*size when the client software inventory is obtained*)
+ (*size of the number-of-clients table*)
+ (*size of deleted software management table*)

#2: Number of device types

#3: Maximum number of suppression history events to be saved

Guidelines for calculating the amount of data usage are provided below.

(a) Size of the software inventory dictionary

887 bytes (size of one table) **x** *number of search result files*

Example: When files with `*.exe` or `*.dll` extensions are collected
Suppose that the number of `*.exe` and `*.dll` files in a client is 1,000.
887 **x** 1000 = 887000 bytes (about 0.85MB)

(b) Size when client software inventory is obtained

342 bytes (size of one table) **x** *number of destinations to be searched* **x** *number of search result files*

Example: When the number of destination clients is 1,000 and each client has 1,000 files
342 **x** 1000 **x** 1000 = 342000000 bytes (about 326MB)

(c) Size of the number-of-clients table

108 bytes (size of one table) **x** *number of files to be processed by license management*

Example: When 100 of the 1,000 files are to be processed by license management
108 **x** 100 = 10800 bytes (about 0.01MB)

(d) Size of deleted software management table

384 bytes (size of one table) **x** *number of files to be processed by deletion management*

Example: When 100 software programs are not added to the software inventory dictionary
384 **x** 100 = 38400 bytes (about 0.04MB)

Note that no software program is duplicated between the software inventory dictionary and deleted software management table.

(2) Disk space required for the rollback table area

The size of the rollback table area is usually 10% of the user table area.

(3) Disk space required for the index table area

- Initial size = *total of all index tables*
- Size of one index table = *number of bytes per item* **x** *number of items*
- Number of bytes per item = *header size* + *size of one index line*
- Header size = 3 + *number of short columns* + (3 **x** *number of long columns*)

(A short column has up to 128 bytes; a long column has 129 bytes or more.)

Size of index table area (bytes) =
{[36 **x** *number of ID groups*]
+ [112 **x** (*number of ID groups* **x** *number of ID groups per client*)]
+ [73 **x** (*number of clients* **x** *average number of system information items to be acquired*)]

+ [387 **x** (*number of jobs* + *number of folders*)]

+ [168 **x** (*number of ID groups* **x** *average number of relays per ID group* **x** *average number of clients registered per ID group*)]

+ [242 **x** ((*number of jobs* **x** *average number of clients per job*) + *number of folders*)]

+ [168 **x** (*number of Get software information from client jobs defined* + *number of folders*)]

+ [168 **x** (*number of Get user inventory information jobs defined* + *number of folders*)]

+ [270 **x** (*number of ID groups managed by the relay managing the ID* **x** *total number of ID groups specified by ID group jobs*)]

+ [40 **x** (*number of items in the software search list* + 1)]

+ [76 **x** *number of hosts in the system configuration when the OpenView Linkage is used*]

+ [86 **x** (*number of remote installation-related jobs* **x** *average number of packages per job* **x** *average number of clients per job*)

+ (*number of jobs other than remote installation-related jobs* **x** *average number of clients per job*)]

+ [36 **x** *number of automatic ID group maintenance policies*]

+ [76 **x** *number of clients*]

+ [133 **x** (*number of Transfer user inventory schema to client jobs defined* **x** *number of folders*)]

+ [339 **x** (*number of clients* **x** *average number of software information items to be acquired*)]

+ [321 **x** (*number of all-lower-clients jobs defined* **x** *total number of relay managers specified by all-lower-clients jobs*)]

+ [173 **x** *number of relay managers/systems in system configuration*]

+ [330 **x** *number of hosts* **x** *number of registry items to be acquired*]

+ [264 **x** *number of registry acquisition items created*]

+ [297 **x** *number of hosts in the system configuration*]

+ [*size of software inventory*][#1]

+ [35 **x** *number of uninstalled JP1/Software Distribution hosts*]

+ [14 **x** *number of conditions set in search host*]

+ [14 **x** *number of community names specified in search host settings* **x** *number of conditions set in search host*]

+ [27 **x** *number of hosts found by search host*]

+ [68 **x** *number of software operation monitoring policies*]

+ [101 **x** (*number of software operation monitoring policies* **x** 7[#2])]

+ [75 **x** *number of programs to be monitored*]

+ [377 **x** *number of programs for which operation time is to be acquired*]

+ [347 **x** *number of permitted information items for software operation monitoring*]

+ [331 **x** *number of filtering conditions specified in operation monitoring policies*]

+ [68 **x** *number of Web access log filtering conditions*]

+ [68 **x** *number of access suppression exclusion conditions for USB media*]

+ [68 **x** 10000[#3]]

+ [88 **x** *number of software operation monitoring history information items*][#4]

+ [109 **x** *number of operation time information items acquired*][#5]

+ [305 **x** (*number of domains* + *number of OUs* + *number of groups* + *number of computers* + *number of users*)]

+ [36 **x** ((*number of OUs* **x** *number of items to be collected from OUs*) + (*number of groups* **x** *number of items to be collected from groups*) + (*number of computers* **x** *number of items to be collected from computers*) + (*number of users* **x** *number of items to be collected from users*))]

+ [25 **x** (*number of items to be collected from OUs* + *number of items to be collected from groups* + *number of items to be collected from computers* + *number of items to be collected from users*)]

+ [38 **x** *number of domains*]

+ [69 **x** *number of members belonging to groups*]}

#1: *size of software inventory*

= (*size of the software inventory dictionary*)
+ (*size when the client software inventory is obtained*)
+ (*size of deleted software management table*)
= (292 **x** *number of search result files*)

+ (331 **x** *number of destinations to be searched* **x** *number of search result files*)

+ (292 **x** *number of files to be processed by deletion management*)

#2: Number of device types

#3: Maximum number of suppression history events to be saved

#4: number of software operation monitoring history information items =
number of clients subject to software operation monitoring
x *size of operation information acquired for 1 client per day*
x *number of days operation information is to be retained*

#5: Number of operation time information items acquired =
220 **x** *number of clients* **x** *number of programs for which operation time is to be acquired*

(4) Disk space required for the temporary table area

The size of the temporary table area is usually 60% of the user table area.

(5) Disk space required for the software operation monitoring log table space

Size of a software operation monitoring log table space (bytes) =
[1861 **x** *number of software operation monitoring log information entries*]#1
+ [80 **x** *number of operation time information items acquired*]#2

#1: To determine the number of software operation monitoring log entries, use the following formula:

number of software operation monitoring log information entries =
number of clients subject to software operation monitoring
x *size of operation information acquired for 1 client per day*
x *number of days operation information is to be retained*

#2: *number of operation time information items acquired* =
220 **x** *number of clients* **x** *number of programs for which operation time is to be acquired*

For clients in a virtual environment, the number of information items collected increases in proportion to the number of login users. Therefore, add the number of expected login users to *number of clients*.

If you use the `dcmmonrst` command provided by JP1/Software Distribution, in the database you can also store the operation information whose retention days specified at setup have expired. When you determine the number of days operation information is to be retained, take into account the number of days operation information is stored in the database by the `dcmmonrst` command.

(6) Disk space required for the updated program management table area

Updated program management table area (bytes) =
[939 **x** *number of patch information items*]
+ [4024433 **x** *number of downloaded patches*#1]
+ [3403 **x** *number of installed scripts*]
+ 280#2

#1: Excludes OS service packs.

#2: Patch management information

5.4.4 Estimating disk space required for Asset Information Manager Subset

This subsection provides formulas for estimating the disk space required to use the Asset Information Manager Subset database. If the calculation results in a decimal fraction, round it up to the next integer.

Size of database capacity (kilobytes) = (**Σ** (*size of an information item used* **x** *number of items registered*) + 30720) **x** 1.4 **x** 1.5

The following table lists the information used by Asset Information Manager Subset, as well as the sizes and the default number of registration entries for that information.

Information used	Size (kilobytes)	Default number of registration entries
Hardware asset information	51.7[#1]	1,000
Installed software list	0.4	200
Patch list	0.2	100
IP group information	0.8	300
IP address management information[#2]	0.3	2,000
Installation site information[#3]	1.2	100
User management information[#3]	0.8	1,000
Group name information	1.0	200
Permission management information[#3]	0.4	100
Modification history	0.8	3,000
Software modification history	0.4	2,000
Number of search patterns for operation log totals	--	15
Number of days for holding operation log totaled results	--	7

Legend:

--: No value.

#1

The size of hardware asset information is an approximate value based on the assumption that the following information is included, where parentheses enclose the size for each entry:

- 1 asset information entry (2.7 kilobytes)
- 1 hardware asset information entry (1.4 kilobytes)
- 3 network information entries (0.6 kilobytes)
- 20 transfer log entries (1.2 kilobytes)
- 60 installed software information entries (0.3 kilobytes)
- 10 patch information entries (0.1 kilobytes)
- 1 virus definition information entry (0.5 kilobytes)
- 1 component information entry (0.3 kilobytes)
- 1 inventory information entry (2.0 kilobytes)

#2

You need as many IP address management information entries as there are IP addresses that can be used in the address range registered in the IP group information.

#3

You do not need to calculate these sizes if you are totaling operation logs.

If you are totaling operation logs, the following disk space is required for data:

Data size required for totaling operation logs (kilobytes) =
(*number of patterns used for totaling* **x** *number of days to hold totals* **x** *number of groups*) **x** 0.4

6 Setting Up the Environment for a JP1/Software Distribution System

This chapter describes the environment setup for a network running JP1/Software Distribution and for achieving efficient operation.

6.1 Evaluating the network environment

This section explains the network environment used by JP1/Software Distribution. It also explains the settings required to use JP1/Software Distribution in a system that contains a firewall or in a multi-LAN environment.

6.1.1 JP1/Software Distribution network environment

A JP1/Software Distribution system uses the TCP/IP protocol only. Therefore, it does not depend on a specific network operating system, such as Windows NT Server or NetWare. JP1/Software Distribution can also be used in an environment in which multiple network operating systems and client-side communication programs (TCP/IP protocol stacks) coexist.

When you use JP1/Software Distribution Client (client) under Windows, you must use the TCP/IP protocol stack that is bundled with Windows.

Both WINS and DNS can be used for managing host names. However, a system in which a single name server manages all clients is not recommended. In such a system, name resolution queries will concentrate in the single name server, resulting in significantly lower system performance. In such a case, using a `hosts` file to manage names can be effective in reducing the network load.

6.1.2 Determining the ID key used to identify hosts

In networks that use JP1/Software Distribution, you must determine the key used to identify hosts. There are two types of keys:

- Host ID

  This key is unique within the system and identifies each client individually. A host ID is generated when each client is installed and is reported automatically to the higher system. Therefore, unlike the node identification key described below, host IDs are not affected by changes in the network configuration. A host ID is created when each client is installed and saved in the host ID management file.
- Node identification key

  You can use either host names or IP addresses as the node identification key; you select one or the other during setup. Because both cannot be used at the same time, select one before starting operation of your JP1/Software Distribution system. You can change the node identification key during operation, but this is not recommended because the change results in deletion of some information. For details, see *4.2.8(2) Notes on changing the node identification key* in the *Setup Guide*.

To determine the ID key used to identify JP1/Software Distribution hosts, evaluate the following items:

- Whether to use host IDs
- Whether to use host names or IP addresses as the node identification key

(1) Evaluating whether to use host IDs

We recommend using host IDs for network management in the following types of systems:

- Systems that integrate multiple domains, so that there might be duplicated host names and IP addresses.
- Environments in which the network configuration changes frequently due to changes in the configuration of clients.

(2) Selecting the node identification key

The type of identifiers used for managing nodes (hosts) in a network that uses JP1/Software Distribution is called the *node identification key*. Either host names or IP addresses can be used as the node identification key.

Because host names and IP addresses cannot both be used, you must select which you will use before starting operations. Note that in a system in which managing servers are configured in a hierarchy, it is not necessary to use the same identification key throughout the entire system. However, you must standardize the node identification key within each system managed by a relay manager.

(a) Using host names to manage JP1/Software Distribution nodes

You must use host names for management of nodes in the following systems:

- Systems in which a firewall is installed
- Systems in which the DHCP is used

Name hosts according to the rules described in *8.1.2 Assigning host names in a JP1/Software Distribution system* in the *Setup Guide*.

(b) Using IP addresses to manage JP1/Software Distribution nodes

If it is difficult to use host names to manage nodes within the network, you can use IP addresses instead. When IP addresses are used, relay systems and clients do not require definitions for name resolution, such as by using the hosts file, but relay managers do.

6.1.3 Using host IDs for network management

As an alternative to the node identification key, you can use host IDs to manage a network. You manage a network using host IDs by specifying appropriate settings during setup of the central manager. All relay systems and clients under the central manager can then be managed by using the host IDs.

(1) Advantages of using host IDs

Use of host IDs offers the following advantages:

- A host ID represents information that is a unique ID within the system. So, even if a multi-domain system contains hosts with identical host names, the host IDs can be used to identify them as separate hosts.
- When a client is moved in a network environment that uses a node identification key, its host name and IP address are changed. This means that the client is no longer recognized as the same client. In contrast, if host IDs are used, the existing asset information for the client is inherited at the client's new location.

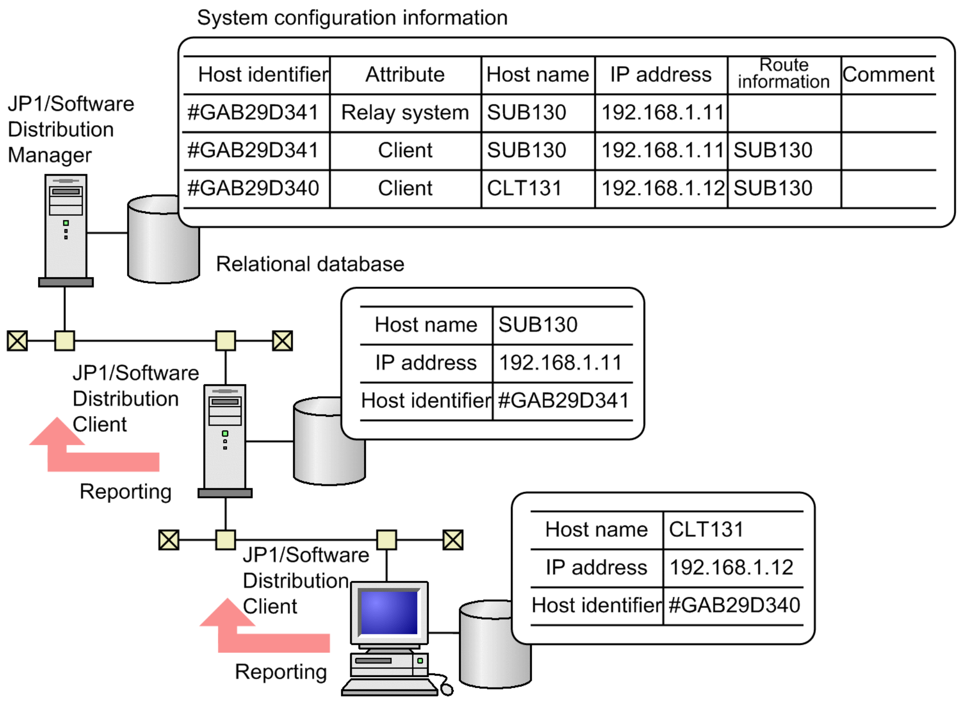
(2) Registering host IDs

A host ID is generated for a client when the client is installed, and is stored in a *host ID management file*. If a client already has a host ID management file when the client is re-installed, a new host ID is not generated.

A generated host ID is registered in the higher systems. To enable registration, in the Software Distribution Manager Setup dialog box, choose the **ID Key for Operations** page, and then select **Yes** for **Use host IDs**.

The host ID is registered automatically in higher systems as shown in the following figure.

Figure 6–1: Automatic registration of host IDs


System configuration information
JP1/Software Distribution Manager
Relational database
JP1/Software Distribution Client
Reporting
JP1/Software Distribution Client
Reporting

Host identifier	Attribute	Host name	IP address	Route information	Comment
#GAB29D341	Relay system	SUB130	192.168.1.11		
#GAB29D341	Client	SUB130	192.168.1.11	SUB130	
#GAB29D340	Client	CLT131	192.168.1.12	SUB130	

Host name	SUB130
IP address	192.168.1.11
Host identifier	#GAB29D341

Host name	CLT131
IP address	192.168.1.12
Host identifier	#GAB29D340

(3) Timing for automatic registration of host IDs

The following table shows the times at which host IDs are registered automatically in the next-higher system, depending on the settings for automatic registration of system configuration information.

Table 6–1: Times at which host IDs are registered automatically in the next-higher system

Is system configuration information registered automatically?	Automatic registration times
Yes	• When the client is installed. • Whenever the connection server is changed during setup • Whenever the host name, IP address, or host ID is changed • Whenever the setup contents are registered • Whenever a connection is made to a higher system (if the host ID has not been registered in that higher system)
No	When connection is established with a higher system (if the host ID has not been registered in that higher system, or after the host ID has been changed)

(4) Notes on using host IDs

In a system in which multiple managing servers are configured in a hierarchy, if you wish to upgrade a JP1/Software Distribution Manager that does not support host IDs and then use host IDs, after you upgrade the higher JP1/Software Distribution Manager you must then upgrade the lower JP1/Software Distribution Managers.

6.1.4 Setting up the TCP/IP environment

Before you install JP1/Software Distribution, you must set up the TCP/IP environment. Two tasks are required:

- Defining the host names and IP addresses
- Defining the port numbers (`services` file)

If IP addresses are to be used as the node identification key, you do not need to define host names for relay systems and clients, however need to define host names for relay managers.

You can define port numbers in the `services` file before installation or during setup. If a port number is defined both in the `services` file and during setup, the definition in the `services` file takes precedence.

(1) Defining host names and IP addresses

You must first define the network's host names and IP addresses.

If host names are used as the node identification key, the host names defined in the user network are used in the windows of the managing server (System Configuration and Destination windows). If you have changed a host name in those windows, you must also change the host name in the user network

JP1/Software Distribution Manager uses TCP/IP host names to identify clients. Therefore, the computer in which JP1/Software Distribution Manager is to be installed must be able to determine an IP address from a host name.

Three methods are available for defining host names and IP address and for enabling the managing server to determine an IP address from the host name of a client:

- Using DHCP and WINS
- Using DNS
- Editing the `hosts` file

The following explains each of these methods.

(a) Using DHCP and WINS

Because DHCP dynamically determines the IP addresses of clients, it can reduce the effort required to assign IP addresses and the volume of maintenance work. However, a JP1/Software Distribution system cannot use a dynamically changing destination as the node identification key. Therefore, if DHCP is used, you must use host names as the node identification key.

If WINS is used to manage the host names of individual hosts, the host names need not be defined at each host (PC). When DHCP dynamically assigns a new IP address to a host that has been moved from one subnet to another subnet, the WINS database is updated automatically. Therefore, there is no need to change definitions manually.

Whenever a client PC is shut down, its information in WINS is released. As a result, the JP1/Software Distribution system will no longer be able to determine an IP address for the client from the host name and jobs may end in an error. For details about how to set up DHCP and WINS, see the Windows Help.

(b) Using DNS

You can use DNS if there are UNIX systems within the network or if hosts connected via the Internet are connection destinations. You can also use DNS if all the connection destination clients are Windows based, because Windows operating systems support DNS clients. If the host names to be managed by DNS are defined by JP1/Software Distribution, jobs such as *Remote installation beyond domains* can be executed.

For details about how to set up DNS, see the Windows help.

Note the following points about using DNS:

- To use DNS, you must use the TCP/IP protocol to set up the network software. Specify the name of the domain to which the computer belongs and the IP address of the server that manages that name.
- Set DNS so that bidirectional conversion is supported, such as from host name to IP address and vice versa.
- To use both a `hosts` file and DNS, do not specify the full domain name (a name consisting of the host name followed by a period and the domain name) of the host using a DNS for another host name in the `hosts` file.
- If a remote host connected directly to the network provider has been assigned a temporary name as its host name, JP1/Software Distribution will not be able to manage it.

(c) Editing the hosts file

If DHCP, WINS, or DNS is not used, you must define each connection-destination host name for each host. In the host where the managing server is running, you must define the host names and IP addresses of the connected relay managers/systems or clients. At each host where a client is running, you must also define the host name and IP address of the managing server.

You edit the following files in order to define host names and IP addresses:

For Windows NT:

Windows-directory`\system32\drivers\etc\hosts`

Format:

IP-address host-name alias

Example:

```
192.0.0.1 hostA NetworkA-hostA
192.0.0.2 hostB NetworkA-hostB
```

For Windows Me or Windows 98:

Windows-directory`\hosts`

Format:

Same as for Windows NT.

(2) Defining port numbers (services)

You can define a port number for each service. If there is no `services` file, the settings specified during setup take effect.

For the service name `netmdm`, set the TCP protocol using the same port number; for the service name `netmdmclt`, set the TCP protocol and the UDP protocol; for the service name `netmdmw`, set the TCP protocol. The recommended port numbers are 30000 for `netmdm`, 30002 for `netmdmclt`, and 30001 for `netmdmw`. Edit the following files:

For Windows NT:

Windows-directory`\system32\drivers\etc\services`

Format:

service-name port-number/protocol-name [*alias*]#

#: *alias* (enclosed in square brackets [ ]) is optional.

Example:

```
netmdm 30000/tcp
netmdmclt 30002/udp
netmdmclt 30002/tcp
netmdmw 30001/tcp
```

For Windows Me or Windows 98:

Windows-directory`\services`

Format:

Same as for Windows NT.

For details about other port numbers, see *B.1 Port numbers*.

(3) Using JP1/Software Distribution Client (client)

To use JP1/Software Distribution Client (client), note the following items:

Check TCP/IP

From the **Control Panel**, choose **Network**. On the **Configuration** page, check that **TCP/IP** is selected in **The following network components installed** option. If **TCP/IP** is not selected, choose the **Add** button in the **Configuration** page and add **TCP/IP**.

Next, from **Network**, select **TCP/IP** and choose the **Properties** button. When the TCP/IP Properties dialog box appears, ensure that the necessary network settings are present.

Setting the communication environment file

The `hosts` file and `services` file can be found under the Windows directory (**windows** is the default setting). In the `hosts` file, define the name of the higher host at the connection destination and its IP address. In the `services` file, define the same service name for the client and the managing server.

6.1.5 Using JP1/Software Distribution in a firewall environment

You can use JP1/Software Distribution in an environment that uses firewalls, without having to compromise security. For example, even if a distribution site contains a managing server within a firewall and departmental networks contain relay systems within firewalls, you can still distribute software from the managing server to the relay systems.

This section describes how to use JP1/Software Distribution in an environment that uses firewalls.

Note that if the firewall is already set up for HTTP and you are using Internet Options, the firewall settings described here are not required. However, even if you are using the Internet, the notes provided in *(5) Notes on use in a firewall environment* also apply. For details about Internet Options, see *E. Using Internet Options to Install JP1/Software Distribution* in the *Setup Guide*.

(1) Supported firewalls

JP1/Software Distribution supports the following types of firewalls:

- Packet filtering
- Application gateway

(a) Packet filtering firewall

A packet filtering firewall restricts the packages that are permitted to pass. Firewall-1 is one of the most popular firewall products of this type.

To use JP1/Software Distribution with a packet filtering firewall, you must set the IP address and port number of the node that has the firewall.

(b) Application gateway firewall

An application gateway firewall prohibits packages from passing and instead uses an application gateway to control access. Gauntlet is one of the most popular firewall products of this type.

Because a gateway controls access on the basis of the application, you must define JP1/Software Distribution to be an accessible application.

For example, in Gauntlet, you use the Virtual Private Network (VPN) facility to make JP1/Software Distribution an accessible application.

(2) About NAT

NAT is a facility for rendering intra-network addresses invisible to external networks. NAT also prevents intra-network addresses from being revealed to external networks.

There are two address translation policies:

- Fixed-address allocation
- Dynamic address allocation

JP1/Software Distribution supports only the fixed-address allocation policy (STATIC mode).

(3) Port numbers used in JP1/Software Distribution

When you use JP1/Software Distribution in a firewall environment, you must set port numbers in the firewall. The following table shows the port numbers used in JP1/Software Distribution.

Communication between:	Port number	Protocol	Sender information	Recipient information
Central manager and relay systems	30002 (Select udp or tcp#1)	udp	Central manager: Ephemeral	Relay system: 30002
			Relay system: Ephemeral	Central manager: 30002
		tcp	Central manager: Ephemeral	Relay system: 30002
			Relay system: 30002	Central manager: Ephemeral
	30000	tcp	Central manager: 30000	Relay system: Ephemeral
			Relay system: Ephemeral	Central manager: 30000
Relay system and clients	30002 (Select udp or tcp#1)	udp	Relay system: Ephemeral	Client: 30002
			Client: Ephemeral	Relay system: 30002
		tcp	Relay system: Ephemeral	Client: 30002
			Client: 30002	Relay system: Ephemeral
	30001	tcp	Relay system: 30001	Client: Ephemeral
			Client: Ephemeral	Relay system: 30001
Central manager and clients	30002 (Select udp or tcp#1)	udp	Central manager: Ephemeral	Client: 30002
			Client: Ephemeral	Central manager: 30002
		tcp	Central manager: Ephemeral	Client: 30002
			Client: 30002	Central manager: Ephemeral
	30000	tcp	Central manager: 30000	Client: Ephemeral
			Client: Ephemeral	Central manager: 30000
Server core facility and Remote Installation Manager#2	30001	tcp	Remote Installation Manager: Ephemeral	Server core facility: 30001
	30000	tcp	Remote Installation Manager: Ephemeral	Server core facility: 30000

Note: Idle ephemeral ports are allocated automatically by TCP/IP, normally within the port number range of 1024-5000.

#1: Select either udp or tcp, depending on the JP1/Software Distribution Manager settings.

#2: Applicable when the Server core facility and Remote Installation Manager are installed on separate PCs.

(4) Settings needed when Embedded RDB is being used

If you install the Server core facility and Remote Installation Manager on separate PCs when you are using Embedded RDB, the ports listed in the following table are used to perform communications between these two components.

Table 6–2: Port numbers used for communication between the Server core facility and Remote Installation Manager (when Embedded RDB is being used)

Communication between:	Port number	Protocol	Sender information	Recipient information
Server core facility and Remote Installation Manager	30000	tcp	Remote Installation Manager: Ephemeral	Server core facility: 30000
	30001	tcp	Remote Installation Manager: Ephemeral	Server core facility: 30001
	30008	tcp	Remote Installation Manager: Ephemeral	Server core facility: 30008

Communication between:	Port number	Protocol	Sender information	Recipient information
Server core facility and Remote Installation Manager	Ephemeral (client connection to database)	tcp	Remote Installation Manager: Ephemeral	Server core facility: Ephemeral
		tcp	Server core facility: Ephemeral	Remote Installation Manager: Ephemeral

Note: Idle ephemeral ports are allocated automatically by TCP/IP, normally within the port number range of 1024 to 5000.

In an environment with a firewall, you must open a port through the firewall from the client side. It is not necessary to open a port on the originating side. The following subsections explain how to open a port through a firewall.

(a) When there is a firewall on the PC containing the Server core facility

If the PC on which the Server core facility is installed contains a firewall, the following ports must be able to pass through the firewall:

- Communications port between the Server core facility and Remote Installation Manager
  30000 and 30001.
- Port for database connection
  This is the port number set on the **Database Environment** page during setup. The default is `30008`.
- Port for connecting a database client
  The default is that the OS assigns this port number automatically. Therefore, you must specify the settings needed to allow passage through the firewall after the port number has been assigned.
  The following shows how to fix the port number for connecting a database client:
  1. On **Control Panel**, choose **Administrative Tools**, then **Services**, and then stop the **Remote Install Server** service.
  2. Stop the database by executing the `netmdb_stop.bat` command stored in the JP1/Software Distribution Manager installation directory `\BIN`.
     When the `netmdb_stop.bat` command finishes, the system waits for an entry from the keyboard. To complete the command without requiring such a keyboard entry, execute the command by specifying `/nopause` in the options.
  3. Use a text editor to open the `pdsys` file that is stored in the JP1/Software Distribution installation directory `\NETMDB\conf`.
  4. Delete `#` at the beginning of `#set pd_service_port = 30009`.
     `30009` is the default port number.
     To change the port number, change the value `30009`.
  5. Start the database by executing `netmdb_start.bat` stored in the JP1/Software Distribution Manager installation directory `\BIN`.
     When the `netmdb_stop.bat` command finishes, the system waits for an entry from the keyboard. To complete the command without requiring such a keyboard entry, execute the command by specifying `/nopause` in the options.
  6. On **Control Panel**, choose **Administrative Tools**, then **Services**, and then start the **Remote Install Server** service.

  The following table lists the port number used by JP1/Software Distribution once you have completed this setup:

Communication between:	Port number	Protocol	Sender information	Recipient information
Server core facility and Remote Installation Manager	Ephemeral (client connection to database)	tcp	Remote Installation Manager: Ephemeral	Server core facility: 30009#

#: Assumes the port number is set to 30009 (default).

(b) When there is a firewall on the PC containing the Remote Installation Manager

If the PC on which Remote Installation Manager is installed contains a firewall, the receive ports used for database clients must be able to pass through the firewall.

The default is that the OS automatically assigns port numbers to receive ports for database clients. Note that more than 10 receive ports are used. Therefore, you must fix the range of port numbers to be used for receive ports and set up passage for them through the firewall.

To fix the range of port numbers to be used for receive ports:

1. Terminate Remote Installation Manager and other JP1/Software Distribution applications.
2. Use a text editor to open `HiRDB.ini`, which is stored in the JP1/Software Distribution Manager installation directory `\NETMDBCLT`.
   If the Server core facility has also been installed, `HiRDB.ini` is stored in *installation-directory*`\NETMDB\CONF\emb`.
3. In `PDCLTRCVPORT=`, specify the range of port numbers to be used.
   Following `PDCLTRCVPORT=`, specify the range of port numbers to be used in the format *port-number−port-number*.
   For example, to specify the range 10000 to 10500 as the port numbers to be used:
   `PDCLTRCVPORT=10000-10500`
   If you specify nothing or `0` following `PDCLTRCVPORT=`, no range of port numbers to be used will be set. The default is that no range of port numbers to be used is set.
4. Start Remote Installation Manager and other JP1/Software Distribution applications.

The following table lists the port numbers used by JP1/Software Distribution once you have completed this setup:

Communication between:	Port number	Protocol	Sender information	Recipient information
Server core facility and Remote Installation Manager	Ephemeral (client connection to database)	tcp	Server core facility: Ephemeral	Remote Installation Manager: 10000 to 10500#

#: Assumes the port number range is set to between 10000 and 10500.

Note the following points when fixing the port numbers for database clients:

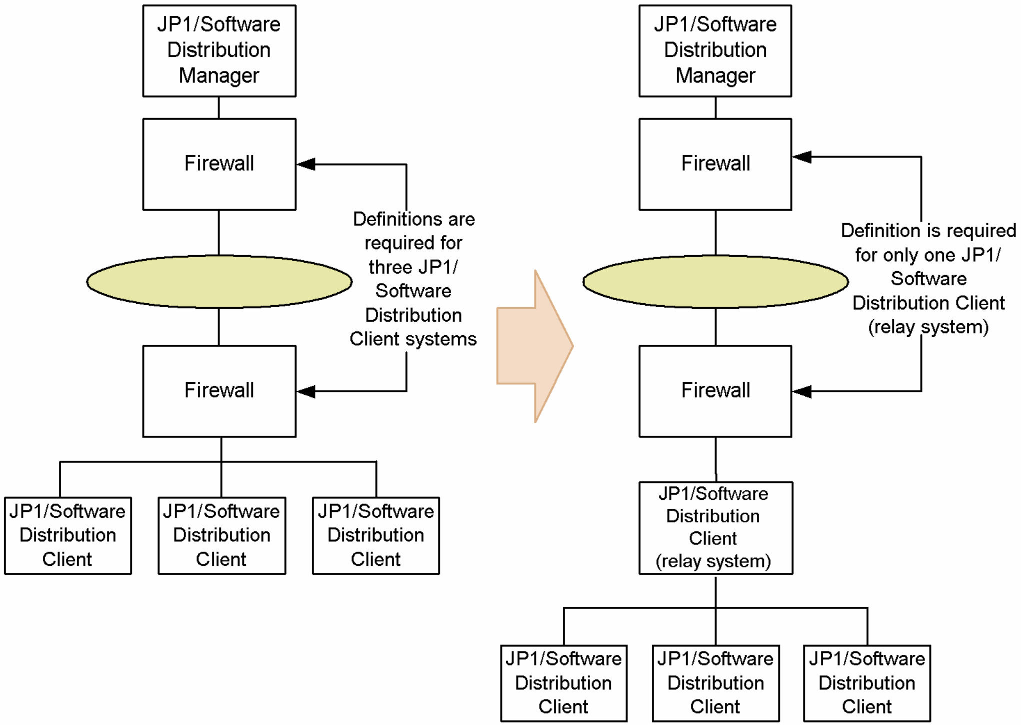
- If there are no available port numbers in the specified range, an error results.
  If the specified range includes a port number that is used by a program other than a database client, contention may occur on assignment of port numbers. Specify an appropriate range of port numbers so that no shortage of ports occurs.
- Make sure that the range of port numbers you specify does not overlap the range of port numbers assigned automatically by the OS. The range of port numbers assigned by the OS varies from one OS to another.
- Provide about 20% extra port numbers from the number of ports actually required. If there is no leeway, efficiency is adversely affected due to searches for available port numbers.
- Ports available to programs that are not database clients are not available to database clients. Similarly, ports available to database clients are not available to programs that are not database clients.
  A program that requires a specified range of port numbers may not be able to start if any of its port numbers is included in your specified range.
- You must manage programs within the firewall so that the port numbers set for the database clients to pass through the firewall will not be used illegally by other programs.

(5) Notes on use in a firewall environment

Note the following points about using JP1/Software Distribution in a firewall environment:

- You can define fewer nodes in a firewall by placing relay systems within the firewall:

Figure 6–2: Example of a configuration in which relay systems are within a firewall


JP1/Software Distribution Manager
Firewall
Definitions are required for three JP1/ Software Distribution Client systems
Firewall
JP1/Software Distribution Client
JP1/Software Distribution Client
JP1/Software Distribution Client
JP1/Software Distribution Manager
Firewall
Definition is required for only one JP1/ Software Distribution Client (relay system)
Firewall
JP1/Software Distribution Client (relay system)
JP1/Software Distribution Client
JP1/Software Distribution Client
JP1/Software Distribution Client

- JP1/Software Distribution uses the host name, IP address, or host identifier as an *ID key for operations* (key for identifying a node). JP1/Software Distribution assigns a created job to an ID key for operations. If you use the NAT facility, addresses are translated and jobs cannot be assigned to the target clients. This is because NAT changes the IP address of JP1/Software Distribution Client (client), so the actual IP address differs from that recognized by JP1/Software Distribution Manager. Therefore, you cannot use the IP address as an ID key for operations in an environment that uses the NAT facility.
- JP1/Software Distribution's facility for automatically registering the system configuration assigns IP addresses to protocols regardless of the ID key for operations. The IP addresses assigned to protocols may be revealed. In a firewall environment, we recommend that you not use the facility for automatically registering the system configuration.
- For operations based on IP addresses, the IP addresses are assigned to protocols. However, IP addresses assigned to protocols may be revealed, so we recommend that, in a firewall environment, you not use JP1/Software Distribution based on IP addresses.

6.1.6 Using JP1/Software Distribution in a multiple LAN connections environment

You can use JP1/Software Distribution in an environment that has *multiple LAN connections.* A PC in such an environment has multiple network adapters, such as NICs.

JP1/Software Distribution supports the following two types of environments that have multiple LAN connections:

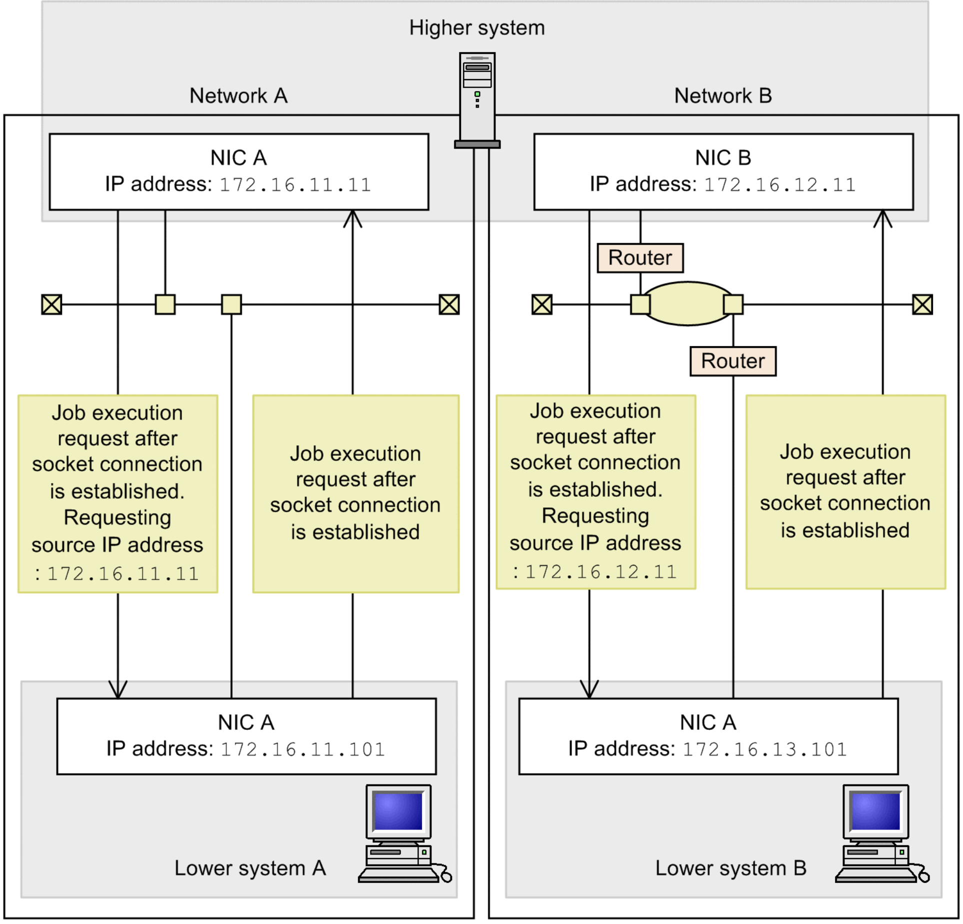
- Environments separated into multiple networks
- Environments with duplex networks (that is, networks in a redundant configuration)

This section describes how to use JP1/Software Distribution in each of these environments.

(1) Multi-network environments

The following shows an example of an environment separated into multiple networks.

Figure 6–3: Example of an environment separated into multiple networks


Higher system
Network A
Network B
NIC A
IP address: 172.16.11.11
NIC B
IP address: 172.16.12.11
Router
Router
Job execution request after socket connection is established. Requesting source IP address :172.16.11.11
Job execution request after socket connection is established
Job execution request after socket connection is established. Requesting source IP address :172.16.12.11
Job execution request after socket connection is established
NIC A
IP address: 172.16.11.101
NIC A
IP address: 172.16.13.101
Lower system A
Lower system B

In a network separated into multiple networks, each job execution request includes the IP address of the requesting higher system. Therefore, requests to receive a job can be sent by the client to the correct destination.

When a higher system requests job execution

The IP address of the local system that has successfully established a socket connection with a lower system is acquired and communicated as the requesting-source IP address to the lower system.

When a lower system requests to receive a job

A request to receive a job is issued by establishing a socket connection for the requesting-source IP address that was communicated when a higher system requested job execution.

However, to use JP1/Software Distribution in such an environment, connections must be established using the TCP protocol. Specify the following:

Higher system

When you set up JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system), select the **TCP Protocol** radio button on the **Communication** page.

For details about the **Communication** page, see *4.2.2 Communication page* in the *Setup Guide* for JP1/Software Distribution Manager, and see *5.2.2 Communication page* in the *Setup Guide* for JP1/Software Distribution Client (relay system).

Lower system

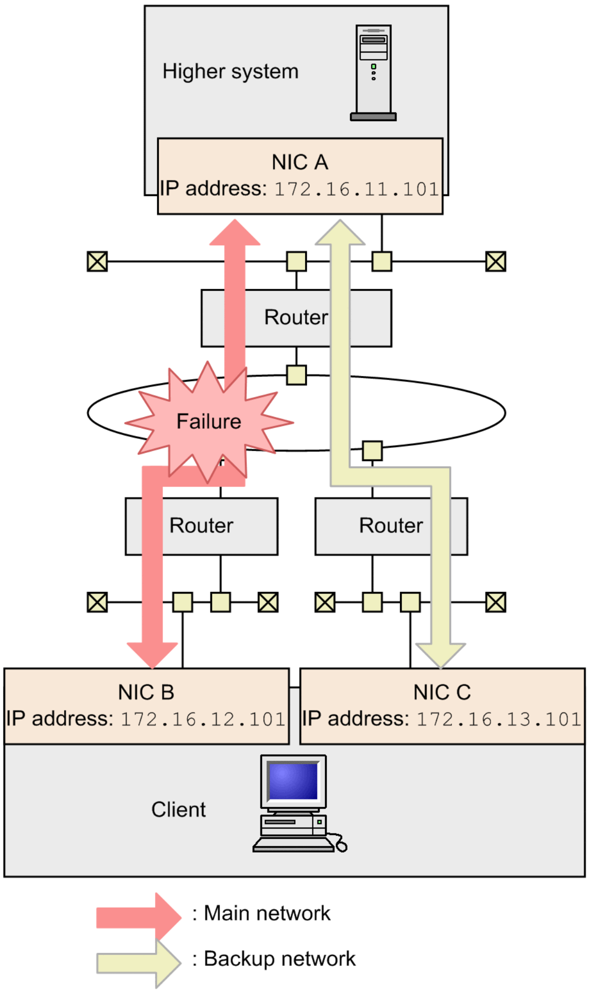
When you set up JP1/Software Distribution Client (client), select the **TCP Protocol** check box and the **Connect to the upper-level system by using the IP address received via the startup request protocol** check box on the **Communication** page.

For details about the **Communication** page, see *6.2.6 Communication page* in the *Setup Guide*.

(2) Duplex networks

The following shows an example of an environment with duplex networks (that is networks, set up in a redundant configuration).

Figure 6–4: Example of an environment with duplex networks



In an environment with duplex networks, when a failure occurs in the main network, for example, operation switches to the backup network. However, the communication lines used by JP1/Software Distribution may be limited to the main network.

To enable JP1/Software Distribution to be used in such an environment, you must set priority orders for the network adapters when you set up clients on PCs. When you set up JP1/Software Distribution, open the **Communication** page and select **Specify multiple network adapters**. For details about the setup method, see *5.2.1 Connection Destination page* in the *Setup Guide*.

6.1.7 Preventing network overload

When you deploy JP1/Software Distribution, the software to be installed and various types of management information are transmitted via the network. To ensure efficient operation, you should minimize the load on the network by running jobs during low-usage periods. JP1/Software Distribution provides several facilities for reducing the network load. These include adjusting network traffic during setup and distributing software to be installed in segments. This section explains how to minimize the network load and distribute software efficiently. In order to distribute software efficiently in JP1/Software Distribution, the settings and operations on the client machines must also be considered. For user tasks at the client, see *11. Using Client Facilities* in the manual *Administrator's Guide Volume 1*.

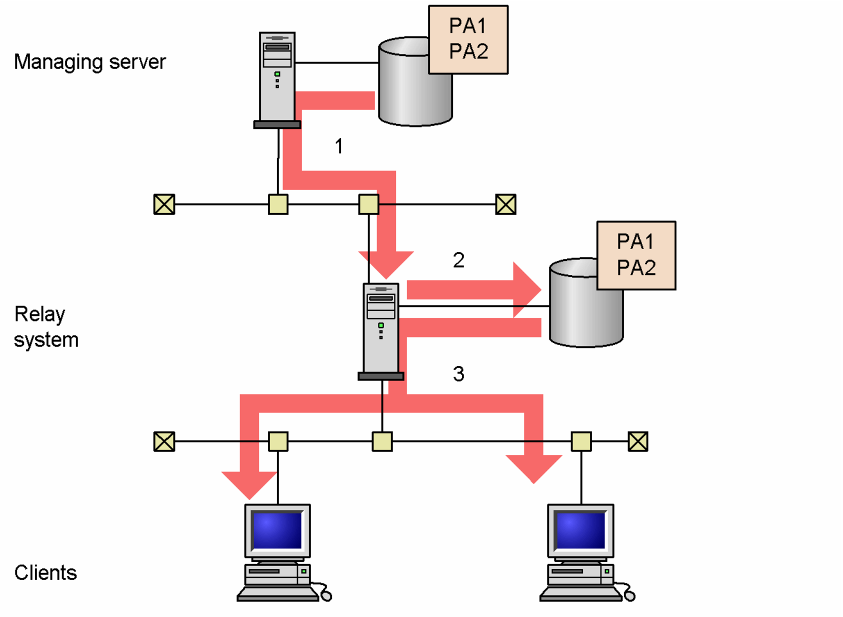
(1) Using a relay system

To transfer packages efficiently during remote installation, you must understand the role of relay systems.

A relay system not only reduces the number of clients connected directly to the managing server but also efficiently transfers a package to the clients under the relay system by creating and saving a copy of the package. Also, by combining a *Transfer package to relay system* job with an *Install package* job, a package can be transferred in separate stages, first to the relay system and then beyond the relay system.

The following figure shows the operation of a relay system during remote installation.

Figure 6–5: Operation of a relay system during remote installation



1: Executes remote installation of packages PA1 and PA2.
2: Creates and saves a copy of packages PA1 and PA2 to the relay system.
3: Installs at the clients the packages saved in the relay system.

A *Transfer package to relay system* job is stored in the relay system. While the job is stored in the relay system, the managing server does not redistribute the same package. During packaging, you can specify the storage period.

(2) Adjusting the maximum number of hosts that can be connected concurrently

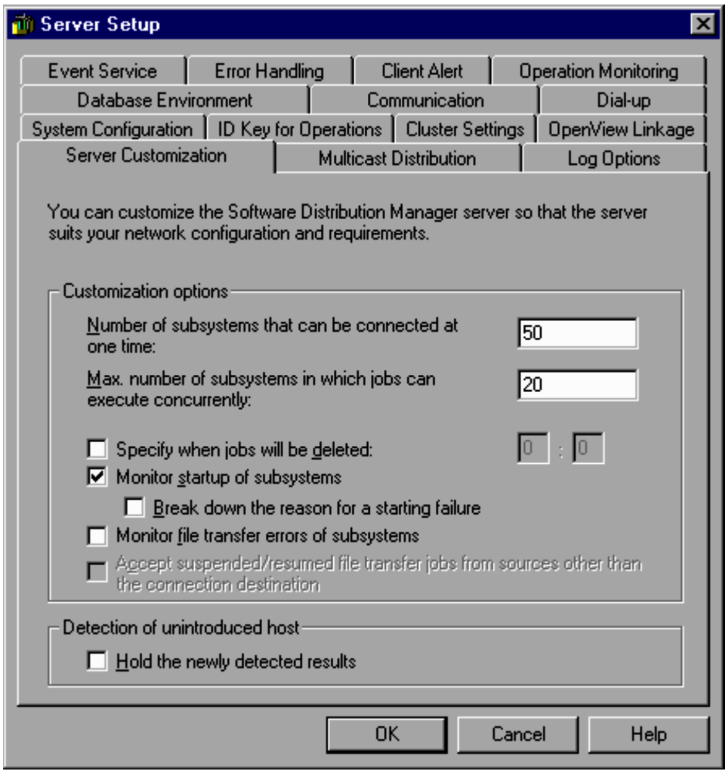
If the number of leased lines is limited, or if the network rejects access, it may be advisable to adjust the number of hosts that can be connected concurrently. The managing server provides the following methods to adjust the number of hosts that can be connected concurrently:

- Adjusting by modifying setup information
- Adjusting by user operations during job execution

(a) Adjusting the max. number by modifying setup information

The managing server can use setup information to control the network traffic. From the menu, choose **Setup** to open the setup window, and then display the **Server Customization** page (for a relay system, use the **Relay System Customization** page):

Figure 6–6: Server Customization page



Server Setup

You can customize the Software Distribution Manager server so that the server suits your network configuration and requirements.

Customization options

Number of subsystems that can be connected at one time: 50

Max. number of subsystems in which jobs can execute concurrently: 20

□ Specify when jobs will be deleted: 0 : 0

☑ Monitor startup of subsystems

□ Break down the reason for a starting failure

□ Monitor file transfer errors of subsystems

□ Accept suspended/resumed file transfer jobs from sources other than the connection destination

Detection of unintroduced host

□ Hold the newly detected results

The option for adjusting the number of hosts that can be connected concurrently is **Max. number of subsystems in which jobs can execute concurrently** (for a relay system, it is **Max. number of relays or clients in which jobs can execute concurrently**).

If a managing server executes jobs for a large number of clients at the same time, the load on the network may become extremely heavy. Therefore, specifying **Max. number of subsystems in which jobs can execute concurrently** can limit the number of lower hosts that can be processed concurrently. For example, if a maximum of 20 is set, a job that remote-installs software in 300 clients concurrently is executed in 15 batches of 20 clients each.

(b) Adjusting the max. number by user operations

During setup, you can specify values that take into account PC performance, network configuration, and operating environment. This provides sufficient reliability in most cases. However, when large amounts of data are transmitted, the network load might increase even if you specify settings to control the traffic during setup. Therefore, it may still be necessary for users to make adjustments.

■ Adjusting the number of target clients for a job

Suppose that a 5-MB package is to be transmitted over a 64-Kbps line. If the line efficiency is 60%, transmission will take some 18 minutes. The package will flow in parallel between the managing server and the relay systems and between the relay systems and the clients. Determine the number of target clients for a single job by considering the load in the connection lines, the speed of the connection lines, and the line efficiency.

■ Adjusting the number of relay systems to be concurrently connected

To avoid concurrently connecting a large number of relay systems to the managing server, we recommend split job execution. Although this method places some burden on the user, it can reliably reduce the network load.

First, by considering the network traffic, determine the number of relay systems to be connected concurrently to the managing server. Next, for each relay system that will be concurrently connected, classify all clients under each relay system as a single group. When you execute the job, leave an interval between job execution times for the different groups. In this way, you can avoid having a large number of relay systems connected concurrently to the managing server.

(3) Scheduled distribution

When you create a remote installation job, you can specify the job execution time. This is the package transmission time. By specifying a late-night hour, when traffic on the network is relatively light, data can be transmitted more efficiently.

If you use separate jobs to execute package transmission from the managing server to the relay systems and from the relay systems to the clients, you can specify different execution times for these jobs.

You can reduce network load by carefully scheduling transmissions rather than reducing the volume of data to be transmitted.

Note that software distribution is not executed if a destination PC is in the power-save mode, because its JP1/Software Distribution Client (client) is not active in that mode. If destination PCs have the power-save mode, exercise care when scheduling jobs.

