Hinemos ver.5.0

Administrator's Guide, 2nd Edition

Contents

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 dump file

  ```
  hinemos_restore.sh
  ```

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

  ```
  hinemos_clear_tmp.sh
  ```

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

  ```
  hinemos_clear_notify.sh
  ```

- Acquire environment summary information

  ```
  hinemos_manager_summary.sh
  ```

- Reset scheduler

  ```
  hinemos_reset_scheduler.sh
  ```

- Import/export a file for Infrastructure Management

  ```
  hinemos_infra_file.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 Outline and Prerequisites for Running of Maintenance Script

Process details	Script Name	JVM	PostgreSQL
Delete unnecessary data	hinemos_delete.sh	Must be stopped	Must be running

Reconstructing the database	hinemos_cluster_db.sh	Must be stopped	Must be running
Backing-up the database	hinemos_backup.sh	Don't care	Must be running
Restoring the database	hinemos_restore.sh	Must be stopped	Must be running
Delete the temporary queue	hinemos_clear_tmp.sh	Must be stopped	Must be running
Delete the notification	hinemos_clear_notify.sh	Must be running	Must be running
Acquire environment summary	hinemos_manager_summary.sh	Must be running	Must be running
Reset scheduler	hinemos_reset_scheduler.sh	Must be stopped	Must be running
Import/export file for Infrastructure Management	hinemos_infra_file.sh	Must be stopped	Must be running

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
- 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. Stop JVM and leave only the PostgreSQL running.

```
(root) # /opt/hinemos/bin/jvm_stop.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 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 JVM.

```
(root) # /opt/hinemos/bin/jvm_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 3.1.3 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. Stop JVM and leave only the PostgreSQL running.

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

2. Run the maintenance script.

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

3. Start JVM.

```
(root) # /opt/hinemos/bin/jvm_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. If -s option is specified, only the set data is backed up. If -c option is specified, a gz-compressed dump file can be created. (Argument 0 to 9 must be specified for -c option. The value means a level of compression. The higher the value is, the higher the compression rate.)

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

   ```
   (root) # ls
   hinemos_pgdump.YYYY-MM-DD_HHmmss
   (hinemos_pgdump_s.YYYY-MM-DD_HHmmss if -s option is specified.)
   ```

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 3.1.5 Backing-up the Database , run hinemos_restore.sh.

1. Stop JVM and leave only the PostgreSQL running.

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

2. Run the maintenance script.

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

3. Start JVM.

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

hinemos_pgdump_s.YYYY-MM-DD_HHmmss can also be restored by using hinemos_restore.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. Stop JVM and leave only the PostgreSQL running.

```
(root) # /opt/hinemos/bin/jvm_stop.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 JVM.

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

3.1.8 Deleting the Notification History

Run hinemos_clear_notify.sh to delete the notification history that satisfied with the suppression standard.

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
```

- To acquire the MD5 hash of a file subordinate to Hinemos Manager

```
(root) # /opt/hinemos/sbin/mng/hinemos_manager_summary.sh -md5
```

3.1.10 Scheduler Adjustment after Changing OS Clock Setting

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) # service hinemos_manager stop
```

2. Change clock setting of the OS where 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
```

   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.

5. Restart Hinemos Manager after stopping PostgreSQL.

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

3.2 Importing/Exporting File for Infrastructure Management

Files using in Infrastructure Management can be imported or exported in Hinemos Client, which can also be done by running hinemos_infra_file.sh.

The following steps show how to import a file to Infrastructure Management.

1. Stop JVM and leave only the PostgreSQL running.

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

2. Run the import/export script.

```
(root) # /opt/hinemos/sbin/mng/hinemos_infra_file.sh import FILE_ID FILE_PATH OWNER_ROLE_ID
```

   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 JVM.

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

The following steps show how to export a file from Infrastructure Management.

1. Stop JVM and leave only the PostgreSQL running.

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

2. Run the import/export script.

```
(root) # /opt/hinemos/sbin/mng/hinemos_infra_file.sh export FILE_ID
```

   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 JVM.

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

3.3 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.

