

Hinemos

Hinemos ver4.1
Administrator's Guide, Edition 1.0

Contents

1	Introduction	6
2	Prerequisites	7
3	Maintenance	8
3.1	Maintenance of the Hinemos Manager	8
3.1.1	Summary	8
3.1.2	Maintenance Script List	8
3.1.3	Deleting Unnecessary Data from the Database	9
3.1.4	Rebuilding the Database	10
3.1.5	Backing-up the Database	11
3.1.6	Restoring the Database	11
3.1.7	Deleting Information Stored in the Temporary Queue	12
3.1.8	Deleting the History Information that is the Suppression Standard for Notification	12
3.1.9	Acquiring Environment Summary Information	12
3.1.10	Scheduler Adjustment after changing the OS clock settings	13
3.2	Deleting the Log File	13
3.2.1	Hinemos Manager Log File	13
3.2.2	Hinemos Agent Log Files	14
3.2.3	Hinemos Client Log Files	14
3.3	Backing-up / Recovering the Hinemos Manager	14
3.3.1	Backing-up the Hinemos Manager	14
3.3.2	Recovering the Hinemos Manager	15
3.4	Backing-up / Recovering the Hinemos Agent	15
3.4.1	Backup the Hinemos Agent	15
3.4.2	Recovering the Hinemos Agent	16
3.5	Backing-up / Recovering the Hinemos Client	16
4	OS/Version	17
4.1	Configuring the File Descriptor	17
4.2	Setting the Number of Connections to the Database	17
4.3	Java Heap Memory Settings	17
4.4	Configuring OS Locale and Character Encoding	18
4.4.1	Hinemos Client	18
4.4.2	Hinemos Manager	18
4.4.3	Hinemos Agent	18
4.5	Hinemos Agent Facility ID Setting	19
5	Notification Feature	20
5.1	Event Notification	20
5.1.1	Configuring the Maximum Number of Downloads	20
5.2	Mail Notification	20
5.2.1	Enabling Email Notification	20
5.2.2	Configuring SMTP AUTH	21
5.2.3	SSH/TLS Settings	22
5.2.4	Configuring the Envelope From	22
5.3	Log Escalation Notification	22
5.3.1	Configuration Method of Embedded Host Name	22

6	Collective Run Feature	24
6.1	Enabling the Collective Run Feature	24
6.1.1	Managed Node Setup	24
6.1.2	Hinemos Manager Remote Shell Setup	26
6.1.3	Starting the FTP Server	27
7	Monitor Settings / Performance Management Feature	28
7.1	SQL Monitor	28
7.1.1	Adding a Monitoring Target RDBMS	28
7.2	Process Monitor	28
7.2.1	Handling when "Failed to get value" Notification Occurs	28
7.3	HTTPS Monitor	29
7.3.1	Preparing the Certificate	30
7.3.2	Register the Certificate to the Keystore	30
7.3.3	Specifying the Keystore File in the Java Startup Options	30
7.4	System Log Monitor	30
7.4.1	Settings Related to syslog Sending	30
7.4.2	Settings Related to syslog Receiving	31
7.4.3	Invalidating the Escape Process for Control Characters	31
7.4.4	Host Name Replacement Process Settings for the syslog Header Part	32
7.5	SNMPTRAP Monitor	32
7.5.1	Settings Related to SNMPTRAP Receiving	32
7.5.2	Default MIB	32
7.6	Windows Service Monitor	41
7.6.1	WinRM Installation	41
7.6.2	Remote Computer Management Authorization	41
7.6.3	Basic Confirmation Authorization	41
7.6.4	Unencrypted Transmission Authorization	42
7.6.5	Set up HTTPS	42
7.6.6	Prepare the Destination OS User	42
7.6.7	Synchronization Confirmation	42
7.7	Custom Monitor	43
7.7.1	Command Action Change	43
7.7.2	Maximum Value from Standard Output Settings	43
7.7.3	New Line Code Included in the Standard Output Setting	43
7.7.4	Command Execution Multiplicity Setting	44
7.8	Polling Protocol Setting	44
7.8.1	Configuring Net-SNMP	44
7.8.2	Method of SNMP/WBEM switchover	44
7.9	Collection Value of the Numeric Value Monitoring Setting	45
7.10	Resource Monitoring	45
7.10.1	Settings for mass storage filesystem monitoring	45
8	Job Management Feature	47
8.1	Changing the Action of the Startup Command	47
8.2	Configuring the Job Schedule Control when Restarting Hinemos Manager	48
8.3	Enabling a File Transfer Job	48

9	Other Features	51
9.1	Self-check Feature	51
9.1.1	Self-check Feature Settings	52
9.2	INTERNAL Events	53
9.2.1	Notification Destination Settings	53
9.2.2	Notified Information	54
9.3	Hinemos Manager Alive Detection	57
10	Security	58
10.1	Change the Database Access Password	58
10.1.1	PostgreSQL (destination) Setting Changes	58
10.1.2	Hinemos Manager (destination) Setting Changes	59
11	Connections between Hinemos Components	61
11.1	Connections to Hinemos Manager via HTTP Proxy	61
11.1.1	Connecting to Hinemos Manager from Hinemos Client	61
11.1.2	Connecting to Hinemos Manager from Hinemos Agent	61
11.2	HTTPS connection to Hinemos Manager	62
11.2.1	Preparing server certificate of Hinemos Manager Server	62
11.2.2	Connections from Hinemos Client to Hinemos Manager	64
12	Log Files	64
12.1	List of Hinemos Manager Log Files	64
12.2	Changing Log Output and Log Rotation of Java Process	66
12.3	Changing Log Output and Log Rotation of PostgreSQL	66
12.4	Changing Log Output and Log Rotation of Operations Log	66
12.5	List of Hinemos Agent Log Files	67
12.6	Changing the Log Output and Log Rotation settings of the Hinemos Agent	68
12.7	List of Hinemos Client Log Files	69
13	List of Hinemos Manager's Configuration Settings	69
14	Hinemos Agent Configuration List	87
15	ChangeLog	96

This software was developed in response to the delegation of the second half open-source-software activity infrastructure improvement enterprise in fiscal year 2004 by the INFORMATION-TECHNOLOGY PROMOTION AGENCY (IPA), an independent administrative agency.

- The theme name is "Development of an Integrated Manager for Distributed Facilities."
- <http://www.ipa.go.jp/about/jigyoseika/04fy-pro/open.html>

For the latest information about Hinemos, please visit the Hinemos web portal (<http://www.hinemos.info>).

1 Introduction

This manual explains the methods for maintenance needed when operating Hinemos, and settings methods related to the basic operations of Hinemos.

The setting methods shown here are for setting files, etc. primarily related to security, performance tuning and basic operations. For methods operated from Hinemos Client, please refer Hinemos User's Manual.

Settings shown in this manual is one of the examples. For actual use, it is recommended that you change settings or configurations following the security policy of the used environment. We are in no way responsible for any damage resulting from the use of this software.

2 Prerequisites

This manual explains the method for maintaining Hinemos, and the setting method for security, performance tuning and changing the basic operation.

Therefore, the contents in this manual is written for environment where the Hinemos Manager, Agent and Client are already installed, according to the Hinemos Installation Manual, and that it can be used.

In addition, behavior of Hinemos may become unstable depending on the setting values and the combinations. Therefore, it is recommended for you to take back up before making any configuration changes.

3 Maintenance

3.1 Maintenance of the Hinemos Manager

3.1.1 Summary

To ensure the use of Hinemos for a long time, you must perform regular maintenance according to the operating condition of the installation environment. The following scripts are provided for maintenance of the Hinemos manger.

- Delete unneeded data (such as log information that no longer needs to be saved) from the database

```
hinemos_delete.sh
```

- Rebuild the database to allow the system to reuse unneeded area (protected area not being used)

```
hinemos_cluster_db.sh
```

- Back up the data (such as settings and history information) in the database

```
hinemos_backup.sh
```

- Restore the data (such as settings and history information) in the database from a temp file

```
hinemos_restore.sh
```

- Delete information (temporary information) stored in the temporary queue

```
hinemos_clear_tmp.sh
```

- Delete history information that is the suppression standard for notification (reset suppression for all notification information)

```
hinemos_clear_notify.sh
```

- Acquire environment summary information

```
hinemos_manager_summary.sh
```

- Reset Scheduler

```
hinemos_reset_scheduler.sh
```

All of the maintenance scripts listed above are located in the /opt/hinemos/sbin/mng directory.

3.1.2 Maintenance Script List

The prerequisites for running each of the maintenance scripts are shown in Table 3-1.

Table 3-1 Maintenance Script List

Process details	Script Name	Hinemos Manager Running	PostgreSQL running java stopped
Delete unnecessary data	hinemos_delete.sh	×	○
Reconstructing the database	hinemos_cluster_db.sh	×	○
Backing-up the database	hinemos_backup.sh	○	○

Restoring the database	hinemos_restore.sh	×	○
Delete the temporary queue	hinemos_clear_tmp.sh	×	○
Delete the notification suppression information	hinemos_clear_notify.sh	○	×
Acquire environment summary information	hinemos_manager_summary.sh	○	×
Reset Scheduler	hinemos_reset_scheduler.sh	×	○

○ : Can Run, × : Cannot Run

3.1.3 Deleting Unnecessary Data from the Database

Run `hinemos_delete.sh` to delete unneeded data (such as log information that no longer needs to be saved) from the database.

The following log information is accumulated in the Hinemos Manager database.

- Log monitoring information (Status)
- Log monitoring information (Event)
- Job execution history
- Batch control execution history
- Collection value of the numeric value monitoring
- Edit Lock holding information

This history information is deleted regularly by the history information delete feature of the maintenance feature. (Refer to the Hinemos User's Manual for details about the history information delete feature)

Use `hinemos_delete.sh` to delete the history manually and immediately rather than the history information delete feature.

1. This will stop the Hinemos manager and leave only the PostgreSQL running.

```
(root) # /opt/hinemos/bin/hinemos_stop.sh
(root) # /opt/hinemos/bin/pg_start.sh
```

2. Specify the options based on the target data for deletion and then run the script.

This script can be used directly if the database (PostgreSQL) password has already been specified at `-w` Options. Enter the password interactively if `-w` option is not set up.

- When deleting all the historical information of monitored result (Status)

```
(root) # /opt/hinemos/sbin/mng/hinemos_delete.sh -S
```

- When deleting all the historical information of confirmed monitored result (event)

```
(root) # /opt/hinemos/sbin/mng/hinemos_delete.sh -e
```

- When deleting all the historical information of monitored result (event)

```
(root) # /opt/hinemos/sbin/mng/hinemos_delete.sh -E
```

- When deleting all the historical information of executed and completed jobs

```
(root) # /opt/hinemos/sbin/mng/hinemos_delete.sh -j
```

- When deleting all the historical information of executed jobs

```
(root) # /opt/hinemos/sbin/mng/hinemos_delete.sh -J
```

- When deleting all the historical information of executed and completed batch control task

```
(root) # /opt/hinemos/sbin/mng/hinemos_delete.sh -c
```

- When deleting all the historical information of executed batch control task

```
(root) # /opt/hinemos/sbin/mng/hinemos_delete.sh -C
```

- When deleting collected values of numeric monitoring settings specified by monitor ID

```
(root) # /opt/hinemos/sbin/mng/hinemos_delete.sh -p [Monitor ID]
```

- When deleting all collected values of numeric monitoring settings

```
(root) # /opt/hinemos/sbin/mng/hinemos_delete.sh -P
```

- When deleting collected values of numeric monitoring settings, specified by monitoring ID, with designation of period not to delete (from current time until the designated period)

```
(root) # /opt/hinemos/sbin/mng/hinemos_delete.sh -p [Monitor ID] -r [Period of Keep Log(Day)]
```

- When deleting collected values of numeric monitoring settings, with designation of period not to delete (from current time until the designated period)

```
(root) # /opt/hinemos/sbin/mng/hinemos_delete.sh -P -r [Period of Keep Log(Day)]
```

- When deleting all Edit Lock holding information

```
(root) # /opt/hinemos/sbin/mng/hinemos_delete.sh -L
```

3. Start up the Hinemos Manager.

```
(root) # /opt/hinemos/bin/pg_stop.sh
(root) # /opt/hinemos/bin/hinemos_start.sh
```

3.1.4 Rebuilding the Database

Run `hinemos_cluster_db.sh` to rebuild the database to allow the system to reuse unneeded area (protected area not being used).

Even if unneeded data is deleted with 'Deleting Unnecessary Data from the Database', the disk space allocated to the database will not be freed up, so the size of the disk area used by the Hinemos database will not change.

The database must be rebuilt in order to free up this space so the system can reuse it.

To avoid performance degradation due to fragmentation (particularly the index) of the data file, it is recommended that you rebuild the database regularly (at least once every 6 months).

Also, it is recommended that you rebuild the database if any of the following apply.

- A large number of notifications are generated due to an error on a monitored target, etc.
- you deleted a large amount of log information that was unnecessary
- The Hinemos Manager has a performance decrease

Further, `hinemos_cluster_db.sh` copies the existing data files to new data files during the rebuild. Ensure that there is sufficient space on the file system where the data file `/opt/hinemos/var/data/` is stored. It is recommended that you secure a workspace of 2 times the size of the current database (file size under `/opt/hinemos/var/data/`).

1. This will stop the Hinemos Manager and leave only the PostgreSQL running.

```
(root) # /opt/hinemos/bin/hinemos_stop.sh  
(root) # /opt/hinemos/bin/pg_start.sh
```

2. Run the maintenance script.

```
(root) # /opt/hinemos/sbin/mng/hinemos_cluster_db.sh
```

3. Start up the Hinemos Manager.

```
(root) # /opt/hinemos/bin/pg_stop.sh  
(root) # /opt/hinemos/bin/hinemos_start.sh
```

3.1.5 Backing-up the Database

Run `hinemos_backup.sh` to backup the data (such as settings and log information) in the database.

To prepare for the case where the setting data is deleted due to an unexpected error with the manger server or a user operation mistake, it is recommended that you regularly back up the data in the database.

1. Move to the output directory (/tmp is used as an example) for the dump file (database backup file).

```
(root) # cd /tmp
```

2. Run the maintenance script.

```
(root) # /opt/hinemos/sbin/mng/hinemos_backup.sh
```

This script can be used directly if the database (PostgreSQL) password has already been specified at `-w` Options. Enter the password interactively if `-w` option is not set up.

3. Confirm the dump file output in the current directory.

```
(root) # ls  
hinemos_pgdump.YYYY-MM-DD_HHmss
```

Further, the dump file can be acquired while the Hinemos Manager is running, but be careful of doing a backup under those conditions.

For example, when you list the dump file acquired when a job is running, the corresponding job will be running when the state at the time of backup is restored. To avoid a job running suddenly, right after a restore, it's recommended that the backup be done at a time when a job is not running.

3.1.6 Restoring the Database

To restore the data (settings - history information, etc.) in the database from a dump file acquired with [Backing-up the Database](#), run `hinemos_restore.sh`.

1. Stopping the Hinemos Manager.

```
(root) # /opt/hinemos/bin/hinemos_stop.sh  
(root) # /opt/hinemos/bin/pg_start.sh
```

2. Run the maintenance script.

```
(root) # /opt/hinemos/sbin/mng/hinemos_restore.sh hinemos_pgdump.YYYY-MM-DD_HHmss
```

3. Start up the Hinemos Manager.

```
(root) # /opt/hinemos/bin/pg_stop.sh
(root) # /opt/hinemos/bin/hinemos_start.sh
```

3.1.7 Deleting Information Stored in the Temporary Queue

To delete information (temporary information) stored in the temporary queue run `hinemos_clear_tmp.sh`.

The information that `hinemos_clear_tmp.sh` will delete from the table in the dump file is the following information stored in the temporary queue.

- Process waiting notification information
- Unknown information that was not processed (such as from a control stop of Hinemos Manager)

Further, since all of the information in the temporary queue will be deleted, the following information that is awaiting processing prior to the Hinemos Manager stop will also be targets for deletion.

- Process waiting notification information (event, status, etc.)

1. This will stop the Hinemos Manager and leave only the PostgreSQL running.

```
(root) # /opt/hinemos/bin/hinemos_stop.sh
(root) # /opt/hinemos/bin/pg_start.sh
```

2. Run the maintenance script

```
(root) # /opt/hinemos/sbin/mng/hinemos_clear_tmp.sh
```

This script can be used directly if the database (PostgreSQL) password has already been specified at `-w` Options. Enter the password interactively if `-w` option is not set up.

3. Start up the Hinemos Manager.

```
(root) # /opt/hinemos/bin/pg_stop.sh
(root) # /opt/hinemos/bin/hinemos_start.sh
```

3.1.8 Deleting the History Information that is the Suppression Standard for Notification

Run `hinemos_clear_notify.sh` to delete the history information that is the suppression standard for notification.

The notification feature provides functionality to suppress duplicate notifications. (Refer to the Hinemos User's Manual for details about the notification feature) The most recent notification history information for suppressing these notifications is saved there.

When you run `hinemos_clear_notify.sh`, the saved notification history information will be cleared, and the suppressed status can be temporarily reset. (The suppression will be released for all notification information)

1. Run the maintenance script

```
(root) # /opt/hinemos/sbin/mng/hinemos_clear_notify.sh
```

3.1.9 Acquiring Environment Summary Information

Run `hinemos_manager_summary.sh` to acquire the manager's environment summary information.

1. Run the maintenance script

- To acquire just the Hinemos Manager's environment summary information

```
(root) # /opt/hinemos/sbin/mng/hinemos_manager_summary.sh -v
```

- To acquire Hinemos Manager's environment summary information and OS information

```
(root) # /opt/hinemos/sbin/mng/hinemos_manager_summary.sh -vv
```

- To acquire the Hinemos Manager's environment summary information (detail version)

```
(root) # /opt/hinemos/sbin/mng/hinemos_manager_summary.sh -vvv
```

- To acquire the Hinemos Manager's environment summary information (detail version) and operation log

```
(root) # /opt/hinemos/sbin/mng/hinemos_manager_summary.sh -o
```

- To acquire the Hinemos Manager's thread dump

```
(root) # /opt/hinemos/sbin/mng/hinemos_manager_summary.sh -t
```

3.1.10 Scheduler Adjustment after changing the OS clock settings

After changing the clock of the Operating System which Hinemos Manager is running, execute `hinemos_reset_scheduler.sh` in order to reset the internal scheduler of Hinemos.

1. Stop Hinemos Manager.

```
(root) # /opt/hinemos/bin/hinemos_stop.sh
```

2. Change the OS Clock which Hinemos Manager is running.
3. Start PostgreSQL only.

```
(root) # /opt/hinemos/bin/pg_start.sh
```

4. execute scheduler reset script.

```
(root) # /opt/hinemos/sbin/mng/hinemos_reset_scheduler.sh
```

When executing this script, "-w" option can be used in order to designate a password of the database(PostgreSQL). When this "-w" option is not used, password of the database will be asked interactively.

5. Start Hinemos Manager.

```
(root) # /opt/hinemos/bin/pg_stop.sh  
(root) # /opt/hinemos/bin/hinemos_start.sh
```

3.2 Deleting the Log File

To avoid a reduction in disk space due to expansion of the log file, confirm the various log files output by the Hinemos Manager, Agent and Client, and delete or move files that have become unnecessary.

3.2.1 Hinemos Manager Log File

The Hinemos Manager log file is output to the directory in Table 3-2.

Table 3-2 List of Hinemos Manager Log Files

Path	Content
/opt/hinemos/var/log/	Various log files output by Hinemos

Further, there is a script provided for Hinemos Manager to delete log files that are past the fixed period (31 days) from the last update date.

- /opt/hinemos/contrib/hinemos_manager

Place this script in /etc/cron.daily/ as shown below to run this script daily.

```
(root) # cp -p /opt/hinemos/contrib/hinemos_manager /etc/cron.daily/
```

3.2.2 Hinemos Agent Log Files

The Linux agent log file is output to the directory in Table 3-3.

Table 3-3 Linux Agent Log Directory

Path	Content
/opt/hinemos_agent/var/log/	Various log files output by Hinemos Agent

The Windows agent log file is output to the directory in Table 3-4.

Table 3-4 Windows Agent Log Directory

Path	Content
<Hinemos Agent install folder>\var\log\	Various log files output by Hinemos Agent

3.2.3 Hinemos Client Log Files

The Hinemos Client log file is output to the directory in Table 3-5.

Table 3-5 List of Hinemos Client Log Directory

Path	Content
<User home directory>\AppData\Roaming\hinemos\Client4.1\	Hinemos Client log file

3.3 Backing-up / Recovering the Hinemos Manager

The backup/recovery method for the Hinemos Manager is explained.

3.3.1 Backing-up the Hinemos Manager

- Database backup
Acquire the dump file according to [Backing-up the Database](#).

- Backup configuration files (settings file, etc.)

A list of files that are generally targets for backup is shown below. (If there is a modified file not on this list, back it up as needed)

- Hinemos Manager settings file
 - All files under /opt/hinemos/etc
- Service scripts (if Hinemos Manager is run as a service)
 - /etc/init.d/hinemos_manager
- Log file deletion scripts
 - /etc/cron.daily/hinemos_manager
- Files used by another process on the same OS
 - /etc/rsyslog.conf
 - /etc/rsyslog_hinemos.conf
 - /etc/sysconfig/rsyslog

3.3.2 Recovering the Hinemos Manager

1. Reinstall the Hinemos Manager

Install Hinemos Manager. If Hinemos Manager is already installed, uninstall it before installing again.

Refer to the Hinemos Installation Manual for details on installation and uninstallation of the Hinemos Manager.

2. Restore the backup data of the database

Take the dump file acquired with [Backing-up the Database](#) and restore following the procedures in [Restoring the Database](#).

3. Apply only the configuration files that were backed up.

Apply only the configuration files (setting files, etc.) that were backed up.

Confirm the contents of the backed up configuration files. If there are items that need to be applied, apply them to the re-installed Hinemos Manager. (The application method depends on the file type and the setting file parameters)

3.4 Backing-up / Recovering the Hinemos Agent

The backup/recovery method for the Hinemos Agent is explained.

3.4.1 Backup the Hinemos Agent

Linux Agent

- Backup configuration files (settings file, etc.)

A list of files that are generally targets for backup is shown below. (If there is a modified file not on this list, back it up individually)

- The Hinemos Agent settings file
 - All files under /opt/hinemos_agent/conf/
- Service script (when added as a service)
 - /etc/init.d/hinemos_agent
- Files used by another process on the same OS
 - /etc/rsyslog.conf
 - /etc/snmp/snmpd.conf
 - /etc/sysconfig/snmpd

Windows Agent

- Backup configuration files (settings file, etc.)

A list of files that are generally targets for backup is shown below. (If there is a modified file not on this list, back it up individually)

- The Hinemos Agent settings file
 - [Hinemos Agent install directory]\conf\ all files in the directory

- SNMP Service Settings

The setting information backup cannot be acquired. (Re-enter this from the GUI for recovery)

3.4.2 Recovering the Hinemos Agent

Platform Common

1. Reinstall the Hinemos Agent

Install the Hinemos Agent. (If Hinemos Agent is already installed, uninstall it before installing again)

Refer to the Hinemos Installation Manual for details on installation and uninstallation of the Hinemos Agent.