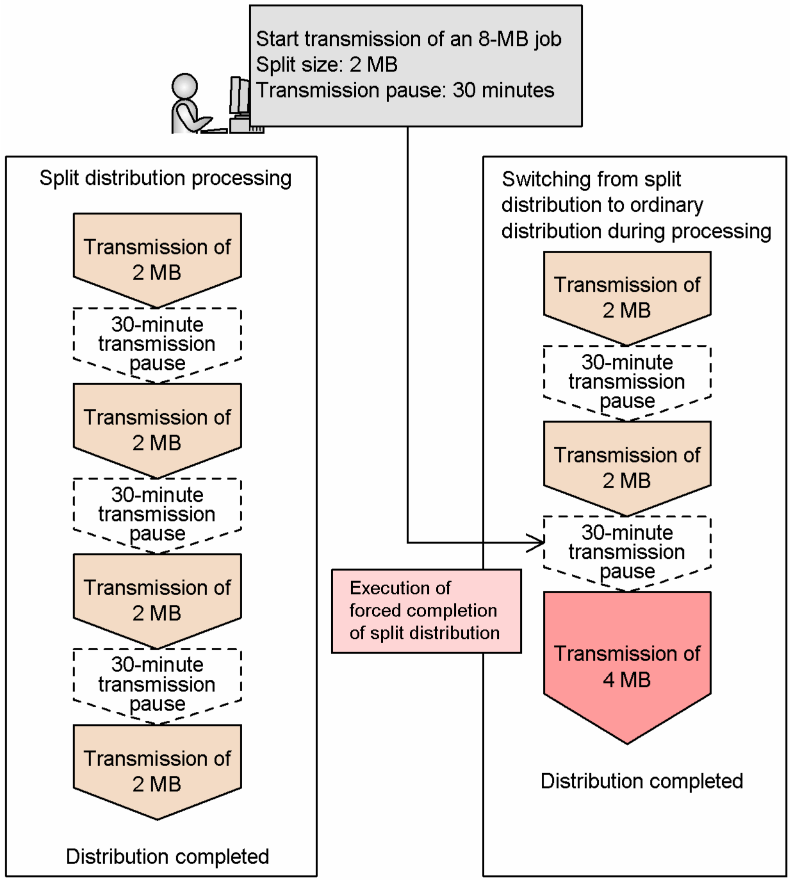
(4) Split package distribution

Software to be installed in a client can be distributed in a single batch or in multiple segments. The latter is called *split distribution*. Split distribution offers the following benefits:

- Network load can be reduced when a large package is distributed.
- Intervals (transmission pauses) can be inserted between the split packages.
- If there are relay managers/systems (relay managers or relay systems) in the distribution route, the package split size and transmission interval can be modified.
- Distribution can be completed during split distribution by transmitting any unsent packages in a batch by means of forced completion of split distribution (ordinary distribution).

The following figure shows software distribution using split package distribution.

Figure 6–7: Software distribution using split package distribution


Start transmission of an 8-MB job
Split size: 2 MB
Transmission pause: 30 minutes
Split distribution processing
Transmission of 2 MB
30-minute transmission pause
Transmission of 2 MB
30-minute transmission pause
Transmission of 2 MB
30-minute transmission pause
Transmission of 2 MB
Distribution completed
Switching from split distribution to ordinary distribution during processing
Transmission of 2 MB
30-minute transmission pause
Transmission of 2 MB
30-minute transmission pause
Execution of forced completion of split distribution
Transmission of 4 MB
Distribution completed

(5) Job multicast distribution

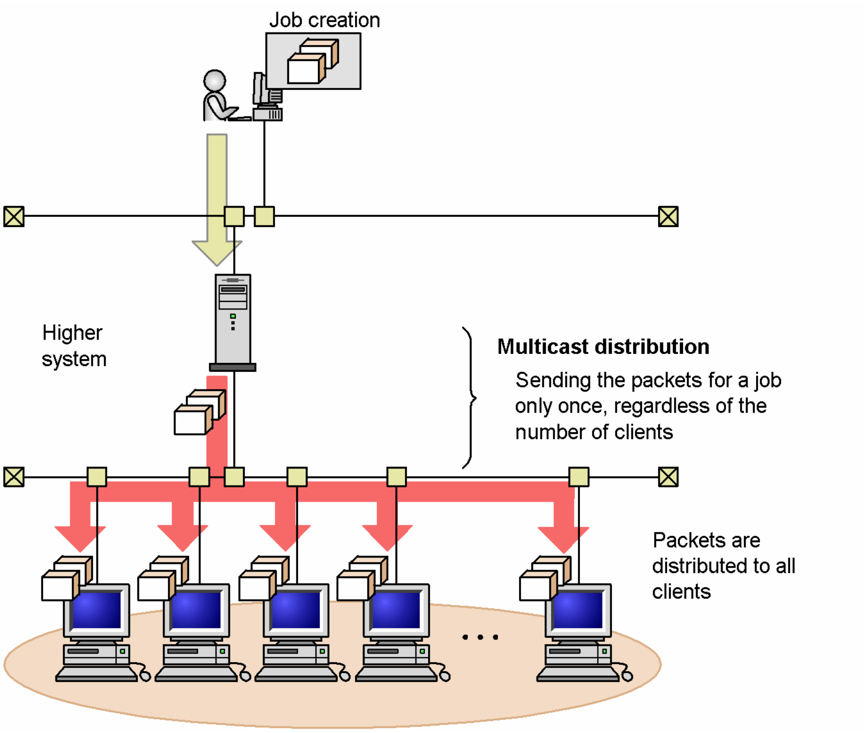
In normal job distribution, the number of packets sent from the higher system increases as the number of clients increases. JP1/Software Distribution supports a distribution method in which the higher system sends the packets for a job only once for distribution to the specified number of clients, reducing the transfer load. This is called *multicast distribution*.

When you specify multicast distribution for distributing software, you reduce the number of packet sends, thus reducing the time required for distribution and reducing the load on the network. Multicast distribution is effective in the following cases:

- Simultaneously distributing software to many clients
- Distributing large software items

The figure below shows software distribution using multicast distribution. You can use multicast distribution only between clients and the higher system to which they are connected.

Figure 6–8: Software distribution by multicast distribution


Job creation
Higher system
Multicast distribution
Sending the packets for a job only once, regardless of the number of clients
Packets are distributed to all clients
...

For details about the system configuration and setup required for multicast distribution, see *6.2 Settings for multicast distribution*.

(6) Suspending and resuming a job

You can suspend job execution temporarily at a host where package transmission or remote installation is underway. For example, if a job is to be executed while a specified application is not running, but the job is not completed when the application must start, you can suspend the job and restart it after the application has terminated.

You can also distribute one job while suspending distribution of another. For example, if it is important to distribute a virus definition file in a hurry, you can suspend the current distribution job and distribute the virus definition file first.

(a) Mechanism of job suspension and resumption

There are three methods for suspending and resuming a job:

- Sending a suspension or resumption instruction from the managing server to the relay manager/system
- Issuing a suspension or resumption instruction to the managing server itself

- Executing the `dcmsusp` command from the managing server

For details about the `dcmsusp` command, see *4.23 dcmsusp.exe (suspending and resuming a file transfer)* in the manual *Administrator's Guide Volume 2*.

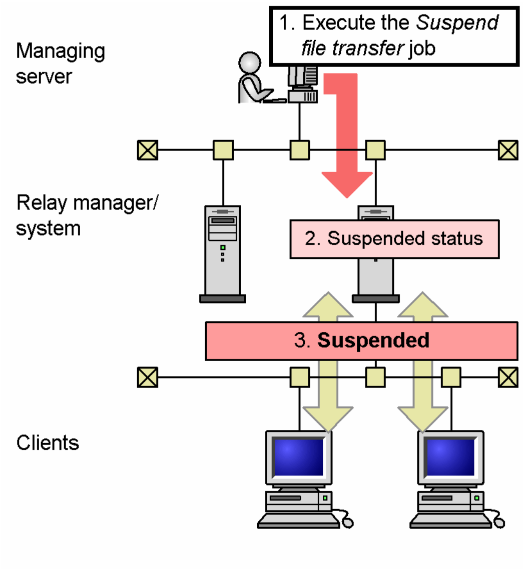
The unit of file transmission that can be suspended is the value of **File transfer buffer size** that was specified during setup of the lower system.

Sending a suspension or resumption instruction from the managing server to the relay manager/system

To instruct suspension or resumption, execute a *Suspend file transfer* job or *Resume file transfer* job from the managing server. For the destination of such a job, specify the higher system directly connected to the hosts where the job is to be suspended or resumed.

The following figure shows the system operation during execution of a *Suspend file transfer* job.

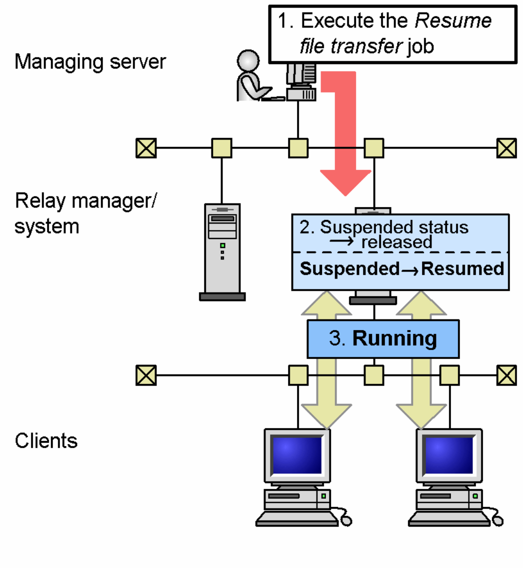
Figure 6–9: System operation during execution of a Suspend file transfer job



1. Execute a *Suspend file transfer* job from the managing server to the relay manager/system.
2. The relay manager/system at the destination of the *Suspend file transfer* job is placed in suspended status.
3. File transmission is suspended between the relay manager/system in suspended status and the systems immediately below it, and the status of the job for the lower systems changes to **Suspended**.

The following figure shows the system operation during execution of a *Resume file transfer* file.

Figure 6–10: System operation during execution of a Resume file transfer job


Managing server
1. Execute the *Resume file transfer* job
Relay manager/ system
2. Suspended status → released
Suspended→Resumed
3. Running
Clients

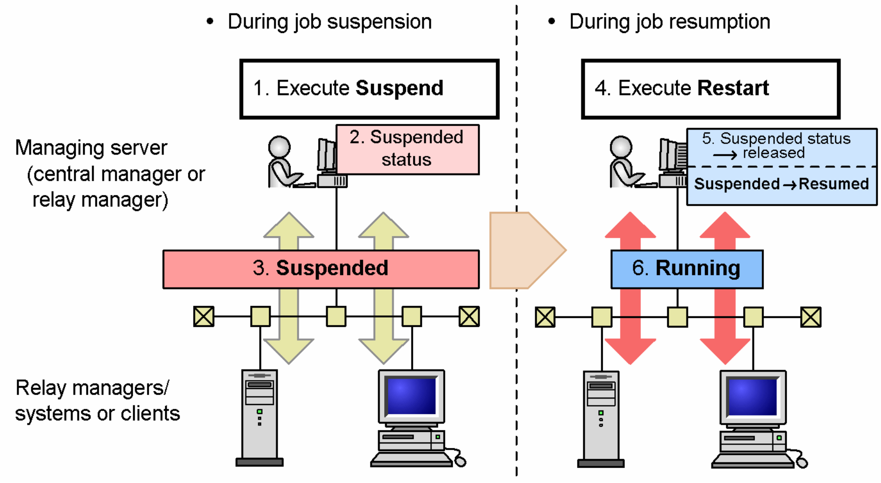
1. Execute a *Resume file transfer* job from the managing server to the relay manager/system that is in suspended status.
2. The suspended status is released at the relay manager/system at the destination of the *Resume file transfer* job, and the status of the job for the lower systems changes to **Resumed**.
3. The suspended file transmission is resumed, and the job status returns to **Running**.

Issuing a suspension or resumption instruction to the managing server itself

You can use the Remote Installation Manager to issue a suspension or resumption instruction to the local system. To do this, from the **Execute** menu, choose **Suspend/Resume File Transfer**, and then **Suspend** or **Resume**.

The following figure shows the system operation during job suspension or resumption at the local system.

Figure 6–11: System operation during job suspension or resumption at the local system



1. From the menu of the Remote Installation Manager, choose **Suspend**.
2. The local system is placed in suspended status.
3. File transfer between the local system and the systems immediately below it is suspended, and the status of the job for the lower systems changes to **Suspended**.
4. From the menu of the Remote Installation Manager, choose **Resume**.

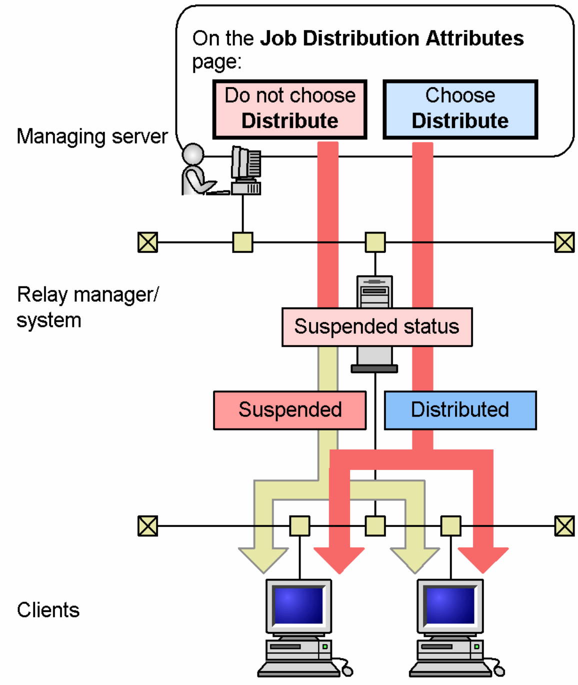
5. The local system is released from suspended status, and the status of the job for the lower systems changes to **Resumed**.
6. The suspended file transfer is resumed, and the status of the job changes to **Running**.

(b) Distributing a job to a suspended destination

You can distribute a job without suspending file transfer even when the system immediately above the destination system is in suspended status. To do this, during job creation, open the Create Job dialog box, choose the **Job Distribution Attributes** tab, and then **Distribute**.

The following figure shows distribution of a job to a suspended destination.

Figure 6–12: Distributing a job to a suspended destination



When a job is suspended, file transfer to destination systems will be suspended while the system immediately above them is in suspended status. However, if you select the **Distribute** option for a job, file transfer will not be suspended.

(c) Scope of job suspension and resumption

The following shows the scope of job suspension and resumption:

- You can suspend the following three types of jobs:
  - *Install package* jobs
  - *Transfer package to relay system* jobs
  - *Send package, allow client to choose* jobs
- The scope of job suspension is from a higher system placed in suspended status to the following systems immediately below it:
  - JP1/Software Distribution 07-00 or later for Windows
  - JP1/Software Distribution 07-00 or later for UNIX

  If there is a client in the same PC as a higher system that is placed in suspended status, the job to that client is also suspended.
- If there is a lower system with a version earlier than 07-00 immediately below the higher system that is placed in suspended status, the job will not be suspended for the lower system with the older version.
- You must use JP1/Software Distribution Manager to create a *Suspend file transfer* or *Resume file transfer* job.

- *Suspend file transfer* and *Resume file transfer* jobs are applicable to the following destinations:
  - JP1/Software Distribution Manager (relay manager) 07-00 or later for Windows
  - JP1/Software Distribution Client (relay system) 08-00 or later and JP1/Software Distribution SubManager 07-00 or later for Windows
  - JP1/Software Distribution Client (relay system) 07-00 or later for UNIX
- To issue a suspension and resumption instruction to the managing server itself, you can use the Remote Installation Manager with JP1/Software Distribution Manager 07-00 or later for Windows.
- To distribute a job even in the **Suspended** status, the managing server, relay managers/systems, and clients must all be JP1/Software Distribution 07-00 or later. The **Distribute** option is also supported by JP1/Software Distribution SubManager 07-00 or later for UNIX and JP1/Software Distribution Client 07-00 or later for UNIX.

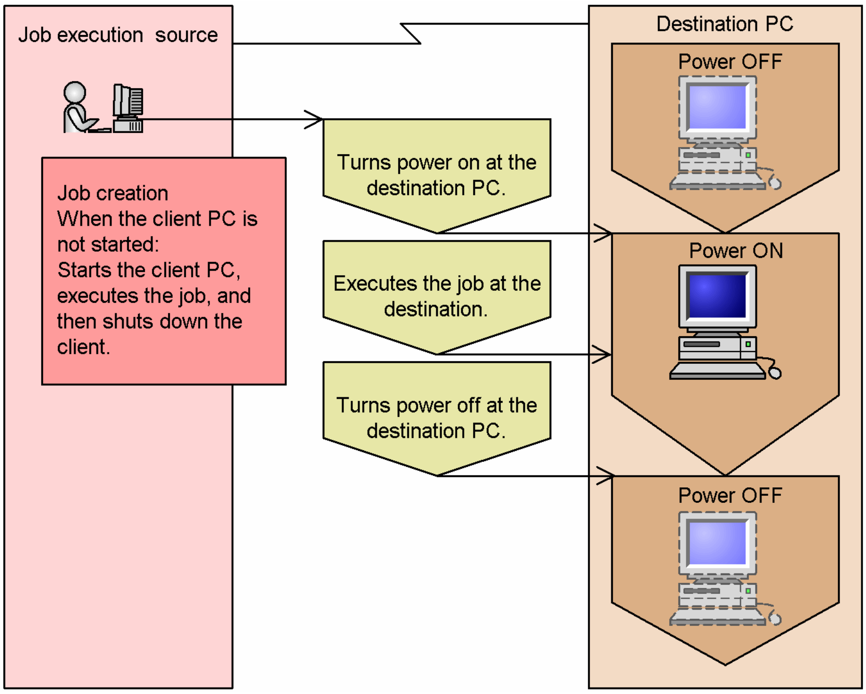
(7) Using client control

JP1/Software Distribution provides a facility that enables remote PCs connected via a network to be started and shut down from the local PC. This facility is called *client control*. JP1/Software Distribution can use this facility to turn on remote PCs and install software in them at night or on a weekend.

To use this facility, the PC must support either AMT or Wake on LAN, and must also support automatic shutdown.

The following figure shows an overview of software remote installation using client control.

Figure 6–13: Remote installation using client control


Job execution source
Destination PC
Power OFF
Turns power on at the destination PC.
Job creation
When the client PC is not started:
Starts the client PC, executes the job, and then shuts down the client.
Power ON
Executes the job at the destination.
Turns power off at the destination PC.
Power OFF

For notes on remote installation using client control, see *6.3 Settings for using the client control facility*.

(8) Using offline installation

You do not need to use a network to install software on a stand-alone PC (offline machine) on which JP1/Software Distribution Client is installed; this is called offline installation.

Offline installation is useful in the following cases:

- When you want to install a package on a PC that is not on a network
- When package transmission will take a long time, perhaps because the line speed of the connected network is slow or the package is large

Offline installation involves storing the files needed for installation on storage media at the managing server and then transporting that media to the offline machine for installation. To use offline installation at the managing server and an offline machine, the following conditions must be met:

Managing server:

- Windows JP1/Software Distribution Manager 07-50 or later (relational database version) has been installed.
- Remote Installation Manager is used on the same PC that runs the above JP1/Software Distribution Manager.

Offline machine:

Windows JP1/Software Distribution Client 07-50 or later has been installed.

For details about the offline installation method, see *7.7.1 Offline installation* in the manual *Administrator's Guide Volume 1*.

6.2 Settings for multicast distribution

If you use *multicast distribution* for job distribution, you can reduce substantially the amount of data that is transferred, reducing the network load and speeding up distribution.

This section provides an overview of multicast distribution and describes how to configure a system to use multicast distribution. It also describes use of multicast distribution and provides notes on its use.

6.2.1 Unicast distribution and multicast distribution

JP1/Software Distribution uses two methods of job distribution, *unicast distribution* and *multicast distribution*. You can specify the distribution method independently for each job.

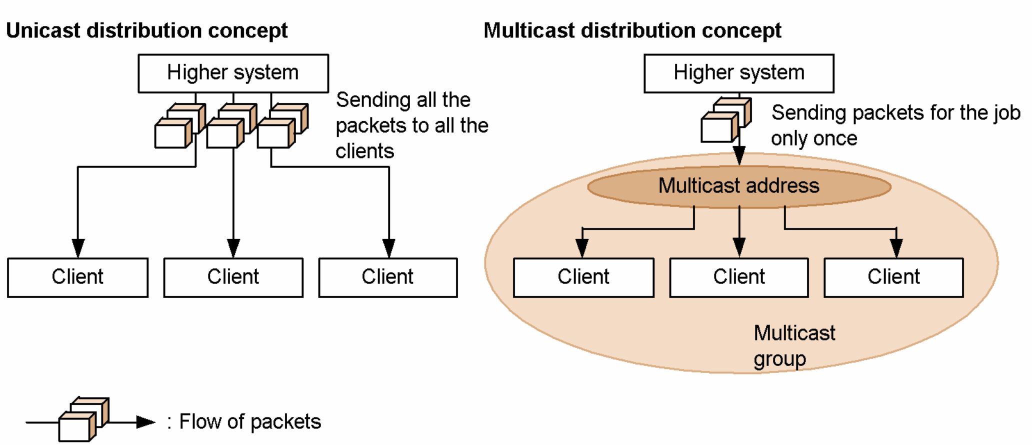
The standard method of sending the packets for a job one-on-one from a higher system to a client is what is called *unicast distribution*. In unicast distribution, the higher system sends individual packets to each destination client. As a result, the number of packets sent increases directly with the number of clients.

In *multicast distribution*, the IP multicast protocol is used to send the packets to specified multiple clients. In multicast distribution, the higher system sends the packets to a conceptual group known as a *multicast group*. The packets are then distributed to each client in that group. Regardless of the number of clients, the higher system has to send the packets only to the multicast group, greatly reducing traffic on the network.

Each multicast group has a unique IP address, known as its *multicast address*, to which the packets are sent. You can specify a multicast address when you set up a client, and the client is thus registered in that multicast group. Packets sent to a multicast address are distributed to all clients registered in that multicast group. Because only one packet is transferred along common routes, jobs can be distributed efficiently without overloading the network.

The following figure illustrates the unicast and multicast distribution concepts.

Figure 6–14: Unicast and multicast distribution concepts


Unicast distribution concept
Higher system
Sending all the packets to all the clients
Client
Client
Client
Multicast distribution concept
Higher system
Sending packets for the job only once
Multicast address
Client
Client
Client
Multicast group
: Flow of packets

(1) Jobs distributed using multicast distribution

JP1/Software Distribution allows only *Install package* jobs to be distributed by means of multicast distribution. You can reduce the communications volume by using multicast distribution for the following types of jobs:

- Jobs that have many destinations
- Jobs requiring distribution of large packages

If a job is to be sent to only a few destinations, or if the package is small, using multicast distribution can actually reduce efficiency. For such jobs, specify unicast distribution when you create the job.

Note that selection of multicast or unicast distribution when you create a job specifies only the method of job distribution. It does not specify the actual destinations of the job. Regardless of whether the job destination is an individual host, a host group, or an ID group, the job is distributed using multicast distribution to the specified destinations. If there is a client in the specified destinations that is not registered in the multicast group, the job is distributed to that client only using the standard unicast method.

(2) Routes used in multicast distribution

When you specify multicast distribution for jobs in JP1/Software Distribution, the packets are sent using multicast distribution only between a higher system and its directly connected clients. Unicast distribution is used between the system that executes the job and the higher system to which the clients are directly connected.

6.2.2 Network environment and JP1/Software Distribution system version required for multicast distribution

This section explains the network environment and the version of the JP1/Software Distribution system required in order to use multicast distribution of jobs.

(1) Network environment

The following network environment is assumed for multicast distribution of jobs:

- If a router is to be installed between the higher system to which the clients are connected and the clients, that router must be compatible with IP multicasting and it must be set up for IP multicasting. If a router installed on the route is not compatible with IP multicasting, jobs will be distributed using unicast distribution on the segment from the router to the clients.

(2) JP1/Software Distribution system version

To use multicast distribution, the version of the JP1/Software Distribution system must satisfy the following conditions:

- The managing server in which the job is created, the higher system to which the clients are connected, and the clients must all be running the Windows version of JP1/Software Distribution 06-71 or later.
- If there are multiple levels of relay managers/systems (relay managers or relay systems), a relay manager/system above the higher system to which the clients are connected must be one of the following products:
  - Windows version of JP1/Software Distribution Manager and JP1/Software Distribution SubManager 06-71 or later or JP1/Software Distribution Client (relay system) 08-00 or later (version supporting multicast distribution)
  - Windows version of JP1/Software Distribution SubManager 06-00 to 06-53 (versions not supporting multicast distribution)
  - UNIX version of JP1/Software Distribution SubManager or the UNIX version of JP1/Software Distribution Client (relay system) 09-00 or later

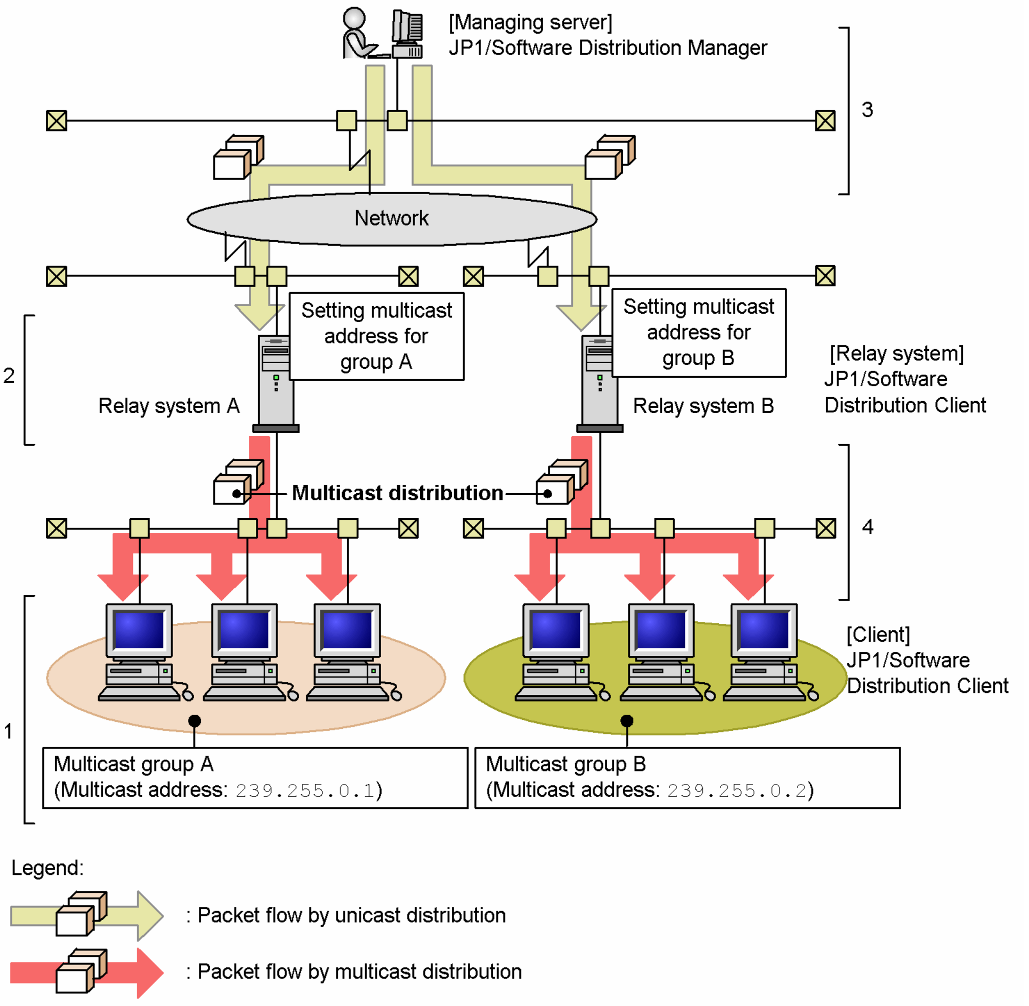
6.2.3 System configuration for multicast distribution

This section explains the system configuration required in order to implement multicast distribution. It also explains how jobs are distributed when the system configuration includes a version of the JP1/Software Distribution product that does not support multicast distribution.

(1) Standard system configuration for multicast distribution

The following figure shows the standard system configuration for implementing multicast distribution and the packet flow.

Figure 6–15: Standard system configuration for implementing multicast distribution and packet flow


[Managing server]
JP1/Software Distribution Manager
3
Network
Setting multicast address for group A
Setting multicast address for group B
2
Relay system A
Relay system B
[Relay system]
JP1/Software Distribution Client
Multicast distribution
4
[Client]
JP1/Software Distribution Client
1
Multicast group A
(Multicast address: 239.255.0.1)
Multicast group B
(Multicast address: 239.255.0.2)
Legend:
: Packet flow by unicast distribution
: Packet flow by multicast distribution

The managing server, higher system to which the clients are connected, and the clients themselves must all be running the Windows version of JP1/Software Distribution 06-71 or later.

You must create a multicast group for each higher system to which clients are connected, and you must assign a unique multicast address to each multicast group. The description below is keyed to the numbers shown in the example system shown in Figure 6-15. Nos. 1 and 2 are system configuration settings; Nos. 3 and 4 are the packet flow when the job is executed.

1. Set the group of clients connected to relay system A to be multicast group A, and the group connected to relay system B to be multicast group B. Specify multicast address `239.255.0.1` for the clients in multicast group A, and `239.255.0.2` for the clients in multicast group B.
2. Specify the multicast address of multicast group A (`239.255.0.1`) for relay system A, and the multicast address of multicast group B (`239.255.0.2`) for relay system B.

   Using multicast distribution, relay system A can now distribute jobs to the clients in multicast group A, and relay system B can now distribute jobs to the clients in multicast group B.
3. At the managing server, create a job with multicast distribution specified, and then execute that job.

   The managing server sends the packets for the job to each of the relay systems. In this example, two relay systems are connected to the managing server, so packets equivalent to two jobs are sent (unicast distribution). The jobs are sent by unicast distribution to relay systems A and B.
4. Relay systems A and B each send the packets for just one job, regardless of the number of clients. The packets for one job flow on the common routes to each client (multicast distribution).

In the same system configuration, if the job were distributed using unicast distribution, the number of job packets flowing from the higher systems to which the clients are connected to the destination clients would be multiplied by the number of clients. Therefore, three times the number of packets would be sent from relay systems A and B along the routes shown in 4.

Jobs can be distributed using multicast distribution even in a configuration in which the clients are connected directly to the managing server. In this case, the multicast address of the multicast group to which the job is to be distributed must be specified at the managing server.

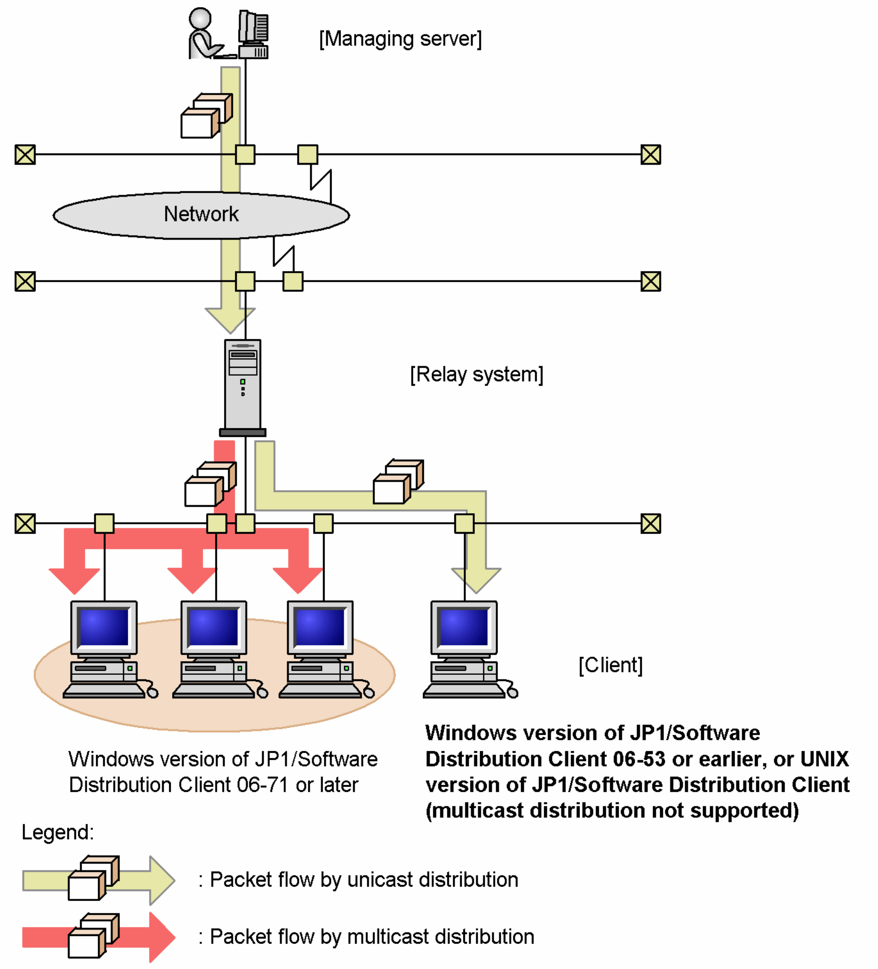
(2) System configurations including versions not supporting multicast distribution

Multicast distribution requires the Windows version of JP1/Software Distribution 06-71 or later. This section explains how jobs are distributed when the configuration of the systems to which the jobs are to be distributed includes a version of JP1/Software Distribution that does not support multicast distribution (Windows version of JP1/Software Distribution 06-53 or earlier or the UNIX version of JP1/Software Distribution).

If a higher system to which the clients are connected is running a version that does not support multicast distribution, multicast distribution cannot be used between that system and its clients. In such a case, even if a job for which multicast distribution is specified is sent from the managing server, it is distributed by unicast distribution.

If a client is running a version that does not support multicast distribution, the job is sent to that client by unicast distribution. The following figure shows the packet flow when the system configuration includes a client that does not support multicast distribution.

Figure 6–16: When a client does not support multicast distribution


[Managing server]
Network
[Relay system]
[Client]
Windows version of JP1/Software Distribution Client 06-71 or later
Windows version of JP1/Software Distribution Client 06-53 or earlier, or UNIX version of JP1/Software Distribution Client (multicast distribution not supported)
Legend:
: Packet flow by unicast distribution
: Packet flow by multicast distribution

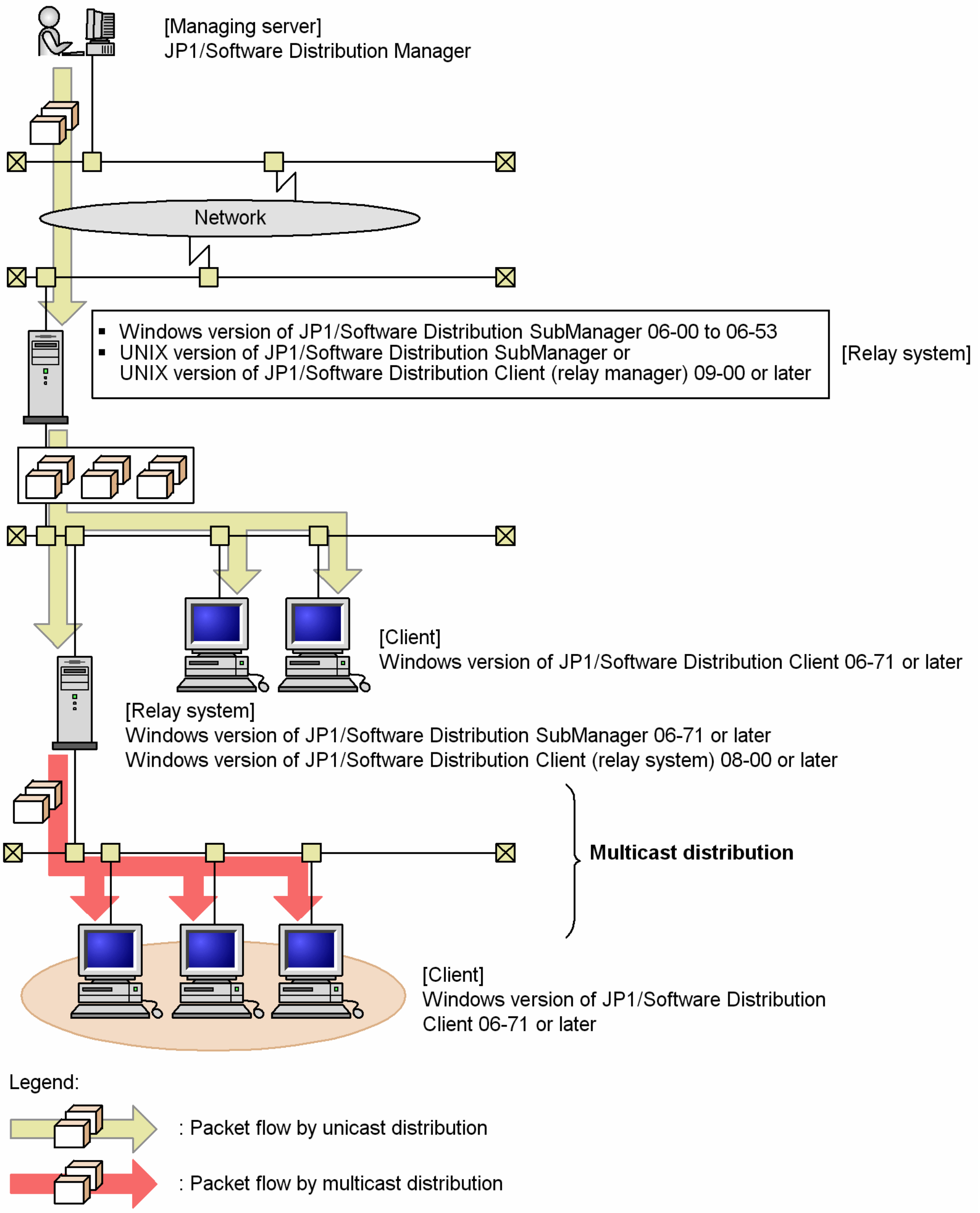
The following explains what occurs when jobs with multicast distribution specified are sent from the managing server in an environment in which there are several relay managers/systems (relay managers or relay systems) arranged in a hierarchy.

When relay managers/systems are arranged hierarchically and a relay manager/system above the higher system to which the clients are connected does not support multicast distribution, jobs are distributed by unicast distribution to the systems below it. However, if the relay manager/system above the higher system to which the clients are connected is one of the following, jobs can be distributed using multicast distribution from the lower relay system to the clients:

- Windows version JP1/Software Distribution SubManager 06-00 to 06-53 or later
- UNIX version of JP1/Software Distribution SubManager or the UNIX version of JP1/Software Distribution Client (relay system) 09-00 or later

The following figure shows the flow when jobs are distributed by multicast distribution between the lower relay system and clients in a configuration that includes multiple relay manager/systems arranged hierarchically.

Figure 6–17: Hierarchical relay managers/systems (multicast distribution on lower routes only)


[Managing server]
JP1/Software Distribution Manager
Network
▪ Windows version of JP1/Software Distribution SubManager 06-00 to 06-53
▪ UNIX version of JP1/Software Distribution SubManager or
UNIX version of JP1/Software Distribution Client (relay manager) 09-00 or later
[Relay system]
[Client]
Windows version of JP1/Software Distribution Client 06-71 or later
[Relay system]
Windows version of JP1/Software Distribution SubManager 06-71 or later
Windows version of JP1/Software Distribution Client (relay system) 08-00 or later
Multicast distribution
[Client]
Windows version of JP1/Software Distribution
Client 06-71 or later
Legend:
: Packet flow by unicast distribution
: Packet flow by multicast distribution

6.2.4 Executing multicast distribution

Once you have determined the system configuration, you can use multicast distribution to distribute jobs.

To execute multicast distribution:

1. Specify multicast distribution when you set up the sender and receivers for multicast distribution.
2. When you create the job at the managing server, specify **Multicast distribution** as the method of distribution.

The following explains the procedure.

(1) Setting up

When you set up a higher system to which clients are connected, specify the sender settings for multicast distribution. Also, when you set up the clients, specify the receiver settings. You specify the necessary settings on the **Multicast Distribution** page in each of the following dialog boxes:

At the sender:

- If the sender is JP1/Software Distribution Manager:
  Server Setup dialog box (server setup)
- If the sender is JP1/Software Distribution Client (relay system):
  Relay System Setup dialog box (basic settings for relay system)

At the receiver:

- If the receiver is JP1/Software Distribution Client (client):
  Client Setup dialog box
- If the receiver is JP1/Software Distribution Client (relay system):
  Detailed Information Setup dialog box (detailed setup for relay system)
- If the receiver is a relay manager of JP1/Software Distribution Manager:
  Detailed Information Setup dialog box (detailed setup for relay manager)

You must set the port numbers and multicast address. You must also set the packet size at the sender. The job is distributed to the multicast addresses specified at the sender. The receivers will receive the jobs distributed to the multicast addresses specified in their setup. For details about the settings, see the manual *Setup Guide*. Note that jobs for which unicast distribution has been specified will be distributed by the unicast method even though you specified multicast distribution during setup.

Notes on setup:

- There is no need to specify multicast distribution in setting up a higher system that is higher than the systems to which the clients are connected. For example, if the systems are connected in a central-manager, relay-system, client sequence, you do not need to specify any settings in the **Multicast Distribution** page when you set up the central manager.
- There is no setting for the sending port number in the **Multicast Distribution** page of the Relay System Setup dialog box of the JP1/Software Distribution ClientSubManager. If you are using multicast distribution from a JP1/Software Distribution SubManager, the port number you specified for receiving multicast distributions in the Detailed Information Setup dialog box of that machine is also used for sending.
- If there is a router that is not compatible with IP multicasting between the clients and the higher system to which the clients are connected, unicast distribution replaces the multicast distribution. In such a case, do not specify multicast distribution when you set up the higher system to which the clients are connected or the clients. If you specify multicast distribution during such a setup, a delay occurs when the switch is made to unicast distribution.

(2) Creating a job for multicast distribution

Multicast distribution can be specified independently for each job. To distribute a job using the multicast distribution method, open the Create Job dialog box, choose the **Job Distribution Attributes** page, and then select **Multicast distribution** under **Distribution methods**. For details about job creation, see *2.3 Executing remote installation* in the manual *Administrator's Guide Volume 1*.

6.2.5 Notes on using multicast distribution

Note the following points about using multicast distribution:

- If you specify the same multicast address in multiple relay managers/systems in a network, the job will be distributed by multicast distribution from all those multiple relay managers/systems to the clients connected to them. To avoid this sort of duplication of job distribution, specify a unique multicast address for each relay manager/system.
- If the multicast addresses of clients and their higher systems are different, jobs are distributed by unicast distribution even if you specify multicast distribution. For example, if a relay system goes down and jobs are to be distributed temporarily via another relay system that has a different multicast address, they will be distributed by unicast distribution.
- Multicast distribution is not available for jobs for which split distribution is specified.
- If a client has not yet started during multicast distribution, or if a client PC has not been turned on, the job is distributed by multicast distribution after the client has been started or after the power to the client PC has been turned on.
- If a client is not resident during multicast distribution but polling at system startup is specified, jobs are distributed by means of multicast distribution when the system is started. However, jobs are distributed by unicast distribution if you choose the **Execute Job Backlog** icon for when the client is not resident.
- If a client is unable to receive an entire job sent by multicast distribution, the remaining part of the job is sent automatically by unicast distribution.
- Do not select both **Multicast distribution** and **Boot the client at the job destination** (**Client Control** page) when you create jobs. If you attempt to distribute jobs for which both are specified, additional time will be required to distribute those jobs to client PCs that are not turned on. Use the following procedure to start client PCs that are not on so that jobs can be distributed by multicast distribution:
    1. Specify **Boot the client at the job destination** for jobs such as *Get system information from client*. When such jobs are executed, power will be turned on at the client PCs, if necessary.
    2. Execute the jobs for which you specified **Multicast distribution**.

6.3 Settings for using the client control facility

This section describes the settings required in order to use the client control facility and provides notes on items that should be taken into consideration.

The client control facility provides two methods for starting client PCs: AMT and Wake on LAN. When you execute the client control facility, it automatically selects the startup method that matches the client environment and executes the job. If the client environment supports both AMT and Wake on LAN, it uses AMT.

6.3.1 Settings for using AMT

This subsection explains the settings required for using AMT to control clients.

Before you install AMT Linkage, you must configure settings for AMT on the clients. For details about the AMT settings, see *5.2.5(1) Settings required before JP1/Software Distribution is installed*.

(1) Settings for using AMT to control clients

To use AMT to control clients, the following settings are required.

Settings in JP1/Software Distribution Manager and JP1/Software Distribution Client (relay system):

> Here, you set the user name and password of the AMT management user, either in the Settings for the AMT Linkage dialog box during installation or on the **AMT Linkage** page at setup.

Settings in JP1/Software Distribution Client (client):

> Here, you set the user name and password of the AMT management user in the Settings for the AMT Linkage dialog box during installation. You cannot configure these settings at setup.

The settings for the user name and password of the AMT management user specified on the client must match those set on the managing server.

If the user name and password of the AMT management user set on the clients differ from those set on the managing server, you can distribute the AMT settings file (`AMTSETUP` file) to change the client settings.

To distribute the AMT settings file:

1. Package the AMT settings file.
   The AMT settings file is stored in *JP1/Software-Distribution-installation-directory*`\DMAMT`. Package the entire folder.
   Specify the installation directory settings as follows:
   - Drive: none
   - Directory: `%NETMDMP%`
2. Distribute the package to the clients.
   Once distribution has been completed, the settings for the client AMT management user are changed.

When multiple notebook PCs that can use AMT are to be brought into a wireless LAN environment as clients, you can use the `dcmamtwc` command to perform a batch operation that specifies the wireless LAN connection settings. If it becomes necessary to modify the wireless LAN connection settings, the `dcmamtwc` command is convenient because it allows you to make changes in a batch operation.

(2) dcmamtwc.exe (wireless LAN connection settings)

An explanation of the `dcmamtwc` command used for wireless LAN connection settings is provided below. You execute this command from the central manager or a relay system.

Function

> Specifies wireless LAN connection settings on notebook PC clients that can use AMT.

Format

```
dcmamtwc.exe /f CSV-output-utility-output-file-name
             /n wireless-LAN-profile-name
             { [/r] |
             [/w ON | OFF | Sx]
             [/p wireless-LAN-profile-priority-order]
             [/i SSID] [/s WPA | RSN] [/e TKIP | CCMP] [/k encryption-key] }
```

Arguments

`/f`

Specify the host for which wireless LAN connection information is being set. To specify a host, use the file to which the CSV output utility outputs the system information. You can also use a file that has the same format as the file to which the CSV output utility outputs the system information.

`/n`

Specify the wireless LAN's profile name as 1-35 characters.

`/r`

If wireless LAN connection information settings already exist, specifying this option will delete them.

If `/w`, `/p`, `/i`, `/s`, `/e`, and `/k` are specified at the same time, these other options are ignored and only `/r` takes effect.

`/w`

Specify `ON`, `OFF`, or `Sx` to connect to or disconnect from the wireless LAN.

If you specify `Sx`, a connection can be established to the wireless LAN even when the client PC is sleeping or hibernating, if it is equipped with AMT 4.0 or later.

`/p`

Specify a value between 0 and 255 for the wireless LAN profile priority order. The default is `0`.

`/i`

Specify the wireless LAN's SSID. If you specify this option, you must also specify the `/s`, `/e`, and `/k` options.

This option is ignored if the `/r` option is specified, or if `OFF` is specified for the `/w` option.

`/s`

Specify the communication method to be used. Select either `WPA` or `RSN` for the communication method. If you specify this option, you must also specify the `/e` and `/k` options.

This option is ignored if the `/r` option is specified, or if `OFF` is specified for the `/w` option.

`/e`

Specify the encryption method to be used. Select either `TKIP` or `CCMP` for the encryption method. If you specify this option, you must also specify the `/s` and `/k` options.

This option is ignored if the `/r` option is specified, or if `OFF` is specified for the `/w` option.

`/k`

Specify the encryption key character string. If you specify this option, you must also specify the `/s` and `/e` options.

This option is ignored if the `/r` option is specified, or if `OFF` is specified for the `/w` option.

Return codes

The following table describes the codes returned when the `dcmamtwc` command executes.

Code	Meaning	Action to take
0	The command was executed for all target machines; and the connection information for a wireless LAN was set or deleted, or the wireless LAN connection was started or stopped.	None
1	The CSV output utility output file cannot be opened, or the file format is invalid.	Check the path of the CSV output utility output file or the file format.
2	A command argument is invalid.	Check the command arguments.

Code	Meaning	Action to take
`12`	An error other than the above occurred.	A system error occurred. Check the execution environment of the command.
`30`	Initialization of AMT's nonvolatile memory failed for at least one client.	Check the log file to determine the cause and the action to take.# • The settings for the AMT management user might not match. Make sure the AMT management user name and password are set in the target clients. • Make sure that **Small Business** is specified as the AMT Provision model. • A targeted PC might not support AMT, or it might not be recognized in the network.
`31`	The command was executed for all target machines; but an attempt to set or delete the connection information for a wireless LAN failed, or an attempt to start or stop the wireless LAN connection failed.	Check the log file to determine the cause and action to take.# • Reset the AMT management user name and password specified for AMT linkage in the JP1/Software Distribution setup. • **Enterprise** might be selected as the Provision model in all machines' AMT setup. Change it to **Small Business**. • A targeted PC might not support AMT, or it might not be recognized in the network.

#: For details about the `dcmamtwc` command log, see *6.3.1(5) Checking the AMT Linkage log* in the manual *Administrator's Guide Volume 2*.

Notes

- After you have stopped the wireless LAN by specifying `OFF` for the `/w` option, to restart it, you need to execute the `dcmamtwc` command by specifying `ON` for the `/w` option from the central manager or relay system of the LAN environment.
- To set the wireless LAN connection information for the first time, you need to set the wireless LAN connection information from the central manager or relay system of the LAN environment.
- If you do not specify the `/r` option, a new profile is added for the specified wireless LAN. If a profile already exists for the same wireless LAN, the existing profile is overwritten.
- If you stop the wireless LAN by specifying `OFF` for the `/w` option, the wireless LAN network is disconnected when the command is executed successfully. Therefore, no return code is reported even when the client terminates normally. Since no return code is reported, the central manager considers that a communication error has occurred, and reports a return code indicating abnormal termination.

Execution example

In the following example, the `dcmamtwc` command is used to set wireless LAN connection information:

```
dcmamtwc.exe /f C:\temp\input.csv /n AMTProfile /w ON /i AMTACCESSPOINT /s
WPA /e TKIP /k P@ssw0rd
```

(3) Notes on using AMT to control clients

Note the following points when using AMT to perform client control:

- AMT Linkage cannot be used in an environment in which a LAN and a wireless LAN are connected to the same subnet.
- You must be able to use AMT Linkage on the target clients. To determine whether a client supports use of AMT Linkage, check the value of the AMT firmware version item in the system information. You can use AMT Linkage if the AMT firmware version is displayed. You cannot use AMT Linkage if no value is displayed or if `N/A` is displayed.
- DHCP must be used to assign the IP addresses for the OS and AMT.

- If the execution-destination client is using a battery in a LAN environment, or is in a wireless LAN environment, power must be turned on for the client. If the client is in the suspend state, hibernation state, or resume state, AMT Linkage cannot be used.
- If an AMT connection failure occurs, the client control facility is re-executed, using client control based on Wake on LAN.

6.3.2 Settings needed to use Wake on LAN

This section explains the settings that must be specified during setup.

(1) Items for which values must be set

For automatic shutdown to be applied to a system that was started by the client control facility, you must set the following information:

If requested by the administrator, shut down or restart the computer

On the **Job Options** page at setup, select **If requested by the administrator, shut down or restart the computer**.

You can specify this option only while you are setting up JP1/Software Distribution Client (client). This option is not available during setup of client facilities for JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system) because relay managers and relay systems must always be running.