3.3.1 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 Directory

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

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/
```

3.3.2 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

3.3.3 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\Client5.0\	Hinemos Client log file

3.3.4 Hinemos Web Client Log Files

Log files of Hinemos Web Client are output to the directory shown in Table 3-6.

Table 3-6 List of Hinemos Web Client Log Directory

Path	Content
/opt/hinemos_web/var/log/	Log files output by Tomcat and Hinemos Web Client

For Hinemos Web Client, the following script is provided to delete expired log files which are older than a specified period (31 days) after the last update.

- /opt/hinemos_web/contrib/hinemos_web

In order to run this script every day, copy the cronjob file into /etc/cron.daily/ as shown below.

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

3.4 Backing-up/Recovering the Hinemos Manager

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

3.4.1 Backing-up the Hinemos Manager

- Database backup

  Acquire the dump file according to 3.1.5 Backing-up the Database .

- Backup configuration files (setting 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 setting 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
  - rsyslog setting file
    - /etc/rsyslog.d/rsyslog_hinemos_manager.conf

3.4.2 Recover 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 3.1.5 Backing-up the Database and restore following the procedures in 3.1.6 Restoring the Database .

3. Apply the configuration files

   Apply 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)

3.5 Backing-up/Recovering the Hinemos Agent

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

3.5.1 Backup the Hinemos Agent

Linux Agent

- Backup configuration files (setting 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 setting file
    - All files under /opt/hinemos_agent/conf/
  - Service script (when added as a service)
    - /etc/init.d/hinemos_agent
  - rsyslog setting file
    - /etc/rsyslog.d/rsyslog_hinemos_agent.conf
  - snmp setting file
    - /etc/snmp/snmpd.conf

Windows Agent

- Backup configuration files (setting 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 setting 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)

3.5.2 Recover 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. Apply 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 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)

Windows Agent

1. Reconfigure the SNMP Service

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

3.6 Backing-up/Recovering the Hinemos Rich Client

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

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

3.7 Backing-up/Recovering the Hinemos Web Client

The following shows how to backup and recover the Hinemos Web Client.

3.7.1 Backup the Hinemos Web Client

- Backup configuration files (setting files, 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 Web Client setting files
    - All files under /opt/hinemos_web/conf/
  - Service script (when added as a service)
    - /etc/init.d/hinemos_web
  - log file cleanup script
    - /etc/cron.daily/hinemos_web

3.7.2 Recover the Hinemos Web Client

1. Reinstall the Hinemos Web Client

   Install Hinemos Web Client. If a Hinemos Web Client is already installed, uninstall it at first and then install again.

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

2. Apply the configuration files

   Apply 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 Web Client. (The application method depends on the file type and the setting file parameters)

4 OS Environment

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 ulimit value assigned in the Java process)

- /opt/hinemos/hinemos.cfg

```
export JAVA_FD_MAXNUM=4098
```

Hinemos Manager must be restarted in order to reflect configuration changes on this property file.

4.2 Java Heap Memory Settings (Hinemos Manager)

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 -Xss25
# for large systems
#export JVM_HEAP_OPTS="-Xms2048m -Xmx2048m -XX:NewSize=640m -XX:MaxNewSize=640m -XX:MaxPermSize=360m -Xss25
```

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 in order to reflect configuration changes on this property file.

4.3 Maximum of Concurrent Connection (Web Client)

The maximum number of concurrently connecting browsers to a Web Client are limited by default (the default is 8 browsers) Modify the following configuration file to change the maximum.

- /opt/hinemos_web/conf/hinemos_web.cfg

```
### JVM - Maximum number of access users
export JVM_MAX_USER_OPTS="-Dmaximum.access.users=8"
```

For instance, if there are requests from 16 browsers concurrently, change "maximum.access.users=8" to " maximum.access.users=16".

- /opt/hinemos_web/conf/server.xml

```
<Connector port="80" protocol="HTTP/1.1"
        connectionTimeout="20000"
        redirectPort="8443"
```

```
        maxThreads="32"
        />
```

The value of "maxThreads" in server.xml should be set to 4 times as the value of "maximum.access.users" in hinemos_web.cfg. For instance, if there are requests from 16 browsers concurrently, you should specify as " maxThreads=64".

/opt/hinemos_web/conf/hinemos_web.cfg

```
### JVM - Performance Tuning
# for small systems
JVM_HEAP_OPTS="-Xms256m -Xmx256m -XX:NewSize=40m -XX:MaxNewSize=40m -XX:MaxPermSize=128m -Xss256k"
# for medium systems
#JVM_HEAP_OPTS="-Xms512m -Xmx512m -XX:NewSize=40m -XX:MaxNewSize=40m -XX:MaxPermSize=128m -Xss256k"
# for large systems
#JVM_HEAP_OPTS="-Xms1024m -Xmx1024m -XX:NewSize=40m -XX:MaxNewSize=40m -XX:MaxPermSize=128m -Xss256k"
```

It is recommended to use "medium" setting for 10 or more browsers, and "large" for 20 or more browsers. For instance, if there are requests from 16 browsers concurrently, the "medium" setting will be suitable.