2. Application of only the configuration files (setting files, etc.) that were backed up

Apply only the configuration files (setting files, etc.) that were backed up.

Confirm the contents of the backed up configuration files. If there are things that need to be applied, apply them to the re-installed Hinemos Agent. (The application method depends on the file type and the setting file parameters)

Windows Agent

1. Reconfigure the SNMP Service

Please refer to "Hinemos Install Manual" for detail information of SNMP Service settings.

3.5 Backing-up / Recovering the Hinemos Client

There are no files that are backup targets for the Hinemos Client. Recover by reinstalling the Hinemos Client.

Refer to the Hinemos Installation Manual for details on installation and uninstallation of the Hinemos Client.

4 OS/Version

Additional settings relative to the server environment upon which Hinemos is about to be installed are explained.

4.1 Configuring the File Descriptor

When the number of the Hinemos Agents connecting to one Hinemos Manager become extremely large, the following message may be outputted in the Hinemos Manager log file (/opt/hinemos/var/log/hinemos_manager.log).

```
(Too many open files)
```

This message indicates that the number of file descriptor handled by the Hinemos Manager's java process has reached its upper limit and that new socket cannot be created, or that a file cannot be newly opened.

In that case, the upper limit of the file descriptor count must be changed. Change the JAVA_FD_MAXNUM setting value defined in the Hinemos Manager's setting file (hinemos.cfg). (Value set as JAVA_FD_MAXNUM is used for the upper limit value assigned in the Java process)

- /opt/hinemos/hinemos.cfg

```
export JAVA_FD_MAXNUM=4098
```

Hinemos Manager must be restarted for the configuration changes to be reflected.

4.2 Setting the Number of Connections to the Database

If the number of java process's connection pool exceeds its upper limit, and the number of connections from JavaVM to PostgreSQL needed for data access becomes insufficient, following settings must be changed, in order to change the number of connections pooled for PostgreSQL. (Default values of Hinemos ver.4.1.0 will be used in the examples shown below)

1. Change the maximum number of connections that PostgreSQL can accept

Change the value for max_connections defined in /opt/hinemos/etc/postgresql/postgresql.conf.

```
max_connections = 200 # (change requires restart)
```

2. Change the number of connection pool

Change the value of eclipselink.connection-pool.initial, eclipselink.connection-pool.min, eclipselink.connection-pool.max, defined in /opt/hinemos/etc/META-INF/persistence.xml

```
<property name="eclipselink.connection-pool.initial" value="160"/>
<property name="eclipselink.connection-pool.min" value="160"/>
<property name="eclipselink.connection-pool.max" value="160"/>
```

Change the value of org.quartz.dataSource.SchedulerDS.maxConnections, defined in /opt/hinemos/etc/scheduler-dbms.properties

```
org.quartz.dataSource.SchedulerDS.maxConnections = 16
```

Hinemos Manager must be restarted in order to apply the configuration changes.

4.3 Java Heap Memory Settings

You can change the following setting file to change the Java heap memory size used by Hinemos Manager.

/opt/hinemos/hinemos.cfg

```
### JVM - Performance Tuning
# for small systems
export JVM_HEAP_OPTS="-Xms512m -Xmx512m -XX:NewSize=160m -XX:MaxNewSize=160m -XX:MaxPermSize=192m -Xss256k"
# for medium systems
#export JVM_HEAP_OPTS="-Xms1024m -Xmx1024m -XX:NewSize=320m -XX:MaxNewSize=320m -XX:MaxPermSize=256m -Xss256k"
# for large systems
#export JVM_HEAP_OPTS="-Xms2048m -Xmx2048m -XX:NewSize=640m -XX:MaxNewSize=640m -XX:MaxPermSize=360m -Xss256k"
```

You can switch the settings by adding or removing the above comment out. It is recommended to keep its default value(512m) when management target node is less than 100. When management target node is more than 100, it is recommended to change its value to 1024m or 2048m.

Hinemos Manager must be restarted for the configuration changes to be reflected.

4.4 Configuring OS Locale and Character Encoding

4.4.1 Hinemos Client

If you are using Hinemos client in Japanese, the OS locale for the Windows OS must be an Japanese locale.(Hinemos Client operation presumes a character code of MS932.) Also, the Hinemos Manager connected from this Hinemos Client must be running on Japanese environment, and Hinemos Manager must be installed with Japanese installer.

If you are using Hinemos client in English, the OS locale for the Windows OS must be an English locale.(Hinemos Client operation presumes a character code of IBM437.) Also, the Hinemos Manager connected from this Hinemos Client must be running on English environment, and Hinemos Manager must be installed with English installer.

4.4.2 Hinemos Manager

When using Hinemos Manager in Japanese Environment, LANG variable of Hinemos Manager server must be ja_JP.UTF-8. Lang Variable can be confirmed with env command.

Also, the install script used when installing Hinemos Manager must be manager_installer_JP.sh. If you install using manager_uninstaller_EN.sh, uninstall and reinstall using manager_installer_JP.sh.

When Hinemos Manager is installed in Japanese environment with manager_installer_JP.sh script. The Hinemos Manager operates where the OS locale is presumed to be ja_JP.UTF-8. This setting can be confirmed in /opt/hinemos/hinemos.cfg.

When using Hinemos Manager in English Environment, LANG variable of Hinemos Manager server must be an english environment (ex. en_US.UTF8, en_JP.UTF8) Lang Variable can be confirmed with env command.

Also, the install script used when installing Hinemos Manager must be manager_installer_EN.sh. If you install using manager_uninstaller_JP.sh, uninstall and reinstall using manager_installer_EN.sh.

```
export LANG=ja_JP.UTF-8
```

4.4.3 Hinemos Agent

Common with Various Platforms

- Character code for standard output and standard error output for jobs

Job execution result includes standard output and standard error output of processes which were executed as "startup command" of jobs. The character code for this standard output and the standard error output can be specified per Hinemos Agent. Further more, this can only be specified per Hinemos Agent process unit, and not per job settings.

This character code is specified in the Agent.properties input.encoding parameter. This parameter can be selected from UTF-8, EUC-JP and MS932. If input.encoding parameter is not specified (default), the OS system locale will be used.

When a byte sequence which cannot be decoded to the specified character code, it will be replaced with a particular code point (uFFFFD).

An example of setting the character code of standard output and standard error output as EUC-JP is as below.

```
## character encoding of job's stdout and stderr
input.encoding=EUC-JP
```

The Hinemos Agent must be restarted if the setting is changed.

- Character code of the log file that is the monitored target

The character code for the log file that is the target of the Monitor Logfile feature can be set. You can select from UTF-8, EUC-JP and MS932 for the parameter. (This is specified at the Hinemos Agent process unit and not at the log file unit)

The character code can be defined in the Agent.properties log.file.encoding parameter. The OS system locale will be followed if the log.file.encoding is not specified (default).

If a byte sequence other than that which can be decoded by the specified character code is read, it will be replaced with a particular code point (uFFFFD).

An example with the character code for standard output and standard output errors as MS932 is shown below.

```
## character encoding of log file
log.file.encoding=MS932
```

The Hinemos Agent must be restarted if the setting is changed.

- Character code of the OS system log that is the monitored target

Hinemos Manager operation presumes a character code for the received system log of UTF-8. Therefore, when receiving a system log for Hinemos Manager from the management target node, they must be sent in ASCII characters only or in UTF-8 (when including multi-byte characters).

4.5 Hinemos Agent Facility ID Setting

Hinemos Agent uses its IP address and host name to specify its own facility ID. However, in an environment where things such as NAT is used, and where IP addresses are changed, this feature of identifying itself will not operate correctly.

In such cases, facility ID can be set to an Hinemos Agent manually, by adding a line such as follows to the Hinemos Agent's setting file (Agent.properties) (If specifying multiple facility ID, please separate the ID's with comma.)

The example of setting Hinemos Agent's Facility ID as "node01" is as shown below.

```
facilityId=node01
```

The Hinemos Agent must be restarted for the configuration changes to be reflected.

5 Notification Feature

Additional settings for Hinemos notification feature are explained in this chapter.

5.1 Event Notification

5.1.1 Configuring the Maximum Number of Downloads

The maximum number of event downloads is set to 2000 by default. To change this setting, change the following parameters of `/opt/hinemos/etc/hinemos.properties`.

```
## The Maximum Number of Events that can be Downloaded
monitor.common.report.event.count=2000
```

Hinemos Manager must be restarted for the configuration changes to be reflected.

However, if the parameter value for `monitor.common.report.event.count` is large, Hinemos Manager's memory can be insufficient. For this reason, it is recommended that you fundamentally do not change from the default value.

5.2 Mail Notification

5.2.1 Enabling Email Notification

The mail server and the send destination information must be set up to use mail notification.

Configuring the Mail Server

Configure the mail server used for the mail notification feature. Edit the following file.

`/opt/hinemos/etc/mail-service.properties`

```
# mail.transport.protocol=smtp, smtps
mail.transport.protocol=smtp

mail.smtp.host=127.0.0.1
mail.smtp.port=25
mail.smtp.connectiontimeout=15000
mail.smtp.timeout=30000
#mail.smtp.auth=false

# mail.store.protocol=imap, imaps, pop3, pop3s
mail.store.protocol=pop3

mail.pop3.host=127.0.0.1
mail.pop3.port=110
mail.pop3.connectiontimeout=15000
mail.pop3.timeout=30000

mail.debug=false

## Hinemos Configuration

# connection user and password
hinemos.mail.transport.user=nobody
hinemos.mail.transport.password=password

# transport retries
hinemos.mail.transport.tries=1
hinemos.mail.transport.tries.interval=10000
```

```
# mail header
hinemos.mail.from.address=admin@hinemos.com
hinemos.mail.from.personal.name=Hinemos Admin
hinemos.mail.reply.to.address=admin@hinemos.com
hinemos.mail.reply.personal.name=Hinemos Admin
hinemos.mail.errors.to.address=admin@hinemos.com

# charset
hinemos.mail.charset.address=UTF-8
hinemos.mail.charset.subject=UTF-8
hinemos.mail.charset.content=UTF-8
```

Set up the following parameters:

```
mail.smtp.host=[SMTP Server's IP address or host name]
mail.smtp.port=[SMTP Server's listen port number]

# transport retries
hinemos.mail.transport.tries=[number of maximum attempts to send mail to SMTP Server]

hinemos.mail.transport.tries.interval=[interval time between retrial of sending mail to SMTP Server [msec]]

# mail header
hinemos.mail.from.address=[Mail address of the sender]
hinemos.mail.from.personal.name=[Mail sender's Name]
hinemos.mail.reply.to.address=[Mail address to reply To]
hinemos.mail.reply.personal.name=[Name of the reply mail receiver]
hinemos.mail.errors.to.address=[Mail address to be set to the Sent mail's Error-To Header]

# charset
hinemos.mail.charset.address=UTF-8
hinemos.mail.charset.subject=UTF-8
hinemos.mail.charset.content=UTF-8
```

Hinemos Manager must be restarted for the configuration changes to be reflected. Parameters set to the hinemos.mail.*.address parameters must be in format designated in RFC822, RFC1034.

The examples of parameters not following the format designated in RFC822, RFC1034, are as follows.

- the domain name includes characters other than alpha-numeric string, "-", and ".".
- the domain name includes more than one "." in a row.
- the domain name starts or ends with "-", or ".".

When using multibyte characters such as Japanese for Mail sender's Name or Name of the reply mail receiver, tools such as native2ascii is needed in order to encode multibyte characters to UTF-8.

native2ascii is a tool included in Java Development Kit(JDK). For more information about native2ascii, please contact the providers of JDK.

5.2.2 Configuring SMTP AUTH

Configure following files when using a SMTP servers requireing SMTP AUTH, for mail notification.

/opt/hinemos/etc/mail-service.properties

```
mail.smtp.auth=[true:do not use authentication, false:use authentication]

# connection user and password
hinemos.mail.transport.user=[user name used for authentication]
hinemos.mail.transport.password=[password used for authentication]
```

LOGIN, PLAIN and DIGEST-MD5 are supported as authentication methods. In addition, LOGIN, PLAIN, DIGEST-MD5 will be selected in this order, when sending to a SMTP server that has multiple authentication method enabled.

Hinemos Manager must be restarted for the configuration changes to be reflected.

5.2.3 SSH/TLS Settings

Configure the following files to use the SMTP server required for SSH/TLS(STARTTLS) with mail notification.

/opt/hinemos/etc/mail-service.properties

```
mail.smtp.starttls.enable=true
```

Hinemos Manager must be restarted for the configuration changes to be reflected.

When using STARTTLS, Security certificate published from the mail server must be verifiable as an approved certificate, in order to establish SSL/TLS connection from Hinemos Manager server,

For more detail, please refer to [HTTPS Monitor](#) .

5.2.4 Configuring the Envelope From

When configuring the parameters passed to the mail command of SMTP In mail notification, add the following parameters to the following file.

/opt/hinemos/etc/mail-service.properties

```
mail.smtp.from=[mail address to be set as envelope from]
```

Hinemos Manager must be restarted for the configuration changes to be reflected.

5.3 Log Escalation Notification

The settings related to the log escalation notification feature are listed below.

5.3.1 Configuration Method of Embedded Host Name

By changing the parameter common.manager.hostname in the following configuration file, the host name included in the header part of the syslog(RFC3164) the Hinemos Manager sends can be flexibly configured.

/opt/hinemos/etc/hinemos.properties

```
## syslog transfer : Hostname for syslog header
#common.manager.hostname=#{NODE}
```

Table 5-1. Possible Value for the syslog Host Name (common.manager.hostname)

Configured values of hinemos.properties	Embedded strings for the host name	Contents of the sent syslog
Undefined(DEFAULT) or blank	Embed the node name of the source manager server ¹	<PRI> Mmm dd hh:mm:ss hostname message...
String of half-width alphanumeric characters (ex. XXX)	Embed specified string for the host name	<PRI> Mmm dd hh:mm:ss XXX message...

#{FACILITY_ID}	(Notification information for embedded scope ²⁾ Embed the node name of the source manager server (Otherwise) Embed the facility ID of the facility that is subject to notification	<PRI> Mmm dd hh:mm:ss facility id message...
#{NODE}	(Notification information per node) Embed node name of the node that is subject to notification (Otherwise) Embed the node name of the source manager server	<PRI> Mmm dd hh:mm:ss nodename message...

1 Owner Scope, Registered Nodes, Unregistered Nodes, Hinemos Internal scope

2 Result of running the hostname command

Hinemos Manager must be restarted for the configuration changes to be reflected.

6 Collective Run Feature

Additional settings for Hinemos collective run feature are explained.

6.1 Enabling the Collective Run Feature

To use the collective run feature, after Hinemos is installed, the OS environment for the manager server and the managed node must be set up.

6.1.1 Managed Node Setup

To use the collective run feature in Hinemos, you must be able to run the ssh or rsh command for the managed node from the manager server. The setup method for the collective run feature is explained below.

If using ssh

If ssh is the remote shell used in the collective run feature, ssh configuration must be done on the managed node. If rsh is used as the remote shell in the collective run feature, this configuration is not required.

By registering a public key, it can be configured so that commands can be run from the manager server (root user) on the managed node (root user) without a password. The managed node is explained below as agent 01 (192.168.0.10).

1. Run `hinemos_setup_collectiverun.sh` on the manager server that the Hinemos Manager is installed on.

Note) To run `hinemos_setup_collectiverun.sh` on the manager server, the expect package (5.43.0-5.1 or later) must be installed.

```
(root) # cd /opt/hinemos/sbin/
(root) # ./hinemos_setup_collectiverun.sh
```

The menu is displayed. Enter "1" at the prompt.

```
(root) # /opt/hinemos/sbin/hinemos_setup_collectiverun.sh
The setup of the node for the watch to user root begins.

-----
Welcome to the Setup of the collective run function
Hinemos Version 4.1.x

Copyright (C) since 2006 NTT DATA Corporation
-----

the Setup of the collective run function

1) Making of public key for attestation of root user
2) Public key registration to node for monitoring
9) Setup end of collective run function

====> 1
```


2. A confirmation message to create a public key of attestation for the root user will be displayed. Enter "Y".

```
The public key for the attestation of the root user is made without the passphrase.
Is it good? (Y/N default:Y)

Y
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx root@agent01
The key's randomart image is:
+--[ RSA 2048]-----+
|          oo o      |
| (Partially omitted) |
|          +         |
+-----+

The public key was made.
```

3. Enter "2" at the prompt.

```
the Setup of the collective run function

1) Making of public key for attestation of root user
2) Public key registration to node for monitoring
9) Setup end of collective run function

===> 2
```

4. Register the public key of the root user (manager server), to the authorized_keys file for the root user (managed node).

Enter the IP address of the managed node that uses the collective run function.

```
root user's public key is registered in the root user's with node for the authorized_keys file.

Please input IP address of the node that uses the collective run function for the monitoring.
Please input 9 when ending.
192.168.0.10
```

5. Specify the home directory of the user root on the managed node.

```
Please specify the home directory of the root user with the node for the monitoring.
/root/
```

6. The confirmation message for host key registration is displayed. Enter "Y".

```
root user's public key is set to /root/.ssh/authorized_keys.
Is it good? (Y/N default:Y)
Y
```

7. Entry of the password for the root user on the managed node is requested. Enter it.

```
root@192.168.0.10's password: (enter password)

Registration to 192.168.0.10 was completed.
```

8. Enter "9" to end. Enter the IP address of the managed node if continuing with the registration.

```

Please input IP address of the node that uses the collective run function for the monitoring.
Please input 9 when ending.

9

the Setup of the collective run function

    1) Making of public key for attestation of root user
    2) Public key registration to node for monitoring
    9) Setup end of collective run function

===> 9

```

The ssh configuration is now complete.

If changing from the root user on the managed node, run the procedure above, and specify the user name in the command line arguments in `hinemos_setup_collectiverun.sh`.

```

(root) # cd /opt/hinemos/sbin/
(root) # ./hinemos_setup_collectiverun.sh hoge

```

If using rsh

If rsh is used as the remote shell for the collective run feature, the configuration of rsh must be done on the managed node. If ssh is used as the remote shell in the collective run feature, this configuration is not required.

1. Create the `.rhosts` files with the following content in the `/root` directory. If the `.rhosts` file already exists, add the following content.

`/root/.rhosts`

```
(The IP address of the manager server) hinemos
```

Example)

```
192.168.0.1 hinemos
```

2. Add rsh in the `/etc/securetty` file.

`/etc/securetty`

Example)

```

console
vc/1

(Partially omitted)

tty10
tty11
rsh

```

The rsh configuration is now complete.

6.1.2 Hinemos Manager Remote Shell Setup

Select either ssh or rsh to replace the remote shell used by the collective run feature (the default is ssh).

If changing the remote shell to rsh, edit `collective.run.shell` in the `hinemos.properties`. Also, edit `collective.run.user` if changing the user that runs commands on the managed node from root. However, when you change `collective.run.user` from root, you will no longer be able to run commands that are limited to the root user for the collective run feature, so be careful.

/opt/hinemos/etc/hinemos.properties

```
##
## Collective Run function
##

## Collective Run : Run Method (ssh / rsh)
collective.run.shell=ssh
## Collective Run : Remote User
collective.run.user=root
```

Hinemos Manager must be restarted for the configuration changes to be reflected.

6.1.3 Starting the FTP Server

An FTP server that is accessible from the managed node must be prepared if using the collective run feature's "RPM Install" and File Copy". Start up the FTP server in advance, and confirm that it is accessible from the managed node with the FTP user and password that was specified during the installation.

The following describes the startup method if vsftpd in Red Hat Enterprise Linux 6 is used as the FTP server.

- Example of the FTP server configuration

1. Confirm that vsftpd and krb5-workstation are installed.

Execute the following command. Confirm that vsftpd-(version) is displayed. Confirm that krb5-workstation-(version) is displayed.

```
(root) # rpm -q vsftpd
vsftpd-2.2.2-6.el6.i686
(root) # rpm -q krb5-workstation
krb5-workstation-1.9-22.el6.i686
```

2. Startup vsftpd.

Execute the following command at root user.

```
(root) # service vsftpd start
```

- Configure the file transfer source and destination.

Confirm that krb5-workstation is installed.

Execute the following command. Confirm that krb5-workstation-(version) is displayed.

```
(root) # rpm -q krb5-workstation
krb5-workstation-1.9-22.el6.i686
```

- Configuration changes of the FTP server used for Hinemos

The items specified at the time of Hinemos Manager installation are set up for the server used for Hinemos. To change the IP address, the user, or the password for the FTP server used in the collective run function after the installation, edit the following two files.

- /opt/hinemos/lib/cr/cp.sh
- /opt/hinemos/lib/cr/rpminstall.sh

Configure the following parameters.

```
FTP_HOST="(IP Address)"
FTP_USER="(User name)"
FTP_PASSWD="(Password)"
```

7 Monitor Settings / Performance Management Feature

Additional settings for the Hinemos monitor settings/performance management feature are explained.

7.1 SQL Monitor

7.1.1 Adding a Monitoring Target RDBMS

The method of adding a RDBMS monitored by SQL monitoring feature, will be explained in this chapter.

Connect to RDBMS from the Hinemos Manager via the JDBC Driver. For this, in order to add the RDBMS that is the monitoring target, the JDBC Driver must be applied to that RDBMS. (This is the JDBC Driver that operates with Java Runtime Environment 7.0)

- Additional procedures

1. JDBC driver location

Place the provided JDBC driver in /opt/hinemos/plugins/.

```
$ cp new_jdbc.jar /opt/hinemos/plugins/
```

2. Edit the jdbc.properties

Add RDBMS information to /opt/hinemos/etc/jdbc.properties.

First, increase the number of jdbc.drivers and the number of types of RDBMS that can be used with Hinemos SQL monitoring. (This is the number in jdbc.driver.name.X including the added RDBMS)

```
# count of jdbc drivers
jdbc.driver = 4
```

Also, add information related to the new RDBMS and JDBC Driver.

```
jdbc.driver.name.4 = {display name of RDBMS}
jdbc.driver.classname.4 = {class name of JDBC driver}
jdbc.driver.logintimeout.4 = {login timeout configuration of JDBC}
jdbc.driver.properties.4 = {parameter when connecting JDBC}
```

3. Restart the Hinemos Manager

Restart the Hinemos Manager to apply the settings.

From the Monitor Setting[List], the SQL[Create/Change] dialog opens, then confirm that the added RDBMS is shown in the "Connection DB" pull down menu.

7.2 Process Monitor

7.2.1 Handling when "Failed to get value" Notification Occurs

The following 2 processes run asynchronously with process monitor. (Figure 7-1 Reference)

1. The process list information for the target node is acquired by SNMP polling.

- Count the number of processes that are the monitoring target processes from the process list information.