(2) Items requiring special care in setting values

Max. number of subsystems in which jobs can execute concurrently

You will not be able to use client control to start the destination systems if 0 is specified for the following options when you set up a higher system to which clients are connected:

- For the central manager and relay manager: **Max. number of subsystems in which jobs can execute concurrently** on the **Server Customization** page in the Server Setup dialog box
- For a relay system: **Max. number of relays or clients in which jobs can execute concurrently** in the Relay System Setup dialog box

Automatically register this computer in the system configuration

If the system is using JP1/Software Distribution version 06-00 or later, select the **Automatically register this computer in the system configuration** setting.

(3) Item for which a value is recommended

Polling setting

We recommend that you select **Client will poll the managing server** for the polling setting.

(4) Notes

The following subsections provide notes on the use of Wake on LAN to perform client control.

(a) Notes on the system configuration

If you use the client control facility in a system configuration in which a router is installed on the job route, you should use one of the network environments listed below. For security, environment 1 is recommended:

1. Place one or more relay managers or relay systems for each router and keep them always running. (Recommended)
2. Set the router so that it passes the packets with broadcast specified.

   In this environment, there is no need to place a relay manager or relay system for each router. However, in an environment where destination IP addresses are subnetted by routers, the following conditions must be satisfied:

   - The following is installed on each PC that is started by the client control facility: JP1/Software Distribution version 06-51 or later, and WMI.

- Before using the client control facility, a *Get system information from client* job is executed to obtain subnet mask information.
- On the **Relay System Customization** page of JP1/Software Distribution Client (relay system), the **Record the system/software information answered from the lower clients** option is selected.

If you set the router to pass the packets with broadcast specified, the system could be affected by Denial of Service (DoS) attacks. To avoid this, use environment 1.

(b) Notes on hardware

This section discusses hardware considerations when you use the client control facility.

- The client control facility is affected significantly by various settings and compatibilities among individual components. You can use the following provided command to determine whether a PC can be started by the client control facility:

  Command name

  `magicsnd.exe`

  Command storage location

  JP1/Software-Distribution-installation-directory`\bin`

  Usage

  `magicsnd -a` *MAC-address* `[-m` *subnet-mask*`]` *IP-address*

  Execute this command from the MS-DOS prompt. The command starts the specified destination. If this command cannot start a PC, the PC cannot be started by the client control facility.

  The subnet mask specification is required only if you have set up your router to pass packets for which broadcast was specified, in an environment in which destination IP addresses are subnetted by routers.

  Usage examples

  The following is an example of the command when a relay system that is always running is placed for each router:

  ```
  magicsnd -a 0000e2168066 172.17.11.145
  ```

  The following is an example of the command when IP addresses are subnetted and the routers pass packets with broadcast specified:

  ```
  magicsnd -a 0000e2168066 -m 255.255.255.0 172.17.11.145
  ```

- If there are any items relating to Wake on LAN in the BIOS settings, enable them.
- If HUB or NIC supports the LinkChange facility, turning on the power to equipment might start a PC in which Wake on LAN is enabled. To avoid this problem, the equipment must always be kept on or the LinkChange facility must be disabled.
- Three types of signals are produced by a LAN card: RWU-High, RWU-Low, and PME. Because the type of signal that can be used depends on the motherboard, it is necessary to set the jumper pins appropriately. For details about the pin settings, see the documentation from the LAN card supplier.

(c) Notes on startup

This section provides notes on using the client control facility to start clients.

- If you execute multiple jobs that use the client control facility and all the jobs are specified to start a client, after a destination client has been started, subsequent startup requests to the same destination client are ignored.
- Startup and shutdown are disabled if you use the client control facility to execute a job on a PC running a version of JP1/Software Distribution Client earlier than 06-00.
- The client control facility might not be able to start the system in an environment in which more than one network interface card is used on a single PC.
- When you execute a job from JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system) for which **Boot the client at the job destination** has been specified, some PCs might freeze up during startup. This is because the startup intervals sent from the JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system) are shorter than the startup time of the PC. If this occurs, change the following registry value for the JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system) to a value greater than the startup time of the PC:

Registry key:

- When the OS is the 32-bit version of JP1/Software Distribution Manager

`HKEY_LOCAL_MACHINE\SOFTWARE\HITACHI\NETM/DM`

- When the OS is the 64-bit version of JP1/Software Distribution Manager

`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\HITACHI\NETM/DM`

- When the OS is the 32-bit version of JP1/Software Distribution Client (relay system)

`HKEY_LOCAL_MACHINE\SOFTWARE\HITACHI\NETM/DM/P`

- When the OS is the 64-bit version of JP1/Software Distribution Client (relay system)

`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\HITACHI\NETM/DM/P`

Name:

`DeliveryExecSelectInterval`

Data:

Minimum value (seconds): `30`

Maximum value (seconds): `9,999`

Default value (seconds): `60`

6.3.3 Notes on shutdown

This section provides notes on using the client control facility to shut down clients.

- When automatic shutdown is attempted for a Windows NT client, shutdown might fail or a restart might occur. This might be because the hardware or Windows environment does not support automatic shutdown. Check whether your hardware supports automatic shutdown. Execute the most recent update program provided by the hardware supplier to achieve conformity between Windows and the hardware specifications. If your hardware supports automatic shutdown but executing the update program does not solve the problem, consult the documentation provided by the hardware supplier or Microsoft.
- Shutdown specified for a relay manager or relay system is always ignored.
- A UNIX or Windows client whose version is 06-00 or earlier cannot be shut down automatically.
- A Windows NT client whose screen saver is on and is password-protected cannot be shut down automatically.
- A client cannot be shut down automatically if a file is being edited when the job specifying shutdown is received.
- If you execute a job specifying shutdown from a higher system and the client is in one of the following statuses, the specified operation will not be executed:
  - A user is not logged on to the client.
  - A non-Administrator user is logged on to the client and the **Run the client with non-Administrator user permissions** option was not selected during setup.

  In these statuses, if a confirmation dialog box display time was specified in the client settings, the client will be shut down without displaying the confirmation dialog box. If the **How long will the dialog be displayed?** option is set to **Unlimited**, the client cannot be shut down.

  Note that *executing a job from a higher system* does not include job execution from the client using the Package Setup Manager or the **Execute Job Backlog** icon.
- If a *Send package, allow client to choose* job with shutdown specified is executed from the Package Setup Manager of a client, the client will not be shut down until a user entry is made, in the same manner as when **Unlimited** is selected for the **How long will the dialog be displayed?** option, even if a time value was specified for the confirmation dialog box in the client setup.
- If clients are in the Windows XP Mode environment, it might not be possible to automatically shut them down in some cases. For details about how to control clients in the Windows XP Mode environment, see *C.2(2) Notes on job management* in the *Setup Guide*.

6.4 About the operating environment of relay systems

This section describes the polling environment for a relay system JP1/Software Distribution Client (relay system).

6.4.1 Multi-polling environment for a relay system

Normally, a relay system is connected to only one higher system. If you want to establish more than one distribution route to a relay system from a higher level, you must create a multi-polling environment that contains more than one higher system. In a multi-polling environment, a relay system can receive jobs from multiple higher systems and forward them to the lower-level systems.

(1) Setting the multi-polling environment

During relay system setup, in the Specify Higher Systems dialog box specify the higher systems to which you want to connect. You must assign a priority to each higher system. When you specify the name of a higher system, use the *ID key for operations* (host name or IP address) of the higher system. You can specify a maximum of eight higher systems.

In a multi-polling environment, the relay system performs polling on a multi-host basis. Therefore, you cannot use hot-standby polling.

Also, note that in a multi-polling environment, you can only specify either host names or IP addresses of the higher systems as the *ID key for operations*. If you specify host names for some higher systems and IP addresses for the other higher systems, the jobs from the higher systems stop at the relay system and are not forwarded to the subsystems.

(2) Notes on the multi-polling environment

- When you use the facility for automatically registering the system configuration, the system configuration information is reported only to the higher system that has the highest priority.
- You can use ID groups only for the higher system that has the highest priority. You cannot add, as a relay for managing IDs, a relay system to an ID group created by a higher system that does not have the highest priority. If you attempt to do so, the system will be placed in *registering* status and the processing will not proceed. Also, you can only add a relay system to the ID group of a system set during setup as **System for ID group registration** on the **Connection Destination** page.
- If the **Report the ID group job status to the managing server** option is selected during setup, the results of ID group jobs are reported only to the higher system that has the highest priority.
- If the **Suppress periodic jobs when the connection destination of the client is changed** option is selected during setup, the results of periodic jobs are reported only to the higher system that has the highest priority.

6.5 About the operating environment of clients

This section describes how to set the client operating environment in accordance with the network environment and the method of operation.

6.5.1 Storing the client's host ID

When you use AMT Linkage at a client running on a computer that supports AMT, you can store the host ID in AMT's nonvolatile memory.

Storing the host ID in this manner allows you to restore it if, for example, you need to re-install the client when recovering from a disk failure. This enables the higher systems to recognize the newly installed client as being the same asset as it was prior to the failure.

The following subsections explain the settings for storing host IDs in AMT's nonvolatile memory.

(1) Setting method

You must first initialize an area in AMT's nonvolatile memory in which to store the host IDs. To initialize the area, you execute the `dcmamtin` command on the higher system targeting the computer that supports AMT. You can execute this command either before or after the client is installed.

For details about the `dcmamtin` command, see *(2) dcmamtin.exe (initialize AMT's nonvolatile memory)*.

Once initialization of this area is complete, the host ID is saved to AMT's nonvolatile memory at one of the following times.

If the client has not been installed:

The host ID is saved to nonvolatile memory when it is generated during installation of the client.

If the client has been installed:

The host ID that has already been generated is saved in nonvolatile memory when the client communicates with the higher system. If no host ID has been created, the host ID is saved in nonvolatile memory when it is created.

Once the host ID has been stored, it can be restored if the client is re-installed. If, for some reason, the host ID is not restored, see *6.4.2(5) AMT Linkage does not operate correctly* in the manual *Administrator's Guide Volume 2*.

If the host ID cannot be restored from AMT's nonvolatile memory when the client is re-installed, the host ID is regenerated by the client. If this occurs, the host ID in AMT's nonvolatile memory is overwritten when a client service starts.

(2) dcmamtin.exe (initialize AMT's nonvolatile memory)

This subsection describes the `dcmamtin` command. You can use this command in an environment in which AMT Linkage of JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system) is installed.

Function

This command initializes an area in AMT's nonvolatile memory on a client for the purpose of storing the client's host ID.

Format

```
dcmamtin.exe    {/f system-configuration-information-file |
                 /H host-name | /I IP-address}
```

Arguments

`/f`

Specify the full path of the system configuration information file. In this case, the command is then executed for all clients described in the system information configuration file.

Specify this argument when you want to initialize AMT's nonvolatile memory for multiple clients.

For details about the system configuration information file, see *8.1.4(3) Saving the system configuration information to a file* in the *Setup Guide*.

`/H`

Specify the client's host name, using no more than 64 characters.

`/I`

Specify the client's IP address.

Return codes

The following table describes the codes returned when the `dcmamtin` command executes.

Code	Meaning	Action to take
`0`	Initialization of AMT's nonvolatile memory succeeded at all execution targets.	None
`1`	The system configuration file could not be opened, or the syntax in the file is invalid.	Check the path to, and the syntax in, the system configuration information file.
`2`	A command argument is invalid.	Check the command arguments.
`12`	An error other than the above occurred.	A system error occurred. Check the execution environment of the command.
`30`	Initialization of AMT's nonvolatile memory failed for at least one client.	Check the log file to determine the cause and action to take.# • The settings for the AMT management user might not match. Make sure the AMT management user name and password are set in the target clients. • Make sure that `Small Business` is specified as the AMT Provision model. • A targeted PC might not support AMT, or might not be recognized in the network.
`31`	Initialization of AMT nonvolatile memory failed for all clients.	• Check the log file to determine the cause and the action to take.# • The user name and password specified during setup for the AMT management user might be incorrect. Try resetting this information. • Make sure that `Small Business` is specified as the AMT Provision model. • The targeted PCs might not support AMT, or might not be recognized in the network.

#: For details about the `dcmamtin` command, see *6.3.1(5) Checking the AMT Linkage log* in the manual *Administrator's Guide Volume 2*.

Execution example

In the following example, the `dcmamtin` command initializes AMT's nonvolatile memory:

```
dcmamtin.exe /f "D:\Program Files\Hitachi\NETMDM\DMPRM\NETM.NDD"
```

6.5.2 Client polling method

A client receives a job from the managing server and executes the job. A client can receive a job from the managing server only while the client is active. If a communication error occurs or if the client is not active, the client cannot receive jobs from the higher system. In such a case, the client can still monitor whether there are jobs addressed to it. Monitoring for jobs from a higher system is called *polling*.

You can specify the polling timing and execution interval when you set up JP1/Software Distribution Client (client). The available polling methods are listed below. Select the polling method that is appropriate for the manner in which the client operates.

- No polling
- Polling only once at system startup
- Polling at a specified interval beginning at system startup

- Polling once a day at a specified time (applicable to JP1/Software Distribution Client (client) only)
- Polling once a day at system startup (applicable to JP1/Software Distribution Client (client) only)

Note that the default polling method depends on the network environment that is specified during installation of JP1/Software Distribution Client (client).

When JP1/Software Distribution is used in a WAN environment, *Polling only once at system startup* is set as the default. To reduce the volume of unnecessary data transmissions in a low-speed WAN environment, select *No polling*.

When JP1/Software Distribution is used in a LAN environment, *Polling at a specified interval starting at system startup* is set as the default and the interval is set to 30 minutes. Set the polling interval and timing so that they do not place an unnecessary load on the network.

6.5.3 Multi-polling environment for clients

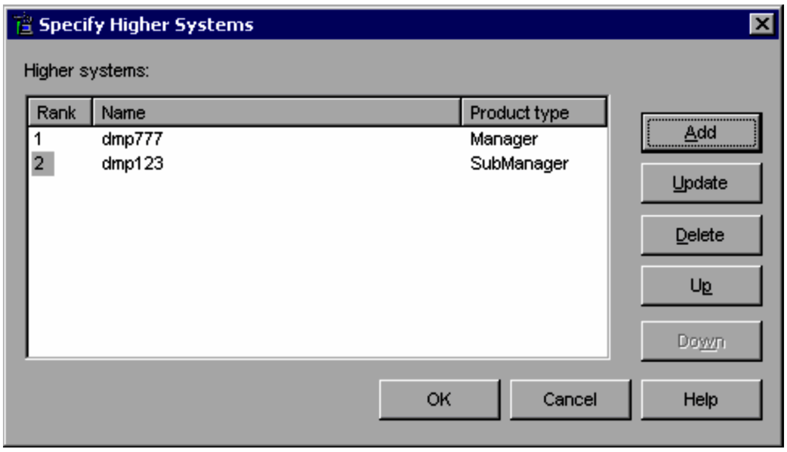
The configuration of the distribution destinations is defined in the system configuration information, so that jobs for a client are executed according to a predetermined route. Also, the only relay system to which a client will connect is the one defined in the system configuration information.

To specify multiple distribution routes for a client or for a client to connect to multiple relay systems, you must create a *multi-polling environment*. The relay systems to which the client will connect can be specified with connection priorities. When a multi-polling environment is used, a job can be executed for a target client via a different relay system if an error occurs in the first relay system that is selected. A client can also connect to multiple relay systems according to the connection priorities.

(1) Setting up a multi-polling environment

When you set up a client, you can use the Specify Higher Systems dialog box to specify multiple relay systems and assign a priority to each of them:

Figure 6–18: Specify Higher Systems dialog box



Rank	Name	Product type
1	dmp777	Manager
2	dmp123	SubManager

Add button

Adds a higher system to be a connection target. You can specify a maximum of eight higher systems. In the Add/Change Higher System dialog box, specify the product type and host name or IP address of the higher system that is to be added.

Update button

Updates the information about a selected higher system. In the Add/Change Higher System dialog box, which is displayed when this button is chosen, specify the product type and host name or IP address.

Delete button

Deletes the selected higher system from the list of higher systems.

Up button

Increases by 1 the priority of the selected higher system.

Down button

Decreases by 1 the priority of the selected higher system.

When you finish specifying the settings, choose the **OK** button. The **Connection Destination** page appears again.

(2) Selecting a polling method in a multi-polling environment

A client checks with the higher relay system to see whether there are any jobs addressed to it. This operation is called polling. The method of polling the relay system is set up on the **Default Running Status/Polling** page of the Client Setup dialog box. The following two polling methods are available:

Hot standby:

With the hot-standby method, only one relay system is polled. Normally, the relay system with the highest priority, as set in the Specify Higher Systems dialog box, is the one that is polled. Only if that relay system cannot be connected is the relay system with the second-highest priority polled. If the second relay system cannot be connected, the relay system with the next-highest priority is polled, and so on, until connection is established with a relay system.

Multiple hosts:

With the multiple-hosts method, all relay systems specified in the Specify Higher Systems dialog box are polled. Polling begins with the relay system with the highest priority.

(3) Notes on the multi-polling environment

Note the following points about operating a client in a multi-polling environment:

- In the case of a client operating in a multi-polling environment, you can register ID groups in the first-priority relay system only.
- Under the hot-standby method, if the relay system with the highest priority recovers from an error, it is possible to have the client poll that relay system again. This method is explained below:

  If the client is resident:

  If the client is resident, either stop the relay system that is connected or execute a job such as *Get system information from client* via the relay system with the higher priority. If the relay system that is connected is stopped, the relay system to be polled will change the next time polling occurs. If a job is executed, the relay system to be polled will change after the job is executed.

  If the client is nonresident:

  If the client is not resident, set the server-polling format at system startup to **Perform polling according to priority when the system starts**. After the client is restarted, the relay system with the highest priority will be polled.
- When jobs are executed on all paths in an environment in which hot standby is used, the job on the path of the relay system to which the client connected is executed, but the jobs on all other paths remain in *unexecuted* status in the relay system. Therefore, you must periodically delete the jobs remaining in the relay system and the completed jobs from the managing server. If a large number of jobs remain in the relay system, its performance might suffer.
- When jobs are executed on all paths in an environment in which multiple hosts are used, the same job is received every time a client polls. In this case, to execute a remote installation job, we recommend that you deselect the **Replace existing package** check box under the job installation condition. If this check box is selected, a package is sent each time the job is executed, and this might place an undue load on the network. If the check box is not selected, any job that the client has already received normally terminates without a package being sent again. The job maintenance code in this case is `900090009000`.

6.5.4 Automatic updating of the client connection destination

If you distribute information to clients in order to determine connection destinations, JP1/Software Distribution uses the IP address of each client PC to determine and automatically set the appropriate higher system to which the client will be connected. Because the connection destination is updated automatically when a client's IP address changes, this feature is useful when a client PC is moved. This subsection describes automatic updating of the connection destinations of clients.

JP1/Software Distribution Client (client) supports this facility.

(1) Setting and updating the higher system automatically

Before you can set or update automatically the higher systems to which clients will be connected, you must create an *information file for higher connection destinations* (`dmhost.txt`) and distribute it to the clients. After distribution to the clients, connection destinations are reset automatically at specific times.

(a) Creating dmhost.txt

`dmhost.txt` is used to determine the higher system to which a client will be connected. The file defines the higher systems corresponding to ranges of IP addresses of client PCs. For example, `dmhost.txt` could be set up to define the connection destination of client PCs with IP addresses in the range from `172.16.22.1` to `172.16.22.255` as the New York branch PC, and the connection destination of client PCs with IP addresses in the range from `172.17.22.1` to `172.17.22.255` as the Detroit branch PC. For details about creating `dmhost.txt`, see *(2) Creating an information file for higher connection destinations (dmhost.txt)*

(b) Distributing dmhost.txt

Once you have created `dmhost.txt`, you must save it to the following directory of each client PC:

`JP1/Software-Distribution-installation-directory``\MASTER\DB`

You can distribute `dmhost.txt` to a large number of clients in the batch mode by using the *Install package* job. To do this, package and distribute `dmhost.txt` using the following settings:

Installation target directory settings on the **System Conditions** page

Drive: None

Directory: `%NETMDMP%\MASTER\DB`

If a client is not connected to a JP1/Software Distribution system, you can manually store `dmhost.txt`.

(c) Timing for changing the connection destination

After storing `dmhost.txt` in the client PC, either execute polling or restart the OS of the client PC. The higher system to which the client will connect will be set on the basis of the contents of this file.

The following are the three types of polling that automatically change a client's connection destination:

- **Start polling when the client program starts**
  In the client settings, the **Start polling when the client program starts** check box is selected on the **Default Running Status/Polling** page.
- **Specify the time to execute polling**
  In the client settings, the **Specify the time to execute polling** check box is selected on the **Default Running Status/Polling** page.
- Polling through execution of the **Execute Job Backlog** icon
  From the **Start** menu, the **Execute Job Backlog** icon is chosen.

Even after these settings have been configured, the connection target is reset if you execute polling or restart the OS after either of the following:

- The IP address of the client PC changes
- `dmhost.txt` is edited or overwritten

If you move a client PC and change its IP address, its connection destination is changed to the appropriate higher system simply by executing polling or restarting the OS. The end user need not be aware of the change in the connection destination.

When the connection destination of a client is set or changed automatically on the basis of `dmhost.txt`, the change is logged into the *installation-folder*`\LOG\USER.LOG` file. For details about the log information, see *6.4.1 Checking log files* in the manual *Administrator's Guide Volume 2*.

If you use dmhost.txt to automatically set the connection destination, and then manually change the connection destination from the client setup, the manually set connection destination remains in effect even after polling or OS restart.

(d) Relationship between automatic updating of connection destination and other facilities

Because automatic updating of the connection destination from dmhost.txt cannot be used with some JP1/ Software Distribution facilities, note the following:

- The facility for automatic updating of the connection destination from dmhost.txt cannot be used if you specify **Automatically specify the higher system that requested a job execution as the connection destination**. Even if you save dmhost.txt, it is not used if you select the **Automatically specify the higher system that requested a job execution as the connection destination** check box on the **Connection Destination** page during client setup.
- To use the facility for automatic updating of the connection destination from dmhost.txt in the case of multiple LAN connections, select the **Use as Client IP address** check box in the Network Adapter Settings dialog box, which is displayed from the **Communication** page of the client setup.
- Do not save dmhost.txt at computers in a multi-polling environment. If you select **Poll multiple higher systems** on the **Connection Destination** page, the priority of the higher system to which the client will be connected will have changed even by the time you save dmhost.txt.
- When the connection destination is changed from dmhost.txt, the new connection destination is not added to the **Servers permitted to execute remote collection jobs** list on the **Remote Collect Options** page of the Client Setup dialog box.
- If you specify * or ? as the connection destination, dmhost.txt cannot be used for automatic change the connection destination. However, once you save dmhost.txt at the client, automatic updating of the connection destination is enabled if a value other than * or ? is specified for the connection destination.

  If you install JP1/Software Distribution Client using the pre-installation facility and copy the hard disk that contains dmhost.txt, the connection destination is updated automatically according to this dmhost.txt when a desired connection destination is specified on the PC after distribution.
- If the current logon user does not have registry write permissions, and if, in the client settings, the **Run the client with non-Administrator user permissions** check box is cleared on the **Security** page, executing the **Execute Job Backlog** icon will not change the connection destination setting.

(2) Creating an information file for higher connection destinations (dmhost.txt)

The information file for higher connection destinations is a text file with the name dmhost.txt. This section explains how to create this file.

(a) Format of dmhost.txt

Each line of dmhost.txt consists of a range of IP addresses of client PCs and information about the corresponding connection destination. Each line can consist of a maximum of 255 characters. Use the comma (,) as the delimiter between items. To add a comment line, begin the line with a semicolon (;).

The file format is as follows:

Format

```
lowest-IP-address,highest-IP-address,connection-destination,product-type-of-
the-connection-destination,multicast-address-of-the-connection-destination
```

Description

lowest-IP-address (required)

Specify the lowest IP address in the range of client IP addresses. Specify the numbers in the format *xxx.xxx.xxx.xxx*.

highest-IP-address (required)

Specify the highest IP address in the range of client IP addresses. Specify the numbers in the format *xxx.xxx.xxx.xxx*.

connection-destination (required)

Specify the host name or IP address of the connection destination. Specify the host name if the connection destination node identification key is set to host names, or the IP address if it is set to IP addresses. A host name must not exceed 64 bytes of alphanumeric characters. If you specify an IP address, specify the numbers in the format *xxx.xxx.xxx.xxx*.

product-type-of-the-connection-destination (required)

Specify `netmdm` if the connection destination is JP1/Software Distribution Manager, or `netmdmw` if the connection destination is JP1/Software Distribution Client (relay system).

multicast-address-of-the-connection-destination (optional)

If you wish to distribute jobs to clients using multicast distribution, specify the multicast address that will be set as the connection destination. Specify the multicast address as numbers in the format *xxx.xxx.xxx.xxx*. You can use the following range of addresses for multicast addresses: `224.0.1.0` to `239.255.255.255`.

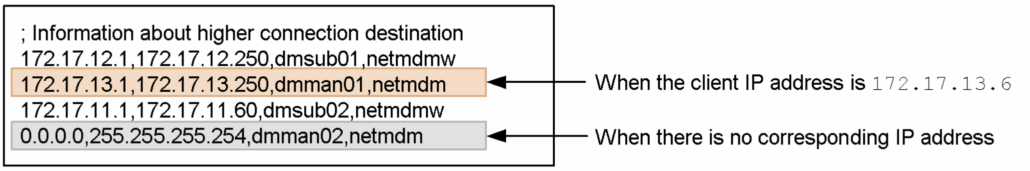
Notes

- If the IP address of a client is not within a defined range, the connection destination setting will not be changed.
- If the IP address of a client is the loopback address 127.0.0.1, the connection destination setting will not be changed.
- If you specify a range of client IP addresses that overlaps another specified range, the range that is defined first takes effect.
- A line is ignored in the following cases:
    - When any of the four required items is omitted
    - When an invalid IP address is specified
    - When *connection-destination* is more than 64 bytes
    - When the specified product type is neither `netmdm` nor `netmdmw`
- If you omit the *multicast-address-of-the-connection-destination* parameter or if you specify an invalid value, the multicast address cannot be set. However, the range of IP addresses and corresponding connection destination information specified in the other parameters are still valid.
- If you specify more than five items on one line, the additional items are ignored.
- If a line exceeds 255 characters, the 256th and subsequent characters are ignored.

(b) Example of creating dmhost.txt

The following shows an example of creating `dmhost.txt`.

Figure 6–19: Example of creating dmhost.txt



```
; Information about higher connection destination
172.17.12.1,172.17.12.250,dmsub01,netmdmw
172.17.13.1,172.17.13.250,dmman01,netmdm
172.17.11.1,172.17.11.60,dmsub02,netmdmw
0.0.0.0,255.255.255.254,dmman02,netmdm
```

When the client IP address is `172.17.13.6`

When there is no corresponding IP address

Line 2 of the file contains the IP address range `172.17.13.1` to `172.17.13.250`. For a client whose IP address is `172.17.13.6`, the higher system is therefore changed automatically to `dmman01`.

If the range from `0.0.0.0` to `255.255.255.254`, which includes the range of all IP addresses, is defined on the last line of `dmhost.txt`, the higher system at the connection destination is changed to `dmman02` for a client that had no corresponding IP address.

(c) Notes on when the information file for higher connection destinations has been distributed

If you change the IP address of a connection destination host after the information file for higher connection destinations has been distributed to the clients and automatic updating of their connection destinations has been performed, first delete from the clients the information file for higher connection destinations that you had been using. The change in the IP address will then act as a trigger to activate the facility for automatic updating of the connection destination.

6.5.5 Using a client in a low-capacity PC

JP1/Software Distribution Client is always running on a client PC. The memory and CPU are being used even when JP1/Software Distribution Client is not being used. If you use JP1/Software Distribution Client on a low-capacity PC, you can make JP1/Software Distribution Client nonresident and run it only when needed.

The following explains the operation in a client in which JP1/Software Distribution Client is not kept resident:

- When the client PC is started, polling is executed only once. If there is a job addressed to the local system, the job is executed. Upon completion, JP1/Software Distribution Client becomes nonresident.
- To receive a job from the managing server, choose the **Execute Job Backlog** icon. The system polls for jobs addressed to the local system and executes any that are found.

6.5.6 Connection settings when the name of the higher system cannot be resolved

In an environment that uses host names as ID keys for operations, if the connection to the DNS server is interrupted for some reason (for example, because the system is a quarantined system), the client might no longer be able to resolve the name of a connection-target higher system. In such a situation, the client can resolve the name from the IP address in the communications protocol when it receives execution request information from the connection-target higher system. If the environment is such that it prevents the client from using this method to resolve the name of the connection-target higher system, the client can still poll for jobs and send inventory information to the higher system. During this time, the client will recognize the higher system that originates the execution request as the connection target.

To use this function, the following settings must be specified during client setup:

- On the **Default Running Status/Polling** page, select the **Client starts automatically at system boot** check box.
- On the **Communication** page, select the **Connect to the upper-level system by using the IP address received via the startup request protocol** check box.

When this function is enabled, a *file for higher system addresses* is automatically created on the client when it receives an execution request from a higher system. This file contains a mapping of the IP addresses and host names of the higher systems. Subsequently, the client uses the information in this file to perform name resolution and connect to the higher system.

Normally, there is no need to edit the file for higher system addresses. However, in an environment in which the name of the higher system cannot be resolved, you will need to create the file before you initially install a host name-keyed client.

For details about the settings to use when initially installing a host-name keyed client in an environment in which the name of the higher system cannot be resolved, see *(1) Settings to use when initially installing a client in an environment in which the name of the higher system cannot be resolved*. For details about the syntax required in the file for higher system addresses, see *(2) Syntax in the file for higher system addresses*.

Notes

- You do not need to specify these settings when the IP address is used as the ID key for operations.
- For higher systems of version 06-71 and earlier, the connection cannot be established correctly even if these check boxes are selected.
- If the higher system is a cluster system, the connection might not be established correctly.
- If the communication protocol of the execution request information is UDP in an environment in which the higher system uses multiple network adapters, the connection might not be established correctly.

(1) Settings to use when initially installing a client in an environment in which the name of the higher system cannot be resolved

If you initially install a host name-keyed client in an environment in which the name of the higher system cannot be resolved, the client will not be recognized as a target because it cannot connect to a higher system. In such a case, create a file for higher system addresses beforehand, and use one of the following methods to save the file at the client.

- Save the file for higher system addresses at the client after the client is installed.
  After you have installed the client, save the file in the following folder:
  `JP1/Software-Distribution-installation-directory\MASTER\DB`
- Use the JP1/Software Distribution Administrator Kit to copy the file for higher system addresses.
  Use the file copying function of the JP1/Software Distribution Administrator Kit. To do this, specify the following settings on the **Copying Files** page of the Create or Edit Installation Set dialog box while creating the installation set:

Setting	Specification
Copy file	File for higher system addresses you created
To directory	`%NETMDMP%\MASTER\DB`

When you restart the client after setup has been completed, the client will connect to the higher system based on the information in the file for higher system addresses.

(2) Syntax in the file for higher system addresses

The file for higher system addresses contains mappings for multiple connection targets. The client connects to the higher systems by means of the IP addresses corresponding to the host names as described in this file.

The following shows the syntax in the file for higher system addresses:

File name

`SERVERIP.ini`

Format

```
[host-name]
IPaddress=IP-address
[#-filecheck]
key=Programcheck
```

Description

host-name

Specifies the host name of a connection target for the client. This specification is not case sensitive. If the same host name is specified more than once, the first specification is used.

IP-address

Specifies the IP address that is to be associated with the host whose name is specified.

Multiple combinations of a host name and an IP address can be specified in the file.

Example

The following shows an example of a file for higher system addresses:

```
[host001]
IPaddress=10.100.100.20
[host005]
IPaddress=10.100.100.15
[host007]
IPaddress=10.100.100.57
[#-filecheck]
key=Programcheck
```

Note the following points when creating a file for higher system addresses:

- If an IP address based connection error occurs, the erroneous host name and IP address combination are deleted.
- If the `#-filecheck` line is removed, the file for higher system addresses is deleted.
- Entries in the file for higher system addresses must consist of alphanumeric characters.
- If the client is running Windows 98 or Windows Me, specifying a space or tab character within the brackets enclosing a host name will cause the host name to be recognized as invalid, resulting in an error.

6.6 Settings for dial-up connections

In a WAN environment using dial-up connections, JP1/Software Distribution starts after a line connection is made; however, a connection can also be established by performing auto-dialup when a JP1/Software Distribution system starts. Dial-up connections can be used for the following types of connections:

- Connecting from a client to the managing server or a relay system
- Connecting from a relay system to the managing server
- Connecting from the managing server to a relay system

A dial-up connection cannot be used to establish a connection from the managing server to a client or from a relay system to a client.

In a system in which managing servers are configured in a hierarchy, a dial-up connection cannot be used to connect from the central manager to a relay manager.

For details about dial-up connections with the remote control facility, see the manual *Job Management Partner 1/ Remote Control Description and Operator's Guide*.

6.6.1 Prerequisites

(1) Required applications

To use a dial-up connection, you must have the applications (services) listed below (if the OS is Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, Windows Vista, Windows Server 2003, or Windows XP, no application (service) is required):

OS	Application (service)
Windows NT Service Pack 3 or later	Remote access service
Windows 2000	
Windows Me or Windows 98	Dial-up network

You must set the information about the connection-destination host in the remote access service or dial-up network.

Also, during installation or setup of JP1/Software Distribution, you must specify whether a dial-up connection is to be used, and (if so) you must set the user name and a password for dialing.

(2) Facilities that can be used through a dial-up connection

The following table lists the facilities that can be used through a dial-up connection for each program menu that corresponds to a component.

Table 6–3: Facilities that can be used through a dial-up connection

Component	Subcomponent	Program menu	Supported
Server[#1]	Server facilities	N/A (Basic facility)[#2]	Y
		Setup	--
		CSV Output Utility	--
	Remote Installation Manager	**Remote Installation Manager**	--
		Unarchiver	--
		Inventory Viewer	--
	Database Manager	**Database Manager**	--

Component	Subcomponent	Program menu	Supported
OpenView Linkage	N/A	N/A	--
OpenView Gateway Server	N/A	N/A	--
Relay system[#1]	Relay system facilities	N/A (Basic facility)	Y
		CSV Output Utility	--
		Setup	--
	Remote Installation Manager	**Remote Installation Manager**	--
		Unarchiver	--
Client	Client	N/A (Basic facility)	Y
		Local System Viewer	--
		Register in ID Group	Y
		Client Manager	--
		Execute Job Backlog	Y
		Update User Information	--
		Setup	--
		Report to Server	Y
	Package Setup Manager	**Package Setup Manager**	Y
	Additional facility	N/A	Y
	Distribution facility by Visual Test 6.0	N/A	--
	Distribution facility by Visual Test 6.5	N/A	--
Packager	N/A	**Packager**	Y
Asset Information Manager Subset	N/A	N/A	--
Automatic Installation Tool	N/A	**Automatic Installation Tool**	--
Startup Kit facility support tool	N/A	N/A	--

Legend:

Y: Can be used through a dial-up connection.

--: Cannot be used through a dial-up connection, or communication is disabled.

N/A: There is no applicable subcomponent or program menu.

#1

For details about dial-up connections for client facilities of relay managers or relay systems, look down the *Component* column to the *Client* entry.

#2

This is the basic facility that is available in an environment where a server, relay system, or client is installed. There is no special program menu.

(3) Notes on dial-up connections

Note the following points about establishing dial-up connections:

- A client that connects to multiple relay systems can also use a dial-up connection. To do so, all the relay systems to be connected to must be installed in a LAN on the same router.
- Relay systems in two or more hierarchies that are connected through a dial-up connection will not work.

- To set a connection destination in a telephone book using the remote access service, use the telephone book of the system.
- If Windows XP, Windows 2000 Professional, or Windows NT Workstation is used in a managing server or relay system, it cannot establish connection simultaneously with multiple clients or relay systems by dial-up connection.
- If an application other than JP1/Software Distribution has already established connection with the same destination by means of a dial-up connection, JP1/Software Distribution uses that connection. In such a case, connection will not be broken when JP1/Software Distribution processing is completed. You must end the connection by disconnecting from the first application that established the connection or use the OS functionality to specify a timeout setting for dial-up connections.
- In the dialog box displayed by choosing **Internet Options** from the **Tools** menu of Microsoft Internet Explorer, if the **Dial whenever a network connection is not present** option is selected on the **Connections** page, be sure to use the OS functionality to specify a timeout setting for dial-up connections. Such a setting will enable Microsoft Internet Explorer to dial automatically when JP1/Software Distribution is not connected, without user intervention, and will prevent a dial-up connection from going on indefinitely.
- If a connection is being established from a managing server to a relay system by a dial-up connection, an attempt to connect from a relay system to the managing server using a dial-up connection may fail. To avoid this, specify a value of 1 or greater for the **Retry count for establishing socket connection** when you set up the relay system.

6.6.2 Network settings for dial-up connections

To use dial-up connection, you must specify information about the connection destination. In the system at the connection destination, it is necessary to specify server settings and access permission settings.

This section describes the settings for the connection destination for each type of OS. It also describes the server settings and access permission settings.

(1) For Windows Server 2003 or Windows XP

The following describes the connection destination settings for Windows Server 2003 or Windows XP.

If Windows Server 2003 or Windows XP is being used as the server, in the OS settings related to remote access you need to specify server settings as well as access permission settings.

(a) Connection destination settings

To specify the connection destination settings:

1. From the **Start** menu, choose **Control Panel**, and then **Network Connections** (for Windows XP, from the **Start** menu, choose **Connect To**, and then **Show all connections**).
   The `Network Connections` folder opens.
2. Double-click on the **New Connection Wizard** icon.
   The New Connection Wizard starts. According to the displayed instruction, choose the **Next** button. The Network Connection Type dialog box appears.
3. Choose **Connect to the network at my workplace**.
   For **Network Connection Type**, select **Connect to the network at my workplace**, and then choose the **Next** button. A dialog box appears that lets you specify network connection.
4. Choose **Dial-up connection**.
   For **Network Connection**, choose **Dial-up connection**, and then choose the **Next** button. A dialog box appears that lets you specify **Connection name**.
5. Specify the host name of the connection destination.
   For **Connection Name**, specify the host name of the connection destination, and then choose the **Next** button. A dialog box appears that lets you specify a telephone number.
6. Enter the telephone number of the connection destination.
   Specify the telephone number of the connection-destination computer or network, and then choose the **Next** button. A dialog box appears that lets you specify **Anyone's use**.
7. Choose **Anyone's use**.

This enables the created connection to be used by all users.

8. Choose the **Next** button.

   A confirmation dialog box appears that indicates the end of the New Connection Wizard.

9. Choose the **Finish** button.

   The settings are saved, and a dialog box for establishing a dial-up connection with the specified destination appears. Specify the user name and password and check to see if the dial-up connection can be established as specified.

(2) For Windows 2000

The following describes the connection destination, server, and access permission settings for Windows 2000.

(a) Connection destination settings

To specify the connection destination settings:

1. From the **Start** menu, choose **Settings**.
2. From **Settings**, choose **Network and Dial-up Connections**, and then **Make New Connection**.

   The Internet Connection Wizard starts. According to the displayed instruction, choose the **Next** button. The Network Connection Type dialog box appears.
3. Select **Dial-up to private network**.

   For **Network Connection Type**, select **Dial-up to private network**, and then choose the **Next** button. A dialog box appears that lets you specify a phone number to dial.
4. Enter the telephone number of the connection destination.

   Specify the telephone number of the computer or network at the connection destination, and then choose the **Next** button. A dialog box appears that lets you specify connection availability.
5. Select **For all users**.

   This setting makes this connection available to all users.
6. Choose the **Next** button.

   A dialog box appears that lets you specify a name for this connection.
7. For **Type the name you want to use for this connection**, specify the host name of the connection destination.

   As the name of this connection, specify the host name of the connection destination.
8. Choose the **Finish** button.

   The settings are saved, and a dialog box for establishing a dial-up connection with the specified destination appears. Specify the user name and password and check to see if the dial-up connection can be established as specified.

(b) Server settings

Server settings must be specified at the destination of a dial-up connection. If Windows 2000 is being used as the server (not including Windows 2000 Professional), use the remote access service to specify the following server settings.

To specify server settings:

1. From the **Programs** menu, choose **Administrative Tools**, and then **Routing and Remote Access**.

   The management console of **Routing and Remote Access** opens.
2. In the tree, right-click on the icon of the local computer and choose **Configure and Enable Routing and Remote Access**.

   The Routing and Remote Access Server Setup Wizard starts. The following the displayed instructions, set up the remote access server. For details about setting up a remote access server, see the Windows help.

If Windows 2000 Professional is being used as the server, specify the server settings as part of the OS settings related to remote access.

(c) Remote access permission settings

Settings that enable login from clients must be specified at the destination of a dial-up connection. If Windows 2000 is being used as the server (not including Windows 2000 Professional), use the remote access service to specify the following access permission settings.

To specify remote access permission settings:

1. Check that the Routing and Remote Access service is running.
   If the Routing and Remote Access service is not running, open the Routing and Remote Access management console, right-click on the icon of the local computer, choose **All Task**, and then choose **Start**.
2. From **Settings**, choose **Network and Dial-up Connections**, and then **Incoming Connections**.
   The Incoming Connections Properties dialog box appears.
3. Choose the **Users** tab.
4. Select the user name of the client to be connected, and then choose the **OK** button.
   Login from the selected client is now possible.

If Windows 2000 Professional is being used as the server, specify the access permission settings as part of the OS settings related to remote access.

(3) For Windows NT 4.0

The following describes the connection destination, server, and access permission settings for Windows NT 4.0

(a) Connection destination settings

You must specify the connection destination settings in the phonebook provided by Windows NT 4.0. The following shows the setup method:

Creating a new phonebook

If there is no phonebook in the system, create one and then specify the connection destination settings.

To create a phonebook:

1. From the **Programs** menu, choose **Accessories**, and then **Dial-Up Networking**.
   After the message `The phonebook is empty. Press OK to add an entry` is displayed, choose the **OK** button to display the New Phonebook Entry Wizard.
2. For the name of the phonebook entry, enter the host name of the connection destination (host name).
   Choose the **Next** button to display the Server dialog box. If you select **I know all about phonebook entries and would rather edit the properties directly**, you can specify settings in the Edit entry and modem properties dialog box.
   For details about the setup method, see *Editing the existing phonebook* below.
3. Select the **I am calling the Internet** option.
   For other options, specify as appropriate for the user environment. Choose the **Next** button to display the Modem or Adapter dialog box.
4. From the list of devices, select a connection port.
   Choose the **Next** button to display the Phone Number dialog box.
5. Enter the telephone number of the connection destination.
   Choose the **Next** button to display the New Phonebook Entry wizard.
6. Choose the **Finish** button.
   A phonebook that contains the connection destination information is created.

Editing the existing phonebook

If the system already has a phonebook, you can specify the connection destination settings by editing the phonebook.

To edit the existing phonebook:

1. From the **Programs** menu, choose **Accessories**, and then **Dial-Up Networking**.
   The Dial-Up Networking dialog box appears.
2. From **More**, choose **Edit entry and modem Properties**.
   The Edit Phonebook Entry dialog box appears.
3. On the **Basic** page, enter the entry name (host name) and telephone number of the connection-destination host.
4. On the **Server** page, choose **TCP/IP** for **Network Protocols**.
5. Choose the **OK** button.
   A phonebook entry that contains the connection destination information is created.

(b) Server settings

Server settings must be specified at the destination of a dial-up connection. If Windows NT 4.0 is being used as the server, use the remote access service to specify the following server settings.

To specify server settings:

1. From **Control Panel**, choose **Network**, and then **Remote Access Service**.
2. Choose **Network**, and select **TCP/IP**.
3. Choose the **TCP/IP** configuration button, and then select **Use static address pool**.
4. Specify **Begin** and **End**.

(c) Remote access permission settings

Settings that enable login from clients must be specified at the destination of a dial-up connection. If Windows NT 4.0 is being used as the server, use the remote access service to specify the following access permission settings.

To specify remote access permission settings:

1. Start **Remote Access Admin**.
   Check that the remote access service is running. If it is not running, from the **Server** menu, choose **Start Remote Access Service**.
2. From the **Users** menu, choose **Permissions**.
3. Select the user name of the client whose login is to be permitted.
   Select the user name of the client who will be allowed to make connection and select the **Grant dial-in Permission to User** option.

(4) For Windows Me or Windows 98

To establish connection with a higher system from Windows Me or Windows 98 by means of a dial-up connection, you must use **Dial-Up Networking** to specify connection destination settings.

The following shows how to specify connection destination settings.

For Windows Me

To specify connection destination settings:

1. From the **Programs** menu, choose **Accessories**, **Communications**, and then **Dial-Up Networking**.
   The Dial-Up Networking dialog box appears.
2. In the Make New Connection dialog box, in **Type a name for the computer you are dialing** enter the host name of the connection destination.
   Enter necessary information, such as the telephone number, by following the creation procedure in the Make New Connection dialog box.
3. When you finish specifying the settings, choose the **Finish** button.

For Windows 98

To specify connection destination settings:

1. From the **Programs** menu, choose **Accessories**, **Communications**, and then **Dial-Up Networking**.
   The Dial-Up Networking dialog box appears.
2. In the Make New Connection dialog box, in **Type a name for the computer you are dialing** enter the host name of the connection destination.
   Enter necessary information, such as the telephone number, by following the creation procedure in the Make New Connection dialog box.
3. When you finish specifying the settings, choose the **Finish** button.

6.6.3 Settings required during installation and setup of JP1/Software Distribution

(1) For JP1/Software Distribution Manager

In the Setup window, on the **Dial-up** page, select the **Dial-up connection** check box. Also specify the user ID, password, and domain name of the connection destination to be used for logging in.

(2) For JP1/Software Distribution Client

You can specify necessary information during either installation or setup.

To specify the information during installation, in the Network Settings dialog box, select the **Dial-up connection** check box. The Dial-up Settings dialog box appears. In this dialog box, specify the user ID, password, and domain name of the connection destination to be used for logging in.

To specify the information during setup, on the **Dial-up** page, select the **Dial-up Connection** check box. Next, specify the user ID, password, and domain name of the connection destination to be used for logging in.

6.6.4 Verifying remote access service settings

Before using a dial-up connection, verify that the connection can be established correctly. To do this, manually establish a connection using the dial-up connection application provided by Windows, and ping the local host and the connection destination host. Alternate between the connection source and the connection destination about five times to ensure that a solid ping response is received and that the IP address does not change.

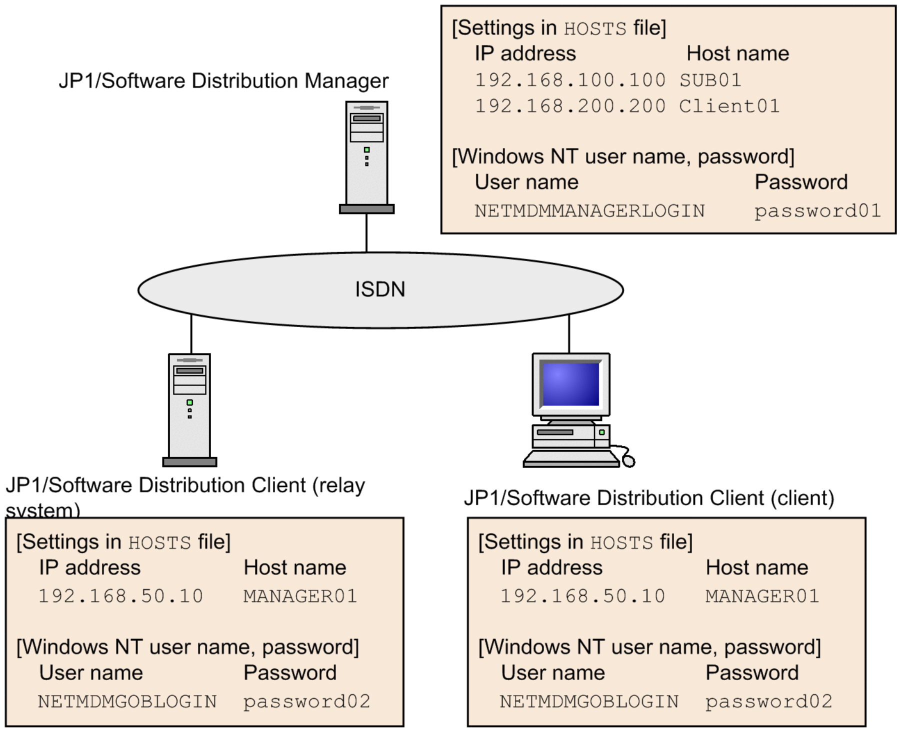
Note that if an IP address is used, the ping should be sent using the normal TCP/IP IP address. If no response is received, a dial-up connection via the IP address cannot be used.

6.6.5 Example of settings for dial-up connections

The figure below shows an example of a configuration for setting up dial-up connections. In this configuration, the following dial-up connections are used:

- Connecting from the managing server to a relay system
- Connecting from a relay system to the managing server
- Connecting from a client to the managing server

Figure 6–20: Example of a dial-up connection configuration


JP1/Software Distribution Manager
ISDN
JP1/Software Distribution Client (relay system)
JP1/Software Distribution Client (client)

[Settings in HOSTS file]

IP address	Host name
192.168.100.100	SUB01
192.168.200.200	Client01

[Windows NT user name, password]

User name	Password
NETMDMMANAGERLOGIN	password01

[Settings in HOSTS file]

IP address	Host name
192.168.50.10	MANAGER01

[Windows NT user name, password]

User name	Password
NETMDMGOBLOGIN	password02

[Settings in HOSTS file]

IP address	Host name
192.168.50.10	MANAGER01

[Windows NT user name, password]

User name	Password
NETMDMGOBLOGIN	password02

(1) Phonebook settings

The following table shows the phonebook settings for the example.

Table 6–4: Example phonebook settings

Setting item	Setting in JP1/Software Distribution Manager	Settings in JP1/Software Distribution Client (relay system or client)
Entry name	Sub01	Manager01
Telephone number	Telephone number of JP1/Software Distribution Client (relay system)	Telephone number of JP1/Software Distribution Manager

(2) Remote access service settings in the server

The following table shows the IP address settings of the hosts in the example (start and end addresses).

Table 6–5: Example of remote access service settings in the server

Setting item	Setting in JP1/Software Distribution Manager	Settings in JP1/Software Distribution Client (relay system)	Settings in JP1/Software Distribution Client (client)
Start address	192.168.50.10	192.168.100.100	192.168.200.200
Finish address	192.168.50.13	192.168.100.101	192.168.200.201

The IP addresses of the remote access service client to be assigned to JP1/Software Distribution SubManager and JP1/Software Distribution Client should be different so that their network IDs are different.

The IP addresses of the remote access service server to be specified in JP1/Software Distribution SubManager and JP1/Software Distribution Client should also be different so that their network IDs are different.

(3) Remote access permission settings

The user name of the client who will be connecting must be selected and **Grant dial-in Permission to User** must be selected. The following table shows the remote access permission settings for the example.

Table 6–6: Example of remote access permission settings

Setting item	Setting in JP1/Software Distribution Manager	Settings in JP1/Software Distribution Client (relay system)
User name for whom login permission is to be granted	User name of JP1/Software Distribution Client	User name of JP1/Software Distribution Manager

(4) JP1/Software Distribution installation and setup settings

The following table shows the settings made during installation and setup of JP1/Software Distribution for the example.

Table 6–7: Example of JP1/Software Distribution installation and setup settings

Setting item	Setting in JP1/Software Distribution Manager	Settings in JP1/Software Distribution Client (relay system and client)
User name	`NETMDMJOBLOGIN`	`NETMDMMANAGERLOGIN`
Password	`password02`	`password01`
Domain name	Domain name of JP1/Software Distribution Client (relay system)	Domain name of JP1/Software Distribution Manager

The Windows NT user name and password at each host must be the same as the settings at the connection destination.