4.4 Configuring OS Locale and Character Encoding

4.4.1 Hinemos Rich Client

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

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

4.4.2 Hinemos Web Client

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

The Hinemos Web Client operates where the OS locale is presumed to be ja_JP.UTF-8. This setting can be confirmed in /opt/hinemos_web/hinemos_web.cfg.

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

4.4.3 Hinemos Manager

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.

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

4.4.4 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. Furthermore, this can only be specified per Hinemos Agent process unit, and not per job settings.

  This character code is specified in the Agent.properties job.stream.charset parameter. This parameter can be selected from UTF-8, EUC-JP and MS932. If job.stream.charset 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 (uFFFD).

  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
  job.stream.charset=EUC-JP
  ```

  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 Specifying Facility ID for Hinemos Agent

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
```

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

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, select Maintenance perspective of Hinemos Client and open Maintenance [Hinemos property] view, and change the following parameter:

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

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. The setting of Email Notification can be found in Maintenance perspective.

Configuring the Mail Server

Configure the mail server used for the mail notification feature.

```
mail.smtp.host=[SMTP Server's IP address or host name]
mail.smtp.port=[SMTP Server's listen port number]
mail.tranport.tries=[number of maximum attempts to send mail to SMTP Server]
mail.tranport.tries.interval=[interval time between retrial of sending mail to SMTP Server [msec]]
mail.from.address=[Mail address of the sender]
mail.from.personal.name=[Mail sender's Name]
mail.reply.to.address=[Mail address to reply To]
mail.reply.personal.name=[Name of the reply mail receiver]
mail.errors.to.address=[Mail address to be set to the Sent mail's Error-To Header]
mail.charset.address=UTF-8
mail.charset.subject=UTF-8
mail.charset.content=UTF-8
```

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 ".".

5.2.2 Configuring SMTP AUTH

To use an SMTP server that needs SMTP AUTH to notify a mail, select Maintenance perspective of Hinemos Client and open Maintenance [Hinemos Property] view, and set the following parameter:

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

```
mail.transport.user=[user name used for authentication]
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.

5.2.3 SSH/TLS Settings

To use an SMTP server that needs SSL/TLS(STARTTLS) to notify a mail, select Maintenance perspective of Hinemos Client and open Maintenance [Hinemos Property] view, and change the following parameter:

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

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 6.3 HTTPS Monitor .

5.2.4 Setting Envelope-From Address

To set an argument that is passed over to the MAIL command of SMTP when a mail is notified, select Maintenance perspective of Hinemos Client and open Maintenance [Hinemos Property] view, and change the following parameter:

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

5.3 Log Escalation Notification

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

5.3.1 Setting Embedded Hostname

By selecting Maintenance perspective of Hinemos Client, opening Maintenance [Hinemos Property] view, and changing parameter notify.log.escalate.manager.hostname, the host name included in the header part of the syslog (RFC3164) the Hinemos Manager sends can be flexibly configured.