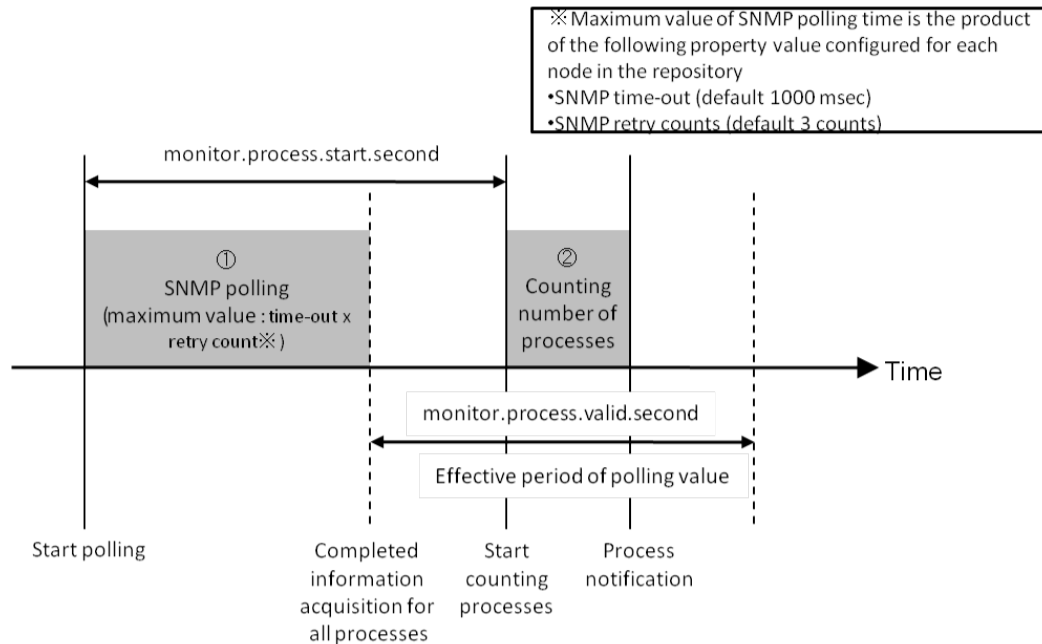


Figure 7-1 Handling Process Monitor

The configured value of `monitor.process.start.second` is the parameter that determines when (in seconds) to run (2) from the time (1) started. This parameter must be an integer between 1 and 59.

The set value of `monitor.process.valid.second` is the parameter that determines how long (in seconds) the process list collected in (1) remains valid information. If (2) is run after the expiration date, the notification of "Data is too old to check" is output with the priority of "Failed to get value". This parameter must be an integer greater than 0.

The time it takes to collect information on process lists via SNMP polling of (1) depends on the response speed of the SNMP polling runtime environment. The maximum SNMP polling time of operation is the timeout time X the retry count (msec). If the process list information cannot be acquired in this time, the result acquired in (1) will be "Time out".

Edit the following files to change the parameters.

`/opt/hinemos/etc/hinemos.properties`

```
## Monitor Management(Process) : Time to start tracking process (1-59 sec)
monitor.process.start.second=30

## Monitor Management(Process) : Permissible Time of Collection (sec)
monitor.process.valid.second=50
```

Hinemos Manager must be restarted for the configuration changes to be reflected. In addition, to apply the configuration changes made on `monitor.process.start.second`, you must "disable" the configuration of the existing process monitoring once, then "enable" it again.

7.3 HTTPS Monitor

In HTTPS monitoring, Hinemos Manager connects to the monitoring target(HTTPS server) as HTTPS client. In order to enable HTTPS monitoring, Security certificate of HTTPS servers must be verifiable as a trusted certificate, in order to establish SSL connection from Hinemos Manager server

- When server certificate is signed with well known public CA

Keystore of OpenJDK bundled in the Operating System contains a public key of well known CA, and because of this, certificate can be verified by pursuing the certificate to well known CA's certificate.

In this case, server certificate signed by well known public CA can be verified as a trusted certificate, and registering server certificate to Hinemos Manager's keystore is not needed.

2. When server certificate is self signed

Target server's certificate can be verified as trusted certificate by registering server certificate to Hinemos Manager's keystore,

The procedures are as follows.

1. Prepare the certificate
2. Register the certificate to the keystore
3. Specify the keystore file in the java start up option
4. Restart the Hinemos Manager

More detail informations on steps 1-3 are listed below.

7.3.1 Preparing the Certificate

Prepare the server certificate for the HTTPS server ([DER encoded binary X.509] or [Base-64 encoded X.509] format).

7.3.2 Register the Certificate to the Keystore

Register the server certificate in /opt/hinemos/.keystore file with the Java keytool commands.

The keystore is created when the first keytool command is executed. Add the server certificate of the monitoring target (HTTPS Server) to .keystore.

An example is shown below with the server certificate placed in the manager server's /tmp directory. Also, the string specified for each server certificate is specified in the menu string (shown here as hinemos).

```
(root) # su - hinemos
(hinemos) $ /usr/bin/keytool -import -file /tmp/(server certificate) -alias hinemos -keystore /opt/hinemos/.keystore
Enter the keystore password: (default is changeit)
Owner: EMAILADDRESS=root@example.com, CN=172.19.188.60, OU=Testing, O=Test
Company, L=Raleigh, ST=North Carolina, C=JP
Issuer: EMAILADDRESS=root@example.com, CN=172.19.188.60, OU=Testing, O=Test Company, L=Raleigh, ST=North Carolina, C=JP
Serial Number: 0
Valid from: Mon Mar 09 16:03:54 JST 2009 until: Tue Mar 09 16:03:54 JST 2010
Certificate fingerprints:
    MD5: 80:F9:93:D1:F9:A3:0B:77:FD:4B:50:32:A8:D5:E2:44
    SHA1: 08:B5:4B:20:51:98:35:29:B1:B8:77:C3:6F:C8:56:7B:80:A9:72:94
Trust this certificate? [no]: yes
The certificate was added to the keystore
```

* Refer to <http://linux.die.net/man/1/keytool-java-1.7.0-openjdk> for the details of the keytool command

7.3.3 Specifying the Keystore File in the Java Startup Options

Change the startup options of Hinemos Manager (java) in order to make Hinemos Manager refer to .keystore file. Remove the comment(#) of JVM_KEYSTORE_OPT parameter of /opt/hinemos/hinemos.cfg file, where Djavax.net.ssl.trustStore is specified.

```
### JVM - keystore (https)
#export JVM_KEYSTORE_OPTS="-Djavax.net.ssl.trustStore=${HINEMOS_HOME}/.keystore"
```

7.4 System Log Monitor

7.4.1 Settings Related to syslog Sending

When using syslogd instead of rsyslog on the monitored node, add the following settings to /etc/syslog.conf

```
*.info;mail.none;authpriv.none;cron.none    @[Hinemos Manager IP Address]
```

The syslog service must be restarted to apply the changes.

```
(root) # service syslog restart
```

7.4.2 Settings Related to syslog Receiving

When receiving a syslog that was sent from an outside device, update the port number of the manager server. Modify the following configuration file.

/etc/rsyslog_hinemos.conf

```
$UDPServerRun 514
$InputTCPServerRun 514
```

To transmit the syslog from the rsyslog to Hinemos Manager (Java), inside the manager server, update the listen address, port number, and system log monitor settings (maximum number of syslog to be cued) written in the following configuration file.

/opt/hinemos/etc/hinemos.properties

```
monitor.systemlog.listen.address=[listen address of java process to wait for syslog]
monitor.systemlog.listen.port=[listen port for java process to wait for syslog]
monitor.systemlog.filter.queue.size=[maximum number of syslog to be cued in systemlog monitoring]
monitor.systemlog.filter.thread.size=[maximum number of threads used for filtering process of systemlog monitoring]
```

These parameters are not written on the original configuration file. When changing and applying these changes, please add these parameters to /opt/hinemos/etc/hinemos.properties and restart Hinemos Manager.

7.4.3 Invalidating the Escape Process for Control Characters

When a syslog arrives to the manager server, it is transmitted to the Hinemos Manager (java) after being received with rsyslog.

At this time, if there is a control character (such as BEL) included in the syslog, the control character part is replaced with a 3 digit base 8 (#007, etc.) by the rsyslog feature. An example of the escape control code is shown in Table 7-1. An example of the escape log is shown in Table 7-2.

Table 7-1 Example of the Escape Control Code

Control code	String after replacement
NUL	#000
BEL	#007

Table 7-2 Example of the Escape Log (the control character NUL is represented as [NUL])

String received from rsyslog	HTTP/1.0[NUL] 50
String transferred to the Hinemos Manager from rsyslog	HTTP/1.0#000 50
Pattern matching expression matching the above	.*HTTP/1.0#000 50.*

Change the following settings to disable the escape.

1. Modify /etc/rsyslog_hinemos.conf of the Hinemos Manager server.

Add the following settings to /etc/rsyslog_hinemos.conf.

```
$EscapeControlCharactersOnReceive off
```

- Restart rsyslog.

```
(root) # service rsyslog restart
```

7.4.4 Host Name Replacement Process Settings for the syslog Header Part

syslog follows RFC3164 and is comprised of PRI, HEADER and MSG.

The syslog HEADER is comprised of TIMESTAMP and HOSTNAME. TIMESTAMP is comprised of date, HOSTNAME, IP address and blank.

An example of the HEADER part (TIMESTAMP HOSTNAME) of the syslog packet is shown below.

```
Feb 25 14:09:07 webserver
```

If the HOSTNAME of the syslog received from rsyslog is not defined (blank), a reverse lookup of the host name is done using the IP address and the result is placed in the HEADER part of the syslog.

Perform the following settings if reverse lookup of the syslog's host name is disabled by rsyslog.

- Edit /etc/sysconfig/rsyslog on the Hinemos Manager server.
Specify the "-x" option in the appropriate place in /etc/sysconfig/rsyslog.

```
SYSLOGD_OPTIONS="-c 4 -x"
```

- Restart rsyslog.

```
(root) # service rsyslog restart
```

7.5 SNMPTRAP Monitor

7.5.1 Settings Related to SNMPTRAP Receiving

When receiving a SNMPTRAP that was sent from an outside device, update the waiting address and port number of the manager server. Modify the following configuration file.

/opt/hinemos/etc/hinemos.properties

```
monitor.snmptrap.listen.address=[listen address of java process to wait for SNMPTRAP]
monitor.snmptrap.listen.port=[listen port for java process to wait for SNMPTRAP]
monitor.snmptrap.filter.queue.size=[maximum number of SNMPTRAP to be cued in SNMPTRAP Monitoring]
monitor.snmptrap.filter.thread.size=[maximum number of threads used for filtering process of SNMPTRAP monitoring]
```

These parameters are not written on the original configuration file. When changing and applying these changes, please add these parameters to /opt/hinemos/etc/hinemos.properties and restart Hinemos Manager.

7.5.2 Default MIB

MIB registered in the master data of Hinemos Manager is listed in Table 7-3.

Table 7-3 List of MIB registered in Hinemos Manager by default

GENERIC TRAP	A3COM-SWITCHING-SYSTEMS-FDDI-MIB
Centrum-MIB	A3Com-DLSW-r1-MIB
LANPLEX-SYSTEMS-MIB	LBHUB-ECS-MIB

SYNC-RESEARCH-MIB	A3Com-Sdlc-r1-MIB
SECURITY-MIB	A3Com-System-r8-MIB
A3COM-SWITCHING-SYSTEMS-POLL-MIB	A3COM-SWITCHING-SYSTEMS-QOS-MIB
A3COM-SWITCHING-SYSTEMS-BRIDGE-MIB	A3COM-SWITCHING-SYSTEMS-MIB
CHIPCOMMIB	CHIPCOM-MIB
PRODUCTMIB	A3COM0007-SYSLOADER
LANPLEX-MIB	LBHUB-BLC-MIB
LBHUB-BRIDGE-MIB	LBHUB-MSH-MIB
LINKB-OPT-FDDI-MIB	LB3GH-1-0-7
LANPLEX-OPT-FDDI-MIB	NCDCHASS-MIB
SWITCHING-SYSTEMS-MIB	USR-TRAP-MIB
VRRP-MIB	ADICLIBMIB
IBM-AIX-MIB	SPAGENT-MIB
BESTPOWER-MIB	XUPS-MIB
PowerNet-MIB	ATM-FORUM-ILMI40-MIB
DPT-SCSI-MIB	ADTRAN-ATLAS-550-MIB
ADTRAN-ATLAS-HSSI-V35-MIB	ADTRAN-ATLAS-MODULE-MIB
ADTRAN-ATLAS-T1-MIB	ADTRAN-ATLAS-UNIT-MIB
ADTRAN-ATLAS-V35NX-MIB	ADTRAN-GENCHASSISTRAP-MIB
Aedilis-MIB	AirDefense-Product-MIB
ALCATEL-IND1-CHASSIS-MIB	ALCATEL-IND1-GROUP-MOBILITY-MIB
ALCATEL-IND1-GVRP-MIB	ALCATEL-IND1-HEALTH-MIB
ALCATEL-IND1-INLINE-POWER-MIB	ALCATEL-IND1-INTERSWITCH-PROTOCOL-MIB
ALCATEL-IND1-IP-MIB	ALCATEL-ISIS-MIB
ALCATEL-IND1-LAG-MIB	ALCATEL-IND1-LPS-MIB
ALCATEL-IND1-MAC-ADDRESS-MIB	ALCATEL-IND1-NETSEC-MIB
ALCATEL-IND1-PIM-BSR-MIB	ALCATEL-IND1-PIM-STD-MIB
ALCATEL-IND1-POLICY-MIB	ALCATEL-IND1-PORT-MIB
ALCATEL-IND1-PORT-MIRRORING-MONITORING-MIB	ALCATEL-IND1-SESSION-MGR-MIB
ALCATEL-IND1-SLB-MIB	ALCATEL-IND1-STACK-MANAGER-MIB
ALCATEL-IND1-TRAP-MGR-MIB	ALCATEL-IND1-UDLD-MIB
ALCATEL-IND1-VLAN-STP-MIB	ALCATEL-IND1-VRRP3-MIB
ALCATEL-IND1-WCCP-MIB	ALCATEL-IND1-WEBMGT-MIB
LUCENT-SECURE-VPN-SOLUTIONS-LSMS-NOTIFICATION-MIB	ALLOT-NX-MIB
ALLOT-SMP-SNMP-MIB	ALLOT-MIB
ALTEON-TRAP-MIB	CHEETAH-TRAP-MIB
ALTIGA-trap-event	WLSR-AP-MIB
WLSX-SWITCH-MIB	WLSX-TRAP-MIB
ASCEND-TRAP	AcBoard
ALARM-MIB	DS1-MIB
ENTITY-MIB	IF-MIB
RMON-MIB	RTCPXR-MIB
SNMPv2-MIB	ACS-TRAP-MIB

CYCLADES-ACS5000-TRAP-MIB	AMX5000-TRAP-MIB
AMX5010-TRAP-MIB	AMX5020-TRAP-MIB
AMX5030-TRAP-MIB	AVCT-CCM-TRAP-MIB
DSR-TRAP-MIB	DSR1021-TRAP-MIB
DSR2010-TRAP-MIB	AVOCENT-MERGEPOINT-TRAP-MIB
PM-TRAP-MIB	BEA-Weblogic-Server-Startup-Event
BEA-Weblogic-Server-Shutdown-Event	BEA-Weblogic-Attribute-Change-Received-Event
BEA-Weblogic-Monitor-Trap-Received-Event	BEA-Weblogic-Log-Filter-Trap-Received-Event
BGP4-MIB	RFC1269-MIB
Backup-Exec-MIB	BLACKBERRYSERVERMIB
BLACKBERRYSERVER-MIB	BNT-GbESM-10Ub-RS-MIB
BLUECOAT-DIRECTOR-TRAP-MIB	BLUECOAT-SG-ATTACK-MIB
BLUECOAT-SG-DISK-MIB	BLUECOAT-SG-HEALTHCHECK-MIB
BLUECOAT-SG-HEALTHMONITOR-MIB	BLUECOAT-SG-POLICY-MIB
BLUECOAT-SG-SENSOR-MIB	BLUECOAT-SG-USAGE-MIB
BLUECOAT-AV-MIB	ATTACK-MIB
POLICY-MIB	SENSOR-MIB
USAGE-MIB	ADONIS-DNS-MIB
FCMGMT-MIB	SW-TRAP
ARCserve-Alarm-MIB	CPQN54NN-MIB
CPQCLUSTER-MIB	CPQCMC-MIB
CPQCR-MIB	CPQDMII-MIB
CPQDSCCS-MIB	CPQFCA-MIB
CPQGEN-MIB	CPQHLTH-MIB
CPQHOST-MIB	CPQHSV110V3-MIB
CPQICA-MIB	CPQIDA-MIB
CPQIDE-MIB	CPQSINFO-MIB
CPQN5226A-MIB	CPQNIC-MIB
CPQPOWER-MIB	CPQRACK-MIB
CPQRECOV-MIB	CPQRPM-MIB
CPQSANAPP-MIB	CPQSANEVENT-MIB
CPQSCSI-MIB	CPQSERVICE-MIB
CPQSM2-MIB	CPQSRVMN-MIB
CPQSTDEQ-MIB	CPQSTSYS-MIB
CPQSWCC-MIB	CPQTHRSH-MIB
CPQ-TRAPS-MIB	CPQUPS-MIB
CPQWCRM-MIB	CPQOS-MIB
CRITAPP-MIB	CISCO-CIDS-MIB
PCUBE-SE-MIB	CISCO-SERVICE-CONTROL-RDR-MIB
CISCO-SERVICE-CONTROL-LINK-MIB	CISCO-SERVICE-CONTROL-SUBSCRIBERS-MIB
AIRESPACE-WIRELESS-MIB	CISCO-LWAPP-DOT11-CLIENT-MIB
ACCOUNTING-CONTROL-MIB	ADSL-LINE-MIB
APPN-MIB	APPN-TRAP-MIB

ATM-SOFT-PVC-MIB	AWCVX-MIB
CISCO-5800-HEALTH-MON-MIB	CISCO-6400-CHASSIS-MIB
Cisco90Series-MIB	CISCO-AAA-SERVER-MIB
CISCO-ACCESS-ENVMON-MIB	CISCO-ALPS-MIB
CISCO-APS-MIB	CISCO-ATM-DUAL-PHY-MIB
CISCO-ATM-NETWORK-CLOCK-MIB	CISCO-BSTUN-MIB
CISCO-C2900-MIB	CISCO-C3800-MIB
CISCO-C8500-REDUNDANCY-MIB	CISCO-CALL-TRACKER-MIB
CISCO-CASA-FA-MIB	CISCO-CASA-MIB
CISCO-CCM-MIB	CISCO-CHANNEL-MIB
CISCO-CIPCMPC-MIB	CISCO-CIPCSNA-MIB
CISCO-CLUSTER-MIB	CISCO-CONFIG-COPY-MIB
CISCO-CONFIG-MAN-MIB	CISCO-CONTENT-ENGINE-MIB
CISCO-CONTENT-NETWORK-MIB	CISCO-DLSW-EXT-MIB
CISCO-DLSW-MIB	CISCO-DOCS-EXT-MIB
CISCO-DOCS-REMOTE-QUERY-MIB	cdspMIB
CISCO-DSPU-MIB	CISCO-ENTITY-ALARM-MIB
CISCO-ENTITY-FRU-CONTROL-MIB	CISCO-ENTITY-SENSOR-MIB
CISCO-ENVMON-MIB	CISCO-EVENT-DISTR-MIB
CISCO-FASTHUB-MIB	CISCO-FIREWALL-MIB
CISCO-FLASH-MIB	CISCO-GATEKEEPER-MIB
CISCOTRAP-MIB	CISCO-GPRS-GTP-MIB
CISCO-GPRS-L2RLY-MIB	CISCO-HSRP-MIB
CISCO-ICSUDSU-MIB	CISCO-IETF-ATM2-PVCTRAP-MIB
CISCO-IF-THRESHOLD-MIB	CISCO-IP-ENCRYPTION-MIB
GWPOA-MIB	CISCO-IPMROUTE-MIB
CISCO-IPSEC-FLOW-MONITOR-MIB	CISCO-IPSEC-MIB
CISCO-ISDN-MIB	CISCO-ISDNU-IF-MIB
CISCO-ITP-SCCP-MIB	CISCO-ITP-SP-MIB
CISCO-LOCAL-DIRECTOR-MIB	CISCO-NETWORK-REGISTRAR-MIB
CISCO-OAM-MIB	CISCO-OPTICAL-PATCH-MIB
CISCO-OSCP-MIB	CISCO-PIM-MIB
CISCO-PING-MIB	CISCO-POP-MGMT-MIB
CISCO-PPPOE-MIB	CISCO-REPEATER-MIB
CISCO-RF-MIB	CISCO-RHINO-MIB
CISCO-RSRB-MIB	CISCO-RTTMON-MIB
CISCO-SDLLC-MIB	CISCO-SIBU-MANAGERS-MIB
CISCO-SIBU-STACKABLE-DUAL-SPEED-HUB-MIB	CISCO-SLB-MIB
CISCO-SNA-LLC-MIB	CISCO-SP-MIB
CISCO-SRP-MIB	CISCO-STACK-MIB
CISCO-STP-EXTENSIONS-MIB	CISCO-STUN-MIB
CISCO-SYSLOG-MIB	CISCO-SYSTEM-MIB
CISCO-TS-STACK-MIB	CISCO-VLAN-MEMBERSHIP-MIB

CISCO-VOICE-APPS-MIB	CISCO-VOICE-DIAL-CONTROL-MIB
CISCO-VTP-MIB	CISCO-WIRELESS-DOCS-EXT-MIB
CISCO-WIRELESS-IF-MIB	CISCO-WIRELESS-P2MP-LINK-METRICS-MIB
CISCO-WIRELESS-P2MP-PHY-MIB	CISCO-WIRELESS-P2MP-RF-METRICS-MIB
STAND-ALONE-ETHERNET-SWITCH-MIB	MADGERSW-MIB
METRO1500-MIB	CISCO-ES-STACK-MIB
CISCO-MVPN-MIB	CISCO-ATM-IF-MIB
CISCO-ATM-PVCTRAP-EXTN-MIB	CISCO-BBSM-MIB
CISCO-BGP4-MIB	CISCO-BULK-FILE-MIB
CISCO-CABLE-AVAILABILITY-MIB	CISCO-CABLE-METERING-MIB
CISCO-CABLE-QOS-MONITOR-MIB	CISCO-CABLE-SPECTRUM-MIB
CISCO-CALLHOME-MIB	CISCO-CAT6K-CROSSBAR-MIB
CISCO-CDL-MIB	CISCO-CDMA-AHDLC-MIB
CISCO-CDMA-PDSN-MIB	CISCO-CSG-MIB
CISCO-DDP-IAPP-MIB	CISCO-DEVICE-EXCEPTION-REPORTING-MIB
CISCO-DIST-DIRECTOR-MIB	CISCO-DM-MIB
CISCO-DOT11-CONTEXT-SERVICES-MIB	CISCO-ENTITY-PFE-MIB
CISCO-EPM-NOTIFICATION-MIB	CISCO-EXT-SCSI-MIB
ciscoFabricC12kMIB	CISCO-FABRIC-HFR-MIB
CISCO-FC-FE-MIB	CISCO-FCC-MIB
CISCO-FCPING-MIB	CISCO-FCS-MIB
CISCO-FCTRACEROUTE-MIB	CISCO-FDMI-MIB
CISCO-FEATURE-CONTROL-MIB	CISCO-FSPF-MIB
CISCO-GGSN-MIB	CISCO-GPRS-ACC-PT-MIB
CISCO-GPRS-CHARGING-MIB	CISCO-GTP-DIRECTOR-MIB
CISCO-GTP-MIB	CISCO-HC-ALARM-MIB
CISCO-HEALTH-MONITOR-MIB	CISCO-IETF-DOT11-QOS-EXT-MIB
CISCO-IETF-PW-MIB	CISCO-IETF-SCTP-EXT-MIB
CISCO-IETF-VDSL-LINE-MIB	CISCO-IMAGE-UPGRADE-MIB
CISCO-IP-LOCAL-POOL-MIB	CISCO-ISCSI-MIB
CISCO-ITP-GRT-MIB	CISCO-ITP-GSCCP-MIB
CISCO-ITP-GSP-MIB	CISCO-ITP-MLR-MIB
CISCO-ITP-MONITOR-MIB	CISCO-ITP-RT-MIB
CISCO-ITP-XUA-MIB	CISCO-IVR-MIB
CISCO-L2-CONTROL-MIB	CISCO-L2-DEV-MONITORING-MIB
CISCO-LICENSE-MGR-MIB	CISCO-MAC-NOTIFICATION-MIB
CISCO-MOBILE-IP-MIB	CISCO-MODULE-AUTO-SHUTDOWN-MIB
CISCO-NBAR-PROTOCOL-DISCOVERY-MIB	CISCO-NMS-APPL-HEALTH-MIB
CISCO-NS-MIB	CISCO-OPTICAL-MONITOR-MIB
CISCO-OSPF-TRAP-MIB	CISCO-OUTAGE-MONITOR-MIB
CISCO-PORT-SECURITY-MIB	CISCO-PORT-STORM-CONTROL-MIB
CISCO-PSA-MICROCODE-MIB	CISCO-PSM-MIB
CISCO-RPMS-MIB	CISCO-RSCN-MIB