Appendixes

A. Processes of JP1/Software Distribution

This appendix lists and explains the resident processes of JP1/Software Distribution. You can use this appendix as a reference when you desire to monitor processes.

For details about the processes of JP1/Remote Control, see the manual *Job Management Partner 1/Remote Control Description and Operator's Guide*.

A.1 Processes of JP1/Software Distribution Manager

The table below lists the processes that are made resident when JP1/Software Distribution Manager is used. The parentheses following a process name enclose the number of instances of the process that can be executed concurrently.

Table A–1: Processes of JP1/Software Distribution Manager

Process name	Function	Supported OS	Conditions for making the process resident
`schserv(1)`	Process for monitoring scheduled jobs	All OSs supported by the product	Always resident
`srvmain(1)`	Process for managing all jobs and inventories	All OSs supported by the product	Always resident
`dmdryctl(1)`	Process for controlling host searches	All OSs supported by the product	Always resident
`dmpadm(1)`	Main process started automatically from a service	All OSs supported by the product	Always resident
`dmpsite(1)`	Process for the relay system facility	All OSs supported by the product	JP1/Software Distribution Manager is a relay manager.
`dmpwtcp(1)`	Process for receiving startup requests	All OSs supported by the product	JP1/Software Distribution Manager is a relay manager.
`dmpicron(1)`	Process for scheduling	All OSs supported by the product	JP1/Software Distribution Manager is a relay manager.
`dmpsetup(1)`	Process for GUI installation	All OSs supported by the product	Both of the following conditions are met: • JP1/Software Distribution Manager is a relay manager. • The user who installed JP1/Software Distribution Manager has logged on.
`alertsrv(1)`	Process for starting system monitoring automatically	All OSs supported by the product	Both of the following conditions are met: • JP1/Software Distribution Manager is a relay manager. • **Monitor the system** is selected during setup.
`inetinfo(1)`	Process of Microsoft Internet Information Services	All OSs supported by the product	Asset Information Manager Subset is running.

A.2 Processes of JP1/Software Distribution Client

The tables below list the processes that are made resident when JP1/Software Distribution Client is used.

(1) Relay system processes

The table below lists the processes that are made resident when JP1/Software Distribution Client (relay system) is used. The parentheses following a process name enclose the number of instances of the process that can be executed concurrently.

Table A–2: Processes of JP1/Software Distribution Client (relay system)

Process name	Function	Supported OS	Conditions for making the process resident
`schserv(1)`	Process for monitoring scheduled jobs	All OSs supported by the product	Always resident
`srvmain(1)`	Process for managing all jobs and inventories	All OSs supported by the product	Always resident
`dmpsite(1)`	Process for the relay system facility	All OSs supported by the product	Always resident
`dmpwtcp(1)`	Process for receiving startup requests	All OSs supported by the product	Always resident
`dmpicron(1)`	Process for scheduling	All OSs supported by the product	Always resident
`dmpserv(1)`	Main process started automatically from a service	All OSs supported by the product	Always resident
`dmpsetup(1)`	Process for GUI installation	All OSs supported by the product	The user who installed JP1/Software Distribution Client (relay system) has logged on.
`dmpusers(1)`	Process for extending the functions that are available when Package Setup Manager is used with non-Administrator user permissions	All OSs supported by the product	**Run the client with non-Administrator user permissions** was selected during setup.
`alertsrv(1)`	Process for starting system monitoring automatically	All OSs supported by the product	**Monitor the system** was selected during setup.

(2) Client processes

The table below lists the processes that are made resident when JP1/Software Distribution Client (client) is used. The parentheses following a process name enclose the number of instances of the process that can be executed concurrently.

Table A–3: Processes of JP1/Software Distribution Client JP1/Software Distribution Client (client)

Process name	Function	Supported OS	Conditions for making the process resident
`dmpwtcp(1)`	Process for receiving start requests	All OSs supported by the product	**Client starts automatically at system boot** is selected during setup.
`dmpicron(1)`	Process for scheduling	All OSs supported by the product	**Client starts automatically at system boot** is selected during setup.
`dmpserv(1)`	Main process started automatically from a service	• Windows 8 • Windows Server 2012 • Windows 7 • Windows Server 2008 • Windows Vista • Windows Server 2003 • Windows XP • Windows 2000 • Windows NT 4.0	**Client starts automatically at system boot** is selected during setup.

Process name	Function	Supported OS	Conditions for making the process resident
`dmpstrup(1)`	Main process started automatically	• Windows Me • Windows 98	**Client starts automatically at system boot** is selected during setup.
`dmpsetup(1)`	Process for GUI installation	• Windows Server 2003 • Windows XP • Windows 2000 • Windows NT 4.0	Either of the following condition combinations are met: Condition combination 1 (all conditions are met): • **Client starts automatically at system boot** is selected during setup. • **Run the client with non-Administrator user permissions** is not selected during setup. • The user who installed JP1/Software Distribution Client has logged on. Condition combination 2 (all conditions are met): • **Client starts automatically at system boot** is selected during setup. • **Run the client with non-Administrator user permissions** is selected during setup. • A user with Administrator permissions has logged on.
`dmpusers(1)`	Process for extending the facilities available to non-Administrator user permissions when using Package Setup Manager or the **Execute Job Backlog** icon	• Windows 8 • Windows Server 2012 • Windows 7 • Windows Server 2008 • Windows Vista • Windows Server 2003 • Windows XP • Windows 2000 • Windows NT 4.0	The process is made resident if either of the following condition combinations are met: Condition combination 1 (all conditions are met): • **Client starts automatically at system boot** is selected during setup. • **Run the client with non-Administrator user permissions** is selected during setup. Condition combination 2 (all conditions are met): • **Client starts automatically at system boot** is not selected during setup. • **Run the client with non-Administrator user permissions** is selected during setup. • **Use the Package Setup Manager or Execute Job Backlog command when a client is not resident** is selected during setup.
`alertsrv(1)`	Process for starting system monitoring automatically	• Windows 8 • Windows Server 2012 • Windows 7 • Windows Server 2008 • Windows Vista • Windows Server 2003 • Windows XP • Windows 2000 • Windows NT 4.0	Both of the following conditions are met: • **Client starts automatically at system boot** is selected during setup. • **Monitor the system** is selected during setup.
`artsrv9x(1)`	Process for starting system monitoring automatically	• Windows Me • Windows 98	Both of the following conditions are met: • **Client starts automatically at system boot** is selected during setup. • **Monitor the system** is selected during setup.

B. List of Port Numbers

This appendix describes the port numbers used by JP1/Software Distribution, as well as the directions in which data passes through a firewall.

B.1 Port numbers

The table below lists the port numbers used for JP1/Software Distribution.

These are the port numbers that are set as the defaults at the time of product release. The table shows the protocols and the port number set for each service name.

Table B–1: Port numbers used for JP1/Software Distribution

Port number	Protocol	Service name	Description
`30000`	TCP	`netmdm`	JP1/Software Distribution server
`30001`	TCP	`netmdmw`	Relay server
`30002`	TCP and UDP	`netmdmclt`	Relay/client startup request
`30008`	TCP	None	Database connection (Embedded RDB)
`30010`	TCP	None	Database connection (Embedded RDB of Asset Information Manager Subset)
`20049`	TCP	None	OpenView Linkage
`22296`	UDP	`netmdmipmclt`	Multicast distribution
`22294`	UDP	`netmdmipm`	Multicast distribution resend request
`22295`	TCP	`netmdmgw`	JP1/Software Distribution HTTP Gateway

B.2 Directions in which data passes through a firewall

The following table shows the directions in which data passes through a firewall.

Table B–2: Directions in which data passes through a firewall

Programs requiring setup	Port number/ protocol	Service name	Direction in which data passes through a firewall
JP1/Software Distribution Manager, JP1/Software Distribution Client	`30000/tcp`	`netmdm`	• *From* JP1/Software Distribution Manager (lower manager) *to* JP1/Software Distribution Manager (higher manager) • *From* JP1/Software Distribution Client (relay system) *to* JP1/Software Distribution Manager • *From* JP1/Software Distribution Client (client) *to* JP1/Software Distribution Manager
JP1/Software Distribution Client	`30001/tcp`	`netmdmw`	• *From* JP1/Software Distribution Client (lower relay system) *to* JP1/Software Distribution Client (higher relay system) • *From* JP1/Software Distribution Client (client) *to* JP1/Software Distribution Client (relay system)
JP1/Software Distribution Manager, JP1/Software Distribution Client	`30002/tcp`	`netmdmclt`	• *From* JP1/Software Distribution Manager (higher manager) *to* JP1/Software Distribution Manager (lower manager) • *From* JP1/Software Distribution Manager *to* JP1/Software Distribution Client (relay system)

Programs requiring setup	Port number/ protocol	Service name	Direction in which data passes through a firewall
JP1/Software Distribution Manager, JP1/Software Distribution Client	`30002/tcp`	`netmdmclt`	• *From* JP1/Software Distribution Manager *to* JP1/Software Distribution Client (client) • *From* JP1/Software Distribution Client (higher relay system) *to* JP1/Software Distribution Client (lower relay system) • *From* JP1/Software Distribution Client (relay system) *to* JP1/Software Distribution Client (client)
JP1/Software Distribution Manager, JP1/Software Distribution Client	`30002/udp`	`netmdmclt`	• *From* JP1/Software Distribution Manager (higher manager) *to* JP1/Software Distribution Manager (lower manager) • *From* JP1/Software Distribution Manager *to* JP1/Software Distribution Client (relay system) • *From* JP1/Software Distribution Manager *to* JP1/Software Distribution Client (client) • *From* JP1/Software Distribution Client (higher relay system) *to* JP1/Software Distribution Client (lower relay system) • *From* JP1/Software Distribution Client (relay system) *to* JP1/Software Distribution Client (client)
JP1/Software Distribution Manager (OpenView Linkage)	`20049/tcp`	None	*Between* a PC containing HP NNM and OpenView Linkage *and* a JP1/Software Distribution NNM gateway server (in both directions)
JP1/Software Distribution Manager, JP1/Software Distribution Client	`22296/udp`	`netmdmipmclt`	• *From* JP1/Software Distribution Manager *to* JP1/Software Distribution Client (client) • *From* JP1/Software Distribution Client (relay system) *to* JP1/Software Distribution Client (client)
JP1/Software Distribution Manager, JP1/Software Distribution Client	`22294/udp`	`netmdmipm`	• *From* JP1/Software Distribution Client (client) *to* JP1/Software Distribution Manager • *From* JP1/Software Distribution Client (client) *to* JP1/Software Distribution Client (relay system)

Note

`22295/tcp` (`netmdmgw`) is the port used for communication between a relay manager or relay system and HTTP Gateway when the relay manager or relay system and HTTP Gateway are installed on the same PC.

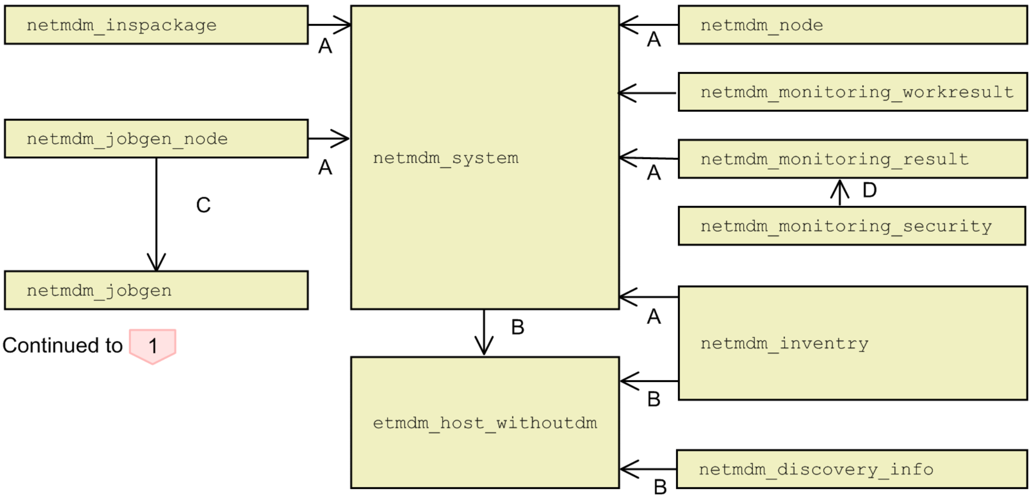
C. Structure of the Relational Database

This appendix describes the structure of the type of relational database supported by JP1/Software Distribution Manager.

C.1 Relationships among relational database tables

Figures C-1 through C-5 show the relationships among the relational database tables.

Figure C–1: Relationships among relational database tables (1/5)

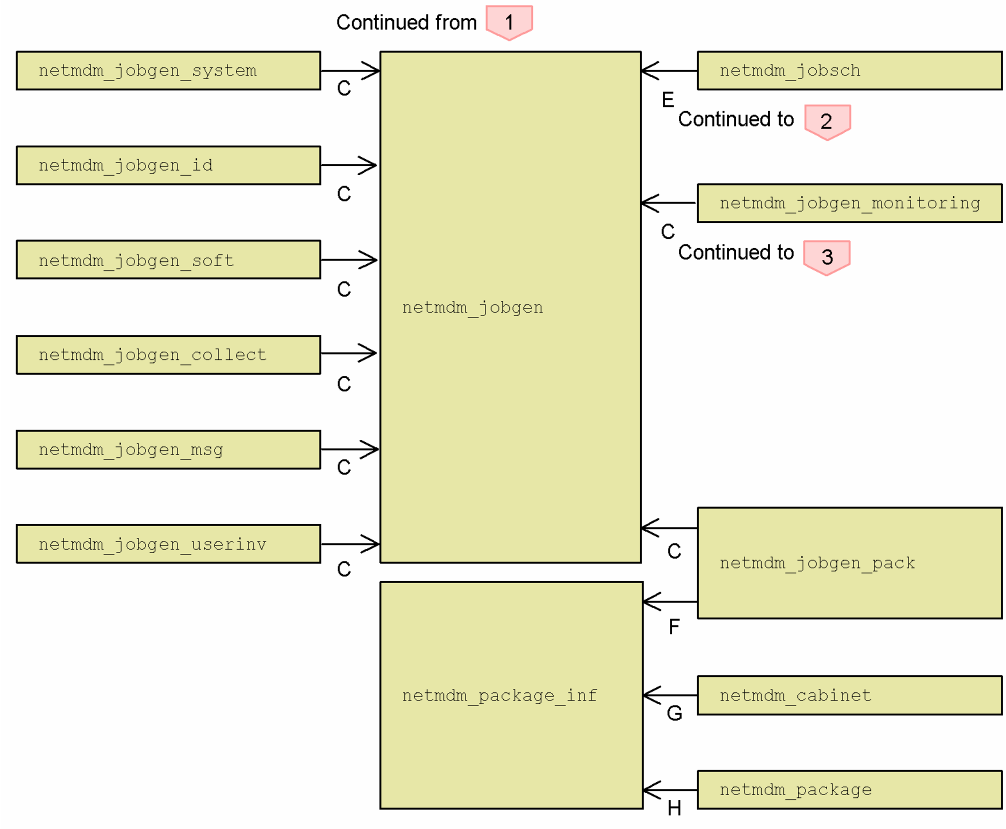


Legend:

→ : Related table

A: Associated with dm_nodename
B: Associated with dm_macaddress
C: Associated with dm_folder1, dm_folder2, dm_folder3, dm_folder4, and dm_jobgenname
D: Associated with all items in netmdm_monitoring_result

Figure C–2: Relationships among relational database tables (2/5)

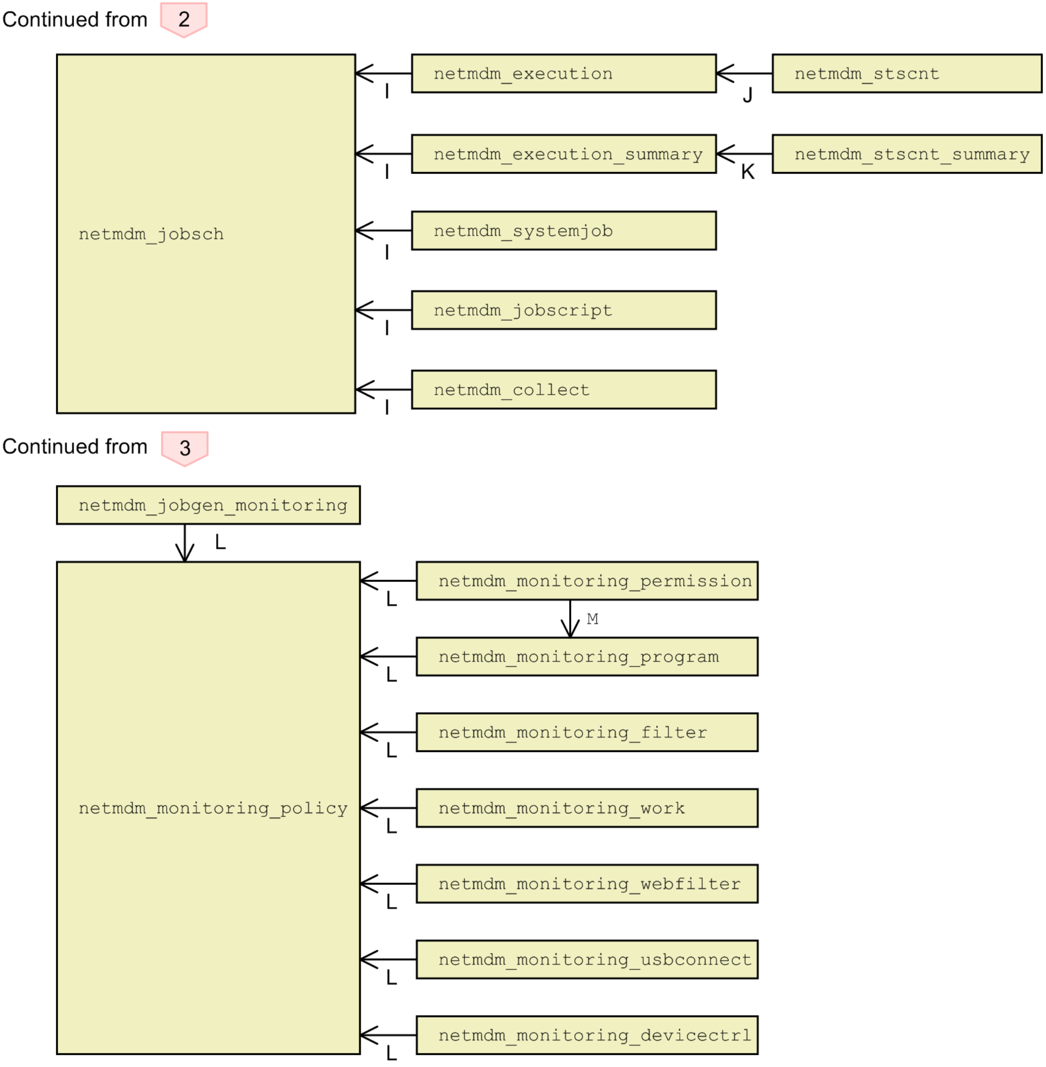


Legend:

⟶ : Related table

C: Associated with dm_folder1, dm_folder2, dm_folder3, dm_folder4, and dm_jobgenname
E: Associated with dm_jobgenname
F: Associated with dm_cabinetid, dm_packageid, dm_version, and dm_generation
G: Associated with dm_dmtype and dm_cabinetid
H: Associated with dm_packagefilename

Figure C–3: Relationships among relational database tables (3/5)



Legend:

→ : Related table

I: Associated with dm_jobno

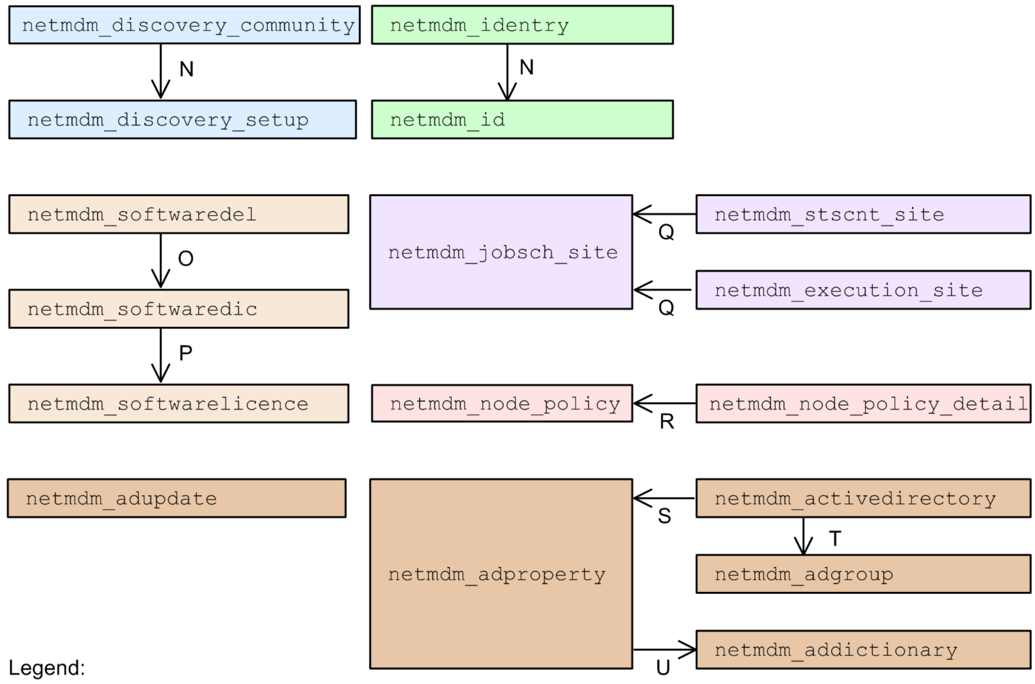
J: Associated with dm_jobno and dm_sitename

K: Associated with dm_jobno and dm_primarykey

L: Associated with dm_policyname

M: Associated with dm_policyname and dm_sepnumber

Figure C–4: Relationships among relational database tables (4/5)

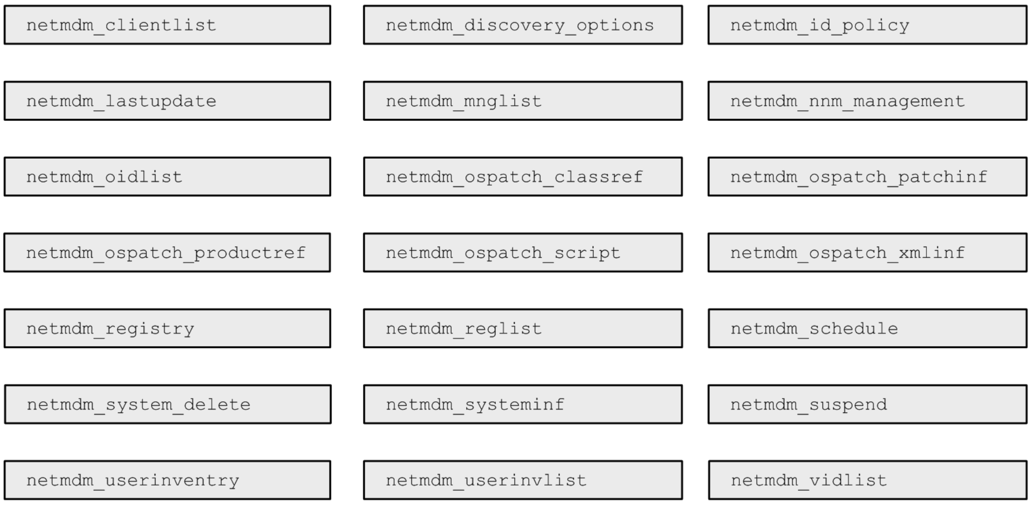


Legend:

→: Related tables

N: Related to `dm_ setup_key`.
O: Related to `dm_ppname` and `dm_sversion`.
P: Related to `dm_filename`, `dm_createdate`, and `dm_filesize`.
Q: Related to `dm_jobno`.
R: Related to `dm_infotype` and `dm_number`.
S: `dm_adguid` and `dm_linkadguid` are related.
T: Related to `dm_adguid`; also, `dm_adguid` and `dm_groupguid` are related.
U: `dm_propertyname` and `dm_propertyname` are related.

Figure C–5: Relationships among relational database tables (5/5)



C.2 List of relational database tables

The following table lists the relational database tables in alphabetical order.

Table C–1: Relational database tables

Table name	Overview	See
`netmdm_activedirectory`	Stores information about domains, computers, users, OUs, and groups.	*C.3*
`netmdm_addictionary`	Manages the correspondence between the property attribute names and display names of the domains, computers, users, OUs, and groups managed by Active Directory.	*C.4*
`netmdm_adgroup`	Manages the relationships between a group and its members.	*C.5*
`netmdm_adproperty`	Stores property information about computers, users, OUs, and groups.	*C.6*
`netmdm_adupdate`	Stores the latest flag information that was updated when linkage to Active Directory was established.	*C.7*
`netmdm_cabinet`	Stores information about a package cabinet.	*C.8*
`netmdm_clientlist`	Stores a search results list obtained by searching the software inventory by file name for each client.	*C.9*
`netmdm_collect`	Stores information on remote collection jobs and *Collect files from client to relay system* jobs.	*C.10*
`netmdm_discovery_community`	Stores a community name specified in host search settings.	*C.11*
`netmdm_discovery_info`	Stores the host information obtained by host search.	*C.12*
`netmdm_discovery_options`	Stores the option settings for host search.	*C.13*
`netmdm_discovery_setup`	Stores host search settings.	*C.14*
`netmdm_execution`	Stores the execution status of each package for each host that is a target of executed jobs.	*C.15*
`netmdm_execution_site`	Stores the execution status of each package for each host that is subject to ID group jobs executed at a relay system.	*C.16*
`netmdm_execution_summary`	Stores information about each all-lower-clients job executed at the central manager.	*C.17*
`netmdm_host_withoutdm`	Stores information about a host on which JP1/Software Distribution is not installed.	*C.18*
`netmdm_id`	Stores the ID groups handled by JP1/Software Distribution.	*C.19*
`netmdm_id_policy`	Stores conditions (policy) for automatic maintenance of ID groups.	*C.20*
`netmdm_identry`	Stores the clients registered in each ID group.	*C.21*
`netmdm_inspackage`	Stores the package installation status for each client.	*C.22*
`netmdm_inventry`	Stores system information for each client.	*C.23*
`netmdm_jobgen`	Stores job definition information.	*C.24*
`netmdm_jobgen_collect`	Stores information about remote collection specified in a job.	*C.25*
`netmdm_jobgen_id`	Stores job definition information for processing ID groups and ID group entries.	*C.26*
`netmdm_jobgen_monitoring`	Stores information about the software operation monitoring specified in a job.	*C.27*
`netmdm_jobgen_msg`	Stores the following part of the job definition information: information about the message to be sent to the client	*C.28*
`netmdm_jobgen_node`	Stores the following part of the job definition information: information about the hosts that are targets of executed jobs.	*C.29*

Table name	Overview	See
`netmdm_jobgen_pack`	Stores the following part of the job definition information: package information specified in the job.	*C.30*
`netmdm_jobgen_soft`	Stores the following part of the job definition information: information about a software search job.	*C.31*
`netmdm_jobgen_system`	Stores information needed to link system configuration information an ID group.	*C.32*
`netmdm_jobgen_userinv`	Stores the following part of the job definition information: job information for user inventory.	*C.33*
`netmdm_jobsch`	Stores header information for job execution status.	*C.34*
`netmdm_jobsch_site`	Stores header information for the execution status of an ID group job that was executed at a relay system.	*C.35*
`netmdm_jobscript`	Stores job script file during remote installation.	*C.36*
`netmdm_lastupdate`	Stores the last update date and time of certain tables.	*C.37*
`netmdm_mnglist`	Stores a search list used by a *Get software information from client* job.	*C.38*
`netmdm_monitoring_devicectrl`	Stores the suppression or activation setting information for each device.	*C.39*
`netmdm_monitoring_filter`	Stores filtering information to be used during logging for software operation monitoring.	*C.40*
`netmdm_monitoring_permission`	Stores permission conditions for software operation monitoring.	*C.41*
`netmdm_monitoring_policy`	Stores an operation monitoring policy for software operation monitoring.	*C.42*
`netmdm_monitoring_program`	Stores information about a program being monitored for software operation monitoring.	*C.43*
`netmdm_monitoring_result`	Stores suppression history for software operation monitoring.	*C.44*
`netmdm_monitoring_security`	Stores suppress history and operation history that are managed in the Operation Log List window.	*C.45*
`netmdm_monitoring_usbconnect`	Manages USB memory information whose access is excluded from being suppressed.	*C.46*
`netmdm_monitoring_webfilter`	Manages the Web access log filtering setting.	*C.47*
`netmdm_monitoring_work`	Stores information about programs from which operation times are acquired.	*C.48*
`netmdm_monitoring_workresult`	Stores information about the software operation times acquired by software operation monitoring.	*C.49*
`netmdm_nnm_management`	Stores information about OpenView Linkage.	*C.50*
`netmdm_node`	Stores destination information.	*C.51*
`netmdm_node_policy`	Stores conditions (policy) for maintaining host groups and ID groups automatically.	*C.52*
`netmdm_node_policy_detail`	Area reserved for function extensions.	--
`netmdm_oidlist`	Stores the software information obtained by using the **Search for Microsoft Office products** option of a *Get software information from client* job.	*C.53*
`netmdm_ospatch_classref`	Stores class information about patches.	*C.54*
`netmdm_ospatch_patchinf`	Stores patch information and acquired patch data.	*C.55*
`netmdm_ospatch_productref`	Stores information about the programs to be patched.	*C.56*

Table name	Overview	See
`netmdm_ospatch_script`	Stores script files for installing patches.	*C.57*
`netmdm_ospatch_xmlinf`	Stores the version of the patch information file.	*C.58*
`netmdm_package`	Stores the package and installation script body.	*C.59*
`netmdm_package_inf`	Stores the package attribute information.	*C.60*
`netmdm_registry`	Stores the registry information for a client.	*C.61*
`netmdm_reglist`	Stores the registry collection items.	*C.62*
`netmdm_schedule`	Stores the schedule of a registered job.	*C.63*
`netmdm_softwaredel`	Stores information about the software that was deleted from software inventory.	*C.64*
`netmdm_softwaredic`	Stores the results of searching software inventory at a client.	*C.65*
`netmdm_softwarelicence`	Stores the number of software licenses.	*C.66*
`netmdm_stscnt`	Stores the job execution status expressed as a combination of host and package subject to job execution.	*C.67*
`netmdm_stscnt_site`	Stores the execution status of ID group jobs executed at a relay system, expressed as a combination of host and package.	*C.68*
`netmdm_stscnt_summary`	Stores the execution status of an all-lower-clients job executed from the central manager, expressed as a combination of host and package.	*C.69*
`netmdm_suspend`	Stores information about whether processing is suspended.	*C.70*
`netmdm_system`	Stores system configuration information.	*C.71*
`netmdm_system_delete`	Stores the deletion history of system configuration information.	*C.72*
`netmdm_systeminf`	Stores the database format.	*C.73*
`netmdm_systemjob`	Stores the system information for JP1/Software Distribution.	*C.74*
`netmdm_userinventry`	Stores user inventory information.	*C.75*
`netmdm_userinvlist`	Stores a list of user inventory items.	*C.76*
`netmdm_vidlist`	Stores the software information obtained by using the **Search for anti-virus products** option of a *Get software information from client* job.	*C.77*

Legend:

--: Not applicable

The following sections provide details for all tables.

The tables in these sections use the following conventions:

- The value in the *Size* column is in bytes.
- An entry in *Key No.* indicates a sort key (reference item). The lower the key number, the higher the priority. Records in a table are sorted in ascending order on the basis of the key values.

C.3 netmdm_activedirectory

This table stores information about domains, computers, users, organizational units (OUs), and groups.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_adname	VARCHAR2	255	varchar	255	MVARCHAR	255	Domain name, user name, computer name, OU name, and group name	2
dm_adtype	NUMBER	10	int	4	INTEGER	--	Type of information acquired from Active Directory: • 0x00000000: Domain name • 0x00000001: Computer name • 0x00000002: User name • 0x00000003: OU name • 0x00000004: Group name	3
dm_adguid	VARCHAR2	32	varchar	32	MVARCHAR	32	ID that is set for this object in Active Directory.	1
dm_upperadguid	VARCHAR2	32	varchar	32	MVARCHAR	32	ID of the object to which this object belongs. The highest domain is NULL.	--
dm_manageradguid	VARCHAR2	32	varchar	32	MVARCHAR	32	ID of the manager if this object is a computer and a manager is set for it.	--
dm_usrlinkadguid	VARCHAR2	32	varchar	32	MVARCHAR	32	User ID to be assigned to a user if this object is a computer.	--
dm_nodename	VARCHAR2	64	varchar	64	MVARCHAR	64	Working key when it can be assigned to netmdm_system. NULL if no assignment can be made.	--
dm_hierarchicalinf	VARCHAR2	2,000	varchar	2,000	MVARCHAR	2,000	Hierarchical information of this object.	--
dm_keyvalue	VARCHAR2	2,000	varchar	2,000	MVARCHAR	2,000	Value of this object's assignment key.	--
dm_host	VARCHAR2	255	varchar	255	MVARCHAR	255	Acquisition-source host information. Host name or IP address.	--
dm_gettype	NUMBER	1	tinyint	1	SMALLINT	--	Flag that indicates whether an object is acquired with OU specification. 0: Acquired with OU specification 1: Not acquired with OU specification.	--

Legend:

--: Not applicable

C.4 netmdm_addictionary

This table manages the correspondence between the property attribute names and display names of the domains, computers, users, organizational units (OUs), and groups managed by Active Directory.

`dm_propertyname` in the `netmdm_adproperty` table is assigned to `dm_propertyname` in this table.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
`dm_propertyname`	`VARCHAR2`	2,000	`varchar`	2,000	`MVARCHAR`	2,000	Property attribute name	--
`dm_displayname`	`VARCHAR2`	2,000	`varchar`	2,000	`MVARCHAR`	2,000	Property display name	--
`dm_adtype`	`NUMBER`	10	`int`	4	`INTEGER`	--	Property information type: • `0x00000000`: Domain name • `0x00000001`: Computer name • `0x00000002`: User name • `0x00000003`: OU name • `0x00000004`: Group name	1
`dm_displayno`	`NUMBER`	10	`int`	4	`INTEGER`	--	Property display order Map table description order	2

Legend:

--: Not applicable

C.5 netmdm_adgroup

This table manages the relationships between a group and its members.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
`dm_groupguid`	`VARCHAR2`	32	`varchar`	32	`MVARCHAR`	32	ID indicating the group to which this object belongs	1
`dm_adguid`	`VARCHAR2`	32	`varchar`	32	`MVARCHAR`	32	ID of this object	2

C.6 netmdm_adproperty

This table stores property information about computers, users, organizational units (OUs), and groups.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
`dm_propertyname`	`VARCHAR2`	2,000	`varchar`	2,000	`MVARCHAR`	2,000	Property attribute name	--
`dm_propertyvalue`	`VARCHAR2`	2,000	`varchar`	2,000	`MVARCHAR`	2,000	Property attribute value	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_linkadguid	VARCHAR2	32	varchar	32	MVARCHAR	32	ID indicating the object to which this property belongs	1
dm_host	VARCHAR2	255	varchar	255	MVARCHAR	255	Acquisition-source host information Host name or IP address	--

Legend:

--: Not applicable

C.7 netmdm_adupdate

This table stores the latest flag information that was updated when linkage to Active Directory was established.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_updateflg_ou	VARCHAR2	16	varchar	16	MVARCHAR	16	OU update flag managed by each Active Directory	--
dm_updateflg_com	VARCHAR2	16	varchar	16	MVARCHAR	16	Computer update flag managed by each Active Directory	--
dm_updateflg_usr	VARCHAR2	16	varchar	16	MVARCHAR	16	User update flag managed by each Active Directory	--
dm_host	VARCHAR2	255	varchar	255	MVARCHAR	255	Acquisition-source host information Host name or IP address	1
dm_invocationid	VARCHAR2	2,000	varchar	2,000	MVARCHAR	2,000	Check flag managed by each Active Directory	--
dm_ckey	VARCHAR2	2,000	varchar	2,000	MVARCHAR	2,000	Computer assignment key	--
dm_ukey	VARCHAR2	2,000	varchar	2,000	MVARCHAR	2,000	User assignment key	--
dm_updateflg_grp	VARCHAR2	16	varchar	16	MVARCHAR	16	Update flag of groups managed by each Active Directory	--

Legend:

--: Not applicable

C.8 netmdm_cabinet

This table stores information about a package cabinet.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_dmtype	CHAR	1	char	1	CHAR	1	Type of Packager used for packaging: • C: WS (UNIX) • D: PC (Windows)	1
dm_cabinetid	CHAR	2	char	2	MCHAR	2	Cabinet ID: • Space: Management record for each Packager type • Other: Cabinet ID	2
dm_cabinetname	VARCHAR2	32	varchar	32	MVARCHAR	32	Cabinet name	--
dm_systeminf	BLOB	--	image	--	BINARY	96	JP1/Software Distribution Manager management information	--

Legend:

--: Not applicable

C.9 netmdm_clientlist

This table stores a search results list obtained by searching the software inventory by file name for each client.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_ppno	NUMBER	10	int	4	INTEGER	--	Internal information of JP1/Software Distribution (program product number)	2
dm_nodename	VARCHAR2	64	varchar	64	MVARCHAR	64	Client name	1
dm_serchdate	CHAR	19	char	19	CHAR	19	Search date for specified software	--
dm_pathname	VARCHAR2	255	varchar	255	MVARCHAR	255	Path to specified software	3

Legend:

--: Not applicable

C.10 netmdm_collect

This table stores information on remote collection jobs and *Collect files from client to relay system* jobs.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_jobname	VARCHAR2	64	varchar	64	MVARCHAR	64	Job name	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_jobno	CHAR	16	char	16	MCHAR	16	Number assigned to the job automatically	1
dm_mngfilename	CHAR	8	char	8	MCHAR	8	Remote collection management filename	2
dm_mngnumber	NUMBER	10	int	4	INTEGER	--	Remote collection management number	--
dm_nodename	VARCHAR2	64	varchar	64	MVARCHAR	64	Host name of the client subject to remote collection	--
dm_servpath	BLOB	--	image	--	BINARY	260	Name of the file containing the remote-collected file	--

Legend:

--: Not applicable

C.11 netmdm_discovery_community

This table stores a community name specified in host search settings.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_setup_key	NUMBER	10	int	4	INTEGER	--	Key information for identifying the host search settings	1
dm_cmnty_name	VARCHAR2	255	varchar	255	MVARCHAR	255	Community name	--
dm_order_key	NUMBER	3	tinyint	1	SMALLINT	--	Order of the community name	2

Legend:

--: Not applicable

C.12 netmdm_discovery_info

This table stores the host information obtained by host search.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_mac_address	VARCHAR2	12	varchar	12	VARCHAR	12	MAC address delimited by a lower-case hexadecimal character and stored without the characters	1
dm_ip_address	VARCHAR2	15	varchar	15	VARCHAR	15	IP address delimited by the decimal point symbol (.)	--
dm_ip_addr_num	NUMBER	10	numeric	10	DECIMAL	10	dm_ip_address expressed as a numeric value	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_subnet_mask	VARCHAR2	15	varchar	15	VARCHAR	15	Subnet mask	--
dm_nwaddr	VARCHAR2	15	varchar	15	VARCHAR	15	Network address	--
dm_nodetype	NUMBER	2	tinyint	1	SMALLINT	--	Node type: • 0: Computer • 1: Router • 2: Bridge • 3: Repeater • 4: Printer • 5: RMON	--
dm_hostname	VARCHAR2	80	varchar	80	MVARCHAR	80	Host name	--
dm_description	VARCHAR2	256	varchar	256	MVARCHAR	256	Description	--
dm_last_dsry_time	DATE	--	datetime	8	TIMESTAMP	--	Last search date and time	--

Legend:

--: Not applicable

C.13 netmdm_discovery_options

This table stores an option setting for host search.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_validity	NUMBER	10	int	4	INTEGER	--	Validity period of search results	--

Legend:

--: Not applicable

C.14 netmdm_discovery_setup

This table stores host search settings.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_setup_key	NUMBER	10	int	4	INTEGER	--	Key information for identifying the search settings	1

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_mgmt_name	VARCHAR2	64	varchar	64	MVARCHAR	64	Name	--
dm_from_ip	VARCHAR2	15	varchar	15	VARCHAR	15	Start IP address for host search	--
dm_from_ip_num	NUMBER	10	numeric	10	DECIMAL	10	dm_from_ip expressed as a numeric value	--
dm_to_ip	VARCHAR2	15	varchar	15	VARCHAR	15	End IP address for host search	--
dm_to_ip_num	NUMBER	10	numeric	10	DECIMAL	10	dm_to_ip expressed as a numeric value	--
dm_schedule	NUMBER	1	tinyint	1	SMALLINT	--	• 0: Immediate execution • 1: Scheduled execution	--
dm_schdl_period	NUMBER	10	int	4	INTEGER	--	• NULL: Immediate execution • 0: Daily • 1: Weekly • 2: Monthly	--
dm_schdl_hour	NUMBER	2	tinyint	1	SMALLINT	--	Time set for scheduled execution (hour)	--
dm_schdl_min	NUMBER	2	tinyint	1	SMALLINT	--	Time set for scheduled execution (minute)	--
dm_schdl_day	NUMBER	2	tinyint	1	SMALLINT	--	If dm_schdl_period is Weekly: • 1: Sunday • 2: Monday • 3: Tuesday • 4: Wednesday • 5: Thursday • 6: Friday • 7: Saturday If dm_schdl_period is Monthly, this is the scheduled execution date.	--
dm_exec_status	NUMBER	10	int	4	INTEGER	--	Host search status: • 0: Completed • 1: Cancelled • 2: Error • 3: Executing • 4: Unexecuted	--
dm_total_count	NUMBER	10	numeric	10	DECIMAL	--	Total number of addresses in the IP address range	--
dm_exec_count	NUMBER	10	numeric	10	DECIMAL	--	Total number of IP addresses over which host search was executed	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_start_time	DATE	--	datetime	8	TIMESTAMP	--	Date and time the host search began	--
dm_end_time	DATE	--	datetime	8	TIMESTAMP	--	Date and time the host search ended	--
dm_lock	NUMBER	2	tinyint	1	SMALLINT	--	Internal lock and option settings for host search: • 0: Not locked - Acquire host name - Acquire information from all terminals - Do not check startup • 1: Currently locked - Acquire host name - Acquire information from all terminals - Do not check startup • 2: Not locked - Acquire host name - Acquire information from router - Do not check startup • 3: Not locked - Do not acquire host name - Acquire information from all terminals - Do not check startup • 4: Not locked - Do not acquire host name - Acquire information from router - Do not check startup • 5: Not locked - Do not acquire host name - Acquire information from all terminals - Check startup • 6: Not locked - Acquire host name - Acquire information from all terminals - Check startup • 7: Currently locked - Acquire host name - Acquire information from router - Do not check startup • 8: Currently locked - Do not acquire host name - Acquire information from all terminals - Do not check startup	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_lock	NUMBER	2	tinyint	1	SMALLINT	--	• 9: Currently locked - Do not acquire host name - Acquire information from router - Do not check startup • 10: Currently locked - Do not acquire host name - Acquire information from all terminals - Check startup • 11: Currently locked - Acquire host name - Acquire information from all terminals - Check startup	--
dm_next_exec_time	DATE	--	datetime	8	TIMESTAMP	--	Next host search date and time Null in the case of immediate execution	--

Legend:

--: Not applicable

C.15 netmdm_execution

This table stores the execution status of each package for each host that is a target of executed jobs. For jobs that do not use packages, such as a *Get system information from client* job, one record is created for each host.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_jobno	CHAR	16	char	16	MCHAR	16	Number assigned to the job automatically	--
dm_jobkind	CHAR	1	char	1	CHAR	1	Job type code: • A: *Acquire collected files from relay system* • C: *Batch delete packages on relay system* • D: *Install package* • E: *Report job deletion* • F: *Resume file transfer* • G: *Collect files from client* • H: *Hold report* • I: *Get software information from client* • J: *Send package, allow client to choose*	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_jobkind	CHAR	1	char	1	CHAR	1	• K: *Delete collected files from relay system* • L: *ID group operation* • M: *Transfer package to relay system* • N: *Get system configuration information* • O: *Edit system configuration information* • P: *Suspend file transfer* • S: *Collect files from client to relay system* • T: *Hold-report release* • U: *Transfer user inventory schema to client* • V: *Get system configuration information* • Y: *Transfer registry collection definition* • 1: *Report message* • 8: *Set the software monitoring policy* • 9: *Get software monitoring information from the client*	--
dm_jobtype	CHAR	1	char	1	CHAR	1	Job type subcode: • D: Daily execution • F: Forced installation • M: Monthly execution • U: User installation • W: Weekly execution • Space: Subcode not specified	--
dm_clientname	VARCHAR2	64	varchar	64	MVARCHAR	64	Name of the lowest system at the destination (client) that is stored in the dm_nodename column	2
dm_primarykey	CHAR	16	char	16	MCHAR	16	Primary key (number assigned to each job detail)	1
dm_sitename	VARCHAR2	64	varchar	64	MVARCHAR	64	Name of the highest system at the destination that is stored in the dm_nodename column	--
dm_status	CHAR	6	char	6	CHAR	6	Status code	--
dm_installdate	DATE	--	datetime	8	TIMESTAMP	--	Installation completion date	--
dm_dmtype	CHAR	1	char	1	MCHAR	1	Type of Packager used for packaging: • C: WS (UNIX) • D: PC (Windows)	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_cabinetid	CHAR	2	char	2	MCHAR	2	ID of the cabinet containing the package	--
dm_packageid	VARCHAR2	44	varchar	44	MVARCHAR	44	Package ID	--
dm_version	VARCHAR2	8	varchar	8	MVARCHAR	8	Package version	--
dm_generation	VARCHAR2	4	varchar	4	MVARCHAR	4	Package generation number	--
dm_deliverytime	DATE	--	datetime	8	TIMESTAMP	--	Package transfer date and time	--
dm_installtime	DATE	--	datetime	8	TIMESTAMP	--	Installation date and time	--
dm_packagename	VARCHAR2	50	varchar	50	MVARCHAR	50	Package name	--
dm_deletetime	DATE	--	datetime	8	TIMESTAMP	--	Deletion date and time	--
dm_eventtime	DATE	--	datetime	8	TIMESTAMP	--	Job execution date and time	--
dm_systeminf	BLOB	--	image	--	BLOB	--	JP1/Software Distribution Manager management information	--
dm_idname	VARCHAR2	32	varchar	32	MVARCHAR	32	ID group name	--
dm_userstatus	CHAR	2	char	2	MCHAR	2	User status (in hexadecimal)	--
dm_detailstatus	VARCHAR2	28	varchar	28	MVARCHAR	28	Maintenance information	--
dm_execday	VARCHAR2	2	varchar	2	MVARCHAR	2	Execution date of periodic job	--
dm_execweek	NUMBER	3	tinyint	1	SMALLINT	--	Periodic job execution day of the week: • 0x01: Sunday • 0x02: Monday • 0x04: Tuesday • 0x08: Wednesday • 0x10: Thursday • 0x20: Friday • 0x40: Saturday	--
dm_exectiming	VARCHAR2	1	varchar	1	MVARCHAR	1	Job execution timing: • B: When client starts • E: While client is running • S: When client terminates	--
dm_nodename	VARCHAR2	255	varchar	255	MVARCHAR	255	Route information about the destination that consists of an ID	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
`dm_nodename`	`VARCHAR2`	255	`varchar`	255	`MVARCHAR`	255	key for operations (host ID or node identification key)	--
`dm_attrflag`	`RAW`	1	`binary`	1	`BINARY`	1	Attribute flag: • `0x00`: Job of the local system • `0x01`: Job transferred from another system	--
`dm_userinfoption`	`RAW`	1	`binary`	1	`BINARY`	1	User inventory acquisition option: • `0x00`: Acquire both system information and user inventory information • `0x01`: Acquire only user inventory information	--
`dm_managername`	`VARCHAR2`	64	`varchar`	64	`MVARCHAR`	64	Supervising manager name	--
`dm_orgprimekey`	`CHAR`	16	`char`	16	`MCHAR`	16	Primary key for an all-lower-clients job	--
`dm_nodename2`	`VARCHAR2`	255	`varchar`	255	`MVARCHAR`	255	Route information about the destination that consists of a node identification key (host name or IP address)	--
`dm_woloption`	`CHAR`	1	`char`	1	`VARCHAR`	1	Client control and distribution method: • `0x01`: Start the destination • `0x02`: Shut down the destination • `0x04`: Execute multicast distribution • `0x08`: Distribute (even to suspended destination) • `0x40`: Do not archive the software operation information	--
`dm_splitsize`	`NUMBER`	10	`int`	4	`INTEGER`	--	Split size	--
`dm_transsize`	`NUMBER`	10	`int`	4	`INTEGER`	--	Transfer package size	--
`dm_transinterval`	`NUMBER`	10	`int`	4	`INTEGER`	--	Distribution interval	--
`dm_downlevel`	`CHAR`	1	`char`	1	`MCHAR`	1	Hierarchical level	--

Legend:

--: Not applicable

C.16 netmdm_execution_site

This table stores the execution status of each package for each host that is subject to ID group jobs executed at a relay system (*Install package* and *Send package, allow client to choose* jobs).