```
notify.log.escalate.manager.hostname=#[NODE]
```

Table 5-1 Possible Value for the syslog Host Name (notify.log.escalate.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	<PRI> Mmm dd hh:mm:ss facilityid 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

6 Monitor Settings / Performance Feature

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

6.1 SQL Monitor

6.1.1 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. Editing Hinemos property

   Add information on RDBMS to be added by selecting Maintenance perspective of Hinemos Client and Maintenance [Hinemos Property] view.

   First, increase the number of monitor.sql.jdbc.driver 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)

   ```
   monitor.sql.jdbc.driver = 4
   ```

   Also, add information related to the new RDBMS and JDBC Driver (Select "String" as the Hinemos Property Type).

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

   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.

6.2 Process Monitor

6.2.1 Handling when "Failed to get value" Notification Occurs

The following 2 processes run asynchronously with process monitor. (Refer to Figure 6-1)

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

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

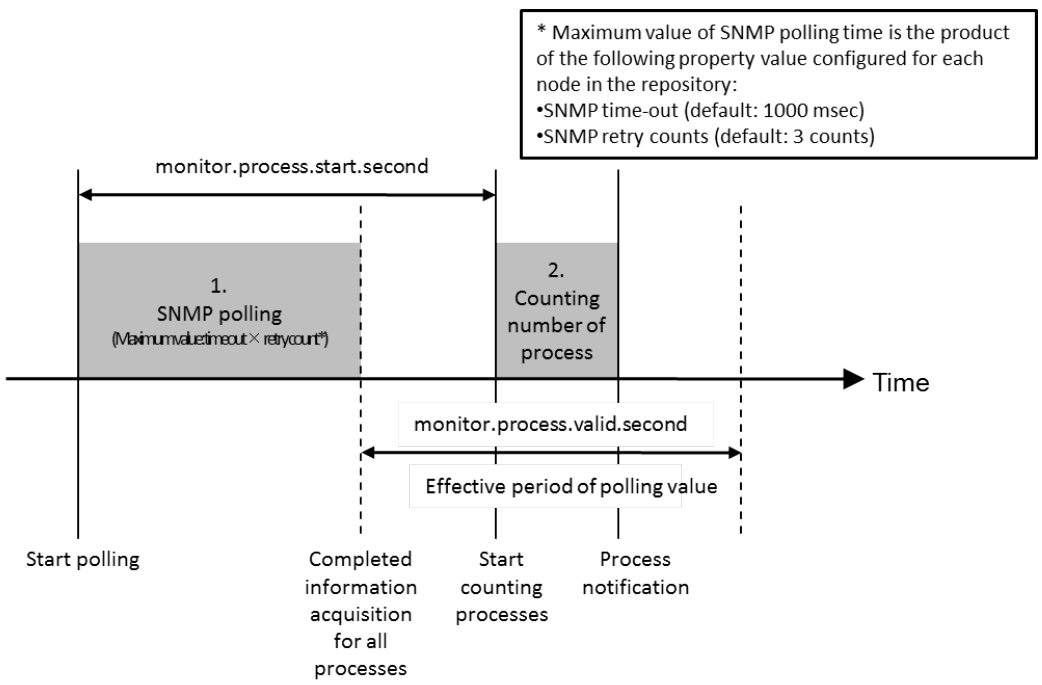

Figure 6-1 Handling Process Monitor

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 " Timeout".

To change the parameter, select Maintenance perspective of Hinemos Client and open Maintenance [Hinemos Property] view, and change the following parameter:

```
## 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
```

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.

6.3 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

1. 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 an 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

- Hinemos Manager does not have to be restarted. To “specify the keystore file in the java start up option” in step 3, however, Hinemos Manager must be restarted.

Details of steps 1-3 are listed below.

6.3.1 Preparing Certificate

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

6.3.2 Registering Certificate to Keystore

Register the server certificate in /opt/hinemnos/. 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).

```
(hinemos) $ su - root
(root) # /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=
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

6.3.3 Specifying Keystore File in 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_OPTS parameter of /opt/hinemos/hinemos.cfg file, where

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

- After changing the configuration, Hinemos Manager must be restarted.

6.4 System Log Monitor

6.4.1 Settings for Sending Syslog

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
```

6.4.2 Settings for Receiving Syslog

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.d/rsyslog_hinemos_manager.conf

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

The waiting address and port number used when syslog is transferred from rsyslog to Hinemos Manager (java) can be changed by selecting Maintenance perspective of Hinemos Client and Maintenance [Hinemos Property] view.

```
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]
```

Hinemos Manager must be restarted in order to reflect the configuration change.

6.4.3 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 6-1. An example of the escape log is shown in Table 6-2.

Table 6-1 Example of the Escape Control Code

Control code	String after replacement
NUL	#000
BEL	#007

Table 6-2 Example of the Escape Log (the control character NUL is represented as [NUL])

String received from rsyslog HTTP/1.0[NUL] 50	HTTP/1.0[NUL] 50
String transferred to the Hinemos Manager from rsyslog HTTP/1.0#000 50	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.d/rsyslog_hinemos_manager.conf of the Hinemos Manager server.

   Add the following settings to /etc/rsyslog.d/rsyslog_hinemos_manager.conf.

   ```
   $EscapeControlCharactersOnReceive off
   ```

2. Restart rsyslog.

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

6.4.4 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.

1. 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"
   ```

2. Restart rsyslog.

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

6.5 SNMPTRAP Monitor

6.5.1 Settings for Receiving SNMPTRAP

For the waiting address and port number of the manager server used when SNMPTRAP sent from an external device, change the following parameter by selecting Maintenance perspective of Hinemos Client and opening Maintenance [Hinemos Property] view:

```
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]
```

6.5.2 Default MIB

MIB registered in the master data of Hinemos Manager is listed in Table 6-3 .