CISCO-SCSI-MIB	CISCO-SLB-EXT-MIB
CISCO-SONET-MIB	CISCO-SSG-MIB
CISCO-SSL-PROXY-MIB	CISCO-SYS-INFO-LOG-MIB
CISCO-SYSTEM-EXT-MIB	cTapMIB
CISCO-TAP-MIB	CISCO-VIRTUAL-NW-IF-MIB
CISCO-VISM-TRAPS-MIB	CISCO-VOICE-DNIS-MIB
CISCO-VPDN-MGMT-MIB	CISCO-VSAN-MIB
CISCO-WAN-TOPOLOGY-MIB	CISCO-WLAN-VLAN-MIB
CISCO-WWNMGR-MIB	CISCO-ZS-MIB
CISCOWORKS-MIB	CISCO-SME-MIB
CISCO-SLB-HEALTH-MON-MIB	CISCO-STACKWISE-MIB
CISCO-ENHANCED-SLB-MIB	CISCO-MODULE-VIRTUALIZATION-MIB
CLARENT-MIB	CSI-P2-MIB
COLUBRIS-802DOT11-MIB	COLUBRIS-MAINTENANCE-MIB
COLUBRIS-PUBLIC-ACCESS-MIB	COLUBRIS-PUBLIC-ACCESS-RETENTION-MIB
COLUBRIS-SATELLITE-MANAGEMENT-MIB	COLUBRIS-SYSLOG-MIB
COLUBRIS-SYSTEM-MIB	COLUBRIS-TOOLS-MIB
COLUBRIS-VPN-MIB	SERVERVANTAGE-TRAP-MIB
CDM-625	DiagnosticsMonitor
CXC-MIB	Cricket-Threshold-exceeded
Cricket-Threshold-cleared	Crossbeam-Hardware-Event
Crossbeam-Module-Event	Crossbeam-VAP-Group-Event
Crossbeam-VRRP-Event	DISMAN-PING-MIB
DISMAN-EVENT-MIB	DMTF-DMI-MIB
DMTF-MOBILE-MIB	DMTF-SYSTEMS-MIB
DPS-MIB	VM-MIB
MIB	ArrayManager-MIB
DELL_ASF-MIB	StorageManagement-MIB
DELL-RAC-MIB	INTEL-LAN-ADAPTERS-MIB
EMC-CELERRA	CLARIION-MIB
EMC-MIB	A3COM51-SS9000SX
EXTREME-CABLE-MIB	EXTREME-CLEARFLOW-MIB
EXTREME-DOS-MIB	EXTREME-ENH-DOS-MIB
EXTREME-ESRP-MIB	EXTREME-IP-SECURITY-MIB
EXTREME-PORT-MIB	EXTREME-SOFTWARE-MONITOR-MIB
EXTREME-STACKING-MIB	EXTREME-SYSTEM-MIB
EXTREME-TRAP-MIB	EXTREME-UPM-MIB
EXTREME-V2TRAP-MIB	EXTREME-WIRELESS-MIB
LOAD-BAL-SYSTEM-MIB	WAN-TRAP-MIB
F5-3DNS-MIB	F5-BIGIP-COMMON-MIB
Fore-Switch-MIB	FORTIOS-300-MIB
FOUNDRY-SN-TRAP-MIB	SNI-HD-MIB
SNI-MYLEX-MIB	SNI-SERVER-CONTROL-MIB

FSC-SERVERCONTROL2-MIB	SERVERVIEW-STATUS-MIB
SERVERVIEW-DUPLEXDATAMANAGER-MIB	SIEMENS-DUPLEXWRITE-MIB
DESKTRAP-MIB	SIEMENS-MULTIPATH-MIB
SNI-NT-CLUSTER-MIB	PCI-HOTPLUG-MIB
SNI-SERVERVIEW-MIB	SNI-TRAP-MIB
FSC-HACL-MIB	WSA-TRAP-MIB
GGSN-MIB	GWAPIMIB
GWADA-MIB	NGWASYNC
GWIAMIB	GWMTA-MIB
GWOVMMIB	GWPAGERMIB
GWSMTPMIB	GWSNADSMIB
NGWX400MIB	HPNSAECC-MIB
HP-ENTITY-MIB	HP-httpManageable-MIB
HP-ICF-8023-RPTR	HP-ICF-BASIC
HP-ICF-CHAIN	HP-ICF-CHASSIS
HP-ICF-FAULT-FINDER-MIB	HP-ICF-GENERIC-RPTR
HP-ICF-VG-RPTR	ICF-VG-RPTR
HP-MCSG	HP-SN-TRAP-MIB
JETDIRECT3-TRAP	HPNSATRAP-MIB
TapeAlert-MIB	UMSEVENT-MIB
IBM-Director-Alert-MIB	IBM-SERVERAID-MIB
Converged-Power-System-Trap	RSASPPALT-MIB
IEEE802dot11-MIB	IPUNITY-SES-MIB
IPV6-MIB	ISS-MIB
INTEL-GEN-MIB	INTEL-S500-MIB
RMM2-MIB	PET-MIB
AOLAN-MIB	PET_EVENTS
I3IC-MIB	ASYN COS-MAIL-MIB
Juniper-System-MIB	Juniper-CLI-MIB
Juniper-RADIUS-CLIENT-MIB	Juniper-System-Clock-MIB
Juniper-ADDRESS-POOL-MIB	Juniper-REDUNDANCY-MIB
Juniper-MROUTER-MIB	BGP4-V2-MIB
JUNIPER-CFGMGMT-MIB	JUNIPER-MIB
JUNIPER-LDP-MIB	MPLS-MIB
JUNIPER-MPLS-LDP-MIB	JUNIPER-PING-MIB
JUNIPER-PMon-MIB	JUNIPER-RMON-MIB
JUNIPER-SONET-MIB	APS-MIB
JUNIPER-VPN-MIB	JUNIPER-USER-AAA-MIB
JUNIPER-COLLECTOR-MIB	JUNIPER-SP-MIB
OSPFV3-MIB	JUNIPER-SYSLOG-MIB
JUNIPER-CHASSIS-CLUSTER-MIB	JUNIPER-JS-AUTH-MIB
JUNIPER-V1-TRAPS-BGP	JUNIPER-V1-TRAPS-CHAS
JUNIPER-V1-TRAPS-MPLS	JUNIPER-V1-TRAPS-OSPF

LLDP-MIB	LIEBERT-SERIES-600-UPS-MODULE-MIB
LIEBERT-GP-AGENT-MIB	LIEBERT-GP-NOTIFICATIONS-MIB
Linksys-Connection-Trap	AGG-TRAP-MIB
CDR-TRAP-MIB	EXCEL-SWITCH-MIB
FC-TRAP-MIB	H323-TRAP-MIB
MANTRA-TRAP-MIB	PSAX-TRAP-MIB
RM-TRAP-MIB	SIP-TRAP-MIB
SPINS-TRAP-MIB	MG-SNMP-UPS-MIB
MPLS-VPN-MIB	MPLS-L3VPN-STD-MIB
MPLS-LSR-STD-MIB	MPLS-TE-STD-MIB
DEV-CFG-MIB	MSCR-MIB
VLAN-MIB	NSTACK-MIB
OADWDM-MIB	OA-VDSL-MIB
OA-VOICE-MIB	OAATERESCOPE-MIB
DRAFT-MSDP-MIB	MADGECAU-MIB
TVD-MIB	mcafee_EVENT_NEW_MIB
LanMgr-Alerts-II-MIB	PIM-MIB
MSDP-MIB	MYLEXRAID-MIB
CONTIVITY-TRAPS-V1-MIB	NETWORK-APPLIANCE-MIB
NET-SNMP-AGENT-MIB	NETBOTZ-MIB
NETGEAR-SWITCHING-MIB	NS-ROOT-MIB
NETSCREEN-TRAP-MIB	NOKIA-ENHANCED-SNMP-SOLUTION-SUITE-ALARM-IRP
NOKIA-ENHANCED-SNMP-SOLUTION-SUITE-PM-IRP	NOKIA-IPSO-LBCLUSTER-MIB
NOKIA-IPSO-SYSTEM-MIB	DHCP-MIB
IPX	Novell-Directory-Services-Trap-MIB
Windows-NT-Server-Trend-MIB	NetWare-Server-Alarm-MIB
NetWare-Server-Trend-MIB	NWTRAPCONFIGURATION
OSPF-TRAP-MIB	OPENNMS-MIB
RDBMS-MIB	ORALISTENER-MIB
ORAINTERCHANGE-MIB	ORACLE-AGENT-MIB
ORACLE-ENTERPRISE-MANAGER-4-MIB	OVERTURE-FAULTS-MIB
BLUECOAT-PACKETSHAPER-MIB	PATROL-MIB
SIPXCS-ALARM-NOTIFICATION-MIB	PIXMET-ATM-MIB
PIXMET-COFDM-MIB	PIXMET-DVBT-MIB
PIXMET-DVSTATION-MIB	PIXMET-IQ-MIB
PIXMET-QAM-MIB	PIXMET-QMM-MIB
PIXMET-QPSK-MIB	PIXMET-SLF-MIB
PIXMET-TSP-MIB	PIXMET-VSB-MIB
POLYCOM-VIDEO-MIB	CV-MIB
RADLAN-MIB	RAPID-CITY
RFC1382-MIB	UPS-MIB
RANCID-CUSTOM-MIB	REDLINE-TRAPv2-MIB
AVTC-COMMON-MIB	STEELHEAD-MIB

SNA-NAU-MIB	SNMP-REPEATER-MIB
SENSAPHONE-MIB	Sentry3-MIB
SNORT-INTRUSION-DETECTION-ALERT-MIB	SONICWALL-FIREWALL-TRAP-MIB
SONUS-COMMON-MIB	SONUS-TRUNK-GROUP-RESOURCES-MIB
SONUS-SYSTEM-TIMING-MIB	SONUS-SOFTSWITCH-CLIENT-SERVICES-MIB
SONUS-SS7-SERVICES-MIB	SONUS-SS7-MTP3-MIB
SONUS-SS7-MTP2-MIB	SONUS-SONET-MIB
SONUS-SOFTWARE-UPGRADE-SERVICES-MIB	SONUS-SIP-SIGNALLING-MIB
SONUS-RTCP-MIB	SONUS-REDUNDANCY-SERVICES-MIB
SONUS-OSPF-MIB	SONUS-NTP-SERVICES-MIB
SONUS-IP-INTERFACE-MIB	SONUS-NODE-RESOURCES-MIB
SONUS-NODE-MIB	SONUS-MASTER-TRUNK-RESOURCE-MANAGER-MIB
SONUS-MGCP-SERVICES-MIB	SONUS-LOG-STREAMING-SERVICES-MIB
SONUS-JAPANST-MIB	SONUS-ISUP-SERVICE-GROUP-MIB
SONUS-ISDN-SERVICE-GROUP-MIB	SONUS-IP-FILTER-MIB
SONUS-H323-SIGNALLING-MIB	SONUS-GATEWAY-SIGNALLING-MIB
SONUS-EVENT-LOG-MIB	SONUS-DS3-MIB
SONUS-DS3THRESHOLD-MIB	SONUS-DS1-MIB
SONUS-DS1THRESHOLD-MIB	SONUS-DSP-RESOURCES-MIB
SONUS-CAS-MIB	SONUS-ACCOUNTING-SERVICES-MIB
SONUS-COMMON-CALL-PROCESS-MIB	SONUS-BT-SERVICE-GROUP-MIB
SONUS-ATM-EXTENSIONS-MIB	SONUS-ANNOUNCEMENT-RESOURCES-MIB
SONUS-APS-MIB	SONUS-SONET-APS-MIB
SONUS-ALARM-CONTACT-MIB	IPOA-MIB
ATM2-MIB	SONUS-DATASTREAM-INTEGRATOR-MIB
SONUS-DSI-TRANSPORTER-MIB	SONUS-AGT-SGX-EVENT-MIB
SONUS-HA-MIB	SONUS-HSX-MIB
SONUS-SOFTSWITCH-DBREP-MIB	SONUS-SOFTSWITCH-PIPE-MIB
SONUS-SOFTSWITCH-POLICY-EXECUTION-SERVER-MIB	SONUS-SOFTSWITCH-PROXY-GATEKEEPER-MIB
SONUS-SOFTSWITCH-SCPA-MIB	SONUS-SOFTSWITCH-SIP-ENGINE-MIB
SONUS-SOFTSWITCH-SSREQ-MIB	BRIDGE-MIB
DIAL-CONTROL-MIB	DLSW-MIB
DOCS-CABLE-DEVICE-TRAP-MIB	DS3-MIB
IMA-MIB	ISDN-MIB
PTOPO-MIB	RFC1315-MIB
SNA-SDLC-MIB	TN3270E-RT-MIB
SUN-PLATFORM-MIB	SUN-HW-TRAP-MIB
SWISSQUAL-NQAGENT-MIB	SYMBOL-CC-WS2000-MIB
SYMBOL-DSSS-ENTERPRISE-PRIVATE-MIB	SYMBOL-WS5000-MIB
EMPIRE	TUT-T2-MIB
TRIPPUPS-MIB	UPTIME-ROOT-MIB
VMWARE-ENV-MIB	VMWARE-TRAPS-MIB
VMWARE-OBSOLETE-MIB	VMWARE-VC-EVENT-MIB

VMWARE-VMINFO-MIB	IPVREMS-MIB
CCU3000PMAC-TRAPS-MIB	WBSN-APPLIANCE-MIB
XEROX-HOST-RESOURCES-EXT-MIB	XEROX-JOB-MONITORING-EXT-MIB
XEROX-JOB-MONITORING-MIB	XEROX-RESOURCES-MIB
XEROX-SERVICE-MONITORING-MIB	XEROX-SIMPLE-JOB-MGMT-MIB

7.6 Windows Service Monitor

7.6.1 WinRM Installation

Windows management framework WinRM 1.1, WinRM 2.0, and WinRM 3.0 must be installed on the monitored node which are targets of Windows Service Monitor. If the OS of the monitored node is Windows Server 2008 R2, WinRM 2.0 is installed by default, and if the OS of the monitored node is Windows Server 2012, WinRM 3.0 is installed by default. For these environment, there are no need to install WinRM manually.

To check the version of WinRM installed in the environment, execute a command shown below from a command prompt, and check the value of "Stack" from command execution result.

```
> winrm id
IdentifyResponse
  ProtocolVersion = http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd
  ProductVendor = Microsoft Corporation
  ProductVersion = OS: 6.1.7600 SP: 0.0 Stack: 2.0
```

Refer to the Microsoft support site for detail information on WinRM and the method of downloading and installing.

7.6.2 Remote Computer Management Authorization

Run the following command from the monitored node's command prompt and authorize remote computer management.

```
> winrm quickconfig
WinRM is not set up for remote access of this computer for management.
The following changes must be made.

(Partially omitted)

Make these changes [y/n]? y

WinRM has been updated for remote management.
```

Run the following command and confirm the HTTP/HTTPS port for WinRM. For WinRM 1.1, 80 is the default port for HTTP and 443 is the default port for HTTPS. For WinRM 2.0 and WinRM 3.0, 5985 is the default port for HTTP and 5986 is the default port for HTTPS.

```
> winrm get winrm/config
```

Run the following command and confirm that the HTTP/HTTPS port for WinRM is LISTEN.

```
> netstat -an
```

7.6.3 Basic Confirmation Authorization

Run the following command and authorize basic confirmation.

```
> winrm set winrm/config/service/auth @{Basic="true"}
Auth
  Basic = true
```

7.6.4 Unencrypted Transmission Authorization

Run the following command and authorize unencrypted transmission by HTTP.

```
> winrm set winrm/config/service @{AllowUnencrypted="true"}
Service
  AllowUnencrypted = true
```

7.6.5 Set up HTTPS

The following steps are necessary if using HTTPS with Windows Service Monitor.

1. Prepare the certificate
Prepare the certificate used with a WinRM HTTP connection.
2. Register the certificate to WinRM
Execute the following command.

```
> winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="[IP Address]";
CertificateThumbprint="[Certificate Thumbprint (base 16)]"}
```

3. Register the certificate to the Hinemos Manager's keystore
Refer to [Register the Certificate to the Keystore](#) and [Specifying the Keystore File in the Java Startup Options](#) and register the certificate in the Hinemos Manager's keystore.
4. Restart the Hinemos Manager

7.6.6 Prepare the Destination OS User

The OS user of Windows server is used for remote access to WinRM. For this reason, the OS user used for remote access by Hinemos must be prepared on the monitored node.

* This user must belong to the Administrators group.

Run the following command to set the access permissions for the corresponding user for WinRM.

- For WinRM 1.1

```
> winrm configSDDL
```

- For WinRM 2.0 and WinRM 3.0

```
> winrm configSDDL default
```

The access permission setting dialog is displayed when you run the following command. Select the prepared OS user and set the access permissions. Further, read permission is required for Windows Service Monitor.

7.6.7 Synchronization Confirmation

Run the following command on the manager server and confirm that it can synchronize with the monitored node. In order to execute these commands, you will need to install wsmancli package to a Red Hat Enterprise Linux environment.

```
(root) # wsman -u [Destination OS user name] -p [Password] -y basic -h [IP Address] -P [HTTP/HTTPS default port]
-d 6 enumerate http://schemas.microsoft.com/wbem/wsman/1/wmi/root/cimv2/Win32_Service
(root) # wsman -u [Destination OS user name] -p [Password] -y basic -h [IP Address] -P [HTTP/HTTPS default port]
-d 6 get http://schemas.microsoft.com/wbem/wsman/1/wmi/root/cimv2/Win32_Service?Name=wudfsvc
```

7.7 Custom Monitor

7.7.1 Command Action Change

Commands set up in Custom Monitor are run by the Hinemos Agent.

The Hinemos Agent will automatically identify the OS platform when running. The command action will be converted to match the OS platform.

The OS platform identification method can be changed with the `collector.command.mode` parameter of the following setting file. Further, the default value of the `collector.command.mode` parameter is "auto".

- `/opt/hinemos_agent/conf/Agent.properties` (Linux Agent)
- `[Hinemos Agent install directory]\conf\Agent.properties` (Windows Agent)

```
collector.command.mode=auto
```

The Custom Monitor's `collector.command.mode` parameter has the same action as the Hinemos Agent's `command.create.mode` parameter. The values that can be set in the `collector.command.mode` parameter and the differences in operation by OS platform can be found by referring to the Hinemos Agent's [Changing the Action of the Startup Command](#).

The Hinemos Agent must be restarted for the configuration changes to be reflected.

7.7.2 Maximum Value from Standard Output Settings

The value acquired from Custom Monitor can be extracted from the command's standard output.

However, if a large amount of information is suddenly output from the command as standard output, the Hinemos Agent's memory may be insufficient, which may cause a malfunction.

In order to prevent this type of malfunction, the maximum size read from the standard output with Hinemos Agent is specified. The maximum size (the default value is 512[bytes]) for the read can be changed in the following setting value.

- `/opt/hinemos_agent/conf/Agent.properties` (Linux Agent)
- `[Hinemos Agent install directory]\conf\Agent.properties` (Windows Agent)

```
collector.command.buffer=512
```

The Hinemos Agent must be restarted for the configuration changes to be reflected.

7.7.3 New Line Code Included in the Standard Output Setting

Custom monitor extracts the value for 1 monitoring target with a 1 line unit as the command's standard output.

The new line code for identifying the row can be changed with the following setting value. By default, this is LF for the Linux Agent and CRLF for the Windows Agent.

- `/opt/hinemos_agent/conf/Agent.properties` (Linux Agent)
- `[Hinemos Agent install directory]\conf\Agent.properties` (Windows Agent)

```
collector.command.returncode=LF
```

Restart the Hinemos Agent after changing the settings.

7.7.4 Command Execution Multiplicity Setting

The thread pool used for command execution by the Custom Monitor is set up in the Hinemos Agent.

When a command is executed, a thread that is not used is allocated from the thread pool, and the thread that was used is released after the command execution ends or timeout.

The number of threads prepared for the thread pool (the default is 8 threads) can be defined with the following setting value.

- /opt/hinemos_agent/conf/Agent.properties (Linux Agent)
- [Hinemos Agent install directory]\conf\Agent.properties (Windows Agent)

```
collector.command.workerthreads=8
```

If a large volume of custom monitoring is assigned for the same monitoring target, adjust this setting value if the command execution timing will be delayed.

7.8 Polling Protocol Setting

Polling of the Performance Management feature and Performance Management feature (Resource Monitor, Process Monitor and SNMP Monitor) for monitoring objects is performed from Hinemos Manager using SNMP and WBEM. The information required for each feature is acquired.

So, when using the above feature, it must be set on the monitored target side so that it can respond to SNMP or WBEM polling from the Hinemos Manager.

Also, if monitoring using WBEM, it must be able to notify the CIM server (top-pegasus) and HTTP of the target node.

Follow the specifications for each device that will be a monitored node, and set them so they can respond to polling from the Hinemos Manager.

7.8.1 Configuring Net-SNMP

For the management target that is installed on the Linux Agent, the following settings are added to the snmpd.conf while the Hinemos Agent installer is running.

/etc/snmp/snmpd.conf

```
view systemview included .1.3.6.1
```

7.8.2 Method of SNMP/WBEM switchover

With the performance management function and the monitor function (resource monitoring), the polling means (SNMP and WBEM) are switched by category (CPU, memory, disk, network and file system). Further, obtaining a backup file by following the procedures in [Backing-up the Database](#) is recommended when applying the procedures.