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
`dm_jobno`	`CHAR`	16	`char`	16	`MCHAR`	16	Number assigned to the job automatically	--
`dm_jobkind`	`CHAR`	1	`char`	1	`CHAR`	1	Job type code: • `D`: *Install package* • `J`: *Send package, allow client to choose*	--
`dm_jobtype`	`CHAR`	1	`char`	1	`CHAR`	1	Job type subcode: • `F`: *Forced installation* • `U`: *User installation* • Space: *Subcode not specified*	--
`dm_clientname`	`VARCHAR2`	64	`varchar`	64	`MVARCHAR`	64	Name of the lowest system at the destination (client) that is stored in the `dm_nodename` column	--
`dm_primarykey`	`CHAR`	16	`char`	16	`MCHAR`	16	Primary key (number assigned to each job detail)	1
`dm_sitename`	`VARCHAR2`	64	`varchar`	64	`MVARCHAR`	64	Name of the highest system at the destination that is stored in the `dm_nodename` column	--
`dm_status`	`CHAR`	6	`char`	6	`CHAR`	6	Status code	--
`dm_installdate`	`DATE`	--	`datetime`	8	`TIMESTAMP`	--	Installation completion date	--
`dm_dmtype`	`CHAR`	1	`char`	1	`MCHAR`	1	Type of Packager used for packaging: • `C`: WS (UNIX) • `D`: PC (Windows)	--
`dm_cabinetid`	`CHAR`	2	`char`	2	`MCHAR`	2	ID of the cabinet containing the package	--
`dm_packageid`	`VARCHAR2`	44	`varchar`	44	`MVARCHAR`	44	Package ID	--
`dm_version`	`VARCHAR2`	8	`varchar`	8	`MVARCHAR`	8	Package version	--
`dm_generation`	`VARCHAR2`	4	`varchar`	4	`MVARCHAR`	4	Package generation number	--
`dm_deliverytime`	`DATE`	--	`datetime`	8	`TIMESTAMP`	--	Distribution date and time	--
`dm_installtime`	`DATE`	--	`datetime`	8	`TIMESTAMP`	--	Installation date and time	--
`dm_packagename`	`VARCHAR2`	50	`varchar`	50	`MVARCHAR`	50	Package name	--
`dm_deletetime`	`DATE`	--	`datetime`	8	`TIMESTAMP`	--	Deletion date and time	--
`dm_eventtime`	`DATE`	--	`datetime`	8	`TIMESTAMP`	--	Job execution date and time	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_systeminf	BLOB	--	image	--	BLOB	--	JP1/Software Distribution Manager management information	--
dm_idname	VARCHAR2	32	varchar	32	MVARCHAR	32	ID group name	--
dm_userstatus	CHAR	2	char	2	MCHAR	2	User status (in hexadecimal)	--
dm_detailstatus	VARCHAR2	28	varchar	28	MVARCHAR	28	Maintenance information	--
dm_execday	VARCHAR2	2	varchar	2	MVARCHAR	2	Execution date for periodic job	--
dm_execweek	NUMBER	3	tinyint	1	SMALLINT	--	Periodic job execution day of the week: • 0x01: Sunday • 0x02: Monday • 0x04: Tuesday • 0x08: Wednesday • 0x10: Thursday • 0x20: Friday • 0x40: Saturday	--
dm_exectiming	VARCHAR2	1	varchar	1	MVARCHAR	1	Job execution timing: • B: When client starts • E: While client is running • S: When client terminates	--
dm_nodename	VARCHAR2	255	varchar	255	MVARCHAR	255	Route information about the destination that consists of an ID key for operations (host ID or node identification key)	2
dm_nodename2	VARCHAR2	255	varchar	255	MVARCHAR	255	Route information about the destination that consists of a node identification key (host name or IP address)	--

Legend:

--: Not applicable

C.17 netmdm_execution_summary

This table stores information about an all-lower-clients job executed at the central manager.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_jobno	CHAR	16	char	16	MCHAR	16	Number assigned to the job automatically	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_nodename	VARCHAR2	255	varchar	255	MVARCHAR	255	Name of destination (including route)	1
dm_primarykey	CHAR	16	char	16	MCHAR	16	Primary key (number assigned to each job detail)	2
dm_status	CHAR	6	char	6	MCHAR	6	Status code	--

Legend:

--: Not applicable

C.18 netmdm_host_withoutdm

This table stores information about a host on which JP1/Software Distribution is not installed.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_macaddress	VARCHAR2	12	varchar	12	MVARCHAR	12	MAC address as hexadecimal lowercase letters without delimiting characters	1
dm_targetflag	NUMBER	3	tinyint	1	SMALLINT	--	Flag indicating whether the node is to be subject to detection: • 0: Subject to detection • 1: Not subject to detection • 2: Hold • 9: Remove	--
dm_name	VARCHAR2	80	varchar	80	MVARCHAR	80	Node name (normally the host name)	--
dm_description	VARCHAR2	255	varchar	255	MVARCHAR	255	Node description	--
dm_ipaddress	VARCHAR2	15	varchar	15	MVARCHAR	15	IP address	--
dm_subnet	VARCHAR2	15	varchar	15	MVARCHAR	15	Subnet mask	--
dm_nwaddr	VARCHAR2	15	varchar	15	MVARCHAR	15	Network address	--
dm_finddate	DATE	--	datetime	8	TIMESTAMP	--	First date and time the node was detected	--
dm_lastupdatetime	DATE	--	datetime	8	TIMESTAMP	--	Last date and time the node was updated	--
dm_nodetype	NUMBER	2	tinyint	1	SMALLINT	--	Node type: • 0: Computer • 1: Router • 2: Bridge	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_nodetype	NUMBER	2	tinyint	1	SMALLINT	--	• 3: Repeater • 4: Printer • 5: RMON	--
dm_ip_addr_num	NUMBER	10	numeric	10	DECIMAL	10	dm_ipaddress expressed in as numeric value	--

Legend:

--: Not applicable

C.19 netmdm_id

This table stores the ID groups handled by JP1/Software Distribution.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_genno	RAW	1	binary	1	BINARY	1	Generation number: • 0x01: ID group created by old interface • 0x02: ID group created by new interface	--
dm_idname	VARCHAR2	32	varchar	32	MVARCHAR	32	ID group name	1
dm_procflag	NUMBER	3	tinyint	1	SMALLINT	--	Processing flag: • 0x0000: Valid ID group • 0x0001: ID group being deleted	--
dm_attrflag	RAW	1	binary	1	BINARY	1	Attribute flag: • 0x00: ID group created in the local system • 0x01: ID group created by from the higher managing server	--

Legend:

--: Not applicable

C.20 netmdm_id_policy

This table stores conditions (policy) for automatically maintaining ID groups.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_infotype	NUMBER	10	int	4	INTEGER	--	Policy type: • 8: ID group is registered by means of a user inventory item.	--
dm_nodeattrrange	NUMBER	10	int	4	INTEGER	--	Node attributes to be grouped: • 0: All node types • 1: Only client nodes	--
dm_condition1_string	VARCHAR2	64	varchar	64	MVARCHAR	64	Condition 1 (user inventory item) character string data	--
dm_condition1_logical	VARCHAR2	10	varchar	10	MVARCHAR	10	Logical operator between conditions 1 and 2	--
dm_condition2_string	VARCHAR2	64	varchar	64	MVARCHAR	64	Condition 2 (user inventory item) character string data	--
dm_condition2_logical	VARCHAR2	10	varchar	10	MVARCHAR	10	Logical operator between conditions 2 and 3	--
dm_condition3_string	VARCHAR2	64	varchar	64	MVARCHAR	64	Condition 3 (user inventory item) character string data	--
dm_condition3_logical	VARCHAR2	10	varchar	10	MVARCHAR	10	Logical operator between conditions 3 and 4	--
dm_condition4_string	VARCHAR2	64	varchar	64	MVARCHAR	64	Condition 4 (user inventory item) character string data	--
dm_condition4_logical	VARCHAR2	10	varchar	10	MVARCHAR	10	Logical operator between conditions 4 and 5	--
dm_condition5_string	VARCHAR2	64	varchar	64	MVARCHAR	64	Condition 5 (user inventory item) character string data	--
dm_condition5_logical	VARCHAR2	10	varchar	10	MVARCHAR	10	Logical operators between conditions 5 and 6	--
dm_condition6_string	VARCHAR2	64	varchar	64	MVARCHAR	64	Condition 6 (user inventory item) character string data	--
dm_condition6_logical	VARCHAR2	10	varchar	10	MVARCHAR	10	Logical operator between conditions 6 and 7	--
dm_condition7_string	VARCHAR2	64	varchar	64	MVARCHAR	64	Condition 7 (user inventory item) character string data	--
dm_condition7_logical	VARCHAR2	10	varchar	10	MVARCHAR	10	Logical operator between conditions 7 and 8	--
dm_condition8_string	VARCHAR2	64	varchar	64	MVARCHAR	64	Condition 8 (user inventory item) character string data	--
dm_condition8_logical	VARCHAR2	10	varchar	10	MVARCHAR	10	Logical operator between conditions 8 and 9	--
dm_condition9_string	VARCHAR2	64	varchar	64	MVARCHAR	64	Condition 9 (user inventory item) character string data	--
dm_condition9_logical	VARCHAR2	10	varchar	10	MVARCHAR	10	Logical operator between conditions 9 and 10	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_condition10_string	VARCHAR2	64	varchar	64	MVARCHAR	64	Condition 10 (user inventory item) character string data	--
dm_condition1_value	VARCHAR2	200	varchar	200	MVARCHAR	200	Value selected for condition 1 (user inventory item)	--
dm_condition2_value	VARCHAR2	200	varchar	200	MVARCHAR	200	Value selected for condition 2 (user inventory item)	--
dm_condition3_value	VARCHAR2	200	varchar	200	MVARCHAR	200	Value selected for condition 3 (user inventory item)	--
dm_condition4_value	VARCHAR2	200	varchar	200	MVARCHAR	200	Value selected for condition 4 (user inventory item)	--
dm_condition5_value	VARCHAR2	200	varchar	200	MVARCHAR	200	Value selected for condition 5 (user inventory item)	--
dm_condition6_value	VARCHAR2	200	varchar	200	MVARCHAR	200	Value selected for condition 6 (user inventory item)	--
dm_condition7_value	VARCHAR2	200	varchar	200	MVARCHAR	200	Value selected for condition 7 (user inventory item)	--
dm_condition8_value	VARCHAR2	200	varchar	200	MVARCHAR	200	Value selected for condition 8 (user inventory item)	--
dm_condition9_value	VARCHAR2	200	varchar	200	MVARCHAR	200	Value selected for condition 9 (user inventory item)	--
dm_condition10_value	VARCHAR2	200	varchar	200	MVARCHAR	200	Value selected for condition 10 (user inventory item)	--
dm_idname	VARCHAR2	32	varchar	32	MVARCHAR	32	ID group name at registration target	--

Legend:

--: Not applicable

C.21 netmdm_identry

This table stores the clients registered in each ID group.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_idname	VARCHAR2	32	varchar	32	MVARCHAR	32	ID group name	1
dm_nodename	VARCHAR2	64	varchar	64	MVARCHAR	64	Node name	2
dm_attributes	NUMBER	10	int	4	INTEGER	--	Node attribute: • 1: Client managed by the lower relay system • 2: Client managed by the managing server	3

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_attributes	NUMBER	10	int	4	INTEGER	--	• 3: Lower relay system managing the ID group	3
dm_procflag	NUMBER	3	tinyint	1	SMALLINT	--	Processing flag: • 0x0000: Valid ID group • 0x0001: ID group being deleted • 0x0002: ID group being registered	--
dm_sitename	VARCHAR2	64	varchar	64	MVARCHAR	64	• If dm_attributes is 1: Higher relay managing the ID of the client with dm_nodename • If dm_attributes is not 1: NULL	--
dm_nodename2	VARCHAR2	64	varchar	64	MVARCHAR	64	Node name (the value is not converted to lowercase letters)	--
dm_sitename2	VARCHAR2	64	varchar	64	MVARCHAR	64	• If the node attribute is 1: Only the ID group managed relay is valid (the value is not converted to lowercase letters) • Otherwise: NULL	--

Legend:

--: Not applicable

C.22 netmdm_inspackage

This table stores the package installation status for each client. You can search this table to determine the packages that are installed in each client.

Column name	Oracle		Microsoft SQL Server		Embedded RDB Edition		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_dmtype	CHAR	1	char	1	MCHAR	1	Type of Packager used for packaging: • C: WS (UNIX) • D: PC (Windows)	3
dm_cabinetid	CHAR	2	char	2	MCHAR	2	ID of the cabinet containing the package	--
dm_packageid	VARCHAR2	44	varchar	44	MVARCHAR	44	Package ID	2
dm_nodename	VARCHAR2	64	varchar	64	MVARCHAR	64	Client's host ID (node identification key if no host ID is used)	1
dm_newversion	VARCHAR2	8	varchar	8	MVARCHAR	8	Package version	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB Edition		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_newgeneration	VARCHAR2	4	varchar	4	MVARCHAR	4	Package generation number	--
dm_newdeliverydate	DATE	--	datetime	8	TIMESTAMP	--	Package transfer date	--
dm_newinstalldate	DATE	--	datetime	8	TIMESTAMP	--	Package installation date	--
dm_oldversion	VARCHAR2	8	varchar	8	MVARCHAR	8	Older version of package	--
dm_oldgeneration	VARCHAR2	4	varchar	4	MVARCHAR	4	Generation number of the older version of package	--
dm_olddeliverydate	DATE	--	datetime	8	TIMESTAMP	--	Transfer date of the older version of package	--
dm_oldinstalldate	DATE	--	datetime	8	TIMESTAMP	--	Installation date of the older version of package	--
dm_insstatus	CHAR	6	char	6	MCHAR	6	Status code (the left six digits of a job's maintenance code)	--
dm_installdate	DATE	--	datetime	8	TIMESTAMP	--	Installation date and time or software search date and time	--
dm_packagename	VARCHAR2	50	varchar	50	MVARCHAR	50	Package name	--
dm_capacity	NUMBER	10	int	4	INTEGER	--	Package size	--
dm_systeminf	BLOB	--	image	--	BINARY	960	JP1/Software Distribution Manager management information	--
dm_userstatus	CHAR	2	char	2	MCHAR	2	User status (in hexadecimal)	--
dm_drivetype	NUMBER	3	tinyint	1	SMALLINT	--	Drive type: • 0: Local drive • 1: Network drive	--

Legend:

--: Not applicable

C.23 netmdm_inventry

This table stores system information for each client. Each record contains detailed system information for one client (such as CPU type and free hard disk space).

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_nodename	VARCHAR2	64	varchar	64	MVARCHAR	64	Host name of the client	1

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_sysinfname	RAW	2	binary	1	SMALLINT	--	Type of system information	2
dm_exkind	CHAR	1	char	1	VARCHAR	1	Extension type of system information	3
dm_systeminf	VARCHAR2	200	varchar	200	MVARCHAR	200	Value of system information	--
dm_subinf	VARCHAR2	200	varchar	200	MVARCHAR	200	Subordinate information for system information	--

Legend:

--: Not applicable

The following table shows the values of the individual columns for each system information item:

System information	dm_sysinfname	dm_exkind	dm_systeminf
CPU type	0x01	• 1: Intel x86/Pentium • 2: COMPAQ Alpha or HP Alpha • 3: MIPS R Series • 4: Motorola PowerPC • 6: AMD • 7: Cyrix • 8: IDT • A: RISE • B: Hitachi SH • C: Transmeta • D: ARM • E: Intel IPF • F: AMD64 • G: Intel EM64T • 9: Other	See *CPU type* below.
Existence of coprocessor	0x02	0x00	• 1: Yes • 0: No
Installed RAM	0x03	0x00	Decimal value in megabytes
Workstation type (applicable to UNIX only)	0x04	0x00	UNIX machine type
CPU clock speed	0x05	0x00	CPU clock speed in MHz
Machine information	0x06	0x01: Manufacturer	PC manufacturer
		0x02: Model	PC model
Number of processors	0x07	0x00	Number of processors
WMI	0x08	0x00	Character string indicating the WMI version (if unavailable, N/A)

System information	dm_sysinfname	dm_exkind	dm_systeminf
Clock speed of the external CPU	`0x09`	`0x01`	Clock speed of the external CPU in MHz
OS	`0x10`	• `W`: Workstation • `P`: Personal computer	See *OS* below.
OS version	`0x12`	• `1`: Windows • `2`: Windows NT • `3`: Windows 95 • `4`: Windows 98 • `5`: Windows 2000 • `7`: Windows Me • `8`: Windows XP • `9`: Other • `B`: Windows Server 2003 • `C`: Windows Vista • `D`: Windows Server 2008 • `E`: Windows 7 • `F`: Windows Server 2008 R2 • `G`: Windows 8 • `H`: Windows Server 2012	*vvrr* • *vv*: Version • *rr*: Revision
OS build number/OS patch	`0x13`	`0x00`	In Windows: OS build number In UNIX: OS patch information
OS license (applicable to UNIX only)	`0x14`	`0x00`	• `S`: 2 user licenses • `E`: 8 user licenses • `B`: 16 user licenses • `U`: Unlimited user licenses
UNIX OS version	`0x15`	`0x39`	UNIX OS version
Owner	`0x16`	`0x00`	Owner name
Company name	`0x17`	`0x00`	Company name
OS sub-version	`0x18`	`0x00`	OS type + OS, as a character string Example of adding a service pack to the version: `Windows NT4.0 (Service Pack 1)`
Computer name	`0x19`	`0x00`	Computer name
OS information	`0x1A`	`0x00`: Name of OS family	OS type in characters:: • `Microsoft Windows` (for Windows 95, 98, or Windows Me) • `Microsoft Windows NT Workstation` • `Microsoft Windows NT Server` • `Microsoft Windows NT Enterprise Server`

System information	dm_sysinfname	dm_exkind	dm_systeminf
OS information	`0x1A`	`0x00`: Name of OS family	• `Microsoft Windows 2000 Professional` • `Microsoft Windows 2000 Server` • `Microsoft Windows 2000 Advanced Server` • `Microsoft Windows 2000 Datacenter Server` • `Microsoft Windows XP Home Edition` • `Microsoft Windows XP Professional` • `Microsoft(R) Windows(R) Server 2003,Standard Edition` • `Microsoft(R) Windows(R) Server 2003,Enterprise Edition` • `Microsoft(R) Windows(R) Server 2003,Datacenter Edition` • `Microsoft(R) Windows(R) Server 2003,Web Edition` • `Microsoft(R) Windows(R) Server 2003 Standard x64 Edition` • `Microsoft(R) Windows(R) Server 2003 Enterprise x64 Edition` • `Microsoft(R) Windows(R) Server 2003 Datacenter x64 Edition` • `MicrosoftR Windows Vista? Business`# • `MicrosoftR Windows Vista? Enterprise`# • `MicrosoftR Windows Vista? Ultimate`# • `MicrosoftR Windows Vista? Business x64 Edition`# • `MicrosoftR Windows Vista? Enterprise x64 Edition`# • `MicrosoftR Windows Vista? Ultimate x64 Edition`# • `MicrosoftR Windows ServerR 2008 Standard` • `MicrosoftR Windows ServerR 2008 Enterprise` • `MicrosoftR Windows ServerR 2008 Datacenter` • `MicrosoftR Windows ServerR 2008 Standard x64 Edition` • `MicrosoftR Windows ServerR 2008 Enterprise x64 Edition` • `MicrosoftR Windows ServerR 2008 Datacenter x64 Edition` • `MicrosoftR Windows ServerR 2008 Standard without Hyper-V` • `MicrosoftR Windows ServerR 2008 Enterprise without Hyper-V` • `MicrosoftR Windows ServerR 2008 Datacenter without Hyper-V`

System information	dm_sysinfname	dm_exkind	dm_systeminf
OS information	0x1A	0x00: Name of OS family	• MicrosoftR Windows ServerR 2008 Standard without Hyper-V x64 Edition • MicrosoftR Windows ServerR 2008 Enterprise without Hyper-V x64 Edition • MicrosoftR Windows ServerR 2008 Datacenter without Hyper-V x64 Edition • Microsoft Windows Server 2008 R2 Standard • Microsoft Windows Server 2008 R2 Enterprise • Microsoft Windows Server 2008 R2 Datacenter • Microsoft Windows 7 Professional • Microsoft Windows 7 Enterprise • Microsoft Windows 7 Ultimate • Microsoft Windows 7 Professional x64 Edition • Microsoft Windows 7 Enterprise x64 Edition • Microsoft Windows 7 Ultimate x64 Edition • Microsoft Windows 8 • Microsoft Windows 8 x64 Edition • Microsoft Windows 8 Pro • Microsoft Windows 8 Pro x64 Edition • Microsoft Windows 8 Enterprise • Microsoft Windows 8 Enterprise x64 Edition • Microsoft Windows Server 2012 Standard • Microsoft Windows Server 2012 Datacenter
		0x01: Domain type	Domain type in code: • 0: Stand-alone workstation • 1: Member workstation • 2: Stand-alone server • 3: Member server • 4: Backup domain controller • 5: Primary domain controller
		0x02: Detailed OS type	When the OS is not any of those listed below, the OS type code value that is set by entry type 0x10 is set as 5-byte character string expressed in decimal format. • 00258: Windows NT Workstation • 00514: Windows NT Server • 01538: Windows NT Enterprise Server

System information	dm_sysinfname	dm_exkind	dm_systeminf
OS information	`0x1A`	`0x02`: Detailed OS type	• `00777`: Windows 2000 Professional • `00521`: Windows 2000 Server • `01033`: Windows 2000 Advanced Server • `01289`: Windows 2000 Datacenter Server • `00780`: Windows XP Professional • `01804`: Windows XP Home Edition • `02062`: Microsoft Windows Server 2003, Standard Edition • `02318`: Microsoft Windows Server 2003, Enterprise Edition • `02574`: Microsoft Windows Server 2003, Datacenter Edition • `02830`: Microsoft Windows Server 2003, Web Edition • `03086`: Microsoft Windows Server 2003, Standard x64 Edition • `03342`: Microsoft Windows Server 2003, Enterprise x64 Edition • `03598`: Microsoft Windows Server 2003, Datacenter x64 Edition • `04111`: Windows Vista Business • `04367`: Windows Vista Enterprise • `04623`: Windows Vista Ultimate • `07183`: Windows Vista Business x64 Edition • `03343`: Windows Vista Enterprise x64 Edition • `07439`: Windows Vista Ultimate x64 Edition • `04880`: Microsoft Windows Server 2008, Standard • `04368`: Microsoft Windows Server 2008, Enterprise • `05392`: Microsoft Windows Server 2008 Datacenter • `03088`: Microsoft Windows Server 2008 Standard x64 Edition • `03344`: Microsoft Windows Server 2008 Enterprise x64 Edition • `03600`: Microsoft Windows Server 2008 Datacenter x64 Edition • `05648`: Microsoft Windows Server 2008 Standard without Hyper-V • `05904`: Microsoft Windows Server 2008 Enterprise without Hyper-V • `06160`: Microsoft Windows Server 2008 Datacenter without Hyper-V • `06416`: Microsoft Windows Server 2008 Standard without Hyper-V x64 Edition • `06672`: Microsoft Windows Server 2008 Enterprise without Hyper-V x64 Edition • `06928`: Microsoft Windows Server 2008 Datacenter without Hyper-V x64 Edition • `04882`: Microsoft Windows Server 2008 R2 Standard

System information	dm_sysinfname	dm_exkind	dm_systeminf
OS information	0x1A	0x02: Detailed OS type	• 04370: Microsoft Windows Server 2008 R2 Enterprise • 05394: Microsoft Windows Server 2008 R2 Datacenter • 00785: Windows 7 Professional • 04369: Windows 7 Enterprise • 04625: Windows 7 Ultimate • 05137: Windows 7 Professional x64 Edition • 03345: Windows 7 Enterprise x64 Edition • 07441: Windows 7 Ultimate x64 Edition • 07699: Windows 8 • 04371: Windows 8 Enterprise • 07955: Windows 8 Pro • 08211: Windows 8 x64 Edition • 03347: Windows 8 Enterprise x64 Edition • 08467: Windows 8 Pro x64 Edition • 05396: Windows Server 2012 Datacenter • 04884: Windows Server 2012 Standard
		0x03: Computer description	Description of the computer expressed as a character string
		0x04: Domain/Workgroup	Domain/work group expressed as a character string
		0x05: Logon user name	Logon user name expressed as a character string
		0x06: Full name of user	Full name of user expressed as a character string
		0x07: User description	Description of user expressed as a character string
		0x08: Current time zone	Time zone expressed as a numeric value
		0x09: Machine UUID	Machine UUID expressed as a character string
		0x0A: Machine serial number	Machine serial number expressed as a character string
		0x0B: Boot device	Startup device expressed as a character string
		0x0D: OS installation date/time	Installation date expressed as a character string
		0x0E: Last startup date/time	Last startup date/time expressed as a character string
		0x10: Locale	Locale expressed in UINT
		0x11: OS language	OS language expressed in UINT
		0x12: Windows directory	Windows directory expressed as a character string
		0x13: System directory	System directory expressed as a character string
		0x14: OS serial number	OS serial number expressed as a character string
		0x15: Internet Explorer version	Internet Explorer version expressed as a character string
		0x16: Windows Installer	Windows Installer version expressed as a character string (if it has not been installed, N/A is set)

System information	dm_sysinfname	dm_exkind	dm_systeminf
OS information	0x1A	0x17: MBSA	Product version of the MBSA command line interface stored in *client-installation-directory*\CLIENT\MBSA (mbsacli.exe file) expressed as a character string If no value is stored, the following character string is set: - If WUA has been installed: "N/A (The Windows Update Agent is available)" - If WUA has not been installed: "N/A"
		0x18: Windows Update Agent	WUA version expressed as a character string (if WUA is not installed, "N/A" is set)
		0x19: WSUS computer ID	WSUS computer ID expressed as a character string
IE Patch	0x1B	- 0x01: Overall information - 0x02 to 0xFF: Division information (separated by a semicolon)	IE patch information expressed as a character string. (If there is no registry or the value is blank, character string N/A is set in 0x01 and 0x02.)
Client version	0x21	- 8: JP1/Software Distribution SubManager - 9: JP1/Software Distribution Client - A: JP1/Software Distribution Workstation - B: JP1/Software Distribution Manager - C: JP1/Software Distribution SubManager for UNIX - D: JP1/Software Distribution Client for UNIX	*vvrrss* - *vv*: Version - *rr*: Revision - *ss*: Restriction code
Drives	0x2F	Drives A-Z	Drive type expressed as one of the following character strings: - Removable hard disk - Network disk - CD-ROM
Free space	0x31	Drives A-Z For UNIX V5 or earlier: - 0x31: UNIX root partition number - 0x01 to 0x2F: Partition number other than for the UNIX root partition For UNIX version V6 or later and UNIX partition identification number:	Decimal value in megabytes

System information	dm_sysinfname	dm_exkind	dm_systeminf
Free space	0x31	• 0x01: UNIX root partition number • 0x02 to 0x2F: Partition number other than for the UNIX root partition	Decimal value in megabytes
Usable user memory size	0x32	0x00	Decimal value in megabytes
Usable system resource size	0x33	0x00	Decimal number in kilobytes
Name of UNIX special file	0x34	Corresponds to extended information 0x01 to 0x400x31	Name of special file
UNIX mount path name	0x35	Corresponds to extended information 0x01 to 0x400x31	Name of special file
Memory size	0x36	0x00: Available physical memory	Available physical memory in megabytes
		0x01: Available virtual memory	Available virtual memory in megabytes
		0x02: Total capacity of virtual memory	Total capacity of virtual memory in megabytes
		0x03: Size of page file	Size of page file in megabytes
Memory slot capacity	0x37	• 0x00: Single • From 0x01 on: Multiple	Memory slot capacity in megabytes
Bus type	0x40	0x00: Type of primary bus	Primary bus expressed as a character string
		0x01: Type of secondary bus	Secondary bus expressed as a character string
BIOS	0x41	0x00:BIOS manufacturer	BIOS manufacturer expressed as a character string
		0x01: BIOS release date/ time	BIOS release date/time expressed as a character string
		0x02: BIOS version	BIOS version expressed as a character string
		0x03: BIOS version (SMBIOS)	BIOS version of SMBIOS expressed as a character string
		0x04: AMT firmware version	AMT firmware version expressed as a character string
Keyboard	0x42	• 0x00: Single • From 0x01 on: Multiple	Keyboard expressed as a character string
Mouse	0x43	• 0x00: Single • From 0x01 on: Multiple	Mouse expressed as a character string
Number of mouse buttons	0x44	• 0x00: Single • From 0x01 on: Multiple	Number of mouse buttons expressed in UCHAR
Partition size	0x51	Drives A-Z	Decimal value in megabytes

System information	dm_sysinfname	dm_exkind	dm_systeminf
File system	`0x52`	Drives A-Z For UNIX, partition number (`0x01-0x2F`)	File system expressed as a character string
Hard disk interface	`0x53`	- `0x00`: Single - From `0x01` on: Multiple	Hard disk interface expressed as a character string
Number of hard disk partitions	`0x54`	- `0x00`: Single - From `0x01` on: Multiple	Number of hard disk partitions expressed in UINT
Hard disk capacity	`0x55`	- `0x00`: Single - From `0x01` on: Multiple	Hard disk capacity in megabytes
Model of hard disk	`0x56`	- `0x00`: Single - From `0x01` on: Multiple	Model of hard disk expressed as a character string
CD-ROM drive	`0x57`	- `0x00`: Single - From `0x01` on: Multiple	Name of CD-ROM drive expressed as a character string
BitLocker-based encryption information	`0x58`	Drives A-Z	BitLocker setting information - `0000000000`: Invalid - `0000000001`: Valid - `0000000002`: Unknown - `0000000003`: Valid (locked)
HIBUN FDE-based encryption information	`0x5A`	Drives A-Z	HIBUN FDE setting information - `0000000000`: Invalid - `0000000001`: Valid
Video driver	`0x61`	`0x00`	Video driver name
Video chip	`0x62`	`0x00`	Video chip name
VRAM	`0x63`	`0x00`	Decimal value in megabytes
Display	`0x64`	`0x00`	*xx* × *yy* *cc* colors: - *xx*: Width - *yy*: Length - *cc*: Number of colors
Monitor type	`0x65`	- `0x00`: Single - From `0x01` on: Multiple	Monitor type expressed as a character string
Sound card manufacturer	`0x66`	- `0x00`: Single - From `0x01` on: Multiple	Sound card manufacturer expressed as a character string
Product name of sound card	`0x67`	- `0x00`: Single - From `0x01` on: Multiple	Product name of sound card expressed as a character string

System information	dm_sysinfname	dm_exkind	dm_systeminf
MAC address	0x81	• 0x00: Single • From 0x01 on: Multiple	MAC address expressed in hexadecimal characters
Network adapter	0x82	• 0x00: Single • From 0x01 on: Multiple	Network adapter
Default router address	0x83	• 0x00: Single • From 0x01 on: Multiple	Default router address expressed as a character string
Subnet mask	0x84	• 0x00: Single • From 0x01 on: Multiple	Subnet mask expressed as a character string
IP address	0x85	• 0x00: Single • From 0x01 on: Multiple	IP address expressed as a character string. If there are multiple IP addresses, all addresses are linked together using a single space as the delimiter.
Primary DNS server address	0x86	• 0x00: Single • From 0x01 on: Multiple	Primary DNS server address expressed as a character string
Secondary DNS server address	0x87	• 0x00: Single • From 0x01 on: Multiple	Secondary DNS server address expressed as a character string
DHCP	0x88	• 0x00: Single • From 0x01 on: Multiple	Whether DHCP is enabled or disabled: • 0: Disabled • 1: Enabled
DHCP server address	0x89	• 0x00: Single • From 0x01 on: Multiple	DHCP server address expressed as a character string
Expiration date/time of DHCP lease	0x8A	• 0x00: Single • From 0x01 on: Multiple	Expiration date/time of DHCP lease expressed as a character string
Acquired date/time of DHCP lease	0x8B	• 0x00: Single • From 0x01 on: Multiple	Acquired date/time of DHCP lease expressed as a character string
WINS server address	0x8C	• 0x00: Single • From 0x01 on: Multiple	WINS server address expressed as a character string. If there are multiple WINS server addresses, all addresses are linked together using a single space as the delimiter.
Printer name	0x90	• 0x00: Single • From 0x01 on: Multiple	Printer name expressed as a character string
Shared name of printer	0x91	• 0x00: Single • From 0x01 on: Multiple	Shared name of printer expressed as a character string
Printer server name	0x92	• 0x00: Single	Printer server name expressed as a character string

System information	dm_sysinfname	dm_exkind	dm_systeminf
Printer server name	0x92	- From 0x01 on: Multiple	Printer server name expressed as a character string
Printer sheet size	0x93	- 0x00: Single - From 0x01 on: Multiple	Printer sheet size expressed as a character string
Printer driver	0x94	- 0x00: Single - From 0x01 on: Multiple	Printer driver expressed as a character string
Printer port	0x95	- 0x00: Single - From 0x01 on: Multiple	Printer port expressed as a character string
Printer type	0x96	- 0x00: Single - From 0x01 on: Multiple	Printer type expressed as a character string
Security-related	0xA0	0x01: Guest account	Guest account enabling status: - 0: Disabled - 1: Enabled - 2: No guest account
		0x02: Weak password	Account in which a weak password is set, as a character string. If no weak password exists, the following character string is set: - @None
		0x03: Time-unlimited password	Account in which a time-unlimited password is set, as a character string. If no time-unlimited password exists, the following character string is set: - @None
		0x04: Automatic logon setting	Automatic logon setting: - 0: Set - 1: Not set
		0x05: Shared folders	Shared folder availability: - 0: No shared folder - 1: A shared folder is available
		0x06: Restriction on anonymous connections	Restriction on anonymous connections: - 0: No restriction - 1: Restricted
		0x07: Screensaver	Screensaver setting: - 0: Disabled - 1: Enabled
		0x08: Password protection for screensaver	Screensaver password protection function setting: - 0: Disabled

System information	dm_sysinfname	dm_exkind	dm_systeminf
Security-related	0xA0	0x08: Password protection for screensaver	• 1: Enabled
		0x09: Power-on password	Power-on password setting: • 0: Not set • 1: Set • 2: Not installed • 3: Unknown
		0x0A: Windows Firewall settings	Windows Firewall settings: • 0: Disabled • 1: Enabled (permits exceptions) • 2: Enabled (does not permit exceptions)
		0x0B: Windows automatic updates	Windows automatic updates setting: • 0: Disabled • 1: Enabled
		0x0C: Unnecessary services	Whether unnecessary services are running: • 0: Not running • 1: Running
	0xA1	Local account names • 0x00: Single • From 0x01: Multiple	Local account names
	0xA2	Days since the Windows password was last updated • 0x00: Single • From 0x01: Multiple	Days since the Windows password was last updated
Distribution	0xA3	0x00	Linux distribution name
Security-related	0xA5	0x01: Turn off monitor (AC)	Time to turn off monitor (AC) (seconds) as a character string: • 0: Not set • 1-2147483647: Time to turn off power (seconds) • N/A: Unknown
		0x02: Turn off monitor (DC)	Time to turn off monitor (DC) (seconds) as a character string: • 0: Not set • 1-2147483647: Time to turn off power (seconds) • N/A: Unknown
		0x03: Processor Throttle (AC)	Processor power management status (processor throttle (AC)) as a character string: • N/A: Unknown • NONE: Always runs at the maximum performance level • CONSTANT: Always runs at the minimum performance level

System information	dm_sysinfname	dm_exkind	dm_systeminf
Security-related	0xA5	0x03: Processor Throttle (AC)	• DEGRADE: Uses the lock throttle stop function • ADAPTIVE: Selected based on the CPU state
		0x04: Processor Throttle (DC)	Processor power management status (processor throttle (DC)) as a character string: • N/A: Unknown • NONE: Always runs at the maximum performance level • CONSTANT: Always runs at the minimum performance level • DEGRADE: Uses the lock throttle stop function • ADAPTIVE: Selected based on the CPU state
		0x05: Turn off hard disks (AC)	Time to turn off hard disks (AC) (seconds) set as a character string: • 0: Not set • 1 to 2147483647: Time to turn off power (seconds) • N/A: Unknown
		0x06: Turn off hard disks (DC)	Time to turn off hard disks (DC) (seconds) set as a character string: • 0: Not set • 1 to 2147483647: Time to turn off power (seconds) • N/A: Unknown
		0x07: System standby/ Sleep (AC)	Time until the computer enters system standby or sleep mode (AC) (seconds) set as a character string: • 0: Not set • 1 to 2147483647: Elapsed time (seconds) • N/A: Unknown
		0x08: System standby/ Sleep (DC)	Time until the computer enters system standby or sleep mode (DC) (seconds) set as a character string: • 0: Not set • 1 to 2147483647: Elapsed time (seconds) • N/A: Unknown
		0x09: System hibernates (AC)	Time until the computer enters hibernation mode (AC) (seconds) set as a character string: • 0: Not set • 1 to 2147483647: Elapsed time (seconds) • N/A: Unknown
		0x0A: System hibernates (DC)	Time until the computer enters hibernation mode (DC) (seconds) set as a character string: • 0: Not set • 1 to 2147483647: Elapsed time (seconds) • N/A: Unknown

#

Characters that cannot be displayed in the language environment being used by the OS are replaced with a question mark (?).

- CPU type

Code	Description	Code	Description
646	Intel 80286	902	Intel 80386
1158	Intel 80486	1414	Intel Pentium series or compatible CPU
4097	Alpha	8193	MIPS R2000 system
12289	PowerPC	20481	PA-RISC
24577	SPARC	28672	Intel Pentium series
28673	Intel Pentium	28674	Intel Pentium MMX
28675	Intel Pentium Pro	28676	Intel Pentium II
28677	Intel Pentium II Xeon	28678	Intel Pentium III
28679	Intel Pentium III Xeon	28680	Intel Celeron
28681	Intel Pentium 4	28682	Pentium III-S
28683	Mobile Intel Celeron	28684	Mobile Intel Pentium 4
28685	Intel Xeon	28686	Intel Xeon MP
28687	Mobile Intel Pentium III-M	28688	Intel Genuine
28689	Mobile Genuine Intel	28690	Intel Celeron M
28691	Intel Pentium M	28692	Intel Pentium D
28693	Intel Celeron D	28694	Intel Core2
28695	Intel Core	28696	Intel Core i7
28697	Intel Atom	28698	Intel Pentium Dual
28699	Intel Core i3	28700	Intel Core i5
32768	Intel Pentium-compatible CPU	33025	AMD K6
33026	AMD K6-2	33027	AMD K6-2 3D Now!
33028	AMD K6-III	33029	AMD Athlon
33030	AMD Duron	33031	AMD Athlon MP
33032	AMD Athlon XP	33033	Mobile AMD Athlon 4
33034	Mobile AMD Duron	33035	AMD Duron MP
33036	Mobile AMD Athlon XP-M	33037	AMD Sempron
33038	Mobile AMD Sempron	33039	AMD Turion
33281	Cyrix MediaGX	33282	Cyrix MII
33283	Cyrix MediaGXm	33537	IDT WinChip
33793	RISE mP6	34049	Transmeta Crusoe Processor TM5600
36864	CPU for Windows CE	37120	CPU for Windows CE (Hitachi)
37377	MIPS R3000 system	37378	MIPS R4000 system

Code	Description	Code	Description
37633	ARM720	40960	Intel IPF CPU
40961	Intel Itanium	40962	Intel Itanium 2
45056	AMD64-compatible CPU	45057	AMDOpteron
45058	AMD Athlon 64	45059	AMD Athlon 64 FX
45060	Mobile AMD Athlon 64	45061	AMD Athlon 64 X2
45062	AMD Turion 64	45063	AMD Athlon II
45064	AMD Turion II	45065	AMD Phenom
45066	AMD Phenom II	45067	AMD V Series
45068	AMD FX	45069	AMD A Series
45070	AMD C Series	45071	AMD E Series
45311	AMD	--	--

Legend:

--: Not applicable

- OS

Code	Description	Code	Description
1	MS-DOS+Windows	2	Windows NT
3	OS/2	4	Windows 95
5	SCO ODT	6	Solaris PC
7	NEXTSTEP	8	Windows 98
9	Windows 2000	11	Windows Me
12	Windows XP	14	Windows Server 2003
15	Windows Vista	16	Windows Server 2008
17	Windows 7	18	Windows Server 2008 R2
19	Windows 8	20	Windows Server 2012
131	HP-UX	132	Solaris
134	HP Tru64 UNIX	135	AIX
137	NEWS-OS	144	UX/4800
145	Linux	146	MP-RAS
147	IRIX	--	--

Legend:

--: Not applicable

C.24 netmdm_jobgen

This table stores job definition information. There is one table for each job that is created, and the table stores the header information for the job. The table is associated with `netmdm_jobgen_node` and `netmdm_jobgen_pack`.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_folder1	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder level 1 (if not used, NULL)	1
dm_folder2	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder level 2 (if not used, NULL)	2
dm_folder3	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder level 3 (if not used, NULL)	3
dm_folder4	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder level 4 (if not used, NULL)	4
dm_kind	NUMBER	10	int	4	INTEGER	--	Line type: • 1: Folder information line • 2: Job definition information line • 5: ID group job definition information line	--
dm_jobgenname	VARCHAR2	32	varchar	32	MVARCHAR	32	Job name	5
dm_jobgenattributes	CHAR	1	char	1	CHAR	1	Job type code: • A: *Acquire collected files from relay system* • C: *Batch delete packages on relay system* • D: *Install package* • E: *Report job deletion* • F: *Resume file transfer* • G: *Collect files from client* • H: *Hold report* • I: *Get software information from client* • J: *Send package, allow client to choose* • K: *Delete collected files from relay system* • L: *ID group operation* • M: *Transfer package to relay system* • N: *Get system configuration information* • O: *Edit system configuration information* • P: *Suspend file transfer* • S: *Collect files from client to relay system* • T: *Hold-report release* • U: *Transfer user inventory schema to client*	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_jobgenattributes	CHAR	1	char	1	CHAR	1	• V: *Get system information from client* • Y: *Transfer registry collection definition* • 1: *Report message* • 8: *Set the software monitoring policy* • 9: *Get software monitoring information from the client*	--
dm_jobtype	CHAR	1	char	1	CHAR	1	Job type subcode: • F: Forced installation • Space: Other than forced installation	--
dm_createtime	DATE	--	datetime	8	TIMESTAMP	--	Date and time the job definition was created	--
dm_updatetime	DATE	--	datetime	8	TIMESTAMP	--	Last date and time the job definition was updated	--
dm_systeminf	RAW	20	binary	20	BINARY	20	JP1/Software Distribution Manager management information	--
dm_workday	VARCHAR2	6	varchar	6	MVARCHAR	6	Execution date at the client expressed in the format *YYMMDD*. This column is applicable when the execution time and execution interval are specified for monthly execution.	--
dm_worktime	VARCHAR2	6	varchar	6	MVARCHAR	6	Execution time at the client expressed in the format *hhmmss*. This column is applicable when the execution time and execution interval are specified.	--
dm_execday	VARCHAR2	2	varchar	2	MVARCHAR	2	Execution date at the client expressed in the format *DD*. This column is applicable when the execution interval is specified for monthly execution.	--
dm_execweek	NUMBER	3	tinyint	1	SMALLINT	--	Execution day of the week at the client. This column is applicable when the execution interval is specified. • 0x01: Sunday • 0x02: Monday • 0x04: Tuesday • 0x08: Wednesday • 0x10: Thursday • 0x20: Friday • 0x40: Saturday	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_exectiming	VARCHAR2	1	varchar	1	MVARCHAR	1	Execution timing at the client: • B: When client starts • E: While client is running • S: When client terminates	--
dm_attrflag	RAW	1	binary	1	BINARY	1	Attribute flag: • 0x00: Job of the local system • 0x01: Job transferred from another system	--
dm_userinfoption	RAW	1	binary	1	BINARY	1	User inventory acquisition option: • 0x00: Acquire both system information and user inventory information • 0x01: Acquire only user inventory information	--
dm_userinfsendoption	RAW	1	binary	1	BINARY	1	Immediate reporting option for user inventory acquisition: • 0x00: Report during job execution • 0x01: Report immediately • 0x02: Report only when a change is made	--
dm_reginfoption	RAW	1	binary	1	BINARY	1	Registry information and system information acquisition option For JP1/Software Distribution version 06-52 or earlier: • 0x00: Acquire differing registry information and all system information. • 0x01: Acquire all registry information and all system information For JP1/Software Distribution version 06-71 or later: • 0x02: Acquire differing registry information and all system information. • 0x03: Acquire all registry information and all system information • 0x06: Acquire differing registry information and differing system information. • 0x07: Acquire all registry information and differing system information.	--
dm_woloption	CHAR	1	char	1	VARCHAR	1	Client control and distribution method:	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_woloption	CHAR	1	char	1	VARCHAR	1	• 0x01: Start the destination. • 0x02: Shut down the destination. • 0x04: Execute multicast distribution. • 0x08: Distribute (even to a suspended destination) • 0x40: Do not archive the software operation information	--
dm_splitsize	NUMBER	10	int	4	INTEGER	--	Split size	--
dm_transinterval	NUMBER	10	int	4	INTEGER	--	Distribution interval	--
dm_schoption	CHAR	1	char	1	VARCHAR	1	Type of scheduling information. The value of this column is a combination of the following numeric values: • NULL: Scheduling not specified • 1: Specify job registration date/time • 2: Specify job execution date/time • 4: Specify job execution time limit	--
dm_entrytime	DATE	--	datetime	8	TIMESTAMP	--	Job registration date/time	--
dm_eventtime	DATE	--	datetime	8	TIMESTAMP	--	Job execution date/time	--
dm_timeout	DATE	--	datetime	8	TIMESTAMP	--	Job execution time limit	--

Legend:

--: Not applicable

C.25 netmdm_jobgen_collect

This table stores information about remote collection specified in a job in the definition of remote collection jobs and *Collect files from client to relay system* jobs. The table is associated with netmdm_jobgen.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_folder1	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder level 1 (if not used, NULL)	1

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_folder2	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder level 2 (if not used, NULL)	2
dm_folder3	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder level 3 (if not used, NULL)	3
dm_folder4	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder level 4 (if not used, NULL)	4
dm_jobgenname	VARCHAR2	32	varchar	32	MVARCHAR	32	Job name	5
dm_dirname	BLOB	--	image	--	BINARY	260	Name of directory for storing collected files	--
dm_scriptfile	LONG RAW	--	image	--	BLOB	--	Job script file entity	--
dm_systeminf	BLOB	--	image	--	BINARY	784	JP1/Software Distribution Manager management information	--

Legend:

--: Not applicable

C.26 netmdm_jobgen_id

This table stores job definition information for processing ID groups and ID group entries.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_folder_1	VARCHAR2	32	varchar	32	MVARCHAR	32	Folder level 1	1
dm_folder_2	VARCHAR2	32	varchar	32	MVARCHAR	32	Folder level 2	2
dm_folder_3	VARCHAR2	32	varchar	32	MVARCHAR	32	Folder level 3	3
dm_folder_4	VARCHAR2	32	varchar	32	MVARCHAR	32	Folder level 4	4
dm_jobgenname	VARCHAR2	32	varchar	32	MVARCHAR	32	Job name	5
dm_idname	VARCHAR2	32	varchar	32	MVARCHAR	32	ID group name	--
dm_request	CHAR	1	char	1	CHAR	1	Request type: • F: Addition of ID group • G: Deletion of ID group • W: Modification of password • R: Addition of entry • E: Deletion of entry	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_nodename	VARCHAR2	64	varchar	64	MVARCHAR	64	Node name	--
dm_option	RAW	1	binary	1	BINARY	1	Internal information for JP1/Software Distribution	--

Legend:

--: Not applicable

C.27 netmdm_jobgen_monitoring

This table stores information about the software operation monitoring specified in a job during definition of the *Set the software monitoring policy* job. It is associated with netmdm_jobgen.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_folder1	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder hierarchy level 1 (if not used, NULL is set)	1
dm_folder2	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder hierarchy level 2 (if not used, NULL is set)	2
dm_folder3	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder hierarchy level 3 (if not used, NULL is set)	3
dm_folder4	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder hierarchy level 4 (if not used, NULL is set)	4
dm_jobgenname	VARCHAR2	32	varchar	32	MVARCHAR	32	Job name	5
dm_policyname	VARCHAR2	64	varchar	64	MVARCHAR	64	Policy name	--
dm_permanent	CHAR	1	char	1	VARCHAR	1	Whether the process being monitored is to be made resident: • 0x00: Resident • 0x01: Not resident	--

Legend:

--: Not applicable

C.28 netmdm_jobgen_msg

This table stores the following part of the job definition information: information about the message to be sent to the client. It is associated with netmdm_jobgen.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_folder1	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder hierarchy level 1 (if not used, NULL is set)	1
dm_folder2	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder hierarchy level 2 (if not used, NULL is set)	2
dm_folder3	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder hierarchy level 3 (if not used, NULL is set)	3
dm_folder4	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder hierarchy level 4 (if not used, NULL is set)	4
dm_jobgenname	VARCHAR2	32	varchar	32	MVARCHAR	32	Job name	5
dm_level	CHAR	1	char	1	CHAR	1	Message icon: • I: Information • N: Note • W: Warning	--
dm_title	VARCHAR2	65	varchar	65	MVARCHAR	65	Message title	--
dm_message	LONG RAW	--	image	--	BLOB	--	Message text	--

Legend:

--: Not applicable

C.29 netmdm_jobgen_node

This table stores the following part of the job definition information: information about the hosts that are targets of executed jobs. There is one table for each host that is specified during job creation. The table is associated with netmdm_jobgen.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_folder1	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder level 1 (if not used, NULL)	1
dm_folder2	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder level 2 (if not used, NULL)	2
dm_folder3	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder level 3 (if not used, NULL)	3
dm_folder4	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder level 4 (if not used, NULL)	4
dm_jobgenname	VARCHAR2	32	varchar	32	MVARCHAR	32	Job name	5
dm_clientname	VARCHAR2	65	varchar	65	MVARCHAR	65	Name of relay system, client, ID group, or host group that is a target of executed jobs#	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_nodeattributes	NUMBER	15	int	4	INTEGER	--	Attribute of dm_nodename: • 0x00000000: Host group specified in the Destination window • 0x00000001: Client specified in the Destination window • 0x00000002: Relay system specified in the Destination window • 0x00000004: ID group specified in the Destination window • 0x01000001: Client specified in the System Configuration window • 0x01000002: Relay system specified in the System Configuration window • 0x80000000: Any host that was specified	7
dm_systeminf	RAW	17	binary	17	BINARY	17	JP1/Software Distribution Manager management information	--
dm_nodename	VARCHAR2	255	varchar	255	MVARCHAR	255	Route information about the destination that consists of an ID key for operations (host ID or node identification key)	6
dm_descriptor	NUMBER	10	int	4	INTEGER	--	JP1/Software Distribution Manager management information	--
dm_nodename2	VARCHAR2	255	varchar	255	MVARCHAR	255	Route information about the destination that consists of a node identification key (host name or IP address)	--

Legend:

--: Not applicable

#

If the stored information is a host group name, the data depends on the version of JP1/Software Distribution:

- JP1/Software Distribution version 06-00 or earlier: Host group name including the route from top to terminal levels
- JP1/Software Distribution version 06-01 or later: Host group name of the terminal level

C.30 netmdm_jobgen_pack

This table stores the following part of the job definition information: package information specified in the job. This table is used only for jobs that specify packages. There is one table for each package that is specified during job creation. This table is associated with netmdm_jobgen.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_folder1	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder level 1	1
dm_folder2	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder level 2	2
dm_folder3	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder level 3	3
dm_folder4	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder level 4	4
dm_jobgenname	VARCHAR2	32	varchar	32	MVARCHAR	32	Job name	5
dm_dmtype	CHAR	1	char	1	MCHAR	1	Type of Packager used for packaging: • C: WS (UNIX) • D: PC (Windows)	6
dm_cabinetid	CHAR	2	char	2	MCHAR	2	ID of the cabinet containing the package	7
dm_packageid	VARCHAR2	44	varchar	44	MVARCHAR	44	Package ID	8
dm_version	VARCHAR2	8	varchar	8	MVARCHAR	8	Package version	9
dm_generation	VARCHAR2	4	varchar	4	MVARCHAR	4	Package generation number	10
dm_jobtype	CHAR	1	char	1	CHAR	1	Job type subcode: • F: Forced installation • Space: Subcode not specified	--
dm_attrinf	BLOB	--	image	--	BINARY	784	Package attributes	--
dm_scriptfile	LONG RAW	--	image	--	BLOB	--	Job script file entity	--
dm_systeminf	RAW	255	binary	255	BINARY	255	JP1/Software Distribution Manager management information	--
dm_nodename	VARCHAR2	255	varchar	255	MVARCHAR	255	Route information about the destination that consists of an ID key for operations (host ID or node identification key)	--
dm_nodename2	VARCHAR2	255	varchar	255	MVARCHAR	255	Route information about the destination that consists of a node identification key (host name or IP address)	--
dm_installationturn	NUMBER	10	int	4	INTEGER	--	Package installation order	--

Legend:

--: Not applicable

C.31 netmdm_jobgen_soft

This table stores the following part of the job definition information: information about a software search job. This table is associated with `netmdm_jobgen`.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
`dm_folder1`	`VARCHAR2`	32	`varchar`	32	`MVARCHAR`	32	Job definition folder level 1 (if not used, `NULL`)	1
`dm_folder2`	`VARCHAR2`	32	`varchar`	32	`MVARCHAR`	32	Job definition folder level 2 (if not used, `NULL`)	2
`dm_folder3`	`VARCHAR2`	32	`varchar`	32	`MVARCHAR`	32	Job definition folder level 3 (if not used, `NULL`)	3
`dm_folder4`	`VARCHAR2`	32	`varchar`	32	`MVARCHAR`	32	Job definition folder level 4 (if not used, `NULL`)	4
`dm_jobgenname`	`VARCHAR2`	32	`varchar`	32	`MVARCHAR`	32	Job name	5
`dm_refersoftware`	`NUMBER`	10	`int`	4	`INTEGER`	--	Software to be searched: • `0`: Job other than a *Get software information from client* job • `1`: Search software installed by Software Distribution • `2`: Search all software • `3`: Search for a file • `4`: Search software listed in "Add/Remove Programs" • `5`: Search for Microsoft Office products • `6`: Search for anti-virus products	--
`dm_referdrivekind`	`NUMBER`	10	`int`	4	`INTEGER`	--	Drives to be searched: • `0`: Job other than *Get software information from client* job • `1`: All fixed drives • `2`: All fixed drives + network drives • `3`: Specified drives	--
`dm_referdrivename`	`VARCHAR2`	70	`varchar`	70	`MVARCHAR`	70	This column is set only when **Specified drives** is selected as the drives to be searched in a *Get software information from client* job with drives specification. If multiple drives are specified, the semicolon (;) is used as the delimiter.	--
`dm_systeminf`	`RAW`	24	`binary`	24	`BINARY`	24	System information for JP1/Software Distribution Manager	--
`dm_listname`	`VARCHAR2`	32	`varchar`	32	`MVARCHAR`	32	Search list name	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_listkind	NUMBER	3	tinyint	1	SMALLINT	--	Type of search list: • 0: Standard retrieve list or a search list existing at the client • 1: Standard retrieve list and optional software list • 2: No search list • 3: Optional software list	--
dm_conditionfile	LONG RAW	--	image	--	BLOB	--	Name of file containing the file search definition information	--

Legend:

--: Not applicable

C.32 netmdm_jobgen_system

This table stores information needed to link system configuration information an ID group. This table is associated with netmdm_jobgen.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_folder1	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder level 1	1
dm_folder2	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder level 2	2
dm_folder3	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder level 3	3
dm_folder4	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder level 4	4
dm_jobgenname	VARCHAR2	32	varchar	32	MVARCHAR	32	Job name	5
dm_request	CHAR	1	char	1	MCHAR	1	Request code D: Deletion from the system configuration	--
dm_nodename	VARCHAR2	64	varchar	64	MVARCHAR	64	Name of host to be edited	--
dm_timestamp	DATE	--	datetime	8	TIMESTAMP	--	Time stamp of system configuration file	--

Legend:

--: Not applicable

C.33 netmdm_jobgen_userinv

This table stores the following part of the job definition information: job information for user inventory. This table is associated with `netmdm_jobgen`.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
`dm_folder1`	`VARCHAR2`	32	`varchar`	32	`MVARCHAR`	32	Job definition folder level 1	1
`dm_folder2`	`VARCHAR2`	32	`varchar`	32	`MVARCHAR`	32	Job definition folder level 2	2
`dm_folder3`	`VARCHAR2`	32	`varchar`	32	`MVARCHAR`	32	Job definition folder level 3	3
`dm_folder4`	`VARCHAR2`	32	`varchar`	32	`MVARCHAR`	32	Job definition folder level 4	4
`dm_jobgenname`	`VARCHAR2`	32	`varchar`	32	`MVARCHAR`	32	Job name	5
`dm_filename`	`VARCHAR2`	8	`varchar`	8	`MVARCHAR`	8	Name of file to be transferred	--
`dm_option`	`RAW`	1	`binary`	1	`BINARY`	1	Transfer option: • `0x01`: Issue notification to the client. • `0x02`: Suppress startup of Package Setup Manager • `0x04`: Require entry of all items • `0x08`: Ignore cancellation	--
`dm_sendoption`	`RAW`	1	`binary`	1	`BINARY`	1	Notification option: • `0`: User decides whether to save or to save and notify. • `1`: Save. • `2`: Save and notify.	--

Legend:

--: Not applicable

C.34 netmdm_jobsch

This table stores header information for job execution status. The table sums up the completion status of `netmdm_execution` that manages the execution status of each job.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
`dm_folder1`	`VARCHAR2`	64	`varchar`	64	`MVARCHAR`	64	Job definition folder level 1 (if not used, `NULL`)	1

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_folder2	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder level 2 (if not used, NULL)	2
dm_folder3	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder level 3 (if not used, NULL)	3
dm_folder4	VARCHAR2	32	varchar	32	MVARCHAR	32	Job definition folder level 4 (if not used, NULL)	4
dm_kind	NUMBER	10	int	4	INTEGER	--	Line type: • 0: Folder information line • 1: Job information line • 5: ID group job information line	--
dm_jobname	VARCHAR2	64	varchar	64	MVARCHAR	64	Job name	5
dm_jobkind	CHAR	1	char	1	CHAR	1	Job type code: • A: *Acquire collected files from relay system* • C: *Batch delete packages on relay system* • D: *Install package* • E: *Report job deletion* • F: *Resume file transfer* • G: *Collect files from client* • H: *Hold report* • I: *Get software information from client* • J: *Send package, allow client to choose* • K: *Delete collected files from relay system* • L: *ID group operation* • M: *Transfer package to relay system* • N: *Get system configuration information* • O: *Edit system configuration information* • P: *Suspend file transfer* • S: *Collect files from client to relay system* • T: *Hold-report release* • U: *Transfer user inventory schema to client* • V: *Get system information from client* • Y: *Transfer registry collection definition*	6

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_jobkind	CHAR	1	char	1	CHAR	1	• 1: *Report message* • 8: *Set the software monitoring policy* • 9: *Get software monitoring information from the client*	6
dm_jobno	CHAR	16	char	16	MCHAR	16	Number assigned to the job automatically	7
dm_createdate	DATE	--	datetime	8	TIMESTAMP	--	Date and time job registration was instructed	--
dm_totalcount	NUMBER	10	int	4	INTEGER	--	Total execution count	--
dm_entrytime	DATE	--	datetime	8	TIMESTAMP	--	Job registration date and time	--
dm_eventtime	DATE	--	datetime	8	TIMESTAMP	--	Job execution date and time	--
dm_timeout	DATE	--	datetime	8	TIMESTAMP	--	Job time-out date and time	--
dm_nnm_status	RAW	1	binary	1	BINARY	1	HP NNM status: • 0x00: Out of warning range • 0x01: Warning range	--
dm_attrflag	RAW	1	binary	1	BINARY	1	Attribute flag: • 0x00: Job of the local system • 0x01: Job transferred from another system	--
dm_userinfoption	RAW	1	binary	1	BINARY	1	User inventory acquisition option: • 0x00: Acquire both system information and user inventory information • 0x01: Acquire only user inventory information	--
dm_woloption	CHAR	1	char	1	VARCHAR	1	Client control and distribution method: • 0x01: Start the destination • 0x02: Shut down the destination • 0x04: Execute multicast distribution • 0x08: Distribute even to suspended destinations • 0x40: Do not archive the software operation information	--
dm_splitsize	NUMBER	10	int	4	INTEGER	--	Split size	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_transinterval	NUMBER	10	int	4	INTEGER	--	Distribution interval	--
dm_synchroflg	CHAR	1	char	1	VARCHAR	1	Synchronous deletion flag: • 0x00: Synchronous job deletion is not underway • 0x01: Synchronous job deletion is underway	--

Legend:

--: Not applicable

C.35 netmdm_jobsch_site

This table stores header information for the execution status of an ID group job that was executed at a relay system (*Install package* and *Send package, allow client to choose* jobs). This table sums up the completion status of netmdm_execution_site that manages the execution status of each job.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_folder	VARCHAR2	64	varchar	64	MVARCHAR	64	Job definition folder level 1 (host name of the relay system)	1
dm_kind	NUMBER	10	int	4	INTEGER	--	Line type: • 0: Folder information line • 1: Job information line	--
dm_jobname	VARCHAR2	64	varchar	64	MVARCHAR	64	Job definition name (number assigned to the job at the relay system)	2
dm_jobkind	CHAR	1	char	1	CHAR	1	Job type code: • D: *Install package* • J: *Send package, allow client to choose*	3
dm_jobno	CHAR	16	char	16	MCHAR	16	Number assigned to the job automatically	4
dm_createdate	DATE	--	datetime	8	TIMESTAMP	--	Date and time job registration was instructed	--
dm_totalcount	NUMBER	10	int	4	INTEGER	--	Total execution count	--
dm_entrytime	DATE	--	datetime	8	TIMESTAMP	--	Job registration date and time	--
dm_eventtime	DATE	--	datetime	8	TIMESTAMP	--	Job execution date and time	--
dm_timeout	DATE	--	datetime	8	TIMESTAMP	--	Job timeout date and time	--

Legend:

--: Not applicable

C.36 netmdm_jobscript

This table stores the job script file during remote installation.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
`dm_jobname`	`VARCHAR2`	64	`varchar`	64	`MVARCHAR`	64	Job name	--
`dm_jobno`	`CHAR`	16	`char`	16	`MCHAR`	16	Number assigned to the job automatically	1
`dm_mngfilename`	`CHAR`	8	`char`	8	`MCHAR`	8	Script file management filename	2
`dm_scriptfile`	`LONG RAW`	--	`image`	--	`BLOB`	--	Installation script body	--

Legend:

--: Not applicable

C.37 netmdm_lastupdate

This table stores the last update date and time of certain tables.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
`dm_tabletype`	`NUMBER`	3	`tinyint`	1	`SMALLINT`	--	Table type: • 1: `netmdm_system` • 2: `netmdm_system_delete` • 3: `netmdm_host_withoutdm`	--
`dm_lastupdatetime`	`DATE`	--	`datetime`	8	`TIMESTAMP`	--	Table's last update date and time	--

Legend:

--: Not applicable

C.38 netmdm_mnglist

This table stores a search list used by a *Get software information from client* job.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_listname	VARCHAR2	32	varchar	32	MVARCHAR	32	Name of list file	1
dm_listkind	NUMBER	3	tinyint	1	SMALLINT	--	List type: • 0: Standard retrieve list • 1: Optional software list	2
dm_createtime	DATE	--	datetime	8	TIMESTAMP	--	Creation date	--
dm_updatetime	DATE	--	datetime	8	TIMESTAMP	--	Update date	--
dm_list	LONG RAW	--	image	--	BLOB	--	List entity	--

Legend:
--: Not applicable

C.39 netmdm_monitoring_devicectrl

This table stores the suppression or activation setting information for each device.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_policyname	VARCHAR2	64	varchar	64	MVARCHAR	64	Related policy name	1
dm_devicetype	NUMBER	3	tinyint	1	SMALLINT	--	Device type: • 0x01: USB storage device • 0x02: Internal CD/DVD drive • 0x03: Internal floppy disk drive • 0x04: IEEE1394-connected device • 0x05: Internal SD card • 0x06: Bluetooth device • 0x07: Imaging device	2
dm_operationconf	NUMBER	3	tinyint	1	SMALLINT	--	Device operation action is set as an OR value. • 0x00: No setting • 0x01: Acquires connection history • 0x02: Acquires disconnection history • 0x04: Suppresses use	--
dm_detaileconf	NUMBER	3	tinyint	1	SMALLINT	--	The details of device operation action are set as an OR value.	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_detailconf	NUMBER	3	tinyint	1	SMALLINT	--	• 0x00: No setting • 0x01: Acquires suppression history • 0x02: Acquires permission history • 0x04: Issues an alert • 0x08: Displays a message during suppression	--
dm_restmessage	VARCHAR2	2,048	varchar	2,048	MVARCHAR	2,048	Specifies the suppression message to be displayed on a client PC.	--

Legend:

--: Not applicable

C.40 netmdm_monitoring_filter

This table stores filtering information during logging for software operation monitoring.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_policyname	VARCHAR2	64	varchar	64	MVARCHAR	64	Associated policy name	--
dm_type	CHAR	1	char	1	VARCHAR	1	Filtering target. OR of the following value is set: • 0x01: Usage history • 0x02: Operation history • 0x04: File operation history	--
dm_extype	CHAR	1	char	1	VARCHAR	1	Filtering type: • 0x01: Process name • 0x02: Execution account • 0x03: Extension	--
dm_value	VARCHAR2	255	varchar	255	VARCHAR	255	Filtering information: Filtering information for the type specified in dm_extype (process name, execution account, extension)	--
dm_actiontype	CHAR	1	char	1	VARCHAR	1	Whether filtering condition is to be collected: • 0x00: Collect log • 0x01: Do not collect log information	--

Legend:

--: Not applicable

C.41 netmdm_monitoring_permission

This table stores permission conditions for software operation monitoring.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_policyname	VARCHAR2	64	varchar	64	MVARCHAR	64	Associated policy name	--
dm_seqnumber	NUMBER	10	int	4	INTEGER	--	Program sequence number corresponding to the program being monitored for a policy	--
dm_type	NUMBER	10	int	4	INTEGER	--	Type of permission conditions: • 1: User type • 4: Time	--
dm_extype	NUMBER	10	int	4	INTEGER	--	Extended type of permission conditions: If the type is 1 (user type): • 1: User account • 2: User group If the type is 4 (time), extended type is set to 0.	--
dm_value	VARCHAR2	255	varchar	255	MVARCHAR	255	Permitted range and value: If the type is 4 (time) and a range is specified, the time is stored in the following format: "*hh*:*mm*" - "*hh*:*mm*"	--

Legend:

--: Not applicable

C.42 netmdm_monitoring_policy

This table stores an operation monitoring policy for software operation monitoring.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_policyname	VARCHAR2	64	varchar	64	MVARCHAR	64	Policy name	1
dm_permanent	CHAR	1	char	1	VARCHAR	1	Whether the process being monitored is to be started or stopped: • 0x00: Start • 0x01: Stop	--
dm_monitoringconf	CHAR	1	char	1	VARCHAR	1	Whether the operation history is to be monitored: • 0x00: Monitor	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_monitoringconf	CHAR	1	char	1	VARCHAR	1	• 0x01: Do not monitor	--
dm_eventtype	NUMBER	10	int	4	INTEGER	--	Type of event subject to monitoring of operation history. OR of the following values is set: • 0x00000000: No event to be monitored • 0x00000001: Start of process • 0x00000002: Stop of process • 0x00000004: Change to window captions • 0x00000008: Change of active window • 0x00000010: Start or stop of PC • 0x00000020: Log in or out	--
dm_loglevel	NUMBER	10	int	4	INTEGER	--	Log output message level: • 0: Do not output • 1 to 10: Output only Error • 11 to 20: Output Error and Information • 21 to 30: Output Error, Information, and Warning • 30 and above: Output Error, Information, Warning, and trace	--
dm_maxdisplaytime	NUMBER	10	int	4	INTEGER	--	Display time of stop warning dialog box (seconds)	--
dm_sendconf	CHAR	1	char	1	VARCHAR	1	Whether results information is to be sent: • 0x00: Send • 0x01: Do not send	--
dm_sendbasetime	VARCHAR2	5	varchar	5	VARCHAR	5	Reference time for sending results information (24-hour format *hh*:*mm*). This item is applicable when results information is to be sent.	--
dm_sendlimit	NUMBER	10	int	4	INTEGER	--	Maximum delay from the reference time for sending results to the time the transmission of results begins (in seconds). This item is applicable when results information is to be sent.	--
dm_sendinterval	NUMBER	10	int	4	INTEGER	--	Interval at which results information is sent (in seconds). This item is applicable when results information is to be sent.	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_sendoption	CHAR	1	char	1	VARCHAR	1	Whether the transmission is to take place immediately. This item is applicable when results information is to be sent. • 0x00: Send immediately • 0x01: Do not send immediately	--
dm_maxfilesize	NUMBER	10	int	4	INTEGER	--	Maximum size of file for storing the results (in bytes)	--
dm_modifieddatetime	DATE	--	datetime	8	TIMESTAMP	--	Date and time policy was edited	--
dm_eventtype2	NUMBER	10	int	4	INTEGER	--	Event type monitored in file manipulation. OR of the following values is set: • 0x00000000: No event to be monitored • 0x00000001: Copy file/folder • 0x00000002: Move file/folder • 0x00000004: Rename file/folder • 0x00000008: Delete file/folder • 0x00000010: Create file/folder • 0x00000020: Open file	--
dm_actiontype	CHAR	1	char	1	VARCHAR	1	Whether to permit startup of a program other than the monitoring target program: • 0x00: Permit • 0x01: Suppress If the monitoring target program is not set, 0x00 is set.	--
dm_metering	CHAR	1	char	1	VARCHAR	1	Whether to monitor operation time: • 0x00: Monitor. • 0x01: Do not monitor. If no program is set to be monitored, 0x01 is set.	--
dm_boundarytime	CHAR	5	char	5	VARCHAR	5	Boundary time for monitoring operation time, specified in the format *hh*:*mm*.	--
dm_version	VARCHAR2	8	varchar	8	MVARCHAR	8	Policy version	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_generation	VARCHAR2	4	varchar	4	MVARCHAR	4	Policy generation number	--
dm_extmedialogconf	NUMBER	3	tinyint	1	SMALLINT	--	Whether to collect external media operation log: • 0x00: Collects • 0x01: Does not collect	--
dm_usbconf	NUMBER	3	tinyint	1	SMALLINT	--	Whether to permit access to USB-connected media: • 0x00: Permits • 0x01: Suppresses both writing and reading • 0x02: Suppresses only writing	--
dm_cddvdconf	NUMBER	3	tinyint	1	SMALLINT	--	Whether to permit writing via the internal CD/DVD drive: • 0x00: Permits • 0x01: Suppresses	--
dm_fdconf	NUMBER	3	tinyint	1	SMALLINT	--	Whether to permit access to the internal floppy disk drive: • 0x00: Permits • 0x01: Suppresses	--
dm_ieeeconf	NUMBER	3	tinyint	1	SMALLINT	--	Whether to permit access to IEEE 1394-connected media: • 0x00: Permits • 0x01: Suppresses	--
dm_sdconf	NUMBER	3	tinyint	1	SMALLINT	--	Whether to permit access via the internal SD card slot: • 0x00: Permits • 0x01: Suppresses	--
dm_weblogconf	NUMBER	3	tinyint	1	SMALLINT	--	Whether to collect Web access logs: • 0x00: On • 0x01: Off	--
dm_webfilteringconf	NUMBER	3	tinyint	1	SMALLINT	--	Whether to filter Web access logs, and the filtering method to use: • 0x00: Does not filter • 0x01: Collects only those logs that satisfy the filtering condition • 0x02: Collects those logs that do not satisfy the filtering condition	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
`dm_printinglogconf`	`NUMBER`	3	`tinyint`	1	`SMALLINT`	--	Whether to collect print operation logs: • `0x00`: On • `0x01`: Off	--
`dm_printingconf`	`NUMBER`	3	`tinyint`	1	`SMALLINT`	--	Whether to suppress printing: • `0x00`: On • `0x01`: Off	--
`dm_printingpassconf`	`NUMBER`	3	`tinyint`	1	`SMALLINT`	--	Whether to set up a password for canceling print operation suppression: • `0x00`: On • `0x01`: Off	--
`dm_printingpassword`	`VARCHAR2`	30	`varchar`	30	`MVARCHAR`	30	Password for canceling print operation suppression as plain text. 0-30 bytes	--
`dm_usbconnectconf`	`NUMBER`	3	`tinyint`	1	`SMALLINT`	--	Whether or not to exclude access to USB media from being suppressed: • `0x00`: Excludes • `0x01`: Does not exclude	--
`dm_warningmessconf`	`NUMBER`	3	`tinyint`	1	`SMALLINT`	--	Whether or not to display a message on the client's PC while operations to USB media are being suppressed: • `0x00`: Displays • `0x01`: Does not display	--
`dm_restmessconf`	`NUMBER`	3	`tinyint`	1	`SMALLINT`	--	Whether or not to display an optionally-created message on the client's PC while USB operations to media are being suppressed, rather than display the default message: • `0x00`: Displays • `0x01`: Does not display	--
`dm_restmessage`	`VARCHAR2`	2,048	`varchar`	2,048	`MVARCHAR`	2,048	Stores a message to be displayed on the client's PC while operations to USB media are being suppressed.	--
`dm_mergepolicy`	`NUMBER`	3	`tinyint`	1	`SMALLINT`	--	Management information of JP1/Software Distribution Manager	--
`dm_printingtype`	`NUMBER`	3	`tinyint`	1	`SMALLINT`	--	Whether or not a client on which File and Printer Sharing for Microsoft Networks is not installed exists in a shared network printer environment:	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_printingtype	NUMBER	3	tinyint	1	SMALLINT	--	• 0x00: Exists • 0x01: Does not exist	--
dm_usbhistoryconf	NUMBER	3	tinyint	1	SMALLINT	--	Connection history of USB-connected media to be acquired: • 0x01: Acquires connection permission history • 0x02: Acquires connection suppression history	--
dm_devicewriteconf	NUMBER	3	tinyint	1	SMALLINT	--	Whether or not to suppress writing data to a device: • 0x00: Does not suppress writing (off) • 0x01: Suppresses writing (on)	--

Legend:

--: Not applicable

C.43 netmdm_monitoring_program

This table stores information about a program being monitored for software operation monitoring.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_policyname	VARCHAR2	64	varchar	64	MVARCHAR	64	Policy name	1
dm_seqnumber	NUMBER	10	Int	4	INTEGER	--	Sequence number of the program being monitored for a policy	2
dm_filename	VARCHAR2	255	varchar	255	MVARCHAR	255	File name of the program being monitored	--
dm_originalfilename	VARCHAR2	255	varchar	255	MVARCHAR	255	Formal file name of the program being monitored	--
dm_fileversion	VARCHAR2	50	varchar	50	MVARCHAR	50	File version of the program being monitored	--
dm_filelanguage	CHAR	2	char	2	VARCHAR	2	File language of the program being monitored. If no value is specified, NULL is set.	--
dm_productname	VARCHAR2	50	varchar	50	MVARCHAR	50	Name of software containing the program being monitored	--
dm_productversion	VARCHAR2	50	varchar	50	MVARCHAR	50	Product version of the program being monitored	--
dm_productlanguage	CHAR	2	char	2	VARCHAR	2	Product language of the program being monitored.	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_productlanguage	CHAR	2	char	2	VARCHAR	2	If no value is specified, NULL is set.	--
dm_actiontype	CHAR	1	char	1	VARCHAR	1	Whether startup is to be suppressed: • 0x00: Permit startup • 0x01: Suppress startup • 0x02: Reference permission conditions	--
dm_filetype	CHAR	1	char	1	VARCHAR	1	Whether the monitoring target is specified by file name or path name: • 0x00: File name • 0x01: Path name If a path name is specified in dm_filename, 0x01 is set.	--

Legend:

--: Not applicable

C.44 netmdm_monitoring_result

This table stores the software startup suppression history.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_nodename	VARCHAR2	64	varchar	64	MVARCHAR	64	Node name	--
dm_productname	VARCHAR2	50	varchar	50	MVARCHAR	50	Name of the started product	--
dm_productversion	VARCHAR2	50	varchar	50	MVARCHAR	50	Version of the started product	--
dm_productlanguage	CHAR	2	char	2	VARCHAR	2	Language of the started product. (If the language is unknown, NULL is set)	--
dm_filename	VARCHAR2	255	varchar	255	MVARCHAR	255	Name of the file used	--
dm_fileversion	VARCHAR2	50	varchar	50	MVARCHAR	50	File version	--
dm_filelanguage	CHAR	2	char	2	VARCHAR	2	File language. (If the language is unknown, NULL is set)	--
dm_logonuser	VARCHAR2	128	varchar	128	MVARCHAR	128	Login user	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_execaccount	VARCHAR2	128	varchar	128	MVARCHAR	128	Program's execution account	--
dm_startdate	DATE	--	datetime	8	TIMESTAMP	--	Program suppression date and time	--
dm_hostname	VARCHAR2	64	varchar	64	MVARCHAR	64	Host name#	--
dm_ipaddress	VARCHAR2	15	varchar	15	MVARCHAR	15	IP address#	--
dm_flag	NUMBER	3	tinyint	1	SMALLINT	--	Whether or not data is stored in the netmdm_monitoring_security table: • NULL: Not stored • 1: Stored	--

Legend:

--: Not applicable

#

In the case of the suppress history collected by a managing server version 07-50 or earlier, NULL is set when the managing server is upgraded to 08-00.

C.45 netmdm_monitoring_security

This table stores the suppress history and operation history that are managed in the Operation Log List window.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_nodename	VARCHAR2	64	varchar	64	MVARCHAR	64	Node name	--
dm_hostname	VARCHAR2	64	varchar	64	MVARCHAR	64	Host name	--
dm_ipaddress	VARCHAR2	15	varchar	15	MVARCHAR	15	IP address	--
dm_startdate	DATE	--	datetime	8	TIMESTAMP	--	Event start time	--
dm_enddate	DATE	--	datetime	8	TIMESTAMP	--	Event end time	--
dm_eventtype	NUMBER	10	int	4	INTEGER	--	Event type: • 0x00000001: Start process • 0x00000002: Stop process • 0x00000003: Change caption • 0x00000004: Change active window	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_eventtype	NUMBER	10	int	4	INTEGER	--	• 0x00000005: Start PC • 0x00000006: Stop PC • 0x00000007: Log on • 0x00000008: Log off • 0x00010010: Copy file • 0x00010011: Move file • 0x00010012: Rename file • 0x00010013: Delete file • 0x00010014: Create file • 0x00010015: Open file • 0x00020010: Copy folder • 0x00020011: Move folder • 0x00020012: Rename folder • 0x00020013: Delete folder • 0x00020014: Create folder • 0x00030001: Print • 0x00030002: Printing suppression • 0x00030003: Print suppression released • 0x00040001: Web access • 0x00050001: External media connection • 0x00050002: External media disconnection (removal) • 0x00060001: USB connection permission • 0x00060002: USB connection suppression • 0x01000000: Suppress history	--
dm_filename	VARCHAR2	520	varchar	520	MVARCHAR	520	File name or folder name before operation. (The file name or folder name is converted to lower-case letters and its full path is stored. A folder name ends with \.)	--
dm_filenamenew	VARCHAR2	520	varchar	520	MVARCHAR	520	File name or folder name after operation. (The file name or folder name is converted to lower-case letters and its full path is stored. A folder name ends with \.)	--
dm_productname	VARCHAR2	50	varchar	50	MVARCHAR	50	Name of the product used	--
dm_productversion	VARCHAR2	50	varchar	50	MVARCHAR	50	Product version	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_productlanguage	NUMBER	10	int	4	INTEGER	--	Product language. (If the language is unknown, NULL is set)	--
dm_fileversion	VARCHAR2	50	varchar	50	MVARCHAR	50	File version	--
dm_filelanguage	NUMBER	10	int	4	INTEGER	--	File language. (If the language is unknown, NULL is set)	--
dm_logonuser	VARCHAR2	128	varchar	128	MVARCHAR	128	Logon user	--
dm_execaccount	VARCHAR2	128	varchar	128	MVARCHAR	128	Program's execution account	--
dm_caption	VARCHAR2	520	varchar	520	MVARCHAR	520	Window caption	--
dm_processname	VARCHAR2	520	varchar	520	MVARCHAR	520	The following information is stored: For software operation history: Name of the process that resulted in the event For file operation history: Name of the process that manipulated file For software start suppression: Name of the program that suppressed the start	--
dm_drivetypeold	NUMBER	10	int	4	INTEGER	--	Drive type before operation: • 0: Other • 1: Local disk • 2: Network drive • 3: Removable • 4: CDROM • 5: RAMDISK	--
dm_drivetypenew	NUMBER	10	int	4	INTEGER	--	Drive type after operation: • 0: Other • 1: Local disk • 2: Network drive • 3: Removable • 4: CDROM • 5: RAMDISK	--
dm_documentname	VARCHAR2	260	varchar	260	MVARCHAR	260	Name of the document that became the target of printing or printing suppression	--
dm_printername	VARCHAR2	484	varchar	484	MVARCHAR	484	Name of the printer used for printing	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_printingresult	NUMBER	3	tinyint	1	SMALLINT	--	Result of print operation suppression cancellation: • 0x00: Successful • 0x01: Failed	--
dm_url	VARCHAR2	2,083	varchar	2,083	MVARCHAR	2,083	URL of the accessed Web page	--
dm_drivetype	NUMBER	10	int	4	INTEGER	--	Drive type of the external media that was connected or disconnected (removed): • 0x0000: Other • 0x0001: Local disk • 0x0003: Removable • 0x0004: CDROM	--
dm_drivename	CHAR	2	char	2	CHAR	2	Drive name of the external media that was connected or disconnected (removed). Two letters are used to indicate the drive name.	--
dm_usbconnectname	VARCHAR2	1024	varchar	1024	MVARCHAR	1024	Connect name of the device that was permitted or prevented from connecting	--
dm_usbdiskdrive	VARCHAR2	2048	varchar	2048	MVARCHAR	2048	Instance ID of the device that was permitted or prevented from connecting (disk drive)	--
dm_usbcontroller	VARCHAR2	2048	varchar	2048	MVARCHAR	2048	Device instance ID of the device that was permitted or prevented from connecting (USB controller)	--
dm_usballowedcondition	VARCHAR2	2069	varchar	2069	MVARCHAR	2069	Condition used for permitting device connection	--
dm_devicetype	NUMBER	10	int	4	INTEGER	--	Type of device that was connected, disconnected, permitted, or prevented from connecting: • 0x0000: Unknown • 0x0001: USB storage device • 0x0002: Internal CD/DVD drive • 0x0003: Internal floppy disk drive • 0x0004: IEEE1394-connected device • 0x0005: Internal SD card • 0x0006: Bluetooth device • 0x0007: Imaging device	--

Legend:

--: Not applicable

C.46 netmdm_monitoring_usbconnect

This table manages the information read from USB media whose access is excluded from being suppressed.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_policyname	VARCHAR2	64	varchar	64	MVARCHAR	64	Policy name	--
dm_conditiontype	NUMBER	3	tinyint	1	SMALLINT	--	ID indicating the condition type of the device to be excluded: • 0x00: Full-match comparison of connect name • 0x01: Full-match comparison of device instance ID • 0x02: Starts-with comparison of device instance ID • 0x03: Ends-with comparison of device instance ID • 0x04: Contains comparison of device instance ID • 0x05: Starts and ends with comparison of device instance ID • 0x06: Full-match comparison of device instance ID (USB controller) • 0x07: Starts-with comparison of device instance ID (USB controller) • 0x08: Ends-with comparison of device instance ID (USB controller) • 0x09: Contains comparison of device instance ID (USB controller) • 0x0A: Starts and ends with comparison of device instance ID (USB controller) • 0x0B: Full-match comparison of Bluetooth connect name • 0x0C: Full-match comparison of Bluetooth type device instance ID • 0x0D: Starts-with comparison of Bluetooth type device instance ID • 0x0E: Ends-with comparison of Bluetooth type device instance ID • 0x0F: Contains comparison of Bluetooth type device instance ID • 0x10: Starts and ends with comparison of Bluetooth type device instance ID	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_conditiontype	NUMBER	3	tinyint	1	SMALLINT	--	• 0x11: Full-match comparison of Bluetooth controller device instance ID • 0x12: Starts-with comparison of Bluetooth controller device instance ID • 0x13: Ends-with comparison of Bluetooth controller device instance ID • 0x14: Contains comparison of Bluetooth controller device instance ID • 0x15: Starts and ends with comparison of Bluetooth controller device instance ID • 0x16: Full-match comparison of imaging device connect names • 0x17: Full-match comparison of imaging device type device instance ID • 0x18: Starts-with comparison of imaging device type device instance ID • 0x19: Ends-with comparison of imaging device type device instance ID • 0x1A: Contains comparison of imaging device type device instance ID • 0x1B: Starts and ends with match comparison of imaging device type device instance ID • 0x1C: Full-match comparison of imaging device controller device instance ID • 0x1D: Starts-with comparison of imaging device controller device instance ID • 0x1E: Ends-with comparison of imaging device controller device instance ID • 0x1F: Contains comparison of imaging device controller device instance ID • 0x20: Starts and ends with comparison of imaging device controller device instance ID	--
dm_condition	VARCHAR2	2,048	varchar	2,048	MVARCHAR	2,048	USB media suppression exclusion conditions	--
dm_comment	VARCHAR2	64	varchar	64	MVARCHAR	64	Comment on USB media suppression exclusion conditions	--

Legend:

--: Not applicable

C.47 netmdm_monitoring_webfilter

This table manages the Web access log filtering setting.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_policyname	VARCHAR2	64	varchar	64	MVARCHAR	64	Policy name	1
dm_filtername	VARCHAR2	64	varchar	64	MVARCHAR	64	Registered name of the filtering condition type	2
dm_filtertype	NUMBER	3	tinyint	1	SMALLINT	--	Filtering condition type: • 0x00: URL • 0x01: Title	--
dm_filtercondition	VARCHAR2	260	varchar	260	MVARCHAR	260	Filtering condition	--

Legend:

--: Not applicable

C.48 netmdm_monitoring_work

This table stores information about programs from which operation times are acquired.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_policyname	VARCHAR2	64	varchar	64	MVARCHAR	64	Policy name	--
dm_softwarename	VARCHAR2	50	varchar	50	MVARCHAR	50	Name of software from which operation time is acquired.	--
dm_softwareversion	VARCHAR2	50	varchar	50	MVARCHAR	50	Software version (NULL if none is specified)	--
dm_programname	VARCHAR2	255	varchar	255	MVARCHAR	255	Name of the component program of the software	--
dm_programversion	VARCHAR2	50	varchar	50	MVARCHAR	50	Program version (NULL if none is specified)	--
dm_programlanguage	NUMBER	10	int	4	INTEGER	--	• 0x0000: Neutral • Other: Language classification • NULL: No language specified	--

Legend:

--: Not applicable

C.49 netmdm_monitoring_workresult

This table stores information about the software operation times acquired by software operation monitoring.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_nodename	VARCHAR2	64	varchar	64	MVARCHAR	64	Host name	1
dm_getdate	DATE	--	datetime	8	TIMESTAMP	--	Date that the operation time was acquired.	2
dm_softwarename	VARCHAR2	50	varchar	50	MVARCHAR	50	Software name	3
dm_softwareversion	VARCHAR2	50	varchar	50	MVARCHAR	50	Software version	4
dm_softwktime	NUMBER	10	int	4	INTEGER	--	Operation time of the software	5
dm_termwktime	NUMBER	10	int	4	INTEGER	--	Operation time of the machine	6

Legend:

--: Not applicable

C.50 netmdm_nnm_management

This table stores information about OpenView Linkage.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_entryname	VARCHAR2	64	varchar	64	MVARCHAR	64	Name registered to HP NNM (host name or IP address)	1
dm_entryattributes	NUMBER	10	int	4	INTEGER	--	Attributes registered to HP NNM: • 1: Client • 2: Relay system • 8: Relay manager	2
dm_hostname	VARCHAR2	64	varchar	64	MVARCHAR	64	Name in the system configuration (host name or IP address)	--
dm_nodename	VARCHAR2	64	varchar	64	MVARCHAR	64	Not used	--
dm_primarykey	CHAR	16	char	16	MCHAR	16	Not used	--

Legend:

--: Not applicable

C.51 netmdm_node

This table stores destination information.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_nodename	VARCHAR2	64	varchar	64	MVARCHAR	64	Host name or host group name (the value is converted to lowercase letters)	--
dm_nodeattributes	NUMBER	10	int	4	INTEGER	--	Attribute of dm_nodename: • 0x00000000: Host group name • 0x00000001: Host name (client) • 0x00000002: Host name (relay system)	--
dm_nodepath1	VARCHAR2	65	varchar	65	MVARCHAR	65	Name, prefixed by a backslash (\), of the highest group on the destination route (for the highest group, only \ is displayed)	--
dm_nodepath2	VARCHAR2	65	varchar	65	MVARCHAR	65	Name, prefixed by a backslash (\), of the second highest group on the destination route (if not used, spaces are set)	--
dm_nodepath3	VARCHAR2	65	varchar	65	MVARCHAR	65	Name, prefixed by a backslash (\), of the third highest group on the destination route (if not used, spaces are set)	--
dm_nodepath4	VARCHAR2	65	varchar	65	MVARCHAR	65	Name, prefixed by a backslash (\), of the fourth highest group on the destination route (if not used, spaces are set)	--
dm_nodepath5	VARCHAR2	65	varchar	65	MVARCHAR	65	Name, prefixed by a backslash (\), of the fifth highest group on the destination route (if not used, spaces are set)	--
dm_nodepath6	VARCHAR2	65	varchar	65	MVARCHAR	65	Name, prefixed by a backslash (\), of the sixth highest group on the destination route (if not used, spaces are set)	--
dm_comment	VARCHAR2	64	varchar	64	MVARCHAR	64	Comment	--
dm_systeminf	CHAR	8	char	8	MCHAR	8	JP1/Software Distribution Manager management information	--
dm_nodename2	VARCHAR2	64	varchar	64	MVARCHAR	64	Host name or host group name (the value is not converted to lowercase letters)	--

Legend:

--: Not applicable

C.52 netmdm_node_policy

This table stores conditions (policy) for automatically maintaining host groups.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_infotype	NUMBER	10	int	4	INTEGER	--	Policy type: • 1: Group by IP address • 2: Group new hosts • 3: Group by OS type • 4: Group by user inventory • 5: Combined conditions of policy • 6: Registration of new host ID group	1
dm_number	NUMBER	10	int	4	INTEGER	--	Management number for each type	2
dm_status	NUMBER	10	int	4	INTEGER	--	Operating status: • 0: Running • 1: Stopped • 2: Running only under combined conditions	--
dm_nodeattrrange	NUMBER	10	int	4	INTEGER	--	Node attribute subject to grouping: • 0: All node types • 1: Clients only	--
dm_condition1_string	VARCHAR2	64	varchar	64	MVARCHAR	64	Character string data for condition 1	--
dm_condition1_integer	NUMBER	10	numeric	10	DECIMAL	10	Numeric data for condition 1	--
dm_condition1_logical	VARCHAR2	10	varchar	10	MVARCHAR	10	Logical operation between conditions 1 and 2	--
dm_condition2_string	VARCHAR2	64	varchar	64	MVARCHAR	64	Character string data for condition 2	--
dm_condition2_integer	NUMBER	10	numeric	10	DECIMAL	10	Numeric data for condition 2	--
dm_condition2_logical	VARCHAR2	10	varchar	10	MVARCHAR	10	Logical operation between conditions 2 and 3	--
dm_condition3_string	VARCHAR2	64	varchar	64	MVARCHAR	64	Character string data for condition 3	--
dm_condition3_integer	NUMBER	10	numeric	10	DECIMAL	10	Numeric data for condition 3	--
dm_condition3_logical	VARCHAR2	10	varchar	10	MVARCHAR	10	Logical operation between conditions 3 and 4	--
dm_condition4_string	VARCHAR2	64	varchar	64	MVARCHAR	64	Character string data for condition 4	--
dm_condition4_integer	NUMBER	10	numeric	10	DECIMAL	10	Numeric data for condition 4	--
dm_condition4_logical	VARCHAR2	10	varchar	10	MVARCHAR	10	Logical operation between conditions 4 and 5	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_condition5_string	VARCHAR2	64	varchar	64	MVARCHAR	64	Character string data for condition 5	--
dm_condition5_integer	NUMBER	10	numeric	10	DECIMAL	10	Numeric data for condition 5	--
dm_condition5_logical	VARCHAR2	10	varchar	10	MVARCHAR	10	Logical operation between conditions 5 and 6	--
dm_condition6_string	VARCHAR2	64	varchar	64	MVARCHAR	64	Character string data for condition 6	--
dm_condition6_integer	NUMBER	10	numeric	10	DECIMAL	10	Numeric data for condition 6	--
dm_groupname	VARCHAR2	255	varchar	255	MVARCHAR	255	Path or ID group name of the registration target host group	--

Legend:

--: Not applicable

C.53 netmdm_oidlist

This table stores the software information obtained by using the **Search for Microsoft Office products** option of a *Get software information from client* job. The **Software Inventory pag**e of the System Configuration window or Destination window displays only the software information whose parent software ID is NULL. If the parent software ID is not NULL, the software is not treated as a component of Microsoft Office products.

Note that some of the information is not obtained for some products.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_nodename	VARCHAR2	64	varchar	64	MVARCHAR	64	Node name	--
dm_displayname	VARCHAR2	255	varchar	255	MVARCHAR	255	Software name (for display)	--
dm_name	VARCHAR2	255	varchar	255	MVARCHAR	255	Software name	--
dm_version	VARCHAR2	255	varchar	255	MVARCHAR	255	Software version	--
dm_displayversion	VARCHAR2	255	varchar	255	MVARCHAR	255	Software version (for display)	--
dm_language	CHAR	2	char	2	VARCHAR	2	Language	--
dm_publisher	VARCHAR2	255	varchar	255	MVARCHAR	255	Company name	--
dm_productid	VARCHAR2	255	varchar	255	MVARCHAR	255	Product ID	--
dm_regcompany	VARCHAR2	255	varchar	255	MVARCHAR	255	Registered company name	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_regowner	VARCHAR2	255	varchar	255	MVARCHAR	255	Registered owner name	--
dm_installfolder	VARCHAR2	255	varchar	255	MVARCHAR	255	Path	--
dm_filename	VARCHAR2	255	varchar	255	MVARCHAR	255	File name	--
dm_softwareid	VARCHAR2	255	varchar	255	MVARCHAR	255	Software ID	--
dm_parentsoftwareid	VARCHAR2	255	varchar	255	MVARCHAR	255	Parent software ID	--
dm_installdate	VARCHAR2	255	varchar	255	MVARCHAR	255	Installation date	--
dm_searchdate	VARCHAR2	255	varchar	255	MVARCHAR	255	Search date	--
dm_size	NUMBER	10	int	4	INTEGER	--	Size	--
dm_targetos	NUMBER	10	int	4	INTEGER	--	(Not used)	--
dm_accesses	NUMBER	10	int	4	INTEGER	--	(Not used)	--
dm_attributes	NUMBER	10	int	4	INTEGER	--	(Not used)	--
dm_installstate	NUMBER	10	int	4	INTEGER	--	(Not used)	--
dm_installsize	NUMBER	10	int	4	INTEGER	--	(Not used)	--
dm_softwareelementstate	NUMBER	10	int	4	INTEGER	--	(Not used)	--
dm_caption	VARCHAR2	255	varchar	255	MVARCHAR	255	(Not used)	--
dm_softwareelementid	VARCHAR2	255	varchar	255	MVARCHAR	255	(Not used)	--
dm_othertargetos	VARCHAR2	255	varchar	255	MVARCHAR	255	(Not used)	--
dm_lastusedate	VARCHAR2	255	varchar	255	MVARCHAR	255	(Not used)	--
dm_status	VARCHAR2	255	varchar	255	MVARCHAR	255	(Not used)	--

Legend:

--: Not applicable

C.54 netmdm_ospatch_classref

This table stores class information about patches.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_classificationcode	NUMBER	10	int	4	INTEGER	--	Internal class code	--
dm_classificationname	VARCHAR2	200	varchar	200	MVARCHAR	200	Class	--
dm_displaystatus	NUMBER	1	int	4	INTEGER	--	Indicates the display setting selected in **List of software updates**: • 0: Do not display. • 1: Display.	--
dm_autodownloadstatus	NUMBER	1	int	4	INTEGER	--	Indicates the automatic acquisition setting selected: • 0: Do not download. • 1: Download.	--

Legend:
--: Not applicable

C.55 netmdm_ospatch_patchinf

This table stores patch information and acquired patch data.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_patchid	NUMBER	10	int	4	INTEGER	--	Patch ID	--
dm_title	VARCHAR2	800	varchar	800	MVARCHAR	800	Title	--
dm_description	VARCHAR2	1,500	varchar	1,500	MVARCHAR	1,500	Description	--
dm_classification	NUMBER	10	int	4	INTEGER	--	Class	--
dm_products	NUMBER	10	int	4	INTEGER	--	Products (If there is more than one product, the XOR of each product's numeric bits is stored.)	--
dm_releasedate	DATE	--	datetime	8	TIMESTAMP	--	Release date	--
dm_details	VARCHAR2	2,083	varchar	2,083	MVARCHAR	2,083	Detailed information	--
dm_kbarticle	VARCHAR2	16	varchar	16	MVARCHAR	16	Technical information number for support	--
dm_msrcnumber	VARCHAR2	16	varchar	16	MVARCHAR	16	Security number	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_msrcseverity	VARCHAR2	15	varchar	15	MVARCHAR	15	Security level	--
dm_updateid	VARCHAR2	36	varchar	36	MVARCHAR	36	Security update ID	--
dm_updateurl	VARCHAR2	1,024	varchar	1,024	MVARCHAR	1,024	URL from which patch is downloaded	--
dm_language	VARCHAR2	32	varchar	32	MVARCHAR	32	Supported languages	--
dm_ospatchfilename	VARCHAR2	260	varchar	260	MVARCHAR	260	Name of executable patch file	--
dm_scripturl	VARCHAR2	128	varchar	128	MVARCHAR	128	URL of the script file	--
dm_ospatchstatus	NUMBER	10	int	4	INTEGER	--	OS patch acquisition status: • 0x0000: Neither the patch nor the script has been acquired. • 0x0001: Only the patch has been acquired. • 0x0002: Only the script has been acquired. • 0x0004: The patch and the script have both been acquired. • 0x0010: Already packaged	--
dm_ospatchfile1	BLOB	--	image	--	BLOB	--	Patch data (Patches that exceed 100 megabytes are partitioned into 100-megabyte segments for storage.)	--
dm_ospatchfile2	BLOB	--	image	--	BLOB	--		--
dm_ospatchfile3	BLOB	--	image	--	BLOB	--		--
dm_ospatchfile4	BLOB	--	image	--	BLOB	--		--
dm_ospatchfile5	BLOB	--	image	--	BLOB	--		--
dm_ospatchfile6	BLOB	--	image	--	BLOB	--		--
dm_ospatchfile7	BLOB	--	image	--	BLOB	--		--
dm_ospatchfile8	BLOB	--	image	--	BLOB	--		--
dm_ospatchfile	--	--	--	--	BLOB	--	Patch data (maximum of 1,840 megabytes)	--
dm_patchsize	NUMBER	10	int	4	INTEGER	--	Patch size	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_cabinetname	VARCHAR2	83	varchar	83	MVARCHAR	83	Name of the storage destination cabinet, and package name	--

Legend:

--: Not applicable

C.56 netmdm_ospatch_productref

This table stores information about the programs to be patched.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_productcode	NUMBER	10	int	4	INTEGER	--	Internal program code	--
dm_productname	VARCHAR2	200	varchar	200	MVARCHAR	200	Program name	--
dm_displaystatus	NUMBER	1	int	--	INTEGER	--	Indicates the display setting selected in **List of software updates**: • 0: Do not display. • 1: Display.	--
dm_autodownloadstatus	NUMBER	1	int	--	INTEGER	--	Indicates the automatic download setting selected: • 0: Do not download. • 1: Download.	--

Legend:

--: Not applicable

C.57 netmdm_ospatch_script

This table stores the script files for installing patches.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_scripturl	VARCHAR	128	varchar	128	MVARCHAR	128	URL of the script file	--
dm_scriptfile	LONGRAW	--	image	--	BLOB	--	Script file	--

Legend:

--: Not applicable

C.58 netmdm_ospatch_xmlinf

This table stores the version of the patch information file.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_xmlversion	VARCHAR2	12	varchar	12	MVARCHAR	12	Version of the patch information file	--
dm_xmlrevision	VARCHAR2	12	varchar	12	MVARCHAR	12	Revision of the patch information file	--

Legend:

--: Not applicable

C.59 netmdm_package

This table stores the package and installation script body.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_dmtype	CHAR	1	char	1	CHAR	1	Type of Packager used for packaging: • C: WS (UNIX) • D: PC (Windows)	--
dm_cabinetid	CHAR	2	char	2	MCHAR	2	Cabinet ID	--
dm_packageid	VARCHAR2	44	varchar	44	MVARCHAR	44	Package ID	--
dm_version	VARCHAR2	8	varchar	8	MVARCHAR	8	Package version	--
dm_generation	VARCHAR2	4	varchar	4	MVARCHAR	4	Package generation number	--
dm_packagefilename	CHAR	8	char	8	MCHAR	8	Name of package management file	1
dm_scriptfilename	CHAR	8	char	8	MCHAR	8	Script file management file name	--
dm_package	BLOB	--	image	--	BLOB	--	Package body	--
dm_scriptfile	LONG RAW	--	image	--	BLOB	--	Installation script body	--

Legend:

--: Not applicable

C.60 netmdm_package_inf

This table stores package attribute information. This table contains records that are in a one-to-one correspondence with the records of netmdm_package.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_dmtype	CHAR	1	char	1	CHAR	1	Type of Packager used for packaging: • C: WS (UNIX) • D: PC (Windows)	1
dm_cabinetid	CHAR	2	char	2	MCHAR	2	Cabinet ID	2
dm_packageid	VARCHAR2	44	varchar	44	MVARCHAR	44	Package ID	3
dm_version	VARCHAR2	8	varchar	8	MVARCHAR	8	Package version	4
dm_generation	VARCHAR2	4	varchar	4	MVARCHAR	4	Package generation number	5
dm_packagename	VARCHAR2	50	varchar	50	MVARCHAR	50	Package name	--
dm_capacity	NUMBER	10	int	4	INTEGER	--	Package size	--
dm_packagefilename	CHAR	8	char	8	MCHAR	8	Name of the package management file	--
dm_recovery	NUMBER	1	bit	1	SMALLINT	--	Whether to restore in the event of a failure: • 1: Restore • 0: Do not restore	--
dm_compress	NUMBER	1	bit	1	SMALLINT	--	Package compression: • 1: Compressed • 0: Not compressed	--
dm_systeminf	BLOB	--	image	--	BINARY	784	JP1/Software Distribution Manager management information	--

Legend:
--: Not applicable

C.61 netmdm_registry

This table stores the registry information for a client.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_nodename	VARCHAR2	64	varchar	64	MVARCHAR	64	Host name (host name, IP address, or host ID)	1
dm_regpath	VARCHAR2	255	varchar	255	MVARCHAR	255	Registry path	2
dm_regstatus	RAW	1	binary	1	BINARY	1	Registry status:	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
`dm_regstatus`	`RAW`	1	`binary`	1	`BINARY`	1	• `0x00`: Data has not been collected • `0x01`: Data has been collected successfully • `0x02`: Specified registry path was not found • `0x03`: Data was not found • `0x04`: Data has exceeded the maximum value	--
`dm_regtype`	`RAW`	1	`binary`	1	`BINARY`	1	Registry attributes: • `0x01`: Character string • `0x02`: DWORD • `0x03`: Binary	--
`dm_value`	`VARCHAR2`	255	`varchar`	255	`MVARCHAR`	255	Registry data	--
`dm_oskind`	`NUMBER`	10	`int`	4	`INTEGER`	--	OS type of the destination: • `0x02`: Windows NT 4.0 • `0x04`: Windows 2000 • `0x08`: Windows XP • `0x10`: Windows 95 • `0x20`: Windows 98 • `0x40`: Windows Me • `0x80`: Windows Server 2003 • `0x100`: Windows Vista • `0x200`: Windows Server 2008 • `0x400`: Windows 7 • `0x800`: Windows Server 2008 R2 • `0x1000`: Windows 8 • `0x2000`: Windows Server 2012	--

Legend:

--: Not applicable

C.62 netmdm_reglist

This table stores the registry collection items.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_itemname	VARCHAR2	64	varchar	64	MVARCHAR	64	Item name	--
dm_priority	NUMBER	3	int	4	INTEGER	--	Display order	--
dm_regpath	VARCHAR2	255	varchar	255	MVARCHAR	255	Registry path	1
dm_oskind1	NUMBER	10	int	4	INTEGER	--	OS type of higher system: • 0x02: Windows NT 4.0 • 0x04: Windows 2000 • 0x08: Windows XP • 0x10: Windows 95 • 0x20: Windows 98 • 0x40: Windows Me • 0x80: Windows Server 2003 • 0x100: Windows Vista • 0x200: Windows Server 2008 • 0x400: Windows 7 • 0x800: Windows Server 2008 R2 • 0x1000: Windows 8 • 0x2000: Windows Server 2012 • 0xffff: All OSs	--
dm_oskind2	NUMBER	10	int	4	INTEGER	--	OS type of local system: • 0x02: Windows NT 4.0 • 0x04: Windows 2000 • 0x08: Windows XP • 0x10: Windows 95 • 0x20: Windows 98 • 0x40: Windows Me • 0x80: Windows Server 2003 • 0x100: Windows Vista • 0x200: Windows Server 2008 • 0x400: Windows 7 • 0x800: Windows Server 2008 R2 • 0x1000: Windows 8 • 0x2000: Windows Server 2012 • 0xffff: All OSs	--
dm_attrflag	RAW	1	binary	1	BINARY	1	Item attributes:	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_attrflag	RAW	1	binary	1	BINARY	1	• 0x00: Items managed on local server • 0x01: Items managed on higher server • 0x02: Items managed on higher and local servers	--

Legend:

--: Not applicable

C.63 netmdm_schedule

This table stores the schedule of a registered job.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_jobname	VARCHAR2	32	varchar	32	MVARCHAR	32	Scheduled job name	--
dm_jobschnum	VARCHAR2	64	varchar	64	MVARCHAR	64	Scheduled job number#: • J*sxxxxxxxxxxxxxx*: Job registration schedule • J*rxxxxxxxxxxxxxx*: Client job deletion schedule • J*dxxxxxxxxxxxxxx*: Job deletion schedule • J*gxxxxxxxxxxxxxx*: Job definition deletion schedule • J*exxxxxxxxxxxxxx*: Job execution schedule	1
dm_eventtime	DATE	--	datetime	8	TIMESTAMP	--	Schedule execution date/time	--
dm_limittime	DATE	--	datetime	8	TIMESTAMP	--	Schedule execution time limit	--
dm_executetime	DATE	--	datetime	8	TIMESTAMP	--	Schedule registration date/time	--
dm_systeminf	BLOB	--	image	--	BLOB	--	JP1/Software Distribution Manager management information	--

--: Not applicable. *xxxxxxxxxxxxxx*: Job number.