Table 6-3 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
GWOVVMMIB	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	ASYNCOS-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
SIPXECS-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

6.6 Windows Service Monitor

6.6.1 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 or Windows 7, WinRM 2.0 is installed by default, and if the OS of the monitored node is Windows Server 2012, 2012 R2, Windows 8 or 8.1, 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.

6.6.2 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
```

6.6.3 Basic Confirmation Authorization

Run the following command and authorize basic confirmation.

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

6.6.4 Unencrypted Transmission Authorization

Run the following command and authorize unencrypted transmission by HTTP.

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

6.6.5 HTTPS Settings

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 6.3.2 Registering Certificate to Keystore and 6.3.3 Specifying Keystore File in Java Startup Options and register the certificate in the Hinemos Manager's keystore.

4. Restart the Hinemos Manager

*Hinemos Manager must be restarted only if the keystore file is specified for the Java startup option. Only when registering the certificate to the keystore, restart of Hinemos Manager is not requied.

6.6.6 Creating Access 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.

6.6.7 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
```

6.7 Custom Monitor

6.7.1 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 monitor.custom.command.mode parameter of the following setting file. Further, the default value of the monitor.custom.command.mode parameter is "auto".

- /opt/hinemos_agent/conf/Agent.properties (Linux Agent)

- [Hinemos Agent install directory]\conf\Agent.properties (Windows Agent)

```
monitor.custom.command.mode=auto
```

The Custom Monitor's monitor.custom.command.mode parameter has the same action as the Hinemos Agent's job.command.mode parameter. The values that can be set in the monitor.custom.command.mode parameter and the differences in operation by OS platform can be found by referring to the Hinemos Agent's 7.1 Changing the Action of the Startup Command .

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

6.7.2 Changing Maximum of Standard Output

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)

```
monitor.custom.buffer=512
```

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

6.7.3 Changing New Line Code Included in the Standard Output

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)

```
monitor.custom.lineseparator=LF
```

Restart the Hinemos Agent after changing the settings.

6.7.4 Changing Command Execution Multiplicity

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 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)

```
monitor.custom.thread=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.

6.8 Polling Protocol Setting

Polling of the performance feature and monitoring 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.

6.8.1 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
```

6.8.2 Switching Between SNMP and WBEM

With the performance feature and the monitor feature (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 3.1.5 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 setting.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 setting.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".

6.9 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. As necessary, change the following parameter by selecting Maintenance perspective of Hinemos Client and opening Maintenance [Hinemos Property] view:

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.

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

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.

6.10 Resource Monitoring

6.10.1 Settings for mass storage filesystem monitoring

Additional settings shown below is needed for resource monitoring hign capacity filesystems. Monitor-able filesystems are from where device names 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 device names.

2. Restart snmpd of the monitored target node.

```
# service snmpd restart
```

6.11 Log Monitoring

6.11.1 Setting maximum number of files that can be monitored

The maximum number of files (default: 500) that can be monitored through log file monitoring can be set as follows.

To change the number of files, add the following to Agent.properties:

*Do not change the value to a value greater than 500.

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

```
monitor.logfile.filter.maxfiles=500
```

Files exceeding the upper limit are not monitored. If the upper limit is exceeded, the following log is output to agent.log:

```
refresh() too many files for logfile. not-monitoring file=< name of file not monitored>
```

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

7 Job Management

Additional settings for the Hinemos job management feature are explained.

7.1 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 job.command.mode parameter of the following setting file. Further, the default value of the job.command.mode parameter is "auto".

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

```
job.command.mode=auto
```

A list of the values that can be specified in the job.command.mode parameter is shown in Table 7-1.

Table 7-1 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
  (The 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 arguments are separated with one byte space 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.

7.2 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 stooped, 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 3.1.6 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 the "13.1 Behaviour of Job schedules when planned execution time has passed while java porcess was stopped" of Hinemos User's Manual;

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

- Maintenance perspective of Hinemos Client → Maintenance [Hinemos Property] view

```
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 no be executed after restarting Hinemos Manager. Therefore, it is not recommended to set the threshold to less than the default value of 3600000.

7.3 Enabling a File Transfer Job

The following configuration is required if using the file transfer job feature in a Linux Agent.

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.")

Perform the settings from the following procedure if you want 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) via SSH, then register the host key to known_hosts. Please note that if you are login via SSH over ipv6, do not use the abbreviated notation with double-colon(::). It is because when an abbreviated notation with double-colon(::) is used as a argument to the ssh command, the abbreviated form of IP address will be registered to known_hosts and that will cause File Transfer Job to fail.