Stop the Hinemos Manager and run the following commands as the root user. The password is requested so enter the PostgreSQL login password (the initial password is "hinemos").

```
(root) # /opt/hinemos/bin/pg_start.sh

(root) # /opt/hinemos/postgresql/bin/psql -p 24001 -U hinemos -c "UPDATE cc_collector_category_collect_mst
SET collect_method = '(Protocol to be changed)'
WHERE category_code = '(Category to be changed)' and platform_id = 'LINUX'"
Password for user hinemos:

(root) # /opt/hinemos/bin/pg_stop.sh
```

Enter either "SNMP" or "WBEM" (default is SNMP) in the section "Protocol to be Changed". For the section "category to be changed", enter the category to be changed from the five options listed below.

- C000_CPU ... Information related to the CPU
- C001_MEM ... Information related to the memory
- C002_DSK ... Information related to the disk
- C003_NET ... Information related to the network
- C004_FS ... Information related to the file system

(Note) Some values cannot be retrieved using WBEM. Also, only EXT3/EXT2 file systems can be monitored using WBEM.

WBEM and SNMP can switch in the monitoring feature (process monitoring).

Stop the Hinemos Manager and run the following commands. The password is requested so enter the PostgreSQL login password (the initial password is "hinemos").

```
(root) # /opt/hinemos/bin/pg_start.sh

(root) # /opt/hinemos/postgresql/bin/psql -p 24001 -U hinemos -c "UPDATE cc_monitor_process_method_mst
SET collect_method = '(Protocol to be changed)' WHERE platform_id = 'LINUX'"
Password for user hinemos:

(root) # /opt/hinemos/bin/pg_stop.sh
```

Enter either "SNMP" or "WBEM" (default is SNMP) in the section "Protocol to be Changed".

7.9 Collection Value of the Numeric Value Monitoring Setting

You can define for the operation when deleting monitor settings whether or not the collected value for numeric value monitoring is deleted. Change the following setting file when necessary.

If "on", the acquired value will also be deleted at the same time as the monitor settings are deleted. If "off", the acquired value will not be deleted even when the monitor settings are deleted.

- /opt/hinemos/etc/hinemos.properties

```
monitor.common.delete.cascade.perfdata=off
```

Hinemos Manager must be restarted for the configuration changes to be reflected.

The delete history information feature of the maintenance feature is used to delete the value acquired with numeric value monitoring. Further, the value acquired with numeric value monitoring is linked and managed by a Monitor ID.

Because of this, if a new monitor setting is created with the same monitor ID as a monitor setting that already exists, when you display as a graph and download the value acquired by numeric value monitoring, you may unintentionally use the data that was acquired by numeric value monitoring for graph display and download, so be careful.

7.10 Resource Monitoring

7.10.1 Settings for mass storage filesystem monitoring

Additional settings shown below is needed for resource monitoring high capacity filesystems. Monitor-able filesystems are from where mount points are set. (※this can be confirmed by using df command)

1. Edit /etc/snmp/snmpd.conf of the monitored target node.

```
disk / 10000 ←add
disk /dev/shm 10000 ←add
disk /boot 10000 ←add
```

※This is an example of when "/", "/dev/shm", "/boot" are set as mount points.

2. Restart snmpd of the monitored target node.

```
# service snmpd restart
```

8 Job Management Feature

Additional settings for the Hinemos job management feature are explained.

8.1 Changing the Action of the Startup Command

The Hinemos Agent will automatically identify the OS platform when running. The job start command operation will be switched to match the OS platform.

The OS platform identification method can be changed with the `command.create.mode` parameter of the following setting file. Further, the default value of the `command.create.mode` parameter is "auto".

- `/opt/hinemos_agent/conf/Agent.properties` (Linux Agent)
- `[Hinemos Agent install directory]\conf\Agent.properties` (Windows Agent)

```
command.create.mode=auto
```

A list of the values that can be specified in the `command.create.mode` parameter is shown in Table 8-1.

Table 8-1 Changing the Action of the Startup Command

Configured value	Description
auto	Auto identification of the platform(default)
windows	Create command for a Windows Platform
unix	Create command for a Linux Platform
compatible	Hinemos ver3.1/ver3.0 compatibility mode

An example of the operation when `echo XXX` is the start command is shown below.

- When the platform is identified as Windows

```
If the Hinemos Agent startup user and effective user are the same:
Command: echo
1st command line argument: XXX
(command and arguments are separated with one byte space character.
In order to avoid this, please write the commands and parameters in-between double-quotation(").)

If the Hinemos Agent startup user and effective user are not the same:
It will not run
```

- When the platform is identified as Linux

```
If the Hinemos Agent startup user and effective user are the same:
sh -c [Start Command]
Command: sh
1st command line argument: -C
2nd command line argument: echo XXX

If the Hinemos Agent startup user and effective user are not the same:
sudo -u [Effective user] sh -c [Start Command]
Command: sudo
1st command line argument: -u
2nd command line argument: [Effective user]
3rd command line argument: sh
4th command line argument: -c
5th command line argument: echo XXX
```

- When the start command runs in compatible mode

If the Hinemos Agent startup user and effective user are the same:
 Command: echo
 1st command line argument: XXX
 (The command and argument are separated using a half width space as a delimiting character)

If the Hinemos Agent startup user and effective user are not the same:
 Command: su
 1st command line argument: [Effective user]
 2nd command line argument: -c
 3rd command line argument: echo XXX

The Hinemos Agent must be restarted after changing the settings.

8.2 Configuring the Job Schedule Control when Restarting Hinemos Manager

When Hinemos Manager is started, the schedules of jobs which were planned to be executed while Hinemos Manager was stopped, will act in ways written below.

- If the time elapsed from the scheduled run time is below the threshold determined as a start failure (default is 1 hour), the scheduled jobs will run immediately after Hinemos Manager starts.
- If the time elapsed from the trigger time is above the threshold determined as a start failure (default is 1 hour), the scheduled jobs will be postponed, and will run at the next scheduled run time.

When Hinemos Manager is restored with procedure written in [Restoring the Database](#), The schedules of jobs are handled as if Hinemos Manager was stopped from the time when backup was taken, and will act in the same way.

For more detail, please refer to Hinemos User's Manual "13.1 Behaviour of Job schedules when planned execution time has passed while java process was stopped"

Further, the definition of the threshold that determines a start failure is changed by the following method. Define this unit in msec units.

- /opt/hinemos/etc/scheduler-dbms.properties

```
org.quartz.jobStore.misfireThreshold = 3600000
```

Hinemos is designed to execute job schedules which were not executed during stoppage of Hinemos Manager, due to occasions such as restarting of Hinemos Manager, but when this parameter is set too small, job schedules will not be executed after restarting Hinemos Manager. Therefore, it is not recommended to set the threshold to less than the default value of 3600000.

8.3 Enabling a File Transfer Job

The following configuration is required if using the file transfer job feature in a Linux Agent. (This can also be set from the collective run feature. Refer to Hinemos User's Manual "10.9.2 Setting of File Transfer Job" for details.)

Further, the File Transfer Job uses ssh internally, but the ssh feature is not provided in Windows OS, so File Transfer Job cannot be used with Windows agent. (Refer to Hinemos User's Manual "13.4.1 Job Feature Limitations for details.")

Do not use the collective run feature, or, perform the settings from the following procedure if you want the normal user to run the File Transfer Job.

- Register the public key of the user running the transfer in destination Agent.properties
- Register the authorized_keys file of the user running the transfer in source Agent.properties.
- Register the host key

The procedure for configuring file transfer jobs is displayed below. Here, the source node is described as agent01 (192.168.0.10), the destination node as agent02 (192.168.0.11), and the transfer user is hinemos.

※Change the user name "hinemos" to other users such as root, with necessities.

- Transfer source node: The node that is the forwarding source for the file (the server logged in to with the scp command)
- Transfer destination node: The node that is the forwarding destination for the file (the server where the scp command is executed)
- Transfer user: Executing user for the File Transfer Job (user running the scp command)

* In addition, the following procedure assumes that the user already exists in the system, and runs the same transfer on the source node and the destination node.

1. Switch to the transfer user (hinemos) on the destination node (agent02).

```
(root@agent02) # su - hinemos
(hinemos@agent02) $
```

2. Display the public key of the transfer user (hinemos). If the key has not been created yet, create and display the authentication of transfer public key for the user without any pass phrase.

```
(hinemos@agent02) $ cd .ssh/
(hinemos@agent02) $ cat id_rsa.pub
ssh-rsa ****(partially omitted)***** = hinemos@agent02
(hinemos@agent02) $
```

3. Switch the user to the root user, then register the public key displayed above in Agent.properties.

```
(hinemos@agent02) $ su -
Password:
(root@agent02) # vi /opt/hinemos_agent/conf/Agent.properties

##
## Common Function
##

## Common : For JAX-WS XML Invalid Char(true : replace specified char, false : replace Hexa expression)
common.invalid.char.replace=false

(Partially omitted)

##scp(ssh) public key
hinemos.public.key=ssh-rsa ****(partially omitted)***** = hinemos@agent02
hinemos.authorized.keys.path=/home/hinemos/.ssh/authorized_keys
```

Add the following parameter (or change it if it already exists)

(Transfer user) .public.key = (public key displayed above)

(Transfer user) .authorized.keys.path = (path to the authorized_keys file of the source node)

4. Login to the source node (agent01) as the transfer user (hinemos), then register the host key.

```
(root@agent02) # exit
(hinemos@agent02) $ ssh 192.168.0.10
The authenticity of host '192.168.0.10 (192.168.0.10)' can't be established.
RSA key fingerprint is **:**:**:**:**:**:**:**:**:**:**:**:**:**:**:**:**.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.10' (RSA) to the list of known hosts.
hinemos@192.168.0.10's password:
(hinemos@agent01) $
```

5. Create the `authorized_keys` file if it is not present in the source node (agent01).

```
(hinemos@agent01) $ mkdir .ssh
(hinemos@agent01) $ chmod 700 .ssh
(hinemos@agent01) $ cd .ssh
(hinemos@agent01) $ touch authorized_keys
(hinemos@agent01) $ chmod 600 authorized_keys
```

6. Switch to the root user, and configure the above file in `Agent.properties`.

```
(hinemos@agent01) $ su -
Password:
(root@agent01) # vi /opt/hinemos_agent/conf/Agent.properties

##
## Common Function
##

## Common : For JAX-WS XML Invalid Char(true : replace specified char, false : replace Hexa expression)
common.invalid.char.replace=false
(Partially omitted)

##scp(ssh) public key
hinemos.authorized.keys.path=/home/hinemos/.ssh/authorized_keys
```

Add the following parameter (or change it if it already exists)

(Transfer user) `.authorized.keys.path = (path to the authorized_keys file created above)`

The Hinemos Agent that is the transfer destination must be restarted after the settings.

9 Other Features

Additional settings for the other Hinemos features are explained.

9.1 Self-check Feature

The self-check feature is a feature that periodically confirms the internal state of the Hinemos Manager and notifies the result to the user.

The internal states to confirm are as follows.

- Application failure
 - Malfunction from database access failure (selfcheck.monitoring.db)
 - Malfunction from internal scheduler abnormalities (selfcheck.monitoring.scheduler.delay)
 - Malfunction from failure to cooperate with external programs (selfcheck.monitoring.ws.queue)
- Resource drain
 - Depletion of memory space (in Java Virtual Machine) by additional configuration or amount of notifications. (selfcheck.monitoring.jvm)
 - Depletion of free space in the file system used by the Hinemos Manager (selfcheck.monitoring.filesystem)
- Performance decline
 - Enlargement of space used for storing temporarily information, due to receiving large number of syslog and snmptrap (selfcheck.monitoring.systemlog, selfcheck.monitoring.snmptrap)
 - Enlargement of space used for storing temporarily information, due to adding configuration and or increase of notifications (selfcheck.monitoring.asyncntask)
 - Enlargement of historical information (event, performance information, job history, and others) (selfcheck.monitoring.table.size)
 - Increase in number of running job sessions (selfcheck.monitoring.job.runningsession)
 - Increase in number of running threads (selfcheck.monitoring.thread.activity)
 - Swap out of Manager Server (selfcheck.monitoring.swapout)

If notification of an error occurs, it will be notified to the Hinemos internal scope (INTERNAL) in the Monitor[Event] view by default. Also, that overview can be stored as an event, and the original message can be sent as a syslog to an external device. To change the output settings, please refer to [INTERNAL Events](#).

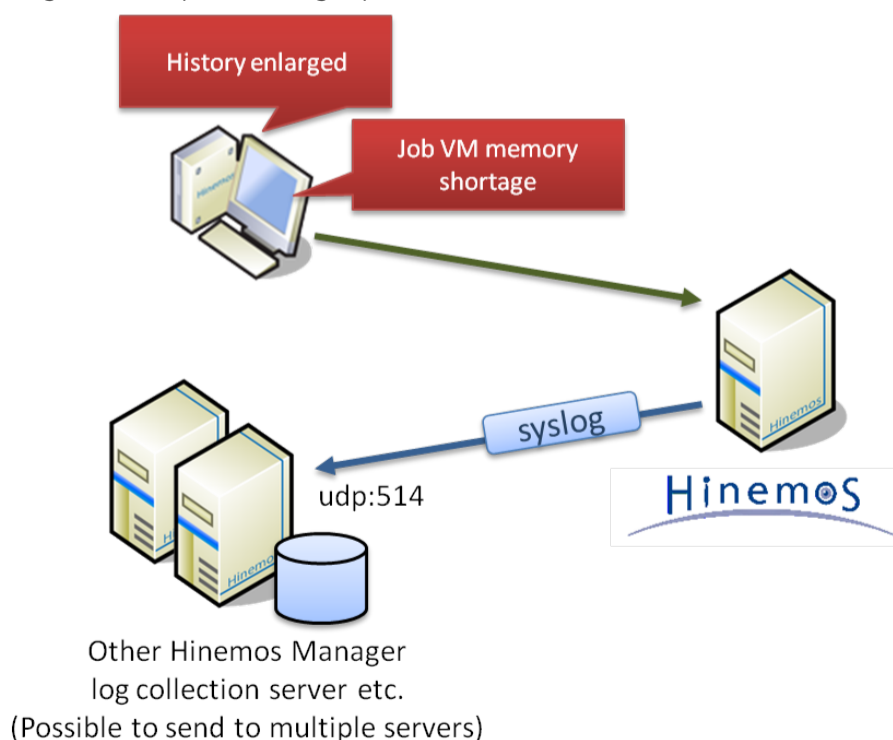


Figure 9-1. Overview of the Self-check Feature

9.1.1 Self-check Feature Settings

Configuration files of the self-check feature are as follows.

/opt/hinemos/etc/selfcheck-service.properties

Table 9-1. Configured Values of the Self-check Feature

Parameter name(excluding selfcheck.)	Content of Settings	Default Value	Lower Limit	Upper Limit
startup.delay	Time to start self check after starting Hinemos[sec]	90	1	2147483647
interval	Time interval to check status of internal component[sec]	150	1	2147483647
alert.threshold	Number of errors detected before the notification	3	1	2147483647
threadpool.size	Number of threads used for self check feature	4	1	2147483647
snmp.community	Community name used by SNMP polling to manager server itself (127.0.0.1)	public	—	—
snmp.port	Port number used by SNMP polling to manager server itself (127.0.0.1)	161	—	—
snmp.version	Version (1/2c) used by SNMP polling to manager server itself (127.0.0.1)	2c	—	—
snmp.timeout	Timeout [sec] used by SNMP polling to manager server itself (127.0.0.1)	3000	1	2147483647
snmp.retries	Retry count used by SNMP polling to manager server itself	3	1	2147483647
monitoring.jvm.freeheap	Set true if enabling free memory space checking of Java VM. Set false if disabling this setting	true	—	—
monitoring.jvm.freeheap.threshold	Checking threshold of free memory space of Java VM[MByte]	32	0	2147483647
monitoring.filesystem.usage	Set true if enabling the free filesystem space checking. Set false if disabling this setting	false	—	—
monitoring.filesystem.usage.list	Checking threshold of free filesystem space of Hinemos Manager Server. Filesystem usage of "/" directory is monitored with its threshold of 50% with its original settings.	/:50,/:50	—	—
monitoring.swapout	Set true if enabling swapout checking. Set false if disabling this setting	false	—	—
monitoring.db	Set true if enabling access check to database. Set false if disabling this setting	true	—	—
monitoring.db.validationquery	SQL used to check access to the database	SELECT 1 FOR UPDATE	—	—
monitoring.scheduler.delay	Set true if enabling scheduler check. Set false if disabling this setting.	true	—	—
monitoring.scheduler.delay.threshold	Upper threshold of delay time [sec] to determine the delay of scheduler.	300	0	2147483647

monitoring.ws.queue	Set true if enabling access cue check of Web Service. Set false if disabling this setting	true	—	—
monitoring.ws.queue.threshold	Upper threshold of messages in access cue of Web Service	10000	0	2147483647
monitoring.systemlog.queue	Set true if enabling internal cue check of system log monitoring Set false if disabling this setting	true	—	—
monitoring.systemlog.queue.threshold	Upper threshold of messages in internal cue used for system log monitoring	10000	0	2147483647
monitoring.snmptrap.queue	Set true if enabling internal cue check of SNMPTRAP monitoring Set false if disabling this setting	true	—	—
monitoring.snmptrap.queue.threshold	Upper threshold of messages in internal cue used for SNMPTRAP monitoring	10000	0	2147483647
monitoring.asyncntask.queue	Set true if enabling cue check of asynchronous processing Set false if disabling this setting	true	—	—
monitoring.asyncntask.queue.list	Upper threshold of messages in cue used for asynchronous processing and name of the cue to be checked	(Note2)	0	2147483647
monitoring.thread.activity	Set true if enabling delaying thread check Set false if disabling this setting	true	—	—
monitoring.thread.activity.threshold	Upper threshold of delaying time of delaying thread[sec]	300	0	2147483647
monitoring.table.size	Set true if enabling size check of internal table Set false if disabling this setting	true	—	—
monitoring.table.size.list	Upper threshold of table size and table name to be checked	(Note3)	—	—
monitoring.job.runningsession	Set true if checking the number of running job session Set false if disabling this setting	true	—	—
monitoring.job.runningsession.threshold	Upper Threshold of the number of job session	1000	0	9223372036854775807

(Note1) ** Default value of these settings are not recommended to be changed, except for selfcheck.snmp.* **

(Note2)NotifyStatusTaskFactory:10000,NotifyEventTaskFactory:10000,NotifyMailTaskFactory:10000,NotifyCommandTaskFactory:10000,NotifyLogEscalationTaskFactory:10000, NotifyJobTaskFactory:10000,CollectiveRunExecuteTaskFactory:10000

(Note3)cc_event_log:5120:MBYTE,cc_calculated_data:20480:MBYTE,cc_job_session:100000:COUNT,cc_crun_session:10000:COUNT

9.2 INTERNAL Events

9.2.1 Notification Destination Settings

Internal event occurring within Hinemos can be changed. Internal event can be notified as Syslog, Mail, Command, or to Monitor[Event] view, hinemos_internal.log. This setting can be changed in /opt/hinemos/etc/hinemos.properties. Hinemos Manager must be restarted in order to reflect configuration changes on this property file.

- Syslog sending

Enabling the syslog sending settings, output level, and the destination syslog to be sent to can be set in `common.internal.syslog` parameter.

```
## Internal Log : Send Syslog
# priority=[critical,unknown,warning,info]
common.internal.syslog=false
common.internal.syslog.priority=info
common.internal.syslog.host=192.168.1.1,192.168.1.2
common.internal.syslog.port=514
# common.internal.syslog.facility=[kern|user|mail|daemon|auth|syslog|lpr|news|uucp|cron|
    authpriv|ftp|local0|local1|local2|local3|local4|local5|local6|local7]
common.internal.syslog.facility=daemon
# common.internal.syslog.severity=[emergency|alert|critical|error|warning|notice|information|debug]
common.internal.syslog.severity=alert
```

- Monitor[Event] view

Enabling the output settings to INTERNAL scope, and output level of event can be set in `common.internal.event` parameter.

```
## Internal Log : Hinemos Event (INTERNAL)
common.internal.event=true
common.internal.event.priority=info
```

- hinemos_internal.log

Enabling the output settings to `hinemos_internal.log`, and output level of log can be set in `common.internal.file` parameter.

```
## Internal Log : Hinemos Log File (hinemos_internal.log)
common.internal.file=true
common.internal.file.priority=info
```

- E-mail Notification

Enabling the mail sending settings, output level, and mail sending destination can be set in `common.internal.mail` parameter.

```
## Internal Log : Send Mail
common.internal.mail=false
common.internal.mail.priority=info
common.internal.mail.address=user1@host.domain,user2@host.domain
```

- Command Execution

Enabling command execution settings, output level, execution user, execution command, execution time out can be set in `common.internal.command` parameter.

```
## Internal Log : Execute Command
common.internal.command=false
common.internal.command.priority=info
common.internal.command.user=root
common.internal.command.commandline=echo #[GENERATION_DATE] #[MESSAGE] >> /tmp/test.txt
common.internal.command.timeout=15000
```

9.2.2 Notified Information

List of INTERNAL Events will be listed below.