#

For an ID group job, the number begins with I, not J.

C.64 netmdm_softwaredel

This table stores information about software that was deleted from software inventory.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
`dm_ppname`	`VARCHAR2`	50	`varchar`	50	`MVARCHAR`	50	Software name	--
`dm_filename`	`VARCHAR2`	255	`varchar`	255	`MVARCHAR`	255	Names of files constituting the software	1
`dm_createdate`	`CHAR`	19	`char`	19	`CHAR`	19	Date and time the software was created	2
`dm_filesize`	`VARCHAR2`	10	`varchar`	10	`VARCHAR`	10	File size of the software	3
`dm_sversion`	`VARCHAR2`	50	`varchar`	50	`MVARCHAR`	50	Version of the software	--
`dm_systemtime`	`CHAR`	19	`char`	19	`CHAR`	19	Creation date (UTC)	--

Legend:
--: Not applicable

C.65 netmdm_softwaredic

This table stores the result of searching software inventory at a client.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
`dm_ppname`	`VARCHAR2`	50	`varchar`	50	`MVARCHAR`	50	Software name	--
`dm_filename`	`VARCHAR2`	255	`varchar`	255	`MVARCHAR`	255	Names of files constituting the software	1
`dm_createdate`	`CHAR`	19	`char`	19	`CHAR`	19	Date and time the software was created	2
`dm_filesize`	`VARCHAR2`	10	`varchar`	10	`VARCHAR`	10	File size of the software	3
`dm_company`	`VARCHAR2`	50	`varchar`	50	`MVARCHAR`	50	Company name of the software	--
`dm_language`	`CHAR`	2	`char`	2	`VARCHAR`	2	Language identifier of the software	--
`dm_charid`	`CHAR`	2	`char`	2	`MCHAR`	2	(Unused)	--
`dm_sversion`	`VARCHAR2`	50	`varchar`	50	`MVARCHAR`	50	Version of the software	--
`dm_productname`	`VARCHAR2`	50	`varchar`	50	`MVARCHAR`	50	Product name of the software	--
`dm_serchdate`	`CHAR`	19	`char`	19	`CHAR`	19	Search date of the software	--
`dm_pflg1`	`CHAR`	1	`char`	1	`MCHAR`	1	Option flag 1 (record status): • `NULL`: Initial status • `0x01`: Displayed	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_pflg1	CHAR	1	char	1	MCHAR	1	• 0x02: Hidden	--
dm_pflg2	CHAR	1	char	1	MCHAR	1	Option flag 2	--
dm_ppno	NUMBER	10	int	4	INTEGER	--	Internal information of JP1/Software Distribution (program product number)	--
dm_pathname	VARCHAR2	255	varchar	255	MVARCHAR	255	Path to the software	--
dm_fversion	VARCHAR2	50	varchar	50	MVARCHAR	50	File version	--
dm_comment	VARCHAR2	50	varchar	50	MVARCHAR	50	Comment	--
dm_systemtime	CHAR	19	char	19	CHAR	19	Creation date (UTC)	--

Legend:

--: Not applicable

C.66 netmdm_softwarelicence

This table stores the number of software licenses.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_ppname	VARCHAR2	50	varchar	50	MVARCHAR	50	Software name	1
dm_version	VARCHAR2	50	varchar	50	MVARCHAR	50	Version	2
dm_licence	NUMBER	10	int	4	INTEGER	--	Number of licenses	--
dm_warning	NUMBER	10	int	4	INTEGER	--	Warning value	--

Legend:

--: Not applicable

C.67 netmdm_stscnt

This table stores the job execution status expressed as a combination of host and package subject to job execution.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_jobno	CHAR	16	char	16	MCHAR	16	Number assigned to the job automatically	1

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_sitename	VARCHAR2	64	varchar	64	MVARCHAR	64	Host name at site	2
dm_waitcount	NUMBER	10	int	4	INTEGER	--	Execution wait count	--
dm_logonwaitcount	NUMBER	10	int	4	INTEGER	--	Logon wait count	--
dm_completecount	NUMBER	10	int	4	INTEGER	--	Completion count	--
dm_execcount	NUMBER	10	int	4	INTEGER	--	Executing status count	--
dm_inswaitcount	NUMBER	10	int	4	INTEGER	--	Installation wait count	--
dm_inserrorcount	NUMBER	10	int	4	INTEGER	--	Installation error count	--
dm_othererrorcount	NUMBER	10	int	4	INTEGER	--	Other error count	--
dm_refusecount	NUMBER	10	int	4	INTEGER	--	Installation rejection count	--
dm_totalcount	NUMBER	10	int	4	INTEGER	--	Total execution count	--
dm_idname	VARCHAR2	32	varchar	32	MVARCHAR	32	ID group name	3
dm_pendingcount	NUMBER	10	int	4	INTEGER	--	Communication error count	--
dm_transmittingcount	NUMBER	10	int	4	INTEGER	--	Of all the jobs to be sent to the relay managing the ID, number of jobs that have not reached the destination	--

Legend:

--: Not applicable

C.68 netmdm_stscnt_site

This table stores the execution status of ID group jobs (*Install package* and *Send package, allow client to choose* jobs) executed at a relay system, expressed as a combination of host and package.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_jobno	CHAR	16	char	16	MCHAR	16	Number assigned to the job automatically	1
dm_sitename	VARCHAR2	64	varchar	64	MVARCHAR	64	Host name at site	2

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_waitcount	NUMBER	10	int	4	INTEGER	--	Execution wait count	--
dm_logonwaitcount	NUMBER	10	int	4	INTEGER	--	Logon wait count	--
dm_completecount	NUMBER	10	int	4	INTEGER	--	Completion count	--
dm_execount	NUMBER	10	int	4	INTEGER	--	Executing status count	--
dm_inswaitcount	NUMBER	10	int	4	INTEGER	--	Installation wait count	--
dm_inserrorcount	NUMBER	10	int	4	INTEGER	--	Installation error count	--
dm_othererrorcount	NUMBER	10	int	4	INTEGER	--	Other error count	--
dm_refusecount	NUMBER	10	int	4	INTEGER	--	Installation rejection count	--
dm_totalcount	NUMBER	10	int	4	INTEGER	--	Total execution count	--
dm_idname	VARCHAR2	32	varchar	32	MVARCHAR	32	ID group name	3
dm_pendingcount	NUMBER	10	int	4	INTEGER	--	Communication error count	--
dm_transmittingcount	NUMBER	10	int	4	INTEGER	--	Of all the jobs to be sent to the relay managing the ID, number of jobs that have not reached the destination	--

Legend:

--: Not applicable

C.69 netmdm_stscnt_summary

This table stores the execution status of an all-lower-clients job executed from the central manager, expressed as a combination of host and package.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_jobno	CHAR	16	char	16	MCHAR	16	Number assigned to the job automatically	1
dm_primarykey	VARCHAR2	16	varchar	16	MVARCHAR	16	Primary key (number assigned to each job detail)	2
dm_logonwaitcount	NUMBER	10	int	4	INTEGER	--	Logon wait count	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_completecount	NUMBER	10	int	4	INTEGER	--	Completion count	--
dm_inswaitcount	NUMBER	10	int	4	INTEGER	--	Installation wait count	--
dm_inserrorcount	NUMBER	10	int	4	INTEGER	--	Installation error count	--
dm_othererrorcount	NUMBER	10	int	4	INTEGER	--	Other error count	--
dm_refusecount	NUMBER	10	int	4	INTEGER	--	Installation rejection count	--
dm_totalcount	NUMBER	10	int	4	INTEGER	--	Total execution count	--
dm_managername	VARCHAR2	64	varchar	64	MVARCHAR	64	Supervising manager name	--

Legend:

--: Not applicable

C.70 netmdm_suspend

This table stores information about whether processing is suspended.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_suspend	NUMBER	10	int	4	INTEGER	--	Whether processing is suspended: • 0: Not suspended • 1: Suspended	--

Legend:

--: Not applicable

C.71 netmdm_system

This table stores system configuration information. The table contains one record for each client and each relay system and manages the route during job execution.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_nodename	VARCHAR2	64	varchar	64	MVARCHAR	64	Host ID (or the node identification key if no host ID is used)	1
dm_nodeattributes	NUMBER	10	int	4	INTEGER	--	Attributes of dm_nodename:	2

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
`dm_nodeattributes`	`NUMBER`	10	`int`	4	`INTEGER`	--	• `0x00000001`: Client • `0x00000002`: Relay system • `0x00000008`: Relay manager	2
`dm_nodepath1`	`VARCHAR2`	65	`varchar`	65	`MVARCHAR`	65	Host ID, prefixed by a backslash (\\), of the highest relay on the destination route (or the node identification key if no host ID is used). If the host is directly below the manager, only \\ is stored.	--
`dm_nodepath2`	`VARCHAR2`	65	`varchar`	65	`MVARCHAR`	65	Host ID, prefixed by a backslash (\\), of the second highest relay/ manager system on the destination route (or the node identification key if no host ID is used). If there is no applicable relay manager/system, `NULL` is stored.	--
`dm_nodepath3`	`VARCHAR2`	65	`varchar`	65	`MVARCHAR`	65	Host ID, prefixed by a backslash (\\), of the third highest relay/ manager system on the destination route (or the node identification key if no host ID is used). If there is no applicable relay manager/system, `NULL` is stored.	--
`dm_nodepath4`	`VARCHAR2`	65	`varchar`	65	`MVARCHAR`	65	Host ID, prefixed by a backslash (\\), of the fourth highest relay/ manager system on the destination route (or the node identification key if no host ID is used). If there is no applicable relay manager/system, `NULL` is stored.	--
`dm_nodepath5`	`VARCHAR2`	65	`varchar`	65	`MVARCHAR`	65	Host ID, prefixed by a backslash (\\), of the fifth highest relay/ manager system on the destination route (or the node identification key if no host ID is used). If there is no applicable relay manager/system, `NULL` is stored.	--
`dm_nodepath6`	`VARCHAR2`	65	`varchar`	65	`MVARCHAR`	65	Host ID, prefixed by a backslash (\\), of the sixth highest relay/ manager system on the destination route (or the node identification key if no host ID is used). If there is no applicable relay manager/system, `NULL` is stored.	--
`dm_comment`	`VARCHAR2`	64	`varchar`	64	`MVARCHAR`	64	Comment	--
`dm_systeminf`	`RAW`	255	`varbinary`	136	`BINARY`	136	JP1/Software Distribution Manager management information	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_hostname	VARCHAR2	64	varchar	64	MVARCHAR	64	Host name	--
dm_ipaddress	VARCHAR2	15	varchar	15	MVARCHAR	15	IP address	--
dm_commonname	VARCHAR2	32	varchar	32	MVARCHAR	32	Client identification name	--
dm_connectkind	NUMBER	10	int	4	INTEGER	--	PPP connection: • 0x00000000: Not used • 0x00000001: Used	--
dm_updatetime	DATE	--	datetime	8	TIMESTAMP	--	System configuration update date and time	--
dm_uinvtranstime	DATE	--	datetime	8	TIMESTAMP	--	User inventory information transfer date and time	--
dm_uinvupdatetime	DATE	--	datetime	8	TIMESTAMP	--	User inventory information last update date and time	--
dm_systemkey	RAW	1	binary	1	SMALLINT	1	Node identification key: • 0x00: Host name • 0x01: IP address	--
dm_managername	VARCHAR2	64	varchar	64	MVARCHAR	64	Supervising manager name	--
dm_holdflag	RAW	1	binary	1	BINARY	1	Results file hold flag: • 0x00: Do not hold • 0x01: Hold	--
dm_hostid	VARCHAR2	64	varchar	64	MVARCHAR	64	Host ID	--
dm_nodepathview	VARCHAR2	255	varchar	255	MVARCHAR	255	Destination route information, consisting of node identification keys (host name or IP address)	--
dm_regtranstime	DATE	--	datetime	8	TIMESTAMP	--	Registry collection item transfer date and time	--
dm_regupdatetime	DATE	--	datetime	8	TIMESTAMP	--	Last update date and time for registry collection item	--
dm_invupdatetime	DATE	--	datetime	8	TIMESTAMP	--	Last update date and time for system information	--
dm_inspupdatetime	DATE	--	datetime	8	TIMESTAMP	--	Last update date and time for installed package information	--
dm_sinvupdatetime	DATE	--	datetime	8	TIMESTAMP	--	Last update date and time for software inventory information	--
dm_nodename2	VARCHAR2	64	varchar	64	MVARCHAR	64	Host name of client or relay system (the value is not converted to lowercase letters)	--
dm_macaddress	VARCHAR2	12	varchar	12	MVARCHAR	12	MAC address	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_createtime	DATE	--	datetime	8	TIMESTAMP	--	Client or relay system creation date	--
dm_transholdflag	NUMBER	10	int	4	INTEGER	--	File transfer suspension flag: • 0x00: Not suspended • 0x01: Suspended	--
dm_lastupdatetime	DATE	--	datetime	8	TIMESTAMP	--	Last update date and time for an inventory (system configuration information, system information, installation package information, and software information)	--
dm_monupdatetime	DATE	--	datetime	8	TIMESTAMP	--	Last update date and time for operation monitoring information	--
dm_monpolicy	VARCHAR2	85	varchar	85	MVARCHAR	85	Operation monitoring policy information	--
dm_version	VARCHAR2	8	varchar	8	MVARCHAR	8	Policy version	--
dm_generation	VARCHAR2	4	varchar	4	MVARCHAR	4	Policy generation number	--

Legend:

--: Not applicable

C.72 netmdm_system_delete

This table stores the deletion history of system configuration information.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_nodename	VARCHAR2	64	varchar	64	MVARCHAR	64	Route information about the destination that consists of an ID key for operations (host ID or node identification key)	--
dm_nodeattributes	NUMBER	10	int	4	INTEGER	--	Attributes of dm_nodename: • 0x00000001: Client • 0x00000002: Relay system • 0x00000008: Relay manager	--
dm_nodepath1	VARCHAR2	65	varchar	65	MVARCHAR	65	Name, prefixed by a backslash (\), of the highest host on the destination route • For the highest host: \ only • If not used: Space	--
dm_nodepath2	VARCHAR2	65	varchar	65	MVARCHAR	65	Name, prefixed by a backslash (\), of the second highest host on the	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_nodepath2	VARCHAR2	65	varchar	65	MVARCHAR	65	destination route (if not used, spaces are set)	--
dm_nodepath3	VARCHAR2	65	varchar	65	MVARCHAR	65	Name, prefixed by a backslash (\), of the third highest host on the destination route (if not used, spaces are set)	--
dm_nodepath4	VARCHAR2	65	varchar	65	MVARCHAR	65	Name, prefixed by a backslash (\), of the fourth highest host on the destination route (if not used, spaces are set)	--
dm_nodepath5	VARCHAR2	65	varchar	65	MVARCHAR	65	Name, prefixed by a backslash (\), of the fifth highest host on the destination route (if not used, spaces are set)	--
dm_nodepath6	VARCHAR2	65	varchar	65	MVARCHAR	65	Name, prefixed by a backslash (\), of the sixth highest host on the destination route (if not used, spaces are set)	--
dm_comment	VARCHAR2	64	varchar	64	MVARCHAR	64	Comment	--
dm_hostname	VARCHAR2	64	varchar	64	MVARCHAR	64	Host name	--
dm_ipaddress	VARCHAR2	15	varchar	15	MVARCHAR	15	IP address	--
dm_commonname	VARCHAR2	32	varchar	32	MVARCHAR	32	Client identification name	--
dm_connectkind	NUMBER	10	int	4	INTEGER	--	PPP connection: • 0x00000000: Not used • 0x00000001: Used	--
dm_updatetime	DATE	--	datetime	8	TIMESTAMP	--	System configuration information update date and time	--
dm_systemkey	RAW	1	binary	1	SMALLINT	--	Node identification key: • 0x00: Host name • 0x01: IP address	--
dm_managername	VARCHAR2	64	varchar	64	MVARCHAR	64	Supervising manager name	--
dm_holdflag	RAW	1	binary	1	BINARY	1	Result file hold flag: • 0x00: Do not hold • 0x01: Hold	--
dm_hostid	VARCHAR2	64	varchar	64	MVARCHAR	64	Host ID	--
dm_nodepathview	VARCHAR2	255	varchar	255	MVARCHAR	255	Destination route information consisting of a node identification key (host name or IP address)	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_nodename2	VARCHAR2	64	varchar	64	MVARCHAR	64	Host name of client or relay system (the value is not converted to lowercase letters)	--
dm_macaddress	VARCHAR2	12	varchar	12	MVARCHAR	12	MAC address	--
dm_createtime	DATE	--	datetime	8	TIMESTAMP	--	Client or relay system creation time	--
dm_deletetime	DATE	--	datetime	8	TIMESTAMP	--	Client or relay system deletion time	--
dm_deletefactor	NUMBER	10	int	4	INTEGER	--	Deletion cause: • 0x00: Deleted by the administrator • 0x01: Reception of uninstallation result • 0x02: Instructed by higher manager	--
dm_transholdflag	NUMBER	10	int	4	INTEGER	--	File transfer suspension flag: • 0x00: Not suspended • 0x01: Suspended	--
dm_lastupdatetime	DATE	--	datetime	8	TIMESTAMP	--	Last update date and time for obtaining the deletion date and time for a node	--

Legend:

--: Not applicable

C.73 netmdm_systeminf

This table stores the database format.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_netminf	VARCHAR2	32	varchar	32	MVARCHAR	32	Version of the product used to create the database	--
dm_dbversion	NUMBER	10	int	4	INTEGER	--	Format version	--

Legend:

--: Not applicable

C.74 netmdm_systemjob

This table stores the system information for JP1/Software Distribution.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_jobno	CHAR	16	char	16	MCHAR	16	Number assigned to the job automatically	1
dm_requestfile	LONG RAW	--	image	--	BLOB	--	Management information for JP1/Software Distribution Manager or the message data specified by *Report message* job	--
dm_resultfile	BLOB	--	image	--	BLOB	--	Management information for JP1/Software Distribution Manager	--

Legend:

--: Not applicable

C.75 netmdm_userinventry

This table stores user inventory information.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_nodename	VARCHAR2	64	varchar	64	MVARCHAR	64	Host name of the client	1
dm_itemname	VARCHAR2	64	varchar	64	MVARCHAR	64	Name of user inventory item	2
dm_systeminf	VARCHAR2	200	varchar	200	MVARCHAR	200	User inventory information	--

Legend:

--: Not applicable

C.76 netmdm_userinvlist

This table stores a list of user inventory items.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_itemname	VARCHAR2	64	varchar	64	MVARCHAR	64	Item name	1
dm_itemlabel	VARCHAR2	64	varchar	64	MVARCHAR	64	Label name	--
dm_priority	NUMBER	3	int	4	INTEGER	--	Display order	--
dm_itemcomment	VARCHAR2	255	varchar	255	MVARCHAR	255	Comment	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_itemvalues	BLOB	--	image	--	BLOB	--	Value of the selected item. If there are multiple items, the values are delimited by the comma (,). If there is no item, a space is stored.	--
dm_systeminf	BLOB	--	image	--	BLOB	--	Management information for JP1/Software Distribution Manager	--
dm_attrflag	RAW	1	binary	1	BINARY	1	Item attribute flag: • 0x00: Items managed on local server • 0x01: Items managed on higher server • 0x02: Items managed on higher and local servers	--
dm_itemtype	VARCHAR2	8	varchar	8	MVARCHAR	8	Item type: • NULL (no value): Text entry • SELECT: Selection • INSERT: Addable selection	--
dm_texttypes	VARCHAR2	128	varchar	128	MVARCHAR	128	Character type If there are multiple settings, the settings are delimited by the plus sign (+). • NULL (no setting): Cannot be set • FREE: Free • 1LARGE: Uppercase letters • 1SMALL: Lowercase letters • 1NUMBER: Numeric characters • PERIOD: Period • HYPHEN: Hyphen • AT: At sign (@) • PLUS: Plus • 1SPACE: Space in text • 1OTHERS: Other	--
dm_itemoption	VARCHAR2	16	varchar	16	MVARCHAR	16	Input option: • NECESSARY-INP: Required • FREE-INP: Optional	--
dm_upperitemop	VARCHAR2	16	varchar	16	MVARCHAR	16	Input option for the higher manager: • NECESSARY-INP: Required • FREE-INP: Optional For items managed on higher servers or items managed on higher and local servers, this	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_upperitemop	VARCHAR2	16	varchar	16	MVARCHAR	16	column contains the input option for this item specified by the higher manager. For items managed on local servers, this column contains FREE-INP.	--
dm_loweritemop	VARCHAR2	16	varchar	16	MVARCHAR	16	Input option for the lower manager: • NECESSARY-INP: Required • FREE-INP: Optional For items managed on local servers or items managed on higher and local servers, this column contains the input option specified for this item by the local manager. For items managed on higher servers, this column contains FREE-INP. This value is merged with the value of dm_upperitemop and the result is stored in dm_itemoption.	--
dm_upperitemname	VARCHAR2	64	varchar	64	MVARCHAR	64	Name of the higher item. If an item is configured in a hierarchy, this column contains the name of the higher item. If the item is not configured in a hierarchy, this column contains NULL.	--
dm_loweritemname	VARCHAR2	64	varchar	64	MVARCHAR	64	Name of the lower item. If an item is configured in a hierarchy, this column contains the name of the lower item. If the item is not configured in a hierarchy, this column contains NULL.	--

Legend:

--: Not applicable

C.77 netmdm_vidlist

This table stores the software information obtained by using the **Search for anti-virus products** option of a *Get software information from client* job. Note that some of the information might not be obtained for some products.

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_nodename	VARCHAR2	64	varchar	64	MVARCHAR	64	Node name	--
dm_displayname	VARCHAR2	255	varchar	255	MVARCHAR	255	Software name (for display)	--
dm_virusversion	VARCHAR2	255	varchar	255	MVARCHAR	255	Version of the virus definition file	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_name	VARCHAR2	255	varchar	255	MVARCHAR	255	Software name	--
dm_version	VARCHAR2	255	varchar	255	MVARCHAR	255	Software version	--
dm_language	CHAR	2	char	2	VARCHAR	2	Language	--
dm_publisher	VARCHAR2	255	varchar	255	MVARCHAR	255	Company name	--
dm_regcompany	VARCHAR2	255	varchar	255	MVARCHAR	255	Registered company name	--
dm_regowner	VARCHAR2	255	varchar	255	MVARCHAR	255	Registered owner name	--
dm_installfolder	VARCHAR2	255	varchar	255	MVARCHAR	255	Path	--
dm_engineversion	VARCHAR2	255	varchar	255	MVARCHAR	255	Version of virus detection engine	--
dm_softwareid	VARCHAR2	255	varchar	255	MVARCHAR	255	Software ID	--
dm_installdate	VARCHAR2	255	varchar	255	MVARCHAR	255	Installation date	--
dm_searchdate	VARCHAR2	255	varchar	255	MVARCHAR	255	Search date	--
dm_size	NUMBER	10	int	4	INTEGER	--	Size	--
dm_permanent	NUMBER	10	int	4	INTEGER	--	Resident or nonresident virus detection	--
dm_productid	VARCHAR2	255	varchar	255	MVARCHAR	255	(Not used)	--
dm_targetos	NUMBER	10	int	4	INTEGER	--	(Not used)	--
dm_accesses	NUMBER	10	int	4	INTEGER	--	(Not used)	--
dm_attributes	NUMBER	10	int	4	INTEGER	--	(Not used)	--
dm_installstate	NUMBER	10	int	4	INTEGER	--	(Not used)	--
dm_installsize	NUMBER	10	int	4	INTEGER	--	(Not used)	--
dm_softwareelementstate	NUMBER	10	int	4	INTEGER	--	(Not used)	--
dm_caption	VARCHAR2	255	varchar	255	MVARCHAR	255	(Not used)	--
dm_softwareelementid	VARCHAR2	255	varchar	255	MVARCHAR	255	(Not used)	--

Column name	Oracle		Microsoft SQL Server		Embedded RDB		Description	Key No.
	Data type	Size	Data type	Size	Data type	Size		
dm_othertargetos	VARCHAR2	255	varchar	255	MVARCHAR	255	(Not used)	--
dm_lastusedate	VARCHAR2	255	varchar	255	MVARCHAR	255	(Not used)	--
dm_status	VARCHAR2	255	varchar	255	MVARCHAR	255	(Not used)	--

Legend:

--: Not applicable

D. Functional Differences

This appendix describes the following types of functional differences in JP1/Software Distribution:

- Functional differences between JP1/Software Distribution Manager and JP1/Software Distribution Client (relay system)
- Functional differences in the UNIX version of JP1/Software Distribution
- Differences in terminology and function between the Windows and UNIX editions of JP1/Software Distribution, and the correspondence between setup items

D.1 Functional differences between JP1/Software Distribution Manager and JP1/Software Distribution Client (relay system)

This appendix describes the functional differences between JP1/Software Distribution Manager and JP1/Software Distribution Client (relay system). You should be aware of these differences when you design a system configuration or operate the system.

For details about the components of JP1/Software Distribution Manager and JP1/Software Distribution Client (relay system) that can be installed, see *1.1.2 Organization of components* in the *Setup Guide*. For details about the jobs that can be executed, see *2.9.2 Types of jobs that can be created*; for details about the available commands, see *4.2.1 Command types* in the manual *Administrator's Guide Volume 2*.

(1) Functional differences to be noted when designing a system configuration

- Windows JP1/Software Distribution Client (relay system) can be placed under a UNIX JP1/Software Distribution Manager, but Windows JP1/Software Distribution Manager (relay manager) cannot.
- Only JP1/Software Distribution Manager (central manager) supports the failover facility for a cluster system. Neither JP1/Software Distribution Manager (relay manager) nor JP1/Software Distribution Client (relay system) supports this facility.
- JP1/Software Distribution Manager can execute jobs via a relay manager/system, but JP1/Software Distribution Client (relay system) can execute jobs only one level lower in the hierarchy.
- JP1/Software Distribution Client (relay system) can poll multiple higher systems, but JP1/Software Distribution Manager (relay manager) cannot.

(2) Functional differences to be noted when operating a system

- The following functions are available only to JP1/Software Distribution Manager; they cannot be used by JP1/Software Distribution Client (relay system):
    - Installing Remote Installation Manager on a separate PC from the server
    - Restricting the users who use JP1/Software Distribution Manager (security enhancement)
    - Displaying System Configuration, List of Software Information, and Directory Information windows
    - Searching in the Destination window
    - Sorting in the Job Status window
    - Function that limits the jobs that can be displayed in the Job Status window (**Filer** menu)
    - Instructing jobs to be suspended and resumed
    - Acquiring registry information
    - Acquiring software inventory
    - Acquiring software information with **Search for Microsoft Office products** or **Search for anti-virus products** specified
    - Searching the software listed in **Add/Remove Programs** by a *Get software information from client* job
    - Acquiring software information using a software search list

  - Obtaining patches
  - Detecting patch information
  - Preparing installation storage media for offline installation
  - Acquiring user inventory
  - Acquiring directory information
  - Collecting inventory and operation information from offline machines
  - Managing security updates with WSUS linkage
  - Monitoring software operation status
  - Sending messages to clients
  - Displaying jobs being deleted
  - Displaying execution status of jobs created in lower-level relay systems
  - Displaying relays that manage ID groups
  - Managing inventory information using Inventory Viewer
  - Using a software search list to narrow down the software to be displayed
  - Selecting all information displayed in the right-hand frame of the Remote Installation Manager window or switching the selection status
  - Checking the detailed package attributes in Remote Installation Manager
  - Automatic maintenance of host groups and ID groups
  - Searching for hosts that are duplicated in the system configuration information
  - Detecting hosts on which JP1/Software Distribution is not installed
  - Setting the range of output to a CSV file
  - Outputting an audit log
  - User management when linked to JP1/Base
  - Managing from JP1/IM
  - Managing from HP NNM version 7.5 or earlier
  - Installation on cluster systems
- An all-lower-clients job can be executed from JP1/Software Distribution Manager only. An all-lower-clients job can not be executed from JP1/Software Distribution Manager (relay manager) or JP1/Software Distribution Client (relay system).

D.2 Differences with JP1/Software Distribution for UNIX

The following describes the differences between the Windows and Unix versions of JP1/Software Distribution. These tables show the operations that the Windows and UNIX managing servers support for the clients.

Table D–1: Remote installation (software distribution)

Item	Windows managing server		UNIX managing server	
	Windows client	UNIX client	Windows client	UNIX client
Managing server-based installation	S	S	S	S
Client user installation	S	S	S	S
Distribution of JP1/Software Distribution Client (client)	S	S	S	S
Distribution of JP1/Software Distribution Client (relay system)	S	S	S	S

Item	Windows managing server		UNIX managing server	
	Windows client	UNIX client	Windows client	UNIX client
Suppressing installation by system conditions	S	--	S	--
Suppressing installation by software conditions	S	--	S	--
Distribution schedule	S	S	S	S
Specifying installation date and time	S	S	S	S
Specifying installation timing	S#1	S#2	S#1	S#2
Auto-booting of client machine after installation	S	S	S	S
Displaying dialogs during processing (setting packages)	S	--	--	--
Displaying processing message (client setup)	S	--	S	--
Starting an external program in linkage to remote installation	S (Before and after distribution, error)	S (Before and after distribution)	S (Before and after distribution, error)	S (Before and after distribution)
Automated installation of a package	S	S	S	S
Installation using a recorder file	S	--	S	--
Installation using an AIT file	S	--	S	--
Installation specifying a host group	S	S	S	S
Installation specifying an ID group	S	S	S#3	S#3
Split distribution	S	S#4	S	S
Multicast distribution	S	--	--	--
Suspending and resuming a job	S	S	--	S
Distributing suspended jobs	S	S	--	--
Remote booting and shutdown by client control	S#5	S#6	--	--
Offline installation	S	--	--	--
Acquiring directory information	S	--	--	--

Legend:

S: supported

--: Not supported

#1

Installation at system startup or normal installation

#2

Installation at system startup, normal installation, or installation at system shutdown

#3

Information on the distribution destinations that are registered in the group ID for the UNIX version of JP1/Software Distribution is managed by the relay system. Therefore, distribution destination systems that are directly connected to the managing server cannot be registered in a group ID.

#4

Split distribution is supported only when the client is an end workstation.

#5

Remote startup via a relay system, by client control, can be used regardless of whether the relay system is a UNIX or a Windows based system.

#6

You can use only remote startup if the client version is 08-10 or later. You can use this operation over a relay system regardless of whether the relay system is UNIX or Windows.

Table D–2: Packaging

Item	Windows managing server		UNIX managing server	
	Windows client	UNIX client	Windows client	UNIX client
Compression of package data	S	S	S	S
Copying packages between managing servers	--	--	S	S

Legend:

S: supported

--: Not supported

Table D–3: Inventory management

Item	Windows managing server		UNIX managing server	
	Windows client	UNIX client	Windows client	UNIX client
Acquiring an inventory periodically	S	S	--	--
Specifying acquisition timing	S#1	S#2	--	--
Automatic reporting of updated inventory information	S	S#3	--	--
Managing system information	S	S	S	S
Managing registry information	S	--	--	--
Managing software information	S	S	S	S
Managing user inventory information	S	S	S	S
Acquiring other companies' software information	S	S	--	--
Acquiring software information by a software search list	S	S	--	--
Searching for a file	S	--	--	--
Acquiring software information with **Search for Microsoft Office products** specified.	S	--	--	--
Acquiring software information with **Search for anti-virus products** specified.	S	S#4	--	--
Acquiring patch information	S	S	S	--
Managing software licenses	S	--	--	--
Managing software generations	S	S	S	S

Item	Windows managing server		UNIX managing server	
	Windows client	UNIX client	Windows client	UNIX client
Managing offline machines	S	--	--	--
Output of management information to a CSV file	S	S	S[#5]	S[#5]

Legend:

S: supported

--: Not supported

#1

Execution at system startup or during system operation

#2

Execution at system startup, during system operation, or at system termination

#3

Available only if the client version is 09-00 or later.

#4

Can be acquired only if the client's OS is Linux version 07-50 or later.

#5

JP1/Software Distribution Web - Console is required.

Table D–4: Remote collection (collecting files)

Item	Windows managing server		UNIX managing server	
	Windows client	UNIX client	Windows client	UNIX client
Remote collection	S	S	S	S
Collection path name[#1]	S	S	S	S
Specifying a collection timing	S[#2]	S[#2]	S[#2]	S[#3]
Starting an external program in linkage with remote collection	S	S (Before and after collection)	S	S (Before and after collection)
Suspending and resuming a job (batch collection)	--	--	--	S
Remote activation and shutdown by client control	S[#4]	S[#5]	--	--
Compressing a collected file	S	S	S	S
Distributing collected inventories	--	--	S	S

Legend:

S: supported

--: Not supported

#1

The maximum number of characters that can be specified for a collection path name is as follows:

- Windows client: 256 single-byte characters
- UNIX client: 63 single-byte characters

#2

At client startup or during client operations

#3

At client startup, during client operations, or at client shutdown

#4

Remote startup via a relay system, by client control, can be used regardless of whether the relay system is UNIX or Windows.

#5

You can use only remote startup if the client version is 08-10 or later. You can use this operation over a relay system regardless of whether the relay system is UNIX or Windows.

Table D–5: Software operation status monitoring

Item	Windows managing server		UNIX managing server	
	Windows client	UNIX client	Windows client	UNIX client
Monitoring of software operation status	S#	--	--	--
Management of operating information with Asset Information Manager Subset	S	--	--	--

Legend:

S: supported

--: Not supported

#

If a relay system is used, this function is available whether the relay system is UNIX or Windows. However, the version must be 07-50 or later.

Table D–6: Remote control

Item	Windows managing server		UNIX managing server	
	Windows client	UNIX client	Windows client	UNIX client
Client remote control	S	--	--	--
File transfer using the remote control facility	S	--	--	--

Legend:

S: supported

--: Not supported

Table D–7: Linkage facility

Item	Windows managing server		UNIX managing server	
	Windows client	UNIX client	Windows client	UNIX client
JP1/Base linkage	S	--	--	--
JP1/AJS2 - SO linkage	--	--	S	S
OpenView Linkage	S	S	--	--
JP1/IM event linkage	S	S	S	S

Legend:

S: supported

--: Not supported

Table D–8: System configuration

Item	Windows managing server		UNIX managing server	
	Windows client	UNIX client	Windows client	UNIX client
Hierarchical implementation of managing servers	S	S	--	--
Multi Software Distribution facility	--	--	--	S[#1]
Relational database capability	S (Embedded RDB, Microsoft SQL Server, Oracle)	S (Embedded RDB, Microsoft SQL Server, Oracle)	S (HiRDB, Oracle)	S (HiRDB, Oracle)
Operation under a cluster system[#2]	S	S	S	S
Multiple LAN connection capability	S	S	S	S
Multiple higher systems capability	S	S	S	S
Auto dialing	S	--	S	--
Priority settings for IP addresses that are to be reported to the higher system	S	S	S	S

Legend:

S: supported

--: Not supported

#1

Requires a relational database as a management file.

#2

JP1/Software Distribution Manager can be clustered.

Table D–9: System configuration information management

Item	Windows managing server		UNIX managing server	
	Windows client	UNIX client	Windows client	UNIX client
Auto generation of system configuration information	S	S	S	S
Managing system configuration information deletion history	S	S	--	--
ID linkage to system configuration information	S	S	--	--
Management based on host IDs	S	S	--	--
Host search function	S	S	--	--
Detection of hosts on which JP1/Software Distribution is not installed	S	S	--	--

Legend:

S: supported

--: Not supported

Table D–10: Client management

Item	Windows managing server		UNIX managing server	
	Windows client	UNIX client	Windows client	UNIX client
Obtaining a patch	S	--	--	--
Detecting patch information	S[#1]	--	--	--
Managing security updates with WSUS linkage	S	--	--	--
Reporting alerts to higher systems	S	--	--	--
Message transmission to client	S[#2]	S[#3]	--	--
Client control using AMT	S	--	--	--

Legend:

S: supported

--: Not supported

#1

If a relay system is used, this function is available whether the relay system is UNIX or Windows.

#2

If a relay system is used, this function is available whether the relay system is UNIX or Windows. However, the version must be 07-50 or later.

#3

A text message can be sent alone if the client OS is Linux and the JP1/Software Distribution version is 09-00 or later.

Table D–11: Client facilities

Item	Windows managing server		UNIX managing server	
	Windows client	UNIX client	Windows client	UNIX client
Nonresident client	S	S	S	S
Job hold and cancellation	S	--	S	--
Local System Viewer and system monitoring	S[#]	--	S[#]	--

Legend:

S: supported

--: Not supported

#

Because these functions are used locally on the client, they are not available for operation from a higher system.

D.3 Correspondence in setup items between Windows and UNIX Editions of JP1/Software Distribution

This section explains the correspondence between setup items in the setup dialog boxes of the Windows Edition of JP1/Software Distribution and the attribute names specified in the UNIX Edition of JP1/Software Distribution.

(1) Correspondence among setup items of JP1/Software Distribution Client (relay system)

The following subsections explain, for each page of the Relay System Setup dialog box, the correspondence between setup items in the Windows Edition of JP1/Software Distribution Client (relay system) and the attribute names specified in the UNIX Edition of JP1/Software Distribution.

(a) Correspondence for basic setup items

Note that there are no setup items on the following pages that correspond attribute names in the UNIX Edition of JP1/ Software Distribution:

- **Dial-up** page
- **Multicast Distribution** page
- **System Configuration** page
- **ID Key for Operations** page
- **Client Alert** page
- **AMT Linkage** page

Table D–12: Setup items on the Connection Destination page and attribute names in the UNIX Edition

Setup item		Attribute name
Higher system	**Software Distribution Manager**	`ConnectionKind` (`HOST` is specified as the setup value.)
	Software Distribution Client (Relay system) or Software Distribution SubManager	`ConnectionKind` (`MASTER` is specified as the setup value.)
	Poll multiple higher systems	--
	Connect using the HTTP Gateway installed on this relay system	--
	Host name or IP address	`ManagingHost`
System for ID group registration	**Software Distribution Manager**	--#
	Software Distribution Client (Relay system) or Software Distribution SubManager	--#
	Host name or IP address	`ManagingHost`

Legend:
--: Not applicable

#: A relay system is always set in the UNIX Edition of JP1/Software Distribution.

Table D–13: Setup items on the Communication page and attribute names in the UNIX Edition

Setup item		Attribute name
Startup protocol	**TCP**	`ClientActionProtocol` (`TCP` is specified as the setup value.)
	UDP	`ClientActionProtocol` (`UDP` is specified as the setup value.)
Interval transfer	**An interval transfer is done for every transfer unit**	--#
	Number of continuous transfer buffers	`FileTransferSleepInterval`
	Transfer interval	`FileTransferSleepTime`

Legend:
--: Not applicable

#: Enabled when `FileTransferSleepInterval` and `FileTransferSleepTime` are set.

Table D–14: Setup items on the Relay System Customization page and attribute names in the UNIX Edition

Setup item		Attribute name
Number of clients that can be connected at one time		`MaxConnectClients`
Max. number of relays or clients in which jobs can execute concurrently		`MaxExecuteClients`
Maximum cache size for the management file		--
Software information to record	**Record the system/ software information answered from the lower clients**	--
	System information	--
	Installed package information	--
Record the results of ID group jobs		`IDCommandDetailInf` (`YES` is specified as the setup value.)
Monitor startup of subsystems		• When the OS is not HP-UX: `/NETMRDS/rdsprm/.cltstsud` • When the OS is HP-UX: `/var/opt/NETMDMW/rdsprm/.cltstsud`
Break down the reason for a starting failure		• When the OS is not HP-UX: `/NETMRDS/rdsprm/.cltstsud` • When the OS is HP-UX: `/var/opt/NETMDMW/rdsprm/.cltstsud`
Monitor file transfer errors of subsystems		`InformLineDown` (`YES` is specified as the setup value.)
Accept suspended/resumed file transfer jobs from sources other than the connection destination		--#

Legend:

--: Not applicable

#: Always enabled in the UNIX Edition of JP1/Software Distribution.

Table D–15: Setup items in the Report To Higher System page and attribute names in the UNIX Edition

Setup item		Attribute name
Send the result file to the server	**When result is received from managed hosts**	`SEND_RESULT=IMMEDIATE`
	After a specific interval	--#
Execute, in parallel, the receiving of jobs from and the sending of result files to the higher system		`ParallelTransfer` (`YES` is specified as the setup value.)
Report the split package distribution execution status of the lower system to the higher system		--

Legend:

--: Not applicable

#: Regularly scheduled transfer is used if `SEND_RESULT=IMMEDIATE` is omitted.

Table D–16: Setup items on the Event Service page and attribute names in the UNIX Edition

Setup item		Attribute name
Enable the event service		`AutoAction` (`YES` is specified as the setup value.)
Event information	**Report when the server is down**	--
	Client alert event	--

Legend:
--: Not applicable

Table D–17: Setup items in the Remote Installation Manager page and attribute names in the UNIX Edition

Setup item	Attribute name
Report the installation status to the managing server	`HighEndManagementHost`
Report the ID group job status to the managing server	--

Legend:
--: Not applicable

(b) Correspondence for detailed setup items

Correspondence for the detailed setup items in JP1/Software Distribution Client (relay system) is the same as that for the setup items in JP1/Software Distribution Client (client). For details about the correspondence of the setup items in JP1/Software Distribution Client (client), see *(2) Correspondence of the setting items in JP1/Software Distribution Client (client)*.

(2) Correspondence among the setup items of JP1/Software Distribution Client (client)

This subsection explains the correspondence between setup items in the Windows Edition of JP1/Software Distribution Client (client) and the attribute names specified in the UNIX Edition of JP1/Software Distribution.

Note that there are no setup items on the following pages that correspond to attribute names in the UNIX Edition of JP1/Software Distribution:

- **Processing Message** page
- **Notification Dialog** page
- **Dial-up** page
- **System Monitoring** page
- **Remote Collect Options** page
- **Multicast Distribution** page
- **Startup** page
- **Setup Protection** page
- **Security** page

Table D–18: Setup items on the Connection Destination page and attribute names in the UNIX Edition

Setup item		Attribute name
Connection destination	**Software Distribution Manager**	`WorkstationType` (`END` is specified as the setup value.)
	Software Distribution Client (Relay System) or Software Distribution SubManager	`WorkstationType` (`CLIENT` is specified as the setup value.)
	Host name or IP address	`ManagingHost`

Setup item	Attribute name
Automatically specify the higher system that requested a job execution as the connection destination	--
Poll multiple higher systems	--
Automatically register this computer in the system configuration	(Set in the operating-environment settings file) `SYSCNS=YES`
Also report this computer's inventory to the server	`INVENTORY_UPLOAD` (`YES` is specified as the setup value.)

Legend:

--: Not applicable

Table D–19: Setup items on the Default Running Status/Polling page and attribute names in the UNIX Edition

Setup item			Attribute name
Client starts automatically at system boot			(Specified in the system file)
Client will poll the managing server			In the case of an end workstation: • When the OS is not HP-UX: `/NETMRDS/rdsprm/.rdsmaauto` • When the OS is HP-UX: `/var/opt/NETMDMW/rdsprm/.rdsmaauto` In the case of a client: `WatchTimeofOrders` (A value other than `MANUAL` is specified as the setup value.)
Polling frequency	**Start polling when the client program starts**		--
	Execute polling only once		`WatchTimeofOrders` (`0` is specified as the setup value.)
	Execute polling once every *XX* hours and *XX* minutes		`WatchTimeofOrders` (A value between `1` and `1280` is specified as the setup value.)
	The first polling is executed: **Before the client starts** **After the client starts**		--
	Maximum polling delay before or after starting the client	**Start polling at a specified time**	--
		Start polling after waiting *XX* seconds	--
	Polling is executed: **Every time the system boots** **When the system boots for the first time each day**		--
	Specify the time to execute polling		--

Setup item		Attribute name
Polling method	**Hot standby**	--
	Multiple hosts	--

Legend:
--: Not applicable

Table D–20: Setup items on the Communication page and attribute names in the UNIX Edition

Setup item		Attribute name
Port number	**Software Distribution Manager [netmdm]**	(Set up in the `/etc/services` file) `netmdm` *port-number*`/tcp`
	Software Distribution Client (Relay System) or Software Distribution SubManager	(Set up in the `/etc/services` file) `netmdm` *port-number*`/tcp`

	Client call [netmdmclt]	(Set up in the `/etc/services` file)
		`netmdmclt` *port-number*`/tcp`
		`netmdmclt` *port-number*`/udp`

Protocol used by the higher system requesting the client to start a job	**TCP**	--#1
	UDP	--#1
	Connect to the upper-level system by using the IP address received via the startup request protocol	--#2
File transfer buffer size		`TransferDataSize`
Wait for response (minutes)		`ReceiveWaitTime`
Specify multiple network adapters		(Set up in the `IFCONFIG` file)

Legend:
--: Not applicable

#1: Always enabled in the UNIX Edition of JP1/Software Distribution.

#2: Enabled when the working key of the managing server is an IP address.

Table D–21: Setup items on the Network Adapter Settings page and attribute names in the UNIX Edition

Setup item		Attribute name
Specify the priority in which network adapters should be used		(Specified in the `/NETMRDS/rdsprm/IFCONFIG` file if the OS is not HP-UX; specified in the `/etc/opt/NETMDMW/rdsprm/IFCONFIG` file if the OS is HP-UX.)
Network Adapters	**Network adapter**	--
	MAC address	--
	IP address	--
	Subnet mask	--
Use as Client IP address		--

Legend:
--: Not applicable

Table D–22: Setup items in the Retry Communication page and attribute names in the UNIX Edition

Setup item			Attribute name
Socket connection	**Retry count for establishing socket connection**		• `RetryCount` • `ServerRetryCount`
	Retry interval for establishing socket connection (seconds)		• `RetryInterval` • `ServerRetryInterval`
When communication fails	**Number of times to retry transmission**		`DeliveryRetryCount`
	Retry interval (seconds)		`DeliveryRetryInterval`
Transmission notification file to the higher system	**Resend the remaining installation result files**		--
	Maximum retry count	**Unlimited**	--
		Specified *XX* times	--
	Retry interval (seconds)		--

Legend:
--: Not applicable

Table D–23: Setup items on the Error Handling page and attribute names in the UNIX Edition

Setup item			Attribute name
Log information	**Generations of log file to be saved**		--
	Maximum lines in a log file	**MAIN file**	`MaxEntryofMessage`
		USER file	--
		COMPO file	--
		FUNC file	--
		LONG file	--
Type of Event Viewer message	**Error**		`SystemLogOutputLevel` (`1` is specified as the setup value.)
	Error, Warning		`SystemLogOutputLevel` (`2` is specified as the setup value.)
	Error, Warning, Information		`SystemLogOutputLevel` (`3` is specified as the setup value.)

Legend:
--: Not applicable

Table D–24: Setup items on the Job Options page and attribute names in the UNIX Edition

Setup item			Attribute name
Job hold facility	**Job holding**	**Confirm jobs before execution**	--

Setup item			Attribute name
Job hold facility	**Job holding**	**The confirmation box stays for *XX* seconds**	--
Allow the administrator to shut down or restart	**If requested by the administrator, shut down or restart the computer**		--
	The confirmation box stays for	**Unlimited**	--
		Specified (seconds)	--
Automatic inventory update			--
Suppress periodic jobs when the connection destination of the client is changed			`REGULARJOB_NOSERVER_NOEXEC=NO`
Suppress reports of the job status "Waiting for installing/collecting" to the higher system			--
Include Hitachi program products in the "Add/Remove Programs"			--
Do not repeat package IDs when collecting software information			--

Legend:

--: Not applicable

Table D–25: Setup items on the Installation Options page and attribute names in the UNIX Edition

Setup item			Attribute name
Installation/file collection job	**Maximum retry count**		`DeliveryRetryCount`
	Retry interval		`DeliveryRetryInterval`
Split package distribution	**Split package distribution settings**	**Split package and then distribute**	--#
		Split size	--#
		Distribution interval (hours and minutes)	--#
Check local disk capacity before unpacking software			--
Delete package information of the system previously connected to the client			--
Maintain the installation history in case an error occurs during installation of the package			--
Delete the work directory for installing Hitachi program products after installation			--
InstallShield time-out (seconds)			--

Legend:

--: Not applicable

#: Becomes enabled according to the settings in the higher system.

E. Version Changes

(1) Changes in version 09-50

- Windows 7 and Windows Server 2008 R2 are now supported.
- If remote installation of JP1/Software Distribution Client (relay system) is performed on a JP1/Software Distribution (relay system) in which Automatic Installation Tool is installed, all components other than Automatic Installation Tool are now updated.
- The user can now set as system information that password protection for screen saver information is to be acquired even if the screen saver is disabled.
- The following inventory information (system information) can now be collected:
  - Encryption information set by BitLocker
  - Drive (hard drive) encryption information set by HIBUN FDE
  - Linux distribution
- Software information can now be collected for additional Microsoft Office products. In addition, greater detail about Microsoft Office products is now provided.
- Software information can now be collected for additional anti-virus products.
- Directory information about groups can now be acquired from Active Directory. In addition, the argument `/d` has been added to the command for acquiring directory information (`dcmadsync.exe`), which enables the user to delete directory information that has already been acquired.
- The operation status of virtual environments can now be monitored.
- Use of the devices listed below can now be suppressed. In addition, their connection history, disconnection history, connection permission logs, and connection suppression logs can now be acquired.
  - Bluetooth devices
  - Imaging devices
- If suppression exclusion conditions are set when access to USB media is suppressed, the following logs can now be acquired:
  - Connection permission log
  - Connection suppression log
- Writing can now be suppressed individually for the following devices, and their connection suppression logs can now be acquired:
  - Internal CD/DVD drives
  - Internal floppy disk drives
  - IEEE 1394 connection devices
  - Internal SD card readers
- Operation of JP1/Software Distribution Client (client) is now supported in Windows XP Mode environments.
- The facilities for acquiring print logs and for suppressing printing can now be used when a shared network printer is being used in Windows Vista or Windows Server 2008.
- In the event that a USB media device for which operations have been suppressed is connected to a client PC, the corresponding JP1 event can now be reported as an alert.
- If one of the devices listed below is connected to a client PC when its use is suppressed, a message indicating that use of that device is suppressed can be displayed on the client PC. In addition, the corresponding JP1 event can be reported to JP1/IM as an alert.
  - Internal CD/DVD drives
  - Internal floppy disk drives
  - IEEE 1394 connection devices
  - Internal SD card readers

  - Bluetooth devices
  - Imaging devices
- If startup of a software program is suppressed, the corresponding JP1 event can be reported as an alert.
- If printing is suppressed, the corresponding JP1 event can be reported as an alert.
- Content on the following pages in the server setup process has been modified:
  - **Operation Monitoring** page
  - **AIM** page
- Operation monitoring history can now be stored using the data partitioning facility provided in Microsoft SQL Server 2008 and Microsoft SQL Server 2005.
- An explanation has been added about the relationship between directory information and system configuration information.
- By assigning divisions to users when inventory information is being managed with Asset Information Manager Subset, a single user can manage information about multiple groups.
- The minimum and recommended CPU performance specifications needed to run products and components of JP1/ Software Distribution have been changed.
- An explanation has been added about the memory requirements on a managing server when Embedded RDB is used as the relational database.
- The formulas used to estimate the disk capacity needed for Microsoft SQL Server and Oracle databases have been revised.
- If operation monitoring logs are set on the **Report To Higher System** page to be relayed to a higher system, the user can now select which information is sent to the higher system.
- The firewall data pass-through direction can now be changed when the port number and protocol are set to 30002/ udp.
- The CPU type can now be acquired as system information.
- The sizes of the following columns in the netmdm_ospatch_patchinf relational database table have been changed:
  - `dm_title`
  - `dm_kbarticle`
- When Embedded RDB is used as the database, a maximum of 1,840 megabytes of patch data can now be stored in the netmdm_ospatch_patchinf relational database table.
- The maximum number of characters that can be used in a collection path name has been increased from 63 half-width characters to 256 half-width characters.
- Explanations have been added about the correspondences between the settings in the Windows and UNIX editions of JP1/Software Distribution.
- A checkbox labeled **Do not repeat package IDs when collecting software information** has been added to the client setup **Job Options** page to allow suppression of duplicate package IDs.
- The following explanation has been moved to the chapter on setting up JP1/Software Distribution Manager:
  - Registry setting for displaying the OS name
- By specification of a registry setting, command processing can now be set to continue even after the user has logged off of Windows.
- By specification of the argument /LC in a command, command processing can now be set to continue even after the user has logged off of Windows.
- Unicode CSV files can now be output using the CSV output utility or the CSV output command (`dcmcsvu.exe`).
- During the client setup process, the user can now select on the **Error Handling** page whether to output messages to the event viewer.
- The following log files can now be output:
  - `DPTExpt.log`
  - `DPTInpt.log`

- The number of log entries has been changed by moving INVENTRY.LOG to the FUNC log.
- The argument `/n` has been added to the command (`dcmmonrst.exe`) that stores operating information in a database; this argument enables the user to check the status of a store process. A log file for checking the store process status has also been added (`MONRST.LOG`).
- The minimum size of the security update management file has been changed to 130 megabytes.
- When upgrading Embedded RDB, the user can now select whether to migrate patches acquired by the security update management facility.
- The command DPTInpt.exe (store patches in database) has been added, which enables the user to migrate patches acquired by the security update management facility.
- An explanation of possible corrective actions to take in order to handle delays in automatic notifications from the relay managing the ID has been added.
- The setting **Manage device change log information** has been added under **Basic Information** in the Server Setup dialog box of Asset Information Manager Subset. This setting allows the user to select whether to manage the initial change history of a device to be managed when the *Delete change log* task is performed.
- Login authentication can now be performed by linking Asset Information Manager Subset to Active Directory. In addition, Active Directory user information can now be acquired.
- The setting **Targets for inventory** has been added under **Link with JP1/SD** in the Server Setup dialog box of Asset Information Manager Subset. This setting allows the user to acquire inventory information from all devices, or only from devices with host IDs, or only from devices with system information.
- The setting **CSC notification count** has been added under **Link with JP1/SD** in the Server Setup dialog box of Asset Information Manager Subset. This setting allows the user to set the timing for reporting acquisition of JP1/Software Distribution inventory information to JP1/Client Security Control.
- The setting **Inventory acquisition method** has been added under **Link with JP1/SD** in the Server Setup dialog box of Asset Information Manager Subset. This setting allows the user to select **Multithreading method** as the method for acquiring inventory information.
- The setting **Multiplex level for inventory** has been added under **Link with JP1/SD** in the Server Setup dialog box of Asset Information Manager Subset. This setting allows the user to specify the multiplex level when inventory information is collected using the multithread method.
- Modification date of system configuration information and modification date of registry information can now be managed as asset information.
- Explanations have been added about upgrading the program version and migrating data in a cluster system environment.
- JP1/Software Distribution Client (client) is now supported for Citrix XenApp (public desktop) running on a terminal server.
- Explanations about starting and stopping the managing server have been added.

  The following explanation has also been included:

  System shutdown procedure when using Embedded RDB as the relational database.
- A facility has been added for backing up operation monitoring results. With this addition, the dmTRUtil.exe command can now be used to output a backup of the operation monitoring results to a CSV file.
- The following capabilities have been added for using device instance IDs to set exclusion conditions for suppressing connection of USB media:
  - The device instance ID of a USB controller can be set as an exclusion condition.
  - A comparison method can be selected for comparing device instance IDs against a specified condition character string.
- A note has been added in the Software Operation Information window stating that software operation history is not displayed for clients if more than 560,000 operation history entries have been stored.
- Explanations have been added about environment variables that cannot be set and other items that are not available when offline installation is performed.
- The dcmstdiv.exe command has been added to enable command-initiated entry of information about offline machines.
- The following items have been added as information that can be output to a CSV file by the CSV output utility or the dcmscvu command:

  - Registry path (registry collection items template)
  - Software indicator ID (Microsoft Office products template)
  - Software indicator ID (anti-virus products template)
- Client configuration settings can now be changed when remote installation of JP1/Software Distribution Client (client) is used.
- The following settings have been added for remote setup of clients:
  - **Host name or IP address**
  - **Product type**
  - **When the system is changed, inventory information is notified to Higher System**
- If operation history on a client is lost, the corresponding JP1 event can now be reported as an alert.
- Descriptions have been added about system maintenance operations that need to be performed. In addition, explanations about the following items have been included:
  - How to change the JP1/Software Distribution Manager settings in a cluster system environment
  - Recommended intervals for performing various database maintenance operations
  - Procedures for backing up and restoring the system
- WMI information can now be collected.
- Messages have been added for the following event IDs:
  - `1081`
  - `1082`
  - `1083`
  - `1084`
  - `1085`
  - `1086`
  - `2021`
  - `11029`
  - `16031`
- A JP1/Software Distribution Client (client) event log message is no longer output for event ID 7009.
- Messages with the following IDs have been added to the section about event log messages for which monitoring is recommended (including the causes and the corrective actions to be taken):
  - `16023`
  - `16024`
  - `16031`
- The basic client log messages KDSF0055-W and KDSF0123-E have been added.
- The contents of the basic client log messages KDSF0010-I and KDSF0020-I have been changed.

(2) Changes in version 09-00

- Microsoft SQL Server 2008 can now be used as a relational database program.
- Additional anti-virus products can now be acquired as software information.
- Specific USB media can now be excluded from being suppressed. In addition, if USB media connected to a client PC is being suppressed, a message indicating that fact can now be displayed.
- When automatic storage of operation information is not being performed, the information can now be manually stored in a database by executing the `dcmmonrst` command with the `/x` argument specified.
- Hitachi bundle-named (name created from multiple products) products stored on Hitachi bundled-product CD-ROMs can now be packaged.

- Output of messages to the event log by Embedded RDB that are not required for operations can now be suppressed.
- Hosts can now be deleted from system configuration information by removing the host from the ID group.
- Remote Installation Manager of JP1/Software Distribution Manager can now be used to add a host group or a host from a file.
- The following items have been changed in the Server Setup dialog box of Asset Information Manager Subset.
    - The minimum value that can be specified for the **Communication-less monitoring time** setting under **Session Information** has been changed to 5 minutes.
    - The **Status to display in device search windows** setting has been added under **Basic Information**, allowing the user to choose the device statuses to display as **Status** search conditions in the Device Totals and Device List windows.
- If **Scheduled Tasks** is used to automatically obtain patches, the following functions can now be used:
    - Deletion of security updates after packaging
    - Non-downloading of packaged security updates
- The user name, host name, and IP address can now be specified as search conditions in the Batch Update window of Asset Information Manager Subset.
- The `Text_Title` (text for dialog box titles) item has been added to the Asset Information Manager Subset `VariousInfo` management class, allowing the user to change the title of operation windows.
- Information about the cause and handling of the `3000AF008300` maintenance code has been added to the event log message.
- Commands for backing up and restoring package files and operation history files have been added when Microsoft SQL Server or Oracle is being used as the relational database:
    - `netmfile_backup.bat`
    - `netmfile_restore.bat`
- The following inventory information items can now be acquired:
    - Turn off hard disks (AC)
    - Turn off hard disks (DC)
    - System standby/Sleep (AC)
    - System standby/Sleep (DC)
    - System hibernates (AC)
    - System hibernates (DC)

  Additionally, operation examples of dealing with clients whose power-save setting is not configured and of shutting down clients have been added.
- The operation monitoring function can now be applied to offline machines through the use of media.
- The maximum size of the management file cache can now be specified during setup of relay systems, so that decreases in job processing throughput can be avoided, even if the number of jobs managed by the relay system increases.
- Re-installation is now performed automatically if the initial installation of JP1/Software Distribution Client fails. In addition, the location of the InstallShield environment deletion tool, which is executed if re-installation of JP1/Software Distribution Client fails, is now noted.
- Procedures have been added describing how to perform an overwrite installation or a re-installation of JP1/Software Distribution Manager in a cluster system.
- Job execution results are now recorded, regardless of the setting specified for the **Record the results of ID group jobs** during setup of the relay system, so that relay system ID group jobs can be re-executed by default.
- If Embedded RDB is used for the JP1/Software Distribution Manager database, the size of the operation table area can now be increased automatically.
- If Embedded RDB is used to create an Asset Information Manager Subset database, the size of the database can be expanded automatically.

- A CSV-format backup of Asset Information Manager Subset databases can now be obtained by executing `jamdbexport.bat`.
- An explanation has been added about `jamemb_backup.bat`, which is used to obtain backup files of Asset Information Manager Subset databases in an Embedded RDB environment.
- An explanation has been added about `jamemb_reorganization.bat`, which is used to re-organize Asset Information Manager Subset databases in an Embedded RDB environment.
- As an option for `jamTakeOperationLog.bat`, the group, user name, and location information can now be output to a CSV file when a search pattern is used to output all items in an operation log.
- Event log messages have been added for the following event IDs:
    - `8060`
    - `8061`
    - `8064`
    - `8065`
    - `8066`
    - `8067`
    - `8068`
    - `8069`

(3) Changes in version 08-51

- WUA 3.0 can now be used to acquire client patch information.
- Active Directory information can now be collected on managing servers, specified for job destinations, and viewed in Inventory Viewer.
- Asset Information Manager Subset can now be used to count inventory information items based on job purpose.
- Web access logs, and the logs of print operations and operations to and from external media, can now be acquired as software operation information. Also, printing and operations to and from external media can now be suppressed.
- When a computer that supports AMT is used as a client, the client's BIOS can now be controlled remotely. Also, a diagnostic program on a floppy disk in the managing server can now be used to perform checks on clients.
- Through the use of Microsoft .NET Framework 3.0, AMT Linkage can now be used for clients in a wireless LAN environment.
- Some JP1/Software Distribution Manager components can now be used on Windows Vista.
- Windows Server 2008 is now supported.
- Security-related items can now be acquired as system information.
- The following power management information can now be acquired as system information:
    - Turn off monitor (AC)
    - Turn off monitor (DC)
    - Processor throttle (AC)
    - Processor throttle (DC)
- Software information can now be acquired for additional anti-virus products. A description has also been added about the ability to determine the resident/nonresident status of various anti-virus products.
- Software information on Hitachi program products can now be acquired by using **Search software listed in "Add/Remove Programs"**.
- Whether to save operation information reported to a central manager or relay manager from lower-level systems is now selectable. Whether or not to report operation information received by a relay manager from a lower-level system to a higher-level system can now be selected as well.
- Operation monitoring policies can now be output to a file. Operation monitoring policies can also now be added by importing these output files.

- Operation monitoring functions can now be used for clients running the 64-bit version of Windows Vista.
- File operation history can now be acquired from clients running Windows Server 2008 or Windows Vista.
- Network drives can now be used as directories for storing operation history and backups.
- Database Manager can now be used to create a database area for acquired patches. Windows Mail has also been added as a program type for which patches can be acquired.
- JP1/Software Distribution can now link to WSUS 3.0. When linked to a hierarchically configured WSUS system, downstream WSUS servers can now be synchronized with the top-level WSUS server, and clients can now be registered to computer groups of downstream WSUS servers.
- Windows Remote Desktop operations are now supported.
- Software inventory information can now be managed under Coordinated Universal Time (UTC).
- The default, minimum, and maximum sizes of the Embedded RDB database area have been changed. The size of the Embedded RDB work table area can also now be specified with Database Manager.
- A formula for calculating the size of the operation monitoring logs has been added to the formulas for estimating the area required for the Embedded RDB database.
- A formula for calculating the size of the registry acquisition items has been added to the formulas for estimating the area required for the Microsoft SQL Server database.
- The Windows Server 2008 and Windows Vista versions of JP1/Software Distribution Client can now be used for relay systems.
- The check box for displaying the Readme file when installation finishes has been removed.
- A description has been added about the log files in which the number of managed log generations and entries cannot be set.
- The following Embedded RDB commands now output return codes:
    - `netmdb_backup.bat`
    - `netmdb_reload.bat`
    - `netmdb_reorganization.bat`
    - `netmdb_unload.bat`
- A description of the backup procedure for Asset Information Manager Subset has been added.
- The date and time that software registered in **Add/Remove Programs** is installed can now be acquired along with other software information.
- When automatic host group maintenance is used to create a host group based on user inventory information, the maximum number of characters that can be used in the host group name has been changed to 32.
- The `JOB_DESTINATION_ID` tag used by the command parameter file can now be used to specify a relay managing the ID on which to execute the job.
- A command can now be used to acquire information about problems that occur in JP1/Software Distribution.
- Event log messages assigned the following event IDs have been added:
    - `11026`
    - `11027`
    - `11028`
    - `16029`
    - `16030`

  Also, it is now recommended to monitor for event ID `16030` event log messages.

(4) Changes in version 08-10

- Functionality has been added to enable management of users of JP1/Software Distribution when linked to JP1/Base.
- The following functionalities can now be used when computers that support AMT are used as clients:
    - Control of clients that use the AMT power control feature

  - Storing of host IDs in nonvolatile memory provided by AMT
- Software operation time at clients can now be acquired by the function for monitoring software operation status. In addition, a function has been added that totals the acquired operation times in the Software Operation Status window.
- Operation logs can now be traced by using the File Operation Trace window.
- A function has been added that obtains security updates, service packs, and other patches provided by Microsoft.
- A function has been added that provides HTML message notifications to clients.
- Operation logs can now be totaled by group using the Operation Log Total window.
- Support for Windows Vista has been added in the following program product:
  - JP1/Software Distribution Client
- Anti-virus products for which software information can be acquired have been added.
- Version and generation numbers have been added to operation monitoring policies, to make it easier to understand which operation monitoring policy is being applied.
- Text-format files that contain policy information for automatic maintenance of host groups and ID groups can now be imported and exported.
- A user inventory item has been added as a policy type for automatic maintenance of ID groups.
- The description of the number of clients that can be connected directly to a relay system has been modified.
- The data types of some database items in Embedded RDB have been changed, and the size of the database that is created has been reduced.
- The descriptions of the formulas for estimating database size have been improved by clarifying the items targeted by the calculations.
- Functionality has been added so that clients using the host name as the ID key for operations and which are unable to resolve the name of the connection-target higher system through normal means can perform name resolution and connect to the higher system based on the IP address received in the execution request information.
- A function has been added for output of JP1/Software Distribution's operation as audit logs.
- The method of setting up Asset Information Manager Subset and creating a database has been changed.
- A setting has been added to disable display of dialogs while JP1/Software Distribution Client is being installed remotely.
- An additional facility has been added as a JP1/Software Distribution Client component.
- The function that detects hosts on which JP1/Software Distribution is not installed can now detect hosts in a VPN environment with routers that do not support SNMP in the search path.
- The single quotation mark (`'`) can now be entered in text-entry user inventory items.
- The basic log message at the client (KDSF0096-W) has been changed.
- A program product ID file can now be created from the Package Information tool when an AIT file is created.
- The following messages about editing AIT files have been added: AITG123-E, AITG124-E, AITG125-E

(5) Changes in version 08-00

- Microsoft SQL Server 2005 is now supported as a relational database program.
- Embedded RDB is supported as the standard relational database provided by JP1/Software Distribution Manager. Basic databases are no longer supported.
- In the Find dialog box, hosts can now be searched by using the host name or IP address as the key value.
- The automatic host group maintenance facility enables hosts to be grouped by the client's OS sub-version.
- The software operation monitoring facility enables the user to select whether startup of specified software and path is to be permitted. It also enables the user to select whether startup of all software other than specified items is to be permitted.
- The software operation monitoring facility can acquire a file manipulation log.
- Client operation information can now be viewed in the Operation Log List window.

- WUA can be used to acquire information on installed patches.
- Anti-virus products that can be acquired as software information have been added.
- The Add Destination, Add Package, and Save Job dialog boxes can now be resized.
- The maximum number of user inventory items that can be selected has been changed from 255 items to a total size of 51,254 bytes. For hierarchized user inventory items, a maximum size of 102,509 bytes, including the higher items, has been added.
- In split package distribution, the status of execution from relay system to lower system can now be checked at the higher system.
- Polling has been added as a timing for automatically changing a client's connection destination.
- A function for setting client security management has been added for use when JP1/Client Security Control is linked.
- The JP1/Software Distribution management facility and the client installation facility are no longer supported for Web browsers.
- The differing-components distribution facility is no longer supported.
- WUA can be used to acquire information on uninstalled patches.
- WSUS can be linked to manage security updates.
- Windows Server 2003 (x64) is now supported.
- Parentheses (`(` and `)`) are now permitted in installation and work directory names.
- The system configuration information can be searched for duplicate hosts and the hosts with the older update dates/times can be deleted.
- An option for delaying a client's polling start time has been added.
- A description of Embedded RDB settings in a firewall environment has been added.
- CPU types have been added to the system information that can be acquired.
- The user can now select whether to use the standard retrieve list when software information is acquired.
- When a package is distributed to a UNIX client and an external program is started, the external program's termination code can now be referenced by the server.
- JP1/Software Distribution can now install security update data on the security PC.
- Additional anti-virus products for which information can be acquired have been added.
- Descriptions of environment variables that can be specified in **Skip directory** on the **Options** page and in **File name by full path** on the **Collect File** page of the Create Job dialog box have been added.
- Name of a hotfix whose format is changed when it is displayed as software information by Remote Installation Manager has been added.
- Contents of client's basic log messages `KDSF0060-I` and `KDSF0090-I` have been changed.
- `KDSF0097-I`, `KDSF0098-W`, and `KDSF0099-E` have been added to client's basic log messages.
- In Remote Installation Manager's Job Status window, a folder is now created to store the *Report message* job executed from JP1/Client Security Control.
- During a host search, the user can now select whether host names are to be acquired. The user can also select the range of host information to be acquired.
- Inventory information for Microsoft Office products and anti-virus products can now be acquired from offline machines.
- A description of how to make a backup of suppress history and operation history has been added.
- Event log message with event ID `19003` has been added.
- System security measures can now be enhanced by linking to JP1/Client Security Control.

(6) Changes in version 07-50

- The *Get software information from client* job now provides the capability to acquire information about patches that have not been installed on a computer. This also allows Remote Installation Manager to display information on patches that have not been installed on a computer.

An event log message maintenance code (3000EF300000) has also been added.

- Capabilities to monitor the operating status of client software, suppress startup of software, and obtain the operation history of software are now provided. Remote Installation Manager can now also display suppression logs and operation logs.

  Event IDs 16016 and 16020 messages have also been added.
- An administrator can now send messages to clients.
- Notification of event information that has been updated on a client can now be reported automatically to the higher system.
- A facility for automatic maintenance of ID groups has been added, which provides the capability to register automatically new clients added to an ID group by setting a policy for that ID group.
- JP1/Software Distribution Manager Embedded RDB Edition has been added.
- Capability to search hosts that exist on a network and to detect hosts on which JP1/Software Distribution is not installed is now provided.
- Information that enables JP1/Asset Information Manager to monitor updating of inventory information has been added to several tables in the database.
- Causes and actions to take for event log messages that recommend monitoring have been added.
- Client's basic log message KDSF0103-I has been added.
- Contents of client's basic log messages KDSF0060-I and KDSF0092-E have been changed.
- AIT files provided by JP1/Software Distribution have been added.
- Capability to install software on a PC on which JP1/Software Distribution Client is installed without using a network has been added.
- Because an installation set can now be used to overwrite a previous installation of JP1/Software Distribution Client, the overwrite installation item has been deleted from the table that indicates differences between using an installation set and installing from a Web browser.

  Descriptions of the use of an installation set when performing an overwrite installation have also been added to the procedure for configuring JP1/Software Distribution Client setup information.
- Hosts on which JP1/Software Distribution is not installed (hosts without JP1/Software Distribution installed) can now be detected by reading a CSV file containing information about the hosts in the network.
- CPU types have been added as system information that can be acquired.
- A description of operating JP1/Software Distribution in the terminal service environment has been added.
- Support has been added for running Microsoft Windows Server 2003, Enterprise Edition, as a cluster system OS for JP1/Software Distribution.
- The *Get software information from client* job now provides the capability to acquire information about patches that have been installed on a computer. The acquired patch information can also be displayed by Remote Installation Manager and Package Setup Manager.
- Anti-virus products have been added as system information that can be acquired.
- When user inventory items are being created, the only characters that cannot be used in a comment field now are the semicolon (;) and percent sign (%).
- When a *Transfer user inventory schema to client* job is being created, functionality has been added so that you can specify whether to allow a client user to cancel the dialog box that sets the user inventory, and to set an action to be performed after the user inventory has been set at the client.
- Acquired Microsoft Office product and anti-virus product information can now be output to a CSV-format file.
- Notes about creating and using AIT files have been added.
- The capability to distribute software and check distribution status from operation windows of JP1/Asset Information Manager has been added.
- JP1/Software Distribution Client can no longer be installed on PCs on which Client Installation by Web and the Startup Kit Support Tool are installed.
- JP1/Software Distribution SubManager can now be used by a user logged on without administrator permissions to perform remote installation.

- If an error occurs while an overwrite installation is being performed, information on the previously installed package can now be retained.
- By setting a priority for use of network adapters, a client's IP address can now be reported to the higher system.
- Host inventory information not included in the system configuration can now be deleted.
- *Windows Installer* has been added to system information to maintain Windows Installer version information. *Windows Installer* can now be counted in Inventory Viewer as well.
- Registered tools can now be started from Remote Installation Manager.
- Silent installation of programs can now be performed using Windows Installer.
- For the UNIX version of JP1/Software Distribution Client 07-50 and later, whether to restart the client machine automatically after a package has been installed can now be specified.
- When in the Job Definition window a job selected with the **F5** key is executed, a confirmation dialog box is now displayed.
- The method for acquiring the CPU clock speed has been changed.
- Microsoft Office products have been added as software information that can be acquired.
- *OS language* can now be counted in Inventory Viewer.
- The following commands can now be executed from JP1/Software Distribution SubManager:
  `dcmcoll.exe`, `dcminst.exe`, `dcmjbrm.exe`, `dcmjexe.exe`, `dcmpkrm.exe`, `dcmrmgen.exe`, `dcmrtry.exe`, `dcmstat.exe`, `dcmstsw.exe`
- The causes and actions to take for event log messages of maintenance codes `300097140000` and `30009F070000` have been changed.
- A section has been added that describes the functional differences between JP1/Software Distribution Manager and JP1/Software Distribution SubManager.
- An AIT file for distributing Windows Installer modules has been provided.

(7) Changes in version 07-00

- Windows 95 is no longer supported by JP1/Software Distribution Client. However, because JP1/Software Distribution Client versions earlier than 07-00 can connect to a higher system of version 07-00, explanations for Windows 95 were added to the manual.
- For a *Get software information from client* job, **Search for Microsoft Office products** and **Search for anti-virus products** were added to the **Software to be searched** option. Also, the number of hosts can now be counted for each product name, virus-definition file version, and residency setting of anti-virus products.
- AIT files, which are script files used to send responses to a software installer automatically, are supported. If an AIT file is packaged and remote-installed together with software, the software can be installed automatically.
- Extraction and packaging of differing-components is no longer supported by JP1/Software Distribution versions 07-00 or later (differing-components packages created with JP1/Software Distribution versions earlier than 07-00 can still be used).
- Client information can now be checked using Local System Viewer.
- Client systems can be monitored and alerts can be sent to the local PC or higher system in the event of errors.
- Alerts reported from clients can be checked at the higher system using alert information files, Event Viewer, and JP1/IM.
- The default values for client setup were changed.
- The **Remote Installation Client** and **Remote Installation Logon Manager** icons are no longer created in the Windows **Startup** group.
- The user can now choose to create the Software Distribution Client Setup folder.
- When the connection destination is undetermined, JP1/Software Distribution Client can be run by specifying `?`.
- The following features were added regarding job suspension and restart:
  - A relay manager can be specified as the destination of *Suspend file transfer* and *Resume file transfer* jobs.

  - Remote Installation Manager of JP1/Software Distribution Manager can suspend and restart file transfer between the local system and its lower systems.
  - Jobs can be suspended and restarted between lower systems in UNIX versions.
  - The `dcmsusp` command was added to suspend and restart file transfer.
- On the **Job Distribution Attributes** page, the user can specify whether to distribute jobs even if file transfer is currently suspended.
- Even if the client is not resident, a client user who logs on with non-Administrator user permissions can now install packages that could not be installed previously.
- A procedure was added for upgrading a relational database at the same time that JP1/Software Distribution was upgraded to Version 7i.
- When a version is not set in the software search list and acquisition of version information from the version resource for a specified file fails, `0000` is set as the version.
- During a search using a software search list, a file whose size is 0 bytes can now be searched.
- The detailed information about a destination can be displayed by starting Event Viewer from the Job Status window.
- When the Count Clients facility is executed from the System Configuration or Destination window, the selection status of hosts and host groups is also applied to the host selection window of Inventory Viewer. Additionally, the Count Clients facility can now be executed by specifying a template from the System Configuration or Destination window.
- The user can now specify a desired font in the Software Distribution Manager Unarchiver window (or Software Distribution SubManager Unarchiver window), JP1/Software Distribution Packager window, and Package Setup Manager window.
- The *Suspend file transfer* and *Resume file transfer* job types were added to enable file transfer to be suspended and restarted between a relay system and its lower systems.
- Remote startup and shutdown by the Client Control facility were implemented without having to place one or more relay managers or relay systems per router.
- JP1/Software Distribution can now establish connection even when another application has already established dial-up connection with the same destination.
- The maneuverability of the installer was improved.
- System configuration information can be used to manage the history of host deletions. Because of this change, the formula for determining the database size was also changed.
- The **Error Handling** page was added to the Server Setup dialog box to specify the number of generations of log files to be saved, the maximum number of entries, and the type of Event Viewer messages.
- The cause of the *Client not started* job execution status can be broken down.
- In the relay manager setup, the **Relay System Customization** page was changed to the **Report To Higher System** page.
- In the relay system setup, the **Report To Higher System** page was added, and the description of the **Send the result file to the server** option was moved from the **Relay System Customization** page to the **Report To Higher System** page.
- The client computer can be restarted automatically after package installation. Also, the client setup includes an option to specify whether to allow restart of the client computer.
- Display of a processing message during package installation can be specified for a package.
- A file was added to output a basic log related to client actions (`USER_CLT.LOG`).
- A facility was added to enable software to be deleted from the software inventory and to use the deleted software management table to manage deleted software. Because of this change, the formula for determining the database size was also changed.
- Partial match search is supported when host names are searched from the System Configuration window.
- In the Find dialog box, the search item **The hosts that have not had inventory updated within a certain period** was added to the **Find by Dates** page.
- Even when a package with installation date/time specified is distributed in a UNIX client, an external program can now be started immediately after installation.

- An option was added to support customization of default values in the Software Distribution Packaging dialog box and the Create Job dialog box dialog box.
- Packager and Remote Installation Manager can be used to check the detailed attributes of stored packages.
- For the following items among the system information that can be obtained, a supplementary explanation was provided:
  Name of OS family, drive capacity, free space, partition size, file system, logon user name, full name of user, user description
- **IE Patch and BIOS version** (SMBIOS) were added to the system information that can be acquired. Because of this change, the items that can be output to a CSV file were supplemented.
- A description was added regarding the handling when multiple Remote Installation Managers attempt to edit registry collection items and user inventory items at the same time.
- **Hold** was added as a software inventory management status. Also, detailed condition settings were supported to display only specific software in the Filter Software Inventory dialog box.
- For counting by Inventory Viewer, ranges that support combined conditions were increased.
- Hosts can be counted for each IE patch, BIOS manufacturer, and BIOS version (SMBIOS).
- **Restart specification** and **Display processing message** were added to the items that can be output to CSV files using the Package attributes template.
- **Restart specification** and **Display processing message** were added in the Package window to the items that can be printed.
- Previously, the client was unable to install some packages when the user was logged on to Windows NT with the non-Administrator user permissions, but the client can now install the packages if the client is in the running status.
- The `dcmstsw.exe` command was added to monitor job execution status.
- The `dcmdice.exe` command was added to save software inventory information to a CSV file. The `dcmdici.exe` command was also added to import software information from CSV file to the software inventory.
- `reboot` and `processing_dialog` of the `OPTION` tag were added as parameters that can be specified in the parameter file for the `dcmpack.exe` command. Because of this change, specifiable arguments were added.
- `JOB_SCHEDULE` and `JOB_DESTINATION_ID` were added as tabs that can be specified in the parameter file for the `dcmcoll.exe` command. Because of this change, specifiable arguments were added.
- Event log messages related to import and export of user inventory items and commands were added.

F. Glossary

AIT file

A file that contains a procedure for installing software interactively using a tool such as a dedicated installer. Automatic Installation Tool is used to create an AIT file. JP1/Software Distribution provides AIT files for use with some other companies' software. Also, users can make AIT files.

alert report

An alert is a single message that is displayed by a program. If a user operation may result in a serious error, an alert is displayed to attract the user's attention or to provide a warning.

With JP1/Software Distribution, when an error such as a hardware error is detected while monitoring a client system, the error event is reported to the user by means of a method such as a pop-up message. This is called an *alert report*.

all lower clients

A destination type specified when the central manager executes a job for all hosts under a relay manager. Such a job is called an *all-lower-clients job*.

application gateway method

A method of building a firewall that prohibits packet relay and controls access by using an application gateway. Users cannot gain direct access to the system from the outside; they must first log in to a gateway and enter a password.

archive

A collection of files.

asset information

Information used by Asset Information Manager Subset to manage hardware and software.

Asset Information Manager Subset

A component that provides a GUI for totaling and searching the inventory information and operation logs collected by JP1/Software Distribution, according to the desired purpose.

By installing Asset Information Manager Subset, you can also open a window for managing software operation information from Remote Installation Manager.

It also provides a GUI for client security management when JP1/Software Distribution Manager links with JP1/Client Security Control.

audit log

A log to which JP1 products output log data in common. It provides a record of who performed each operation, when it was performed, and the type of operation that was performed.

authentication server

A server that uses JP1/Base to manage access permissions for JP1 users. One authentication server must be installed for each user authentication block. This server enables central management of all JP1 users. To manage JP1/Software Distribution users by linking with JP1/Base, the JP1 users must be registered in this server.

automatic maintenance policy file

A text-format file that contains a policy for automatic maintenance of host groups and ID groups.

business filter

A function used by Asset Information Manager Subset to restrict the processes that users can execute from operation windows. The restrictions are based on user permissions.

The constituent elements (buttons, search conditions, edit items, etc.) of each operation window are changed according to the user's permissions.

cabinet

An area in a managing server for storing packages.

central manager

JP1/Software Distribution Manager that is positioned at the top of the system in the case where managing servers are configured in a hierarchy.

change history

Information used by Asset Information Manager Subset to manage changes in the memory size and disk capacity of devices. You can use the change history to determine whether a CPU, memory, or disk has been physically modified without authorization.

A change history includes the change date, disk capacity, memory size, CPU, and so forth.

client

A computer on which the JP1/Software Distribution Client (client) software or the client facility of JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system) is installed. A client receives software programs directly or through a relay manager/ system from the managing server and notifies the managing server of the software installation results.

client control facility

Facility for starting and shutting down remote PCs connected via a network from the local PC. Using this facility, JP1/Software Distribution can install software on a remote PC when its power is off, such as at night and on weekends or holidays. Note that in order to use this facility, the remote PC (the motherboard, BIOS, power supply, LAN card, etc.) must support Wake on LAN and automatic shutdown.

collected file

A file collected from clients by remote collection.

collection script

A script that specifies the procedure for remote collection executed by a client. A collection script is created automatically when remote collection is executed from a Windows higher system. When remote collection is executed from a UNIX higher system, the client users can create user-specific collection scripts to achieve desired processing.

controller

A host in which the Remote Control Manager operates.

count clients

A facility that counts the number of hosts by types of information managed by JP1/Software Distribution Manager. This facility is used in a relational database system.

Database Manager

A JP1 software component used to create and maintain relational databases. Database Manager is provided in two component types, one for JP1/Software Distribution Manager and the other for the Asset Information Manager Subset component.

The Database Manager for JP1/Software Distribution Manager is a component of JP1/Software Distribution Manager that is used to create and maintain relational databases used by JP1/Software Distribution.

The Database Manager for Asset Information Manager Subset component is a subcomponent of Asset Information Manager Subset that is used to create and maintain relational databases for Asset Information Manager Subset.

deleted software management table

An internal table in which software deleted from the software inventory is registered. If a *Get software information from client* job with **Search for a file** specified is executed and software information reported from a host is registered in the deleted software management table, the obtained software information is not added to the software inventory nor to the software inventory of the host.

device operation

A target to which operation monitoring is applied. Reading from or writing to media via a USB storage device, internal CD/DVD drive, internal floppy disk drive, IEEE 1394-connected device, internal SD card slot, Bluetooth device, or imaging device can be suppressed as a *device operation*. This can only be used with clients running version 09-50 or later.

Connection and disconnection (removal) information for these devices is also collected in device operation logs.

directory information

User information and computer information acquired from Active Directory. The acquired directory information can be used as a job destination or for viewing the client information from Inventory Viewer.

division

In Asset Information Manager Subset, this is information that allows a user to manage other groups as a group job. Multiple divisions can be set for each group. By assigning a division to a user, that user can also manage the information of the groups (division groups) set to that division.

division information

In Asset Information Manager Subset, this is information about the groups set to a division.

domain

A unit for managing hosts and users in a network.

Embedded RDB

An embedded relational database provided by JP1/Software Distribution Manager. The user can select whether to install Embedded RDB when JP1/Software Distribution Manager is installed.

external media operations

See *operations to or from external media*.

firewall

A component installed at the boundary between the Internet and an internal system, which prevents unauthorized access to the internal system from the outside.

group information

Information used by Asset Information Manager Subset to manage organizations, such as departments that use the asset management system. Group information includes items such as group name, group code, cost group code, and so forth.

higher system addresses, file for

A settings file that contains the mappings of host names and IP addresses. It is used by a client to recognize the IP address of a higher system when a host name-keyed client cannot resolve the name of the higher system.

host

A networked personal computer or workstation that is a target for JP1/Software Distribution operations.

host group

A method of grouping multiple clients for remote installation of software at those clients. This method allows you to group hosts from a managing system in a way that matches the job, organization, or other distribution purpose.

host ID

A key that uniquely identifies a host in a system. Because host IDs are not affected by the network configuration, the system administrator can use host IDs to reduce the work of managing hosts. To use host IDs, a relational database is required.

host on which JP1/Software Distribution is not installed

A host on which JP1/Software Distribution Manager has not been installed.

host search

Function for searching hosts in a specified range in the network. You perform a host search to detect hosts on which JP1/Software Distribution is not installed.

HP NNM

A generic term for integrated network management programs that manage the configuration, performance, and problems in a network. If the OpenView Linkage facility is used, JP1/Software Distribution inventory information and job execution status can be managed from the monitoring windows of HP NNM version 7.5 or earlier.

ID group

A method of grouping multiple clients for remote installation of software at those clients. Clients are registered into an ID group at the clients or managing server.

ID group job

A job that specifies an ID group as the target (destination) of the job.

installation mode

The mode for installing a package in a client. The two options are **GUI installation mode**, which uses an installer, and **Background installation mode**, which does not use an installer and in which the files are simply copied.

installation script

A script executed by clients that specifies the procedure for an installation. An installation script is created automatically when a package is created. Users can create their own installation scripts to execute user-specific processes.

installation timing

The timing for installing a package in a client. You can select either **Install when system starts**, which installs the package when the client is started, or **Normal installation**, which installs the package when the package is transferred to the client.

installed software information

Information used by Asset Information Manager Subset to manage the software installed in various devices.

Installed software information (that is, the inventory information managed by the managing server) is imported into and used by the database of Asset Information Manager Subset. Therefore, the information (such as the software names and versions) becomes the content managed by an information-importing program, such as JP1/Software Distribution.

installed software list

Information used by Asset Information Manager Subset to manage the names of software installed in various devices. This list is also used for managing the various settings of the installed software.

InstallShield environment deletion tool

A tool that re-initializes the installation environment. It is used before JP1/Software Distribution Client is re-installed after an installation has been stopped due to an installation error.

inventory

Information required for managing clients, such as hardware usage conditions and types of software installed in the client. A client's inventory is retrieved from the client by executing a job from the managing server.

Inventory Viewer

A window for displaying and counting inventory information retrieved from clients. This window provides a wide range of reporting functions. It can be used by JP1/Software Distribution Manager.

job

The execution unit of JP1/Software Distribution facilities. There are 21 job types:

- *Install package*
- *Transfer package to relay system*
- *Batch delete packages on relay system*
- *Collect files from client*
- *Collect files from client to relay system*
- *Acquire collected files from relay system*
- *Delete collected files from relay system*
- *Send package, allow client to choose*
- *Get system configuration information*
- *Get system information from client*
- *Get software information from client*
- *Transfer user inventory schema to client*
- *Get user inventory information*
- *Transfer registry collection definition*
- *Hold report*
- *Hold-report release*
- *Suspend file transfer*
- *Resume file transfer*
- *Report message*
- *Set the software monitoring policy*
- *Get software monitoring information from the client*

JP1 event

Information that is reported to JP1/Base about an event that has occurred in a system.

JP1 user

An account used by JP1/Software Distribution for user authentication when user management is performed in linkage with JP1/Base. Such an account is set up in the authentication server installed with JP1/Base. JP1/IM and JP1/AJS can also be used to perform user authentication of JP1 users.

JP1/AJS

A program for running jobs automatically. JP1/AJS enables you to routinely execute processes in a given order and to start a process when a specified event occurs.

JP1/Asset Information Manager

A program that supports streamlining of IT asset management tasks and reduction of management cost required for such tasks (for example installing assets, managing software licenses, or performing device maintenance) by using a database to centrally manage pertinent information (for example, information about hardware, software, or contracts).

JP1/Base

A program that provides the core functionality for JP1/IM. JP1/Base sends and receives JP1 events, manages users, and controls client startup. It also functions as the JP1/IM system agent. JP1/Base is a prerequisite program for JP1/IM - Manager.

JP1/IM

A program that centrally monitors a distributed system. Information about events (such as job processing and failures in the distributed system) is sent to JP1/IM as JP1 events. JP1/IM registers and manages JP1 events, and displays them on the system administrator's screen.

JP1/Software Distribution not installed, host on which

See *host on which JP1/Software Distribution is not installed*.

JP1/Software Distribution system

The entire network consisting of the hosts on which JP1/Software Distribution is installed.

Local System Viewer

A window that displays information about the hardware and software of clients, including the system monitoring status, alerts history, system information, and installed software. The client user can use this window for local system management purposes, because the information is available even when the client is not connected to a higher system.

managing server

A program that stores software to be remotely installed and gives the instructions for remote installation. This program can check the software installed in each host and the status and results of remote installation.

Microsoft SQL Server

Microsoft Corporation's relational database management system running on Windows NT. Microsoft SQL Server can be used as the relational database management system for JP1/Software Distribution information.

multicast address

The IP address of a multicast group. The address is specified when the sender and receivers for multicast distribution are set up.

multicast distribution

A method of job distribution that uses the IP multicast protocol to send packets to many specific clients from a higher system. Traffic is reduced because the higher system only needs to send the job packet to one multicast group location, regardless of the number of clients.

multicast group

A conceptual group to which jobs are distributed by multicast distribution. A multicast group has a specific IP address, known as the *multicast address*. When a higher system sends job packets to a multicast group, the packets are then distributed to each client within that group.

multiple LAN connections

A JP1 facility for handling systems that consist of multiple LANs.

Using this facility, you can preset the LAN to be used for JP1 transmission on hosts that are connected to multiple LANs. Because JP1 communications can be set up independently of the system and other applications, this facility supports a wide range of networks and modes of operation.

Hosts connected to multiple LANs may also be called multi-homed hosts or multi-NIC (Network Interface Card) hosts.

JP1/Software Distribution supports the following multi-LAN environments:

- Environments separated into multiple networks

- Environments with duplex networks

network configuration information file

A CSV file that contains information, such as the IP and MAC addresses, and subnet mask, of the hosts that are connected to the network.

network information

Information used by Asset Information Manager Subset to manage the location of each device on a network. Network information includes items such as IP addresses, MAC addresses, node names, computer names.

offline folder

A folder for managing inventory information and operation information that is obtained from an offline machine. An offline folder is indicated as **{OFFLINE}** in the System Configuration and Destination windows.

offline installation

Facility for installing software using installation storage media instead of via a network.

offline machine

A Windows client that has not been registered in JP1/Software Distribution's system configuration information, such as the following PCs:

- PC on which a stand-alone JP1/Software Distribution Client (client) has been installed
- PC in a network on which JP1/Software Distribution Client (client) has been installed but not registered in JP1/Software Distribution's system configuration information

Inventory information and operation information can be obtained from offline machines. Software can be installed on offline machines.

offline machine Information

Inventory information and operation information that is obtained from offline machines.

operation history

Information on the software and files manipulated at a client. The operation history includes information about the following:

- Starting of processes
- Stopping of processes
- Changes to a caption
- Change to the active window
- Starting and stopping of machines
- Logons and logoffs
- File operations
- Web access
- Print operations
- Operations to or from external media
- Device operations

Operation Log List window

When client operation information is collected by the managing server, this window can be used to extract the software startup history, the print operations suppression history, and the software and file operation history under various conditions, and to view the extracted history.

operation logs

When the user operation log data stored in the database for the suppression history and operation history acquired by JP1/Software Distribution are checked in the Operation Log List window, the displayed information is referred to in general as *operation logs*.

operation monitoring policy

Conditions specified in order to monitor the software operation status. A policy sets software whose startup is to be suppressed and operations whose history is to be acquired.

operations to or from external media

A target to which operation monitoring is applied. Reading from or writing to media via a USB-connected storage device, internal CD/DVD drive, internal floppy disk drive, IEEE 1394-connection, or an internal SD card slot can be suppressed as an *operation to or from external media*. This can only be used with clients running versions between 08-51 and 09-00.

Connection and disconnection (removal) information for these external media is also collected in external media operation logs. Note that logs are not collected on operations to or from internal floppy disk drives.

package

The unit in which software programs are remotely installed. Packages are stored in the cabinet of a managing server.

Package Setup Manager

A facility that enables clients to select and install desired software programs received from the managing server or relay systems. It can reject installation or change the installation directory.

package type

There are three package types: user programs and data, Hitachi program products, and other companies' software.

Packager

A program that registers, into the managing server, software that is to be remote-installed.

packaging

The process of using Packager to create packages of software programs.

packet filtering method

A method of building a firewall that limits the packets that can pass through the firewall. This method allows access from within the system to the outside but prohibits access into the system from the outside. This method can limit the number of terminals that are permitted to access the Internet.

patch information file

File that contains information for obtaining patches from a Microsoft server. This file is needed by JP1/Software Distribution in order to obtain patches. JP1/Software Distribution obtains the path information file by connecting to a Hitachi Web server. It is updated based on the provisioning status of patches supplied by Microsoft.

patch information, unapplied

Information about patches that have not been applied to the client. Of the scanning results of the `mbsacli.exe` MBSA command, JP1/Software Distribution treats the information for which the most recent patch was not found (information indicated as `NOT Found` in the scanning results) as unapplied patch information.

policy

Conditions for automatic assignment to a host group or ID group of a new host being added to the system configuration by a facility for automatic registration into the system configuration.

RD area

A logical area used by Embedded RDB for storing tables and indexes.

recorder file

A file that defines the procedure for installing software interactively using a dedicated installer. JP1/Software Distribution provides recorder files for some software programs distributed by other companies. The user can also create recorder files.

relational database

In this manual, this term almost always refers to the database used for managing JP1/Software Distribution Manager's information. Supported relational databases are Embedded RDB, Microsoft SQL Server, and Oracle.

relay manager

JP1/Software Distribution Manager positioned under the highest managing server (central manager) in a system where managing servers are configured in a hierarchy. A relay manager relays jobs, such as jobs to perform remote installation or to collect inventory information, between the managing server and clients.

relay manager/system

Collective name for programs that relay jobs, such as jobs to perform remote installation or to collect inventory information, between the managing server and clients.

relay managing the ID

A relay manager or relay system that manages ID group jobs and clients that belong to an ID group. When an ID group job is executed, the relay managing the ID saves the job in the local system and executes it for clients that are registered in the ID group.

relay system

JP1/Software Distribution Client that relays jobs, such as jobs to perform remote installation or to collect inventory information, between the managing server and clients.

remote collection

A facility for collecting files from clients to the managing server. Instructions are issued from the managing server.

remote control

A facility that executes client operations remotely from a managing server.

Remote Control Agent

A program executed on a remote PC that is controlled by remote operations from the Remote Control Manager.

Remote Control Manager

A program that issues remote control operations to the Remote Control Agent.

Remote Desktop

In this manual, the following functions are referred to as *Remote Desktop*:

- Remote Desktop for Administration or Remote Desktop in Windows Server 2012, Windows Server 2008, Windows Server 2003, Windows 8, Windows 7, Windows Vista, and Windows XP
- Terminal Services in Windows 2000 Server

remote installation

A facility that transfers packaged software from a managing server to a client system and installs it in the client.

Remote Installation Manager

A program that provides the interactive (GUI) capability at a managing server.

search pattern

The search conditions used to search for operation logs in the Operation Log List window are saved as search patterns. The search patterns used for the main searching purposes are registered as defaults. You can also edit the default search patterns or register new search patterns.

security PC

A PC that has only the minimally necessary functions, and that is not equipped with any external storage devices, such as a hard disk or floppy disk. A security PC can connect to an agent and remotely control application software and files. You can use JP1/Software Distribution to remotely install the update data for a security PC.

software information

Information about software installed on hosts comprising a JP1/Software Distribution system. It is acquired by executing jobs from a managing server.

software inventory dictionary

A dictionary for specifying the software to be managed by JP1/Software Distribution. From the software obtained through a file search, you can select the software to be managed. You can also specify the license information needed for managing software licenses using Inventory Viewer.

software search list

A list that is used to acquire software information. There are two types of software search lists, the *standard retrieve list*, which is provided by JP1/Software Distribution, and the *optional software list*, which can be edited by the user.

split distribution

A method of reducing the load on the network by dividing a package into units of a user-specified size and transferring them at a user-specified interval (distribution interval). The user can specify the file split size at setup or job creation, or even at relay locations along the package transfer route. Split distribution is useful for distributing large packages.

SQL

Structured Query Language, a language for relational databases.

suppression history

Shows the history of software startup suppression and printing suppression executed at a client

system information

Information about the hardware of hosts comprising a JP1/Software Distribution system. The information is acquired by executing jobs from a managing server.

system monitoring

A facility used by the client to monitor the status of specific hardware according to predefined conditions. During system monitoring, the status of a program being monitored is displayed on the **System Conditions** page of Local System Viewer. If an error occurs in the program being monitored, this event is reported to the user by displaying an alert message or changing the appearance of an icon. While the client is connected to its higher system, alerts can also be reported to the higher system.

System Monitoring icon

An icon displayed in the task bar notification area. The status of the system monitoring facility and the presence of alert messages can be identified by the icon's status (appearance). Double-clicking on the **System Monitoring** icon starts Local System Viewer.

To display the **System Monitoring** icon, in the Client Setup dialog box, on the **System Monitoring** page, choose the **Display the System Monitoring icon in the task bar notification area** option.

terminal server

In this manual, the following servers are referred to as a *terminal server*:

- For Windows Server 2012 or Windows Server 2008 R2, servers on which Remote Desktop Session Host Role Service of Remote Desktop Services is installed
- For Windows Server 2008 or Windows Server 2003, servers on which Terminal Server Role Service of Terminal Services is installed
- For Windows 2000 Server, servers on which Terminal Services has been installed in Application Server Mode

unarchiver

A program that restores archived and compressed files to their original formats during remote collection.

unicast distribution

A method of job distribution in which packets are sent from a higher system to each client individually. Because the higher system has to send each job packet separately to each target client, the number of times a packet is sent increases proportionally to the number of clients in the system.

user inventory information

Information unique to a client (such as name and PC serial number). The managing server executes a job to obtain this information.

user inventory item

An entry item for user inventory information. The user inventory items created in the managing server are distributed to clients by executing jobs.

Visual Test

A program that supports debugging of programs that run in a Windows environment.

Wake on LAN

A standard for turning on a computer in a LAN from another computer in the network.

Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista version of JP1/Software Distribution Client

A program needed in order to manage a computer running a Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, or Windows Vista operating system as a client in a JP1/Software Distribution system. It can also be used as a relay system.

Index