```
(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.

8 Other Features

Additional settings for the other Hinemos features are explained.

8.1 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)
- 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 temporally information, due to recieving large number of syslog and or snmptrap (selfcheck.monitoring.systemlog, selfcheck.monitoring.snmptrap)
  - Enlargement of space used for storing temporally information, due to adding configuration and or increase of notifications (selfcheck.monitoring.asynctask)
  - 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 8.2 INTERNAL Events .

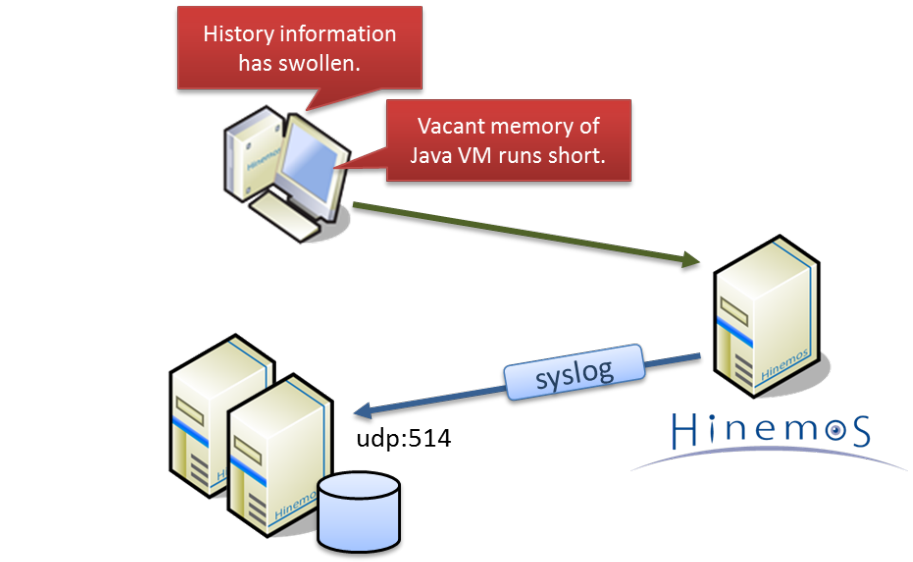

Figure 8-1 Overview of the Self-Check Feature

8.1.1 Self-Check Settings

The self-check feature is set on Maintenance [Hinemos Property] view which is opened by selecting Maintenance perspective of Hinemos Client. Refer to Table 13-8 Configured Values of the Self-check Feature in 13 List of Hinemos Manager's Configuration Settings for details about setting value.

8.2 INTERNAL Events

8.2.1 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. To where the internal event is to be notified can be changed on Maintenance [Hinemos Property] view that can be opened by selecting Maintenance perspective of Hinemos Client.

- Syslog sending

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

```
internal.syslog=false
internal.syslog.priority=info
internal.syslog.host=192.168.1.1,192.168.1.2
internal.syslog.port=514
internal.syslog.facility=daemon
internal.syslog.severity=alert
```

- Monitor[Event] view

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

```
internal.event=true
internal.event.priority=info
```

- hinemos_internal.log

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

```
internal.file=true
internal.file.priority=info
```