Table 9-2 INTERNAL Events

Priority	Plugin ID	MonitorID	Application	Message ID	Message
Info	MNG	SYS	Hinemos Manager Monitor	001	Hinemos Manager started.
Info	MNG	SYS	Hinemos Manager Monitor	002	Hinemos Manager stopped.
Warning	COMMON	SYS	Common Function	001	Long time ({0}min) active polling thread is detected. PollerGroup={1}, PollerName={2} (statistics : long threads = {3}, all polling thread = {4})
Warning	SYS_SFC	SYS	Selfcheck	001	database is not available. if database is alive, perhaps too many configurations (monitoring, job, ...).
Warning	SYS_SFC	SYS	Selfcheck	002	usage of filesystem({0}) is too high ({1} [%] > threshold {2} [%]). remove log files and compact database.
Warning	SYS_SFC	SYS	Selfcheck	003	free heap of jvm ({0} [mbyte]) is not enough (threshold {1} [mbyte]). perhaps too many configurations (monitoring, job, ...), restartup of hinemos manager is recommended.
Warning	SYS_SFC	SYS	Selfcheck	004	scheduler ({0}:{1}:{2} - next fire time {3}) has not been running for {4} [sec]. perhaps scheduled task is not running, restartup of hinemos manager is recommended.
Warning	SYS_SFC	SYS	Selfcheck	005	ram swap-out({0} [blocks]) occurred since {1}. check resources of server and availability of hinemos manager.
Warning	SYS_SFC	SYS	Selfcheck	006	stored data ({0}) is too large ({1} [mbyte], {2} [rows] > threshold {3} {4}). compact database by using maintenance feature.
Warning	SYS_SFC	SYS	Selfcheck	007	job run session count is too large ({0} > threshold {1}). Since it becomes a factor of a performance fall, please stop the job session which has become being under execution with as unnecessarily ("finishing of change", or "end").
Warning	SYS_SFC	SYS	Selfcheck	008	response delay occurs because of too many request to Hinemos Manager tcp:8080 (queued request {0} > threshold {1}). perhaps too many configurations (monitoring, job, ...).
Warning	SYS_SFC	SYS	Selfcheck	009	filtering delay occurs because of too many syslog to Hinemos Manager (queued syslog {0} > threshold {1}). please check transmission of syslog.
Warning	SYS_SFC	SYS	Selfcheck	010	filtering delay occurs because of too many snmptrap to Hinemos Manager (queued snmptrap {0} > threshold {1}). please check transmission of snmptrap.
Warning	SYS_SFC	SYS	Selfcheck	011	task delay occurs because of too many asynchronous task in Hinemos Manager (queued task {0} > threshold {1}). perhaps too many configurations (monitoring, job, ...).
Warning	SYS_SFC	SYS	Selfcheck	012	internal logic (tid {0}, thread name {1}, class name {2}, start time {3}) takes more than {4} [sec].
Warning	NOTIFY	SYS	Notification	004	Failed to get the Notification ID (NotifyId={0})
Warning	NOTIFY	SYS	Notification	006	Failed to get the list of Notification attribute information
Critical	NOTIFY	SYS	Notification	007	Failed to notify Notification ID "{0}"
Critical	NOTIFY	SYS	Notification	008	Failed to notify.The job definition does not exist. (NotifyId={0},MonitorId={1},JobunitId={2},JobunitId={3})
Warning	MAILTEMP	SYS	Mail Template	004	Failed to get MailTemplate information (MailTemplateId={0})
Warning	MAILTEMP	SYS	Mail Template	005	Failed to get list of MailTemplate ID

Warning	MAIL TEMP	SYS	Mail Template	006	Failed to get list of MailTemplate attribute information
Warning	MON	SYS	Monitor Management	001	Failed to get the Scope information (FacilityId={0})
Warning	MON	SYS	Monitor Management	004	Failed to confirm/unconfirm Event (FacilityId={0}, MonitorId={1}, PluginId={2}, ConfirmType={3})
Warning	MON	SYS	Monitor Management	010	Failed to get the monitoring information (MonitorTypeId={0}, MonitorId={1})
Warning	MON	SYS	Monitor Management	011	Failed to get the list of monitoring information (MonitorTypeId={0}, MonitorId={1})
Warning	MON	SYS	Monitor Management	012	Failed to run monitor (MonitorTypeId={0}, MonitorId={1})
Warning	PROC	SYS	Process Monitor	001	Failed to register Poller setting(FacilityId={0})
Warning	PROC	SYS	Process Monitor	002	Failed to unregister Poller setting(FacilityId={0})
Critical	TRAP	SYS	SNMPTRAP Monitor	009	Failed to notify the SNMP TRAP event (trapOid={0}, genericId={1}, specificId={2})
Critical	MON_PNG	SYS	PING Monitor	001	Fping did not respond (MonitorID={0})
Warning	PERF	SYS	Performance Management	010	Failed to get monitoring information (MonitorTypeId={0}, MonitorId={1})
Warning	PERF	SYS	Performance Management	014	Failed to register Poller setting(FacilityId={0})
Warning	PERF	SYS	Performance Management	015	Failed to unregister Poller setting(FacilityId={0})
Critical	JOB	SYS	Job Management	003	Failed to create Job history information(JobID={0})
Warning	JOB	SYS	Job Management	008	Failed to start[Cancel Pause](SessionID={0}, JobID={1})
Warning	JOB	SYS	Job Management	009	Failed to start[Cancel Suspend](SessionID={0}, JobID={1})
Warning	JOB	SYS	Job Management	010	Failed to start[Cancel Skip](SessionID={0}, JobID={1})
Warning	JOB	SYS	Job Management	011	Failed to stop[Command](SessionID={0}, JobID={1}, FacilityID={2})
Warning	JOB	SYS	Job Management	012	Failed to stop[Pause](SessionID={0}, JobID={1})
Warning	JOB	SYS	Job Management	013	Failed to stop[Suspend](SessionID={0}, JobID={1})
Warning	JOB	SYS	Job Management	014	Failed to stop[Skip](SessionID={0}, JobID={1})
Warning	JOB	SYS	Job Management	016	Failed to run scheduled Job (JobID={0}, ScheduleInfo={1})
Warning	JOB	SYS	Job Management	017	Failed to run file-check Job (JobID={0}, ScheduleInfo={1})
Critical	CR	SYS	Collective Run	001	Failed to run Session
Critical	CR	SYS	Collective Run	002	Failed to create history information
Warning	CR	SYS	Collective Run	003	Could not send message of execute instruction(SessionID={0}, FacilityID={1})

Warning	CR	SYS	Collective Run	004	Received the same start message as previous one, so the message was discarded (SessionID={0}, FacilityID={1})
Critical	CR	SYS	Collective Run	005	Cannot find shell script file(FileName={0})
Critical	CR	SYS	Collective Run	006	Failed to read shell script file(FileName={0})
Warning	CR	SYS	Collective Run	007	Failed to create/change master information (ItemType={0}, ID={1}, ParentID={2})
Warning	CR	SYS	Collective Run	008	Failed to delete master information (ItemType={0}, ID={1}, ParentID={2})

9.3 Hinemos Manager Alive Detection

The Hinemos Client can poll the Hinemos Manager. The Hinemos Client attempts to connect to the Hinemos Manager regularly. If there is no response, it is a Hinemos Manager failure, and a dialog like in Figure 9-2 is shown.

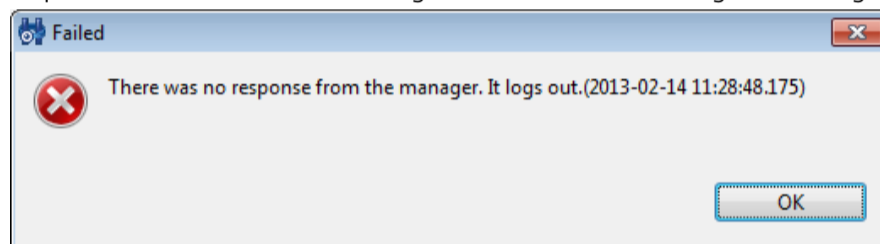


Figure 9-2 Hinemos Manager Polling

The interval for polling for the Hinemos Manager is displayed from the "Client Settings" - "Preferences" in the menu bar. It can be set from the "Manager Polling Interval (min)" setting value in the "Preferences" dialog. (Figure 9-3 Reference)

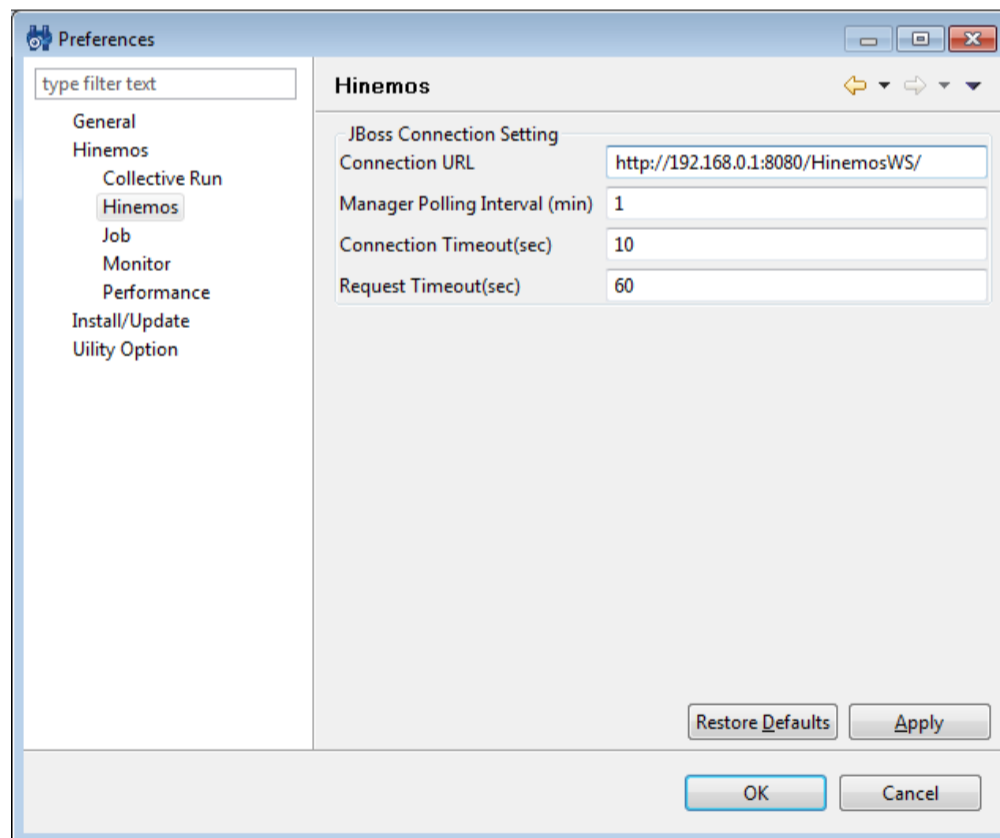


Figure 9-3 Hinemos Manager Polling Interval

10 Security

When changing Hinemos Manager's internal Database, in terms of security, change the password with steps listed below, after stopping Hinemos Manager. Before applying the procedures, it is recommended that you obtain a backup file by following the procedures in [Backing-up the Database](#) .

Restart Hinemos Manager after changing the password and configuration file. Further, if there is not consistency of the password between the source and destination, Hinemos Manager will not run normally and you will not be able to connect from the Hinemos Client.

10.1 Change the Database Access Password

The process for changing the password and access authority for Hinemos Manager's PostgreSQL user hinemos and hinemos_quartz.

10.1.1 PostgreSQL (destination) Setting Changes

- password

Change the PostgreSQL password following the procedure below.

1. Stop the Hinemos Manager and run the following commands as the root user.

Password entry is required. Enter the login password for PostgreSQL (default is "hinemos").

```
(root) # /opt/hinemos/bin/pg_start.sh

(root) # /opt/hinemos/postgresql/bin/psql -p 24001 -U hinemos
Password for user hinemos:
psql (9.1.9)
Type "help" for help.
```

2. The psql prompt is displayed. Run the following command.

```
hinemos=# ALTER USER hinemos PASSWORD '(New password)';
hinemos=# ALTER USER hinemos_quartz PASSWORD '(New password)';
```

3. End psql and stop PostgreSQL.

```
hinemos=# \q

(root) # /opt/hinemos/bin/pg_stop.sh
```

4. Start Hinemos manager

- Access Authority

Edit the following configuration file, and configure the access permission of PostgreSQL.

/opt/hinemos/etc/postgresql/pg_hba.conf

```
(Omitted)

# TYPE DATABASE USER CIDR-ADDRESS METHOD

# "local" is for Unix domain socket connections only
local postgres hinemos md5
local hinemos hinemos md5
local hinemos hinemos_quartz md5
# IPv4 local connections:
host postgres hinemos 0.0.0.0/0 md5
host hinemos hinemos 0.0.0.0/0 md5
host hinemos hinemos_quartz 0.0.0.0/0 md5
# IPv6 local connections:
host postgres hinemos ::/0 md5
host hinemos hinemos ::/0 md5
host hinemos hinemos ::/0 md5

(Omitted)
```

(Note) The following is a setting example. It is recommended that you change the connection settings according to the security policy in use.

10.1.2 Hinemos Manager (destination) Setting Changes

Edit the following two setting files.

- persistence.xml
- scheduler-dbms.properties

1. Edit persistence.xml

persistence.xml is a configuration file containing settings for database access of PostgreSQL User "hinemos"

Set password changed in PostgreSQL (destination) Setting Changes`_ to javax.persistence.jdbc.password

/opt/hinemos/etc/META-INF/persistence.xml

```
(omitted)

<property name="javax.persistence.jdbc.user" value="hinemos"/>
<property name="javax.persistence.jdbc.password" value="hinemos"/>

(omitted)
```

2. Edit scheduler-dbms.properties

scheduler-dbms.properties is a configuration file containing settings for database access of PostgreSQL User "hinemos_quartz"

Set password changed in PostgreSQL (destination) Setting Changes`_ to org.quartz.dataSource.SchedulerDS.password

/opt/hinemos/etc/scheduler-dbms.properties

(omitted)

```
org.quartz.dataSource.SchedulerDS.user = hinemos_quartz  
org.quartz.dataSource.SchedulerDS.password = hinemos_quartz
```

(omitted)

11 Connections between Hinemos Components

11.1 Connections to Hinemos Manager via HTTP Proxy

With Hinemos ver.4.1, Hinemos Manager can be connected from Hinemos Client and Hinemos Agent via HTTP Proxy.

11.1.1 Connecting to Hinemos Manager from Hinemos Client

Set HTTP Proxy settings from Hinemos Client.

1. Select "Client Setup(S)" from Hinemos Client Menu -> Show "Preference" dialog Configure from "HTTP Proxy Connection Setting" (refer figure 11-1)

HTTP Proxy Host

Enter a IP address or a host name of HTTP Proxy Server

HTTP Proxy Port

Enter a listen port of HTTP Proxy Server

HTTP Proxy User

Enter a User Name of HTTP Proxy Server

HTTP Proxy Password

Enter a Password for HTTP Proxy Server

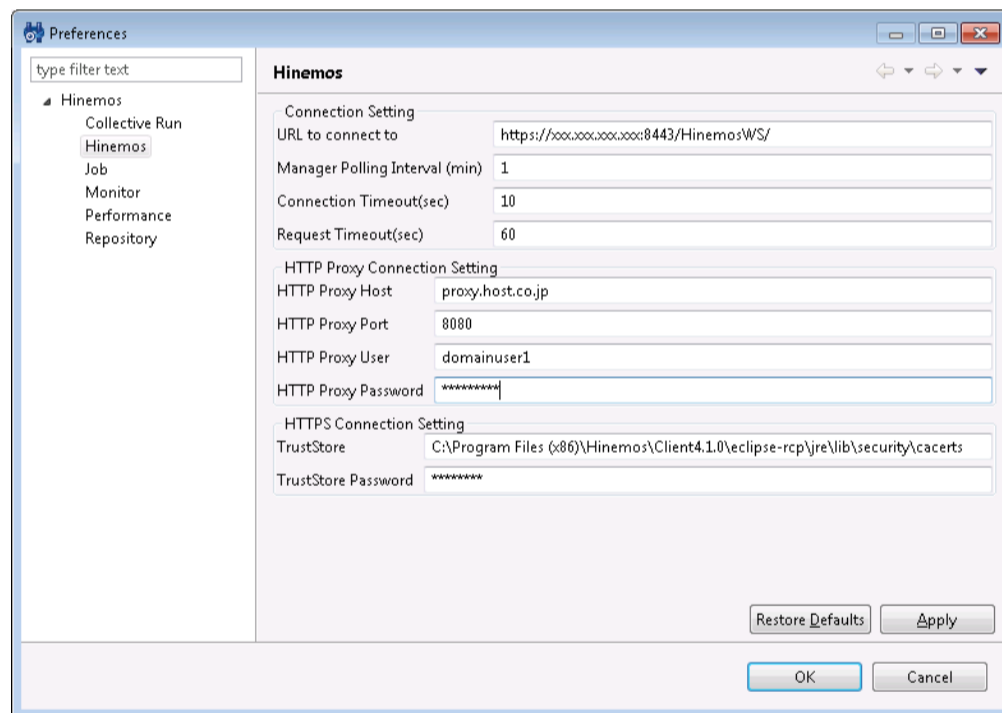


Figure 11-1 Settings of connections in between Components of Hinemos

In order to reflect the configuration changes, restart Hinemos Client.

11.1.2 Connecting to Hinemos Manager from Hinemos Agent

Edit following file of Hinemos Agent.

/opt/hinemos_agent/conf/Agent.properties

```
http.proxy.host=192.168.100.100
http.proxy.port=8080
http.proxy.user=proxyuser1
http.proxy.password=password
```

Configure the following parameters

- http.proxy.host=IP Address or Hostname of HTTP Proxy Server
- http.proxy.port=Listen Port of HTTP Proxy Server
- http.proxy.user=User Name of HTTP Proxy Server
- http.proxy.password=Password for HTTP Proxy Server

In order to reflect the configuration changes, restart Hinemos Agent.

11.2 HTTPS connection to Hinemos Manager

With Hinemos ver.4.1, Hinemos Manager can be connected from Hinemos Client with HTTPS connection. Hinemos Agent can only use HTTP connection to Hinemos Manager.

11.2.1 Preparing server certificate of Hinemos Manager Server

First, prepare a server certificate of Hinemos Manager Server(PKCS#12). In this chapter, the following example will be written as an example of using OpenSSL(OpenSSL 1.0.0-fips 29 Mar 2010) to make self signed certificate.

1. Copy a default openssl.cnf

```
# mkdir /opt/hinemos/etc/ssl
# cd /opt/hinemos/etc/ssl
# cp /etc/pki/tls/openssl.cnf /opt/hinemos/etc/ssl/
```

2. Edit openssl.cnf as written below

```
# vi openssl.cnf

[ req ]
# x509_extensions = v3_ca # The extensions to add to the self signed cert ←Comment Out
x509_extensions = v3_req ←Add

req_extensions = v3_req # The extensions to add to a certificate request ←Undo Comment Out

[ v3_req ]
subjectAltName=IP: 【IP Address of Hinemos Manager Server】 ←Add
```

3. Create the certificate with following command.

```
# openssl genrsa -des3 -out server.key 1024
Generating RSA private key, 1024 bit long modulus
.....++++++
.++++++
e is 65537 (0x10001)
Enter pass phrase for server.key:(Enter hinemos)
Verifying - Enter pass phrase for server.key:(Enter hinemos)
```

```
# openssl req -new -x509 -key server.key -out server.crt -config openssl.cnf -days 3650
Enter pass phrase for server.key:(Enter hinemos)
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:(Press Enter key without entering anything)
State or Province Name (full name) []:(Press Enter key without entering anything)
Locality Name (eg, city) [Default City]:(Press Enter key without entering anything)
Organization Name (eg, company) [Default Company Ltd]:(Press Enter key without entering anything)
Organizational Unit Name (eg, section) []:(Press Enter key without entering anything)
Common Name (eg, your name or your server's hostname) []:(Press Enter key without entering anything)
Email Address []:(Press Enter key without entering anything)
```

```
# openssl pkcs12 -export -in server.crt -inkey server.key -out store.p12
Enter pass phrase for server.key:(Enter hinemos)
Enter Export Password:(Enter hinemos)
Verifying - Enter Export Password:(Enter hinemos)
```

Next, load the server certificate created by the previous steps, to Hinemos Manager. In order to make Hinemos Manager load the server certificate, edit the following file.

/opt/hinemos/etc/hinemos.properties

```
## Web Service
common.ws.address=https://0.0.0.0:8443 ←Change
common.ws.threadpool.size=48
common.ws.queue.size=30000
common.ws.https.protocol=TLS ←Add
common.ws.https.keystore.path=/opt/hinemos/etc/ssl/store.p12 ←Add
common.ws.https.keystore.password=hinemos ←Add
common.ws.https.keystore.type=PKCS12 ←Add
```

Configure the following parameters.

- common.ws.address=Connected address from Hinemos Client to Hinemos Manager (Change protocol to https and port to 8443)
- common.ws.https.protocol=Secure protocol of HTTPS
- common.ws.https.keystore.path=Directory Path of Keystore
- common.ws.https.keystore.password=Password of Keystore
- common.ws.https.keystore.type=Type of Keystore

In order to reflect the configuration changes, restart Hinemos Manager.

11.2.2 Connections from Hinemos Client to Hinemos Manager

Place the server.crt created in steps written in [Preparing server certificate of Hinemos Manager Server](#) to a terminal where Hinemos Client is installed. (In this document, server.crt will be placed in C:\tmp\)

1. Run command prompt as administrator.
2. Import the placed server certificate to the Truststore. From command prompt, execute the following command (in one line) (The following will be an example of command executed in 32bit environment. When executing the command in 64bit environment, change "Program Files" to "Program Files (x86)")

```
>C:\Users>"C:\Program Files\Hinemos\Client4.1.0\eclipse-rcp\jre\bin\keytool.exe" -import -alias hinemos
-file "C:\tmp\server.crt" -keystore "C:\Program Files\Hinemos\Client4.1.0\eclipse-rcp\jre\lib\security\cacerts"

Enter keystore password: (Enter changeit)
Owner: O=Default Company Ltd, L=Default City, C=XX
Issuer: O=Default Company Ltd, L=Default City, C=XX

(Omitted)

Trust this certificate? [no]: yes
Certificate was added to keystore
```

3. Designate the keystore where server certificate was imported, from Hinemos Client. Specify the trust store from Hinemos Client Menu "Client Setup(S)" -> "Setup(S)" -> "Preference" dialog "HTTPS Connection Settings"(Refer Figure 11-1).

TrustStore

specify the directory of truststore file where server certificate of Hinemos Manager Server was imported
 Example) C:\Program Files\Hinemos\Client4.1.0\eclipse-rcp\jre\lib\security\cacerts

TrustStore Password

Example) changeit

4. Restart Hinemos Client, and enter the URL to the "URL to connect" in Connection[Login] dialog (Refer Figure 11-2) .

URL to connect

<https://> 【IP address of Hinemos Manager】 :8443/HinemosWS/

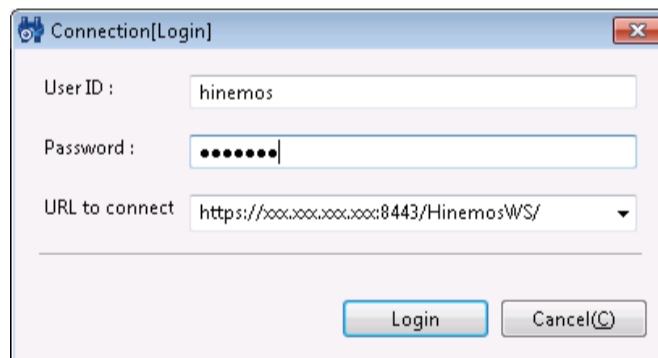


Figure 11-2 "URL to connect" in Connection[Login] dialog

12 Log Files

12.1 List of Hinemos Manager Log Files

Hinemos Manager logs are output in log file displayed in Table 12-1.

Table 12-1 List of Hinemos Manager Log Files

File name	boot.log
Store directory	/opt/hinemos/var/log/

Configured file for log output	/opt/hinemos/etc/log4j.properties
Output level	priority INFO
Rotation	Overwritten when Hinemos Manager starts
Content	Log of java process boot sequence
File name	jvm_stdout.log*
Store directory	/opt/hinemos/var/log/
Configured file for log output	—
Output level	—
Rotation	Overwritten when Hinemos Manager starts
Content	java process's standard output/standard error output/thread dump
File name	hinemos_manager.log*
Store directory	/opt/hinemos/var/log/
Configured file for log output	/opt/hinemos/etc/log4j.properties
Output level	priority INFO
Rotation	Daily (unlimited)
Content	Activity log of java process
File name	postgresql.log.*
Store directory	/opt/hinemos/var/log/
Configured file for log output	/opt/hinemos/etc/postgresql/postgresql.conf
Output level	warning
Rotation	Daily (unlimited)
Content	Activity log of PostgreSQL
File name	hinemos_internal.log
Store directory	/opt/hinemos/var/log/
Configured file for log output	/opt/hinemos/etc/log4j.properties
Output level	priority INFO
Rotation	Daily (unlimited)
Content	INTERNAL event's log
File name	hinemos_operation.log*
Store directory	/opt/hinemos/var/log/
Configured file for log output	/opt/hinemos/etc/log4j.properties
Output level	priority INFO or DEBUG
Rotation	Daily (unlimited)
Content	Hinemos operation log
File name	hinemos_manager_summary.*
Store directory	/opt/hinemos/var/log/
Configured file for log output	—
Output level	—
Rotation	When this script is executed.
Content	/opt/hinemos/sbin/mng/hinemos_manager_summary.sh execution log
File name	gc.log

Store directory	/opt/hinemos/var/log/
Configured file for log output	/opt/hinemos/hinemos.cfg
Output level	—
Rotation	Rotated every 20MByte and last 5 generation will be kept
Content	Garbage Collection log of java process

12.2 Changing Log Output and Log Rotation of Java Process

- File to edit

To change the log output level and the log rotation method of java process used in Hinemos, edit the following file.

/opt/hinemos/etc/log4j.properties

```
log4j.rootCategory=info, manager
```

hinemos_manager.log's log output level and the log rotation method can be changed by editing the following file.

For methods and examples of changing the log rotation settings, please refer <http://logging.apache.org/log4j/1.2/manual.html>

- Method of applying changes

The changes in the log output level will be reflected when you restart the Hinemos Manager, or it will be automatically reflected every 60 minutes(auto configuration loading mechanism).

12.3 Changing Log Output and Log Rotation of PostgreSQL

- File to edit

To change the log output level and the log rotation method of PostgreSQL used in Hinemos, edit the following file.

/opt/hinemos/etc/postgresql/postgresql.conf

Refer to <http://www.postgresql.jp/document/9.1/html/> for a setting example.

- Method of applying changes

The changes in the log output level will be reflected when you restart the Hinemos Manager.

12.4 Changing Log Output and Log Rotation of Operations Log

- File to edit

To change the log output and the log rotation settings of operation log (/opt/hinemos/var/log/hinemos_operation.log), edit the following file.

/opt/hinemos/etc/log4j.properties

```
log4j.category.HinemosOperation=info, operation
```

Further, the support relationship between the priority value and log output target operation is shown in Table 12-2.

Table 12-2. Operation Log Setting Values

priority value	Log output target operations
info	Set up, Run
debug	Refer, Set Up, Run

- Method of applying changes

The changes in the log output level will be reflected when you restart the Hinemos Manager, or it will be automatically reflected every 60 minutes(auto configuration loading mechanism).

12.5 List of Hinemos Agent Log Files

Linux Agent logs are output in the log file displayed in Table 12-3.

Table 12-3 List of Linux Agent Log Files

File name	agent.log.*
Store directory	/opt/hinemos_agent/var/log/
Log output settings file	/opt/hinemos_agent/conf/log4j.properties
Output level	priority INFO
Rotation	File size 20MByte (Maximum of 5 generations including the current log)
Content	Hinemos Agent log
File name	agent_stdout.log
Store directory	/opt/hinemos_agent/var/log/
Configured file for log output	—
Output level	—
Rotation	Overwritten when Hinemos Agent starts
Content	Hinemos Agent's standard output
File name	agent_stderr.log
Store directory	/opt/hinemos_agent/var/log/
Configured file for log output	—
Output level	—
Rotation	Overwritten when Hinemos Agent starts
Content	Hinemos Agent's /standard error output/thread dump
File name	gc.log.*
Store directory	/opt/hinemos_agent/var/log/
Configured file for log output	/opt/hinemos_agent/conf/hinemos_agent.cfg
Output level	—
Rotation	Rotated every 20MByte and last 5 generation will be kept
Content	Garbage Collection log of java process

Windows Agent logs are output in the log file displayed in Table 12-4.

Table 12-4 List of Windows Agent Log Files

File name	agent.log.*
Storage directory	[Hinemos Agent install directory]\var\log\
Log settings file	[Hinemos Agent install directory]\conf\log4j.properties
Output level	priority INFO

Rotation	Rotated every 20MByte and last 5 generation will be kept
Content	Hinemos Agent log
File name	restart.log
Storage directory	[Hinemos Agent install directory]\var\log\
Configured file for log output	—
Output level	—
Rotation	Overwritten at the time of Hinemos Agent startup
Content	Hinemos Agent standard output/standard error output/thread dump
File name	gc.log.*
Store directory	[Hinemos Agent install directory]\var\log\
Configured file for log output	[Hinemos Agent install directory]\bin\RegistAgentService.bat
Output level	—
Rotation	Rotated every 20MByte and last 5 generation will be kept
Content	Garbage Collection log of java process

12.6 Changing the Log Output and Log Rotation settings of the Hinemos Agent

- File to edit

Edit the following file to change the log output level and log rotation settings of the Hinemos Agent.

- [For the Linux Agent]
/opt/hinemos_agent/conf/log4j.properties
- [For the Windows Agent]
[Hinemos Agent install directory]\conf\log4j.properties

```
### direct messages to file agent.log ###
log4j.appender.file=org.apache.log4j.RollingFileAppender <- Designate Appender (Default setting is rotate by filesize)
log4j.appender.file.MaxFileSize = 20MB <- Maximum Filesize
log4j.appender.file.MaxBackupIndex = 4 <- Maximum generation of backup logfile to be kept
log4j.appender.file.Append=true <- overwrite when Hinemos Manager starts or not.
log4j.appender.file.layout=org.apache.log4j.PatternLayout <- Designate a class to specify layout
log4j.appender.file.layout.ConversionPattern=%d %-5p [%t] [%c] %m%n <- output format of log file name pattern

### direct messages to syslog ###
log4j.appender.syslog=org.apache.log4j.net.SyslogAppender
log4j.appender.syslog.Facility=user
log4j.appender.syslog.FacilityPrinting=false
log4j.appender.syslog.layout=org.apache.log4j.PatternLayout
log4j.appender.syslog.layout.ConversionPattern=%m%n

#log4j.rootLogger=info, file
log4j.logger.hinemos.syslog.transfer=debug, syslog <- Designate log level and output destination(syslog)
log4j.logger.com.clustercontrol=info, file <- Designate log level and output destination(agent log)

log4j.appender.file.File=/opt/hinemos_agent/var/log/agent.log <- Designate the Output File
#log4j.appender.syslog.SyslogHost={Host name for the managed node}
```

For details on the configuration, refer to <http://logging.apache.org/log4j/1.2/manual.html>

Note) The output defined by org.apache.log4j.net.SyslogAppender is the function of the Hinemos Agent itself, so if configuration changes related to org.apache.log4j.net.SyslogAppender are made, there is a possibility that the Hinemos Agent may not run correctly.

- Method of applying changes

The change in the log output level is reflected when the Hinemos Agent restarts, or at 10 minute intervals (auto configuration loading mechanism).

12.7 List of Hinemos Client Log Files

Hinemos Client logs are output in log file displayed in Table 12-5.

Table 12-5 List of Hinemos Client Log Files

File name	client.log
Storage directory	C:\Users\[User name]\AppData\Roaming\hinemos\Client4.1
Log settings file	[Hinemos Client install directory]\log4j.properties
Output level	—
Rotation	File size 20MByte (Maximum of 5 generations including the current log)
Content	Hinemos Client Log

13 List of Hinemos Manager's Configuration Settings

Hinemos Manager's settings are defined in /opt/hinemos/etc/hinemos.properties. (If multi-byte characters are used in the properties file, the property file needs to be edited with property editor.)

In order to reflect the configuration changes, restart Hinemos Manager.

Parameter[common.invalid.char.replace]

Property	common.invalid.char.replace
Property name	replacement rule of control character in original message
Description	If this parameter is true, control character in original message will be replaced with a character designated in common.invalid.char.replace.to. If this parameter is false, control character in original message will be replaced with hexadecimal numeration.
Data type	String
Default value	false

Parameter[common.invalid.char.replace.to]

Property	common.invalid.char.replace.to
Property name	character to be replaced with control character in original message.
Description	When common.invalid.char.replace is set true, control character in original message will be replaced with a character designated in this parameter.
Data type	String
Default value	?

Parameter [common.notify.date.format]

Property	common.notify.date.format
Property name	(Notification) Date format of the variable ([GENERATION_DATE]) that can be used in notification
Description	Date format of the variable ([GENERATION_DATE]) that can be used in notification
Data type	String
Default value	yyyy/MM/dd HH:mm:ss

Reference	http://docs.oracle.com/javase/jp/7/api/java/text/SimpleDateFormat.html
-----------	---

Parameter [common.manager.hostname]

Property	common.manager.hostname
Property name	(Notification)Log escalation notification source host name
Description	String specified in HOSTNAME section when a syslog is sent by log escalation notification
Data format	String (\${NODE}, \${FACILITY_ID}, Fixed host name, blank: Manager server host name)
Default value	\${NODE}

Parameter [common.repository.snmp.timeout]

Property	common.repository.snmp.timeout
Property name	Timeout value related to the repository feature's find by snmp
Description	Timeout time for SNMP polling with the repository feature's find by snmp
Data type	Integer (msec)
Default value	5000

Parameter [common.repository.snmp.retry]

Property	common.repository.snmp.retry
Property name	Polling maximum retry count related to the repository feature's find by snmp
Description	Maximum retry count for SNMP polling with the repository management feature's find by snmp
Data type	Integer
Default value	1

Parameter [common.repository.snmp.oid.name]

Property	common.repository.snmp.oid.name
Property name	OID to retrieve node name for find by snmp of Repository Feature
Description	OID to retrieve node name and host name values used from repository feature's find by snmp
Data type	String
Default value	.1.3.6.1.2.1.1.5.0

Parameter [common.repository.snmp.oid.descr]

Property	common.repository.snmp.oid.descr
Property name	OID to retrieve description information for find by snmp of Repository Feature
Description	OID to retrieve description information value used from repository feature's find by snmp
Data type	String
Default value	.1.3.6.1.2.1.1.1.0

Parameter [common.repository.snmp.oid.contact]

Property	common.repository.snmp.oid.contact
Property name	OID to retrieve contact information for find by snmp of Repository Feature

Description	OID to retrieve contact information value used from repository feature's find by snmp
Data type	String
Default value	.1.3.6.1.2.1.1.4.0

Parameter[common.repository.snmp.oid.dev.name]

Property	common.repository.snmp.oid.dev.name
Property name	OID to retrieve device name for find by snmp of Repository Feature
Description	OID to retrieve device name value used from repository feature's find by snmp
Data type	String
Default value	.1.3.6.1.2.1.25.3.2.1.3

Parameter[common.repository.snmp.oid.dev.index]

Property	common.repository.snmp.oid.dev.index
Property name	OID to retrieve device index information for find by snmp of Repository Feature
Description	OID to retrieve device index value used from repository feature's find by snmp
Data type	String
Default value	.1.3.6.1.2.1.25.3.2.1.1

Parameter[common.repository.snmp.oid.dev.type]

Property	common.repository.snmp.oid.dev.type
Property name	OID to retrieve device type information for find by snmp of Repository Feature
Description	OID to retrieve device type value used from repository feature's find by snmp
Data type	String
Default value	.1.3.6.1.2.1.25.3.2.1.2

Parameter[common.repository.snmp.oid.disk.name]

Property	common.repository.snmp.oid.disk.name
Property name	OID to retrieve disk name information for find by snmp of Repository Feature
Description	OID to retrieve disk name value used from repository feature's find by snmp
Data type	String
Default value	.1.3.6.1.4.1.2021.13.15.1.1.2

Parameter[common.repository.snmp.oid.disk.index]

Property	common.repository.snmp.oid.disk.index
Property name	OID to retrieve disk index information for find by snmp of Repository Feature
Description	OID to retrieve disk index value used from repository feature's find by snmp
Data type	String
Default value	.1.3.6.1.4.1.2021.13.15.1.1.1

Parameter[common.repository.snmp.oid.nic.name]

Property	common.repository.snmp.oid.nic.name
Property name	OID to retrieve NIC name for find by snmp of Repository Feature
Description	OID to retrieve NIC name value used from repository feature's find by snmp

Data type	String
Default value	.1.3.6.1.2.1.2.2.1.2

Parameter[common.repository.snmp.oid.nic.index]

Property	common.repository.snmp.oid.nic.index
Property name	OID to retrieve NIC index for find by snmp of Repository Feature
Description	OID to retrieve NIC index value used from repository feature's find by snmp
Data type	String
Default value	.1.3.6.1.2.1.2.2.1.1

Parameter[common.repository.snmp.oid.filesystem.name]

Property	common.repository.snmp.oid.filesystem.name
Property name	OID to retrieve Filesystem name for find by snmp of Repository Feature
Description	OID to retrieve Filesystem name value used from repository feature's find by snmp
Data type	String
Default value	.1.3.6.1.2.1.25.2.3.1.3

Parameter[common.repository.snmp.oid.filesystem.index]

Property	common.repository.snmp.oid.filesystem.index
Property name	OID to retrieve Filesystem index for find by snmp of Repository Feature
Description	OID to retrieve Filesystem index value used from repository feature's find by snmp
Data type	String
Default value	.1.3.6.1.2.1.25.2.3.1.1

Parameter[common.repository.snmp.oid.filesystem.type]

Property	common.repository.snmp.oid.filesystem.type
Property name	OID to retrieve Filesystem type for find by snmp of Repository Feature
Description	OID to retrieve Filesystem type value used from repository feature's find by snmp
Data type	String
Default value	.1.3.6.1.2.1.25.2.3.1.2

Parameter [common.ws.address]

Property	common.ws.address
Property name	Hinemos Manager waiting IP address
Description	Waiting IP address for connection from Hinemos Manager or client
Data type	String
Default value	http://0.0.0.0:8080

Parameter [collective.run.shell]

Property	collective.run.shell
Property name	Batch control executing shell
Description	Shell specification when running the batch control feature
Data type	String(ssh / rsh)

Default value	ssh
---------------	-----

Parameter [collective.run.user]

Property	collective.run.user
Property name	Batch control executing shell
Description	User name that login to execute the batch control feature
Data type	String
Default value	root

Parameter [monitor.common.report.event.count]

Property	monitor.common.report.event.count
Property name	Hinemos event download counts
Description	Maximum download counts for a single download feature in Monitor[Event] view
Data type	Integer
Default value	2000

Parameter [monitor.common.report.event.bom]

Property	monitor.common.report.event.bom
Property name	Distribution definitions for the file BOM that occurred with the Hinemos event download
Description	Whether or not to distribute the BOM to the file created by the download feature in the Monitor[Event] view
Data format	Logical (true, false)
Default value	true

Parameter [monitor.common.report.event.separator]

Property	monitor.common.report.event.separator
Property name	Column delimiter for the file BOM that occurred with the Hinemos event download
Description	Adding BOM to the file created by download feature of Monitor[Event] view if this parameter is set true. If this parameter is set false, BOM will not be added to the file.
Data type	String
Default value	true

Parameter [monitor.common.report.event.format]

Property	monitor.common.report.event.format
Property name	Time format of the time for the file BOM that occurred with the Hinemos event download
Description	Time format of the time for the BOM to the file created by the download feature in the Monitor[Event] view
Time format	String (Follow the SimpleDateFormat date/time pattern)
Default value	yyyy/MM/dd HH:mm:ss
Reference	http://docs.oracle.com/javase/jp/7/api/java/text/SimpleDateFormat.html

Parameter [monitor.common.delete.cascade.perfdata]

Property	monitor.common.delete.cascade.perfdata
----------	--

Property name	Determine whether deleting Performance data when deleting monitor settings.
Description	Settings to determine whether deleting collected performance data when deleting the related monitoring settings. When deleting, set this parameter to "on", if not, set this parameter to "off"
Data type	String("on"/"off")
Default value	on

Parameter[monitor.common.retry.interval]

Property	monitor.common.retry.interval
Property name	Retry interval of Resource monitoring and Performance data collection
Description	Retry interval of Resource data collection for Resource monitoring and Performance data collection
Data type	Integer
Default value	1000

Parameter [monitor.common.thread.pool]

Property	monitor.common.thread.pool
Property name	Maximum number of concurrent monitoring threads
Description	Maximum number of threads for monitoring process
Data type	Integer
Default value	50

Parameter[monitor.ping.fping.enable]

Property	monitor.ping.fping.enable
Property name	Use or not use fping for ping monitoring
Description	If using fping module for ping monitoring, set this parameter to "true", if not, set this parameter to "false"
Data type	Logical(true/false)
Default value	true

Parameter[monitor.ping.fping.path]

Property	monitor.ping.fping.path
Property name	path to fping(IPv4) for Ping Monitoring
Description	path to fping(IPv4) for Ping Monitoring
Data type	String
Default value	/opt/hinemos/sbin/fping

Parameter[monitor.ping.fping6.path]

Property	monitor.ping.fping6.path
Property name	path to fping(IPv6) for Ping Monitoring
Description	path to fping(IPv6) for Ping Monitoring
Data type	String
Default value	/opt/hinemos/sbin/fping6

Parameter[monitor.ping.fping.count]

Property	monitor.ping.fping.count
Property name	Number of ICMP packet sent for Ping Monitoring
Description	Number of ICMP packet sent for Ping Monitoring
Data type	Integer
Default value	1

Parameter[monitor.ping.fping.interval]

Property	monitor.ping.fping.interval
Property name	ICMP packet sending interval for Ping Monitoring
Description	ICMP packet sending interval for Ping Monitoring
Data type	Integer
Default value	1000

Parameter[monitor.ping.fping.timeout]

Property	monitor.ping.fping.timeout
Property name	ICMP packet sending timeout value for Ping Monitoring
Description	ICMP packet sending timeout value for Ping Monitoring
Data type	Integer
Default value	1000

Parameter[monitor.ping.fping.bytes]

Property	monitor.ping.fping.bytes
Property name	Number of bytes used for data section of ICMP Packet sent for Ping Monitoring
Description	Number of bytes used for data section of ICMP Packet, which is specified with fping -b option
Data type	Integer
Default value	56

Parameter [monitor.port.protocol.dns]

Property	monitor.port.protocol.dns
Property name	Host name used in DNS operation monitoring for the Service Port Monitor
Description	Host name that is the inquiry target for the DNS operation monitoring for the Service Port Monitor
Data type	String
Default value	localhost

Parameter [monitor.process.start.second]

Property	monitor.process.start.second
Property name	(Process) Interval from the start of the counting process (seconds)
Description	Interval from the start of process information acquisition polling until the result is checked (seconds)
Data type	Integer
Default value	30

Parameter [monitor.process.valid.second]

Property	monitor.process.valid.second
Property name	(Process) Interval of the process information validity (seconds)
Description	Interval from the start of process information acquisition polling until the process information is valid (seconds)
Data type	Integer
Default value	50

Parameter [monitor.resource.start.second]

Property	monitor.resource.start.second
Property name	(Resource) Start interval for the Resource Monitor threshold value judgment processing (seconds)
Description	Interval from the start of resource information acquisition polling until the result is checked
Data type	Integer
Default value	30

Parameter [monitor.resource.valid.second]

Property	monitor.resource.valid.second
Property name	(Resource) Interval of the resource information validity
Description	Interval from the start of resource information acquisition polling until the process information is valid
Data type	Integer
Default value	50

Parameter [monitor.snmp.valid.second]

Property	monitor.snmp.valid.second
Property name	(SNMP) Interval of the SNMP information validity (second(s))
Description	Interval from the start of SNMP monitor polling until the SNMP information is valid (second(s))
Data type	Integer
Default value	10

Parameter [monitor.systemlog.udp.socket.buffer.size]

Property	monitor.systemlog.udp.socket.buffer.size
Property name	(System log) Receiving packet size for the Socket used by the System Log Monitor (Bytes)
Description	Receiving packet size for the Socket used by the System Log Monitor (Bytes)
Data type	Integer
Default value	8388608

Parameter [repository.find.by.snmp.verbose]

Property	repository.find.by.snmp.verbose
Property name	Presence of additional "find by snmp" duplicate device
Description	Devices (disk, nic) registered by find by snmp are those acquired after the OS starts up that have data IN/OUT more than once, but if this parameter is true, the devices that did not have IN/OUT are obtained as well.

Data type	Logic
Default value	false

Parameter [job.open.forward.file.job]

Property	job.open.forward.file.job
Property name	Show or not to show the detail information of file transfer job
Description	If this parameter is set true, the detail information of file transfer job will be shown in Job[Job Detail] view.
Data type	Logical(true/false)
Default value	false

Parameter [performance.graph.max.plot]

Property	performance.graph.max.plot
Property name	Maximum plot count output as a graph of the performance management feature
Description	Maximum plot count output as a graph of the performance management feature if the plot count exceeds the specified range, only the maximum plot count from the start will be displayed in the graph.
Data type	Integer
Default value	10000

Parameter [performance.export.dir]

Property	performance.export.dir
Property name	Work directory used with export of the performance management feature
Description	Work directory used with export of the performance management, feature after the export data is temporarily exported to this directory, it is sent to the Hinemos Client.
Data type	String
Default value	/opt/hinemos/var/export/

Parameter [performance.export.encode]

Property	performance.export.encode
Property name	Character code of the file created in the export of the performance management feature
Description	Character code of the file created in the export of the performance management feature
Data type	String(MS932, UTF-8, EUC_JP)
Default value	MS932

Parameter [performance.export.line.separator]

Property	performance.export.line.separator
Property name	New line code of the file created in the export of the performance management feature
Description	New line code of the file created in the export of the performance management feature
Data type	String(\r\n, \r, \n)
Default value	\r\n

Parameter [performance.export.fetchsize]

Property	performance.export.fetchsize
Property name	Performance Management monitoring export units read from the database
Description	Performance Management monitoring export units read from the database (SELECT Fetch Size)
Data type	Integer
Default value	1000

Parameter [common.notify.command.thread.pool.count]

Property	common.notify.command.thread.pool.count
Property name	Thread pool for running the command used in command notification
Description	Thread pool (number of threads pooled) for running the command used in command notification
Data type	Integer
Default value	8

Parameter [common.notify.command.create.mode]

Property	common.notify.command.create.mode
Property name	OS platform definition for the command operation of the command notification
Description	OS platform definition for the command operation of the command notification
Data type	String (auto, windows, unix, compatible)
Default value	auto

Parameter [common.notify.command.success.exit]

Property	common.notify.command.success.exit
Property name	Normal value for the command return value of the command notification
Description	Normal value for the command return value of the command notification It will be notified as an INTERNAL event when other return values.
Data type	Integer
Default value	0

Parameter [log.line.max.length]

Property	log.line.max.length
Property name	Maximum string length (byte) with the system log monitor's #[LOG_LINE] included
Description	Maximum string length (bytes) with the system log monitor's #[LOG_LINE] included Syslog messages that exceed this length will be truncated and stored in notification messages.
Data type	Integer
Default value	256

Parameter [common.repository.restart.sleep]

Property	common.repository.restart.sleep
Property name	Hinemos Agent update attempt interval (msec)
Description	The Hinemos Agent update carries out the interval for each agent. Define this attempt interval.