- E-mail Notification

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

```
internal.mail=false
internal.mail.priority=info
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 internal.command parameter.

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

8.2.2 Notification Information

List of INTERNAL Events will be listed below.

Table 8-2 INTERNAL Events

Priority	Plugin ID	Monitor ID	Application	Message ID	Message
Normal	MNG	SYS	Hinemos Manager Monitor	001	Hinemos Manager has been started.
Normal	MNG	SYS	Hinemos Manager Monitor	002	Hinemos Manager has been stopped.
Warning	COMMON	SYS	Internal common mechanism	001	Polling thread that runs for a long time ({0} minute) has been detected. PollerGroup={1}, PollerName={2} (Current statistic: Long-time operating thread ={3}, all polling threads ={4})
Warning	SYS_SFC	SYS	Self-check	001	Database is not available. if database is alive, Reduce the quantity of setting because the quantity of processing to be simultaneous executed (such as monitoring) is too much.
Warning	SYS_SFC	SYS	Self-check	002	usage of filesystem({0}) is too high ({1} [%] > threshold {2} [%] Perform maintenance operation (log file deletion, maintenance function, and script) and remove log files and compact database.
Warning	SYS_SFC	SYS	Self-check	003	free heap of jvm ({0} [mbyte]) is not enough (threshold {1} [mbyte]). Restart up of Hinemos manager is recommended for constant output. Reduce the quantity of setting because too many servers are registered or the quantity of setting of each processing (such as monitoring) is too much.
Warning	SYS_SFC	SYS	Self-check	004	A delay ({4} [sec] or longer) is generated in scheduler ({0}:{1}:{2} - next execution schedule {3}). If this message is continuously output, processing (such as monitoring that is periodically executed does not operate correctly. Restarting Hinemos Manager is recommended because there is a possibility.
Warning	SYS_SFC	SYS	Self-check	005	ram swap-out({0} [blocks]) occured. check resources of server and availability of hinemos manager.
Warning	SYS_SFC	SYS	Self-check	006	stored data ({0}) is too large ({1} mbyte - {2} rows > threshold {3} {4}). Since it becomes a factor of a performance fall, Perform maintenance operation (maintenance function and script).
Warning	SYS_SFC	SYS	Self-check	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	Self-check	008	response delay occurs because of too many request to Hinemos Manager tcp:8080 (queued request {0} > threshold {1}). If this message is always output, reduce the quantity of setting because the quantity of processing (such as monitoring) simultaneously executed is too much.
Warning	SYS_SFC	SYS	Self-check	009	filtering delay occurs because of too many syslog to Hinemos Manager (queued syslog {0} > threshold {1}). check if too many syslogs are sent from the subject to monitoring.
Warning	SYS_SFC	SYS	Self-check	010	filtering delay occurs because of too many snmptrap to Hinemos Manager (queued snmptrap {0} > threshold {1}). check if too many snmptraps are sent from the subject to monitoring.
Warning	SYS_SFC	SYS	Self-check	011	task delay occurs because of too many asynchronous task in Hinemos Manager (queued task {0} > threshold {1}). check if too many notifications or jobs are under execution.

Warning	SYS_SFC	SYS	Self-check	012	internal logic (tid {0}, thread name {1}, class name {2}, start time {3}) takes more than {4} [sec]. more than {4} [sec].
Warning	NOTIFY	SYS	Notification	004	Failed to get the notification. (NotifyId={0})
Warning	NOTIFY	SYS	Notification	006	Failed to get the notification list.
Critica	NOTIFY	SYS	Notification	007	Failed to notify Notification ID "{0}"
Critica	NOTIFY	SYS	Notification	008	Failed to notify. The job definition does not exist. (NotifyId={0},MonitorId={1},JobunitId={2},JobunitId={3})
Warning	MAIL TEMP	SYS	Mail template	004	Failed to get the mail template. (MailTemplateID={0})
Warning	MAIL TEMP	SYS	Mail template	005	Failed to get the list of Mail template ID.
Warning	MAIL TEMP	SYS	Mail template	006	Failed to get the list of Mail template.
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	Falied to execute monitoring. (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 delete Poller (FacilityId={0})
Critica	TRAP	SYS	SNMPTRAP Monitor	009	Failed to notify the SNMP TRAP event (trapOid={0}, genericId={1}, specificId={2})
Critica	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 delete Poller (FacilityId={0})
Critica	JOB	SYS	Job Management	003	Failed to create Job history inforimation (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[Immediate] (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})

8.3 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 8-3 is shown.

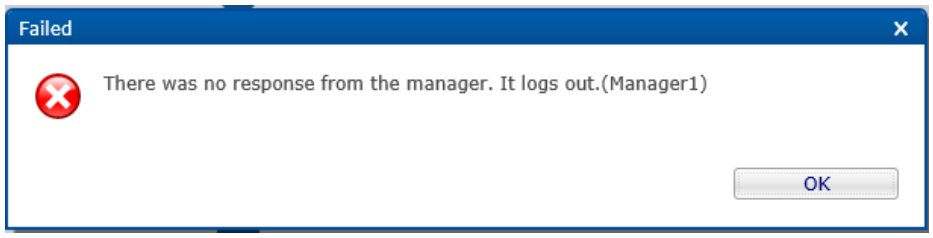

Figure 8-3 Hinemos Manager Alive Detection

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.

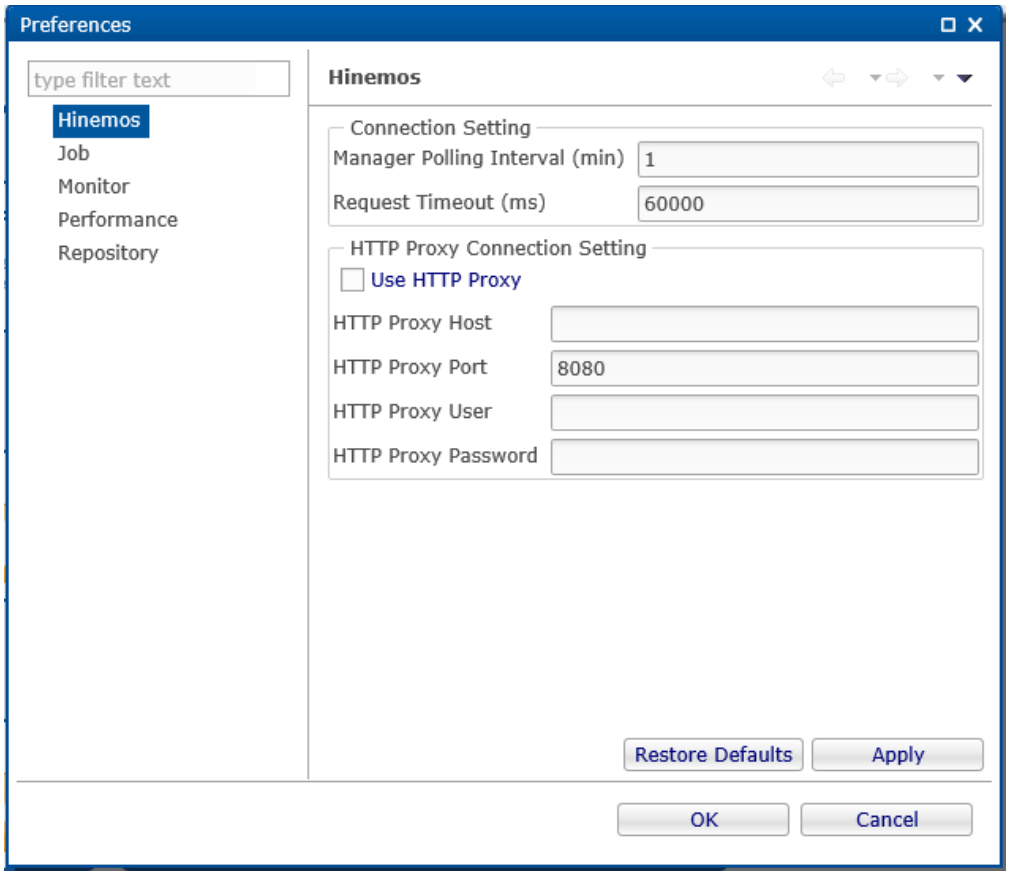

Figure 8-4 Hinemos Manager Polling Interval

9 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 3.1.5 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.

9.1 Change the Database Access Password

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

9.1.1 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 (9.3.5)
     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)

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

9.1.2 Hinemos Manager (destination) Setting Changes

Edit the following two parts.

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

1. Edit persistence.xml

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

   Set password changed in 9.1.1 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 db_account.properties

   Edit settings for database access of PostgreSQL User "hinemos" and "hinemos_quartz".

   Set password changed in 9.1.1 PostgreSQL (destination) Setting Changes . to hinemos_pass, hinemos_quartz_pass

```
hinemos_user=hinemos
hinemos_pass=hinemos
hinemos_quartz_user=hinemos_quartz
hinemos_quartz_pass=hinemos_quartz
```

9.2 Encrypting Password in Database

Passwords of node property (WBEM password and virtualization software connection password) and passwords for SQL monitoring are encrypted and stored in the database (PostgreSQL) of Hinemos Manager. The key for encryption is as follows:

- Edit db_crypt.key

  /opt/hinemos/etc/db_crypt.key

  ```
  hinemos
  ```

This character string, if it is ever change, must be changed immediately after installation. If it is changed after setting and registration, registered passwords will not be decrypted.

9.3 Changing Access Permission of JMX

The internal status of Hinemos Manager can be checked by JMX (Java Management Extensions). The accessible user and password can be changed as follows:

- jmxremote.access

  /opt/hinemos/etc/jmxremote.access

  This access control file defines access permission enabled for each role. It adds a role and access permission.

  ```
  hinemos readwrite
  ```

- jmxremote.password

  /opt/hinemos/etc/jmxremote.password

  The password of the role added by the access control file is added.

  ```
  hinemos hinemos
  ```

10 Connections Between Hinemos Components

10.1 Connections to Hinemos Manager via HTTP Proxy

With Hinemos ver.5.0, Hinemos Manager can be connected from Hinemos