Data type	Integer
Default value	500

Parameter [monitor.snmptrap.filter.queue.size]

Property	monitor.snmptrap.filter.queue.size
Property name	Filtering task maximum queue size for the SNMPTRAP monitoring
Description	Filtering task maximum queue size for the SNMPTRAP monitoring If the volume received from the filtering function of the SNMPTRAP monitor becomes large, SNMPTRAP accumulates in this queue and if it exceeds the maximum size, it will be dropped
Data type	Integer
Default value	27000

Parameter [monitor.snmptrap.filter.thread.size]

Property	monitor.snmptrap.filter.thread.size
Property name	Filtering task thread count for the SNMPTRAP monitoring
Description	Filtering task maximum thread count for the SNMPTRAP monitoring
Data type	Integer
Default value	1

Parameter [snmptrap.stats.interval]

Property	snmptrap.stats.interval
Property name	Output interval for the statistical information of SNMPTRAP monitoring
Description	The statistical information is output to a log file when the SNMPTRAP receive count reaches this multiple
Data type	Integer
Default value	100

Parameter [common.notify.replace.before]

Property	common.notify.replace.before
Property name	Setting for replacement of unknown characters included in the SNMPTRAP monitoring varbind
Description	Setting for replacement of unknown characters included in the SNMPTRAP monitoring varbind Define the byte code for characters that are replacement targets.
Data type	String (can be defined as half width comma delimited with multiple byte codes)
Default value	0

Parameter [common.notify.replace.after]

Property	common.notify.replace.after
Property name	Setting for replacement of unknown characters included in the SNMPTRAP monitoring varbind
Description	Setting for replacement of unknown characters included in the SNMPTRAP monitoring varbind If a character that is a replacement target is found, it is replaced with this setting character.
Default format	String(1 byte)
Default value	?

Parameter[common.ws.https.protocol]

Property	common.ws.https.protocol
Property name	Secure protocol of HTTPS Connection
Description	Secure protocol of HTTPS Connection
Data type	String
Default value	TLS
Reference	http://docs.oracle.com/javase/jp/7/technotes/guides/security/SunProviders.html

Parameter[common.ws.https.keystore.path]

Property	common.ws.https.keystore.path
Property name	Directory Path of the Keystore
Description	Directory Path of the Keystore
Data type	String
Default value	/root/keystore

Parameter[common.ws.https.keystore.password]

Property	common.ws.https.keystore.password
Property name	Password of the keystore
Description	Password of the keystore
Data type	String
Default value	hinemos

Parameter[common.ws.https.keystore.type]

Property	common.ws.https.keystore.type
Property name	Type of the Keystore
Description	Type of the Keystore
Data type	String
Default value	PKCS12
Reference	http://docs.oracle.com/javase/jp/7/technotes/guides/security/SunProviders.html

Parameter[common.scheduler.startup.delay]

Property	common.scheduler.startup.delay
Property name	Timing of the scheduler to start
Description	Timing of scheduled processing to start after the start up of java process [sec]
Data type	Integer
Default value	60

Parameter[plugin.sharedtable.keepalive]

Property	plugin.sharedtable.keepalive
Property name	maximum keeping time of data stored in the shared table
Description	maximum keeping time of data stored in the shared table of java process[msec]
Data type	Integer
Default value	60000

Parameter[monitor.snmptrap.listen.address]

Property	monitor.snmptrap.listen.address
Property name	listen address for receiving SNMPTRAP
Description	listen address of java process to receive monitored SNMPTRAP
Data type	String
Default value	0.0.0.0

Parameter[monitor.snmptrap.listen.port]

Property	monitor.snmptrap.listen.port
Property name	listen port number for receiving SNMPTRAP
Description	listen port number of java process to receive monitored SNMPTRAP
Data type	Integer
Default value	162

Parameter[monitor.snmptrap.filter.queue.size]

Property	monitor.snmptrap.filter.queue.size
Property name	Maximum number of SNMPTRAP to be cued for SNMPTRAP Monitoring
Description	Maximum number of SNMPTRAP to be cued for processing of SNMPTRAP Monitoring
Data type	Integer
Default value	27000

Parameter[monitor.snmptrap.filter.thread.size]

Property	monitor.snmptrap.filter.thread.size
Property name	Maximum number of threads for processing SNMPTRAP Monitoring
Description	Maximum number of threads for processing SNMPTRAP Monitoring
Data type	Integer
Default value	1

Parameter[monitor.systemlog.listen.address]

Property	monitor.systemlog.listen.address
Property name	listen address for receiving syslog
Description	listen address of java process to receive monitored syslog
Data type	String
Default value	0.0.0.0

Parameter[monitor.systemlog.listen.port]

Property	monitor.systemlog.listen.port
Property name	listen port number for receiving syslog
Description	listen port number of java process to receive monitored syslog
Data type	Integer
Default value	24514

Parameter[monitor.systemlog.filter.queue.size]

Property	monitor.systemlog.filter.queue.size
Property name	Maximum number of syslog to be cued for Systemlog Monitoring
Description	Maximum number of syslog to be cued for processing of Systemlog Monitoring
Data type	Integer
Default value	27000

Parameter[monitor.systemlog.filter.thread.size]

Property	monitor.systemlog.filter.thread.size
Property name	Maximum number of threads for processing Systemlog Monitoring
Description	Maximum number of threads for processing Systemlog Monitoring
Data type	Integer
Default value	1

Parameter[agent.ws.threadpool.size]

Property	agent.ws.threadpool.size
Property name	Maximum number of threads for processing requests from Hinemos Agent
Description	Maximum number of threads for processing requests from Hinemos Agent
Data type	Integer
Default value	8

Parameter[agent.ws.queue.size]

Property	agent.ws.queue.size
Property name	Maximum number of request from Hinemos Agent to be cued for processing
Description	Maximum number of request from Hinemos Agent to be cued for processing
Data type	Integer
Default value	1200

Parameter[agent.ws.shutdown.timeout]

Property	agent.ws.shutdown.timeout
Property name	Timeout value for processing requests from Hinemos Agent
Description	Timeout value for processing requests from Hinemos Agent
Data type	Integer
Default value	60000

Parameter[common.ws.threadpool.size]

Property	common.ws.threadpool.size
Property name	Maximum number of threads to process requests from Hinemos Agent
Description	Maximum number of threads to process requests from Hinemos Agent
Data type	Integer
Default value	4

Parameter[common.ws.queue.size]

Property	common.ws.queue.size
----------	----------------------

Property name	Maximum number of requests from components other than Hinemos Agent, to be cued for processing
Description	Maximum number of requests from components other than Hinemos Agent, to be cued for processing
Data type	Integer
Default value	300

Parameter[common.ws.shutdown.timeout]

Property	common.ws.shutdown.timeout
Property name	Timeout value for processing requests from components other than Hinemos Agent
Description	Timeout value for processing requests from components other than Hinemos Agent
Data type	Integer
Default value	10000

Parameter[common.internal.syslog]

Property	common.internal.syslog
Property name	INTERNAL event to be sent out as syslog
Description	If sending INTERNAL event out as syslog, set true for this parameter. If not, set false for this parameter.
Data type	Logical(true/false)
Default value	false

Parameter[common.internal.syslog.priority]

Property	common.internal.syslog.priority
Property name	Priority of syslog when sending out INTERNAL event as syslog
Description	Priority of syslog when sending out INTERNAL event as syslog
Data type	String
Default value	info

Parameter[common.internal.syslog.host]

Property	common.internal.syslog.host
Property name	Host to send INTERNAL event as syslog
Description	Host to send INTERNAL event as syslog
Data type	String
Default value	192.168.1.1,192.168.1.2

Parameter[common.internal.syslog.port]

Property	common.internal.syslog.port
Property name	Port to send INTERNAL event as syslog
Description	Port to send INTERNAL event as syslog
Data type	String
Default value	514

Parameter[common.internal.syslog.facility]

Property	common.internal.syslog.facility
Property name	facility of syslog when sending out INTERNAL event as syslog
Description	facility of syslog when sending out INTERNAL event as syslog
Data type	String
Default value	daemon

Parameter[common.internal.syslog.severity]

Property	common.internal.syslog.severity
Property name	severity of syslog when sending out INTERNAL event as syslog
Description	severity of syslog when sending out INTERNAL event as syslog
Data type	String
Default value	alert

Parameter[common.internal.event]

Property	common.internal.event
Property name	INTERNAL event to be shown in Monitor[Event] view
Description	If INTERNAL event to be shown in Monitor[Event] view, set "true" for this parameter. If not, set "false".
Data type	Logical(true/false)
Default value	true

Parameter[common.internal.event.priority]

Property	common.internal.event.priority
Property name	Priority of Internal event shown in the Monitor[Event] view
Description	Priority of Internal event shown in the Monitor[Event] view
Data type	String
Default value	info

Parameter[common.internal.file]

Property	common.internal.file
Property name	INTERNAL event to be outputted to an log file.
Description	If outputting an INTERNAL event to an log file, set "true" for this parameter. If not, set "false".
Data type	Logical(true/false)
Default value	true

Parameter[common.internal.file.priority]

Property	common.internal.file.priority
Property name	Priority of INTERNAL event when logging out to a log file.
Description	Priority of INTERNAL event when logging out to a log file.
Data type	String
Default value	info

Parameter[common.internal.mail]

Property	common.internal.mail
Property name	INTERNAL event to be sent out as mail.
Description	If sending out INTERNAL event as mail, set "true" for this parameter. If not, set "false".
Data type	Logical(true/false)
Default value	false

Parameter[common.internal.mail.priority]

Property	common.internal.mail.priority
Property name	Priority of INTERNAL event when sending out a mail.
Description	Priority of INTERNAL event when sending out a mail.
Data type	String
Default value	info

Parameter[common.internal.mail.address]

Property	common.internal.mail.address
Property name	Mail address to send mail when sending out INTERNAL event as a mail.
Description	Mail address to send mail when sending out INTERNAL event as a mail.
Data type	String
Default value	user1@host.domain,user2@host.domain

Parameter[common.internal.command]

Property	common.internal.command
Property name	Execute an command when INTERNAL event has been outputted.
Description	If executing a command when INTERNAL event has been outputted, set "true" for this parameter. If not, set "false"
Data type	Logical(true/false)
Default value	false

Parameter[common.internal.command.priority]

Property	common.internal.command.priority
Property name	Priority of INTERNAL event when executing a command triggered by INTERNAL event.
Description	Priority of INTERNAL event when executing a command, triggered by the output of INTERNAL event.
Data type	String
Default value	info

Parameter[common.internal.command.user]

Property	common.internal.command.user
Property name	Execution user of an command triggered by INTERNAL event.
Description	Execution user of an command triggered by the output of INTERNAL event.
Data type	String
Default value	root

Parameter[common.internal.command.commandline]

Property	common.internal.command.commandline
Property name	Executed command triggered by INTERNAL event.
Description	Executed command triggered by the output of INTERNAL event.
Data type	String
Default value	echo #[GENERATION_DATE] #[MESSAGE] >> /tmp/test.txt

Parameter[common.internal.command.timeout]

Property	common.internal.command.timeout
Property name	Timeout value for command triggered by INTERNAL event.
Description	Timeout vlaue for command triggerd by the output of INTERNAL event.
Data type	Integer
Default value	15000

14 Hinemos Agent Configuration List

Hinemos Agent settings are defined with the following setting files.

- /opt/hinemos_agent/conf/Agent.properties (Linux Agent)
- [Hinemos Agent install directory]\conf\Agent.properties (Windows Agent)

(If multi-byte characters are used in the properties file, the property file needs to be edited.)

The Hinemos Agent must be restarted for the configuration changes to be reflected.

Parameter[common.invalid.char.replace]

Property	common.invalid.char.replace
Property Name	replacement rule of control character in original message
Description	If this parameter is true, control character in original message will be replaced with a character designated in common.invalid.char.replace.to. If this parameter is false, control character in original message will be replaced with hexadecimal numeration.
Data type	String
Default value	false

Parameter[common.invalid.char.replace.to]

Property	common.invalid.char.replace.to
Property Name	character to be replaced with control character in original message.
Description	When common.invalid.char.replace is set true, control character in original message will be replaced with a character designated in this parameter.
Data type	String
Default value	?

Parameter [end.message.resend.interval]

Property	end.message.resend.interval
Property name	Time interval to resend a job ending message(sec)
Description	Time interval to resend a job ending message when it fail
Data type	Integer
Default value	30

Parameter [runhistory.clear.delay]

Property	runhistory.clear.delay
Property name	Maximum lifetime (seconds) for the job information received from Hinemos Manager
Description	Maximum lifetime (seconds) for the job information received from Hinemos Manager
Data type	Integer
Default value	604800

Parameter [limit.size.jobmsg]

Property	limit.size.jobmsg
Property name	Maximum byte count handled for the job execution results (standard output, standard error output)
Description	Maximum byte count handled for the job execution results (standard output, standard error output)
Data type	Integer

Default value	1024
---------------	------

Parameter [limit.size.logmsg]

Property	limit.size.logmsg
Property name	Maximum bytes of message monitored by Logfile Monitor/Windows Event Monitor
Description	Maximum bytes of message in monitored result of Logfile Monitor/Windows Event Monitor. If in Logfile Monitor, this maximum bytes are used to read 1 row of log message, and the rest of the message will be cut off.
Data type	Integer
Default value	1024

Parameter [input.encoding]

Property	input.encoding
Property name	Job standard input/output, character code for standard error handling
Description	Standard input/output during job execution, character code for standard error handling
Data type	String
Default value	Hinemos Agent(Linux) : UTF-8,Hinemos Agent(Windows) : MS932

Parameter [command.create.mode]

Property	command.create.mode
Property name	Start command operation mode
Description	OS platform identification (&compatibility mode) during the job execution
Data type	String (auto, unix, windows, compatible)
Default value	auto

Parameter [logfile.run.interval]

Property	logfile.run.interval
Property name	File check interval for the Monitor Logfile (msec)
Description	File check interval for the Monitor Logfile (msec)
Data type	Integer
Default value	10000

Parameter [unchanged.stats.period]

Property	unchanged.stats.period
Property name	Time interval to check the changing file name(sec)
Description	Time interval to check the file switchover the file size does not change during the specified time
Data type	Integer
Default value	5

Parameter [file.max.size]

Property	file.max.size
Property name	Maximum file size(bytes)

Description	Maximum file size threshold subject to Monitor Logfile (when a warning event is occurring)
Data type	Integer
Default value	2147483648

Parameter [syslog.message.priority]

Property	syslog.message.priority
Property name	syslog priority used in the log transfer feature (common to log file transfer features)
Description	Setting for the message added to the log file to be transferred to the syslog. By defining the priority of the syslog, you can have compatible operations for the existing log file transfer feature. If there is no definition, it will not be transferred by the syslog.
Data type	String
Default value	Not defined

Parameter [log.file.encoding]

Property	log.file.encoding
Property name	Encoding the reading log file
Description	Specified encoding when reading log file (one type is fixed by the Hinemos Agent)
Data type	String(MS932, UTF-8, EUC_JP)
Default value	Linux Agent: UTF-8, Windows Agent: MS932

Parameter [log.line.separator]

Property	log.line.separator
Parameter	Newline character of logfile
Description	Newline character of logfile when reading the logfile (1 fixed character can be designated per Hinemos Agent)
Data type	String
Default value	LF

Parameter [log.msg.program]

Property	log.msg.program
Property name	Program name that transfers the log message
Description	Program name that transfers syslog log message
Data type	String
Default value	hinemos_agent

Parameter [collector.command.workerthreads]

Property	collector.command.workerthreads
Property name	Maximum thread count for running commands with custom monitoring
Description	Maximum thread count for running commands with custom monitoring
Data type	Integer
Default value	8

Parameter [collector.command.mode]

Property	collector.command.mode
Property name	OS platform definition for the command operation of the custom monitoring
Description	OS platform definition for the command operation of the custom monitoring
Data type	String (auto, unix, windows, compatible)
Default value	auto

Parameter [collector.command.buffer]

Property	collector.command.buffer
Property name	Maximum size for standard output read with custom monitoring (bytes)
Description	Maximum size for standard output read with custom monitoring (bytes)
Data type	Integer
Default value	512

Parameter [collector.command.charset]

Property	collector.command.charset
Property name	Defined character code for standard output with custom monitoring
Description	Defined character code for standard output with custom monitoring
Data type	String(MS932, UTF-8, EUC_JP)
Default value	Linux Agent: UTF-8, Windows Agent: MS932

Parameter [collector.command.returncode]

Property	collector.command.returncode
Property name	Defined new line code for standard output with custom monitoring
Description	Defined new line code for standard output with custom monitoring
Data type	String (LF, CRLF, CR)
Default value	Linux Agent: LF, Windows Agent: CRLF

Parameter[filecheck.run.interval]

Property	filecheck.run.interval
Property Name	Execution interval of job filecheck
Description	Execution interval of job filecheck(msec)
Data type	Integer
Default value	10000

Parameter[collector.winevent.interval]

Property	collector.winevent.interval
Property Name	Monitoring interval of Windows Event Monitor
Description	Monitoring interval of Windows Event Monitor(msec)
Data type	Integer
Default value	10000

Parameter[collector.winevent.timeout]

Property	collector.winevent.timeout
----------	----------------------------

Property Name	Command timeout of Windows Event Monitor
Description	Command timeout of event retrieving command for Windows Event Monitor(msec). Set -1 to disable timeout.
Data type	Integer
Default value	-1

Parameter[collector.winevent.buffer]

Property	collector.winevent.buffer
Property Name	Buffer size of Windows Event monitor
Description	Buffer size to store standard output of event log retrieving command, for Windows Event monitor(byte).
Data type	Integer
Default value	1000000

Parameter[collector.winevent.maxevents]

Property	collector.winevent.maxevents
Property Name	Maximum event log collected by event log retrieving command.
Description	Maximum event log collected by event log retrieving command used for Windows Event Log monitor. This setting will be unlimited when "-1" is specified.
Data type	Integer
Default value	Windows Server 2008/2012 : -1 Windows Server 2003 : 1000

Parameter[collector.winevent.mode]

Property	collector.winevent.mode
Property Name	Event log retrieving mode for Windows Event monitor.
Description	Event log retrieving mode for Windows Event monitor.
Data type	String(auto, get-winevent, get-eventlog, wevtutil)
Default value	auto
Other	auto : automatically decided by OS (Windows Server 2008/2012 : wevtutil、 Windows Server 2003 : get-eventlog) get-winevent : Use Get-WinEvent commandlet http://technet.microsoft.com/en-us/library/hh849682.aspx get-eventlog : Use Get-EventLog commandlet http://technet.microsoft.com/en-us/library/hh849834.aspx wevtutil : use wevtutil.exe command

Parameter[collector.winevent.return.char.replace]

Property	collector.winevent.return.char.replace
Property Name	Character replaced for newline character in Windows Event monitor.
Description	Character replaced for newline character in Windows Event monitor.
Data type	String
Default value	#n;

Parameter[collector.winevent.gt.char.replace]

Property	collector.winevent.gt.char.replace
Property Name	Character replaced for "<" in Windows Event monitor.

Description	Character replaced for "<" in Windows Event monitor.
Data type	String
Default value	#gt;

Parameter[collector.winevent.lt.char.replace]

Property	collector.winevent.lt.char.replace
Property Name	Character replaced for ">" in Windows Event monitor.
Description	Character replaced for ">" in Windows Event monitor.
Data type	String
Default value	#lt;

Parameter [user]

Property	user
Property name	User to login to Hinemos Manager
Description	User to login to Hinemos Manager
Data type	String
Default value	HINEMOS_AGENT

Parameter [password]

Property	password
Property name	Password to login to Hinemos Manager
Description	Password to login to Hinemos Manager
Data type	String
Default value	HINEMOS_AGENT

Parameter [managerAddress]

Property	managerAddress
Property name	URL for connecting to the Hinemos Manager
Description	URL for connecting to the Hinemos Manager
Data type	String
Default value	http://[Hinemos Manager's IP address]:8080/HinemosWS/

Parameter [topic.interval]

Property	topic.interval
Property name	Hinemos Manager polling interval (msec)
Description	Hinemos Manager polling interval (msec)
Data type	Integer
Default value	30000

Parameter [connect.timeout]

Property	connect.timeout
Property name	Connection timeout to Hinemos Manager (sec)
Description	Timeout time when connecting to the Hinemos Manager

Data type	Integer
Default value	10

Parameter [request.timeout]

Property	request.timeout
Property name	Receive timeout from the Hinemos Manager (sec)
Description	Timeout time when receiving from the Hinemos Manager
Data type	Integer
Default value	60

Parameter[awake.port]

Property	awake.port
Property Name	port for instantly reflecting packet
Description	Port number to receive instantly reflecting packet from Hinemos Manager If this parameter is changed from its default value, the repository information of its node (Hinemos Agent – Awake Port) must be changed.
Data type	Integer
Default value	24005

Parameter [facilityId]

Property	facilityId
Property name	Facility ID for the node that supports Hinemos Agent
Description	Facility ID for the node that supports Hinemos Agent If it is not defined, the corresponding node will be identified from the host name and the IP address. If it is defined, the facility ID is fixed.
Data type	String
Default value	Not defined

Parameter [first.part.data.check.period]

Property	first.part.data.check.period
Property name	File first part check period setting (seconds)
Description	Even when there is no change in the file size in the specified seconds, this is the interval to invoke the feature to check the file size
Data type	Integer
Default value	300

Parameter [first.part.data.check.size]

Property	first.part.data.check.size
Property name	Comparison byte count for file first part check
Description	Comparison byte count for file first part check
Data type	Integer
Default value	256

Parameter [notify.retry.count]

Property	notify.retry.count
----------	--------------------

Property name	Maximum attempt count for send processing of the results of Monitor Logfile
Description	Maximum attempt count for send processing of the results of Monitor Logfile
Data type	Integer
Default value	15

Parameter [notify.retry.sleep]

Property	notify.retry.sleep
Property name	Interval for send processing of the results of Monitor Logfile (msec)
Description	Interval for send processing of the results of Monitor Logfile (msec)
Data type	Integer
Default value	60000

Parameter [file.transfer.skip.keyfile.update]

Property	file.transfer.skip.keyfile.update
Property name	Enabling/disabling key file edit skip when running file transfer jobs
Description	When this parameter is true, the file transfer job will run without editing the authorized_key with the Hinemos Agent. The user must register the public key for the file transfer destination in the authorized_key for the file transfer source in advance.
Data type	Logic
Default value	false

Parameter[http.proxy.host]

Property	http.proxy.host
Property Name	IP address or a host name of HTTP Proxy server
Description	IP address or a host name of HTTP Proxy server
Data type	String
Default value	—

Parameter[http.proxy.port]

Property	http.proxy.port
Property Name	listen port of HTTP Proxy server
Description	listen port of HTTP Proxy server
Data type	Integer
Default value	—

Parameter[http.proxy.user]

Property	http.proxy.user
Property Name	Username for HTTP Proxy server
Description	Username for HTTP Proxy server
Data type	String
Default value	—

Parameter[http.proxy.password]

Property	http.proxy.password
----------	---------------------

Property Name	User Password for HTTP Proxy server
Description	User Password for HTTP Proxy server
Data type	String
Default value	—

15 ChangeLog

ChangeLog

Version	Date	Details
Edition 1.0	10/01/2013	First release

Hinemos Ver. 4.1 Administrator's Guide

Not for sale

- Unauthorized duplication prohibited
- Unauthorized reproduction prohibited
- Unauthorized redistribution prohibited

Hinemos is a registered trademark of NTT DATA CORPORATION.

Linux is a trademark/registered trademark of Linus Torvalds world-wide.

In addition, companies and product names described in this document are trademarks and/or registered trademarks of the respective companies. This holds true even when the TM and R marks are not noted in this manual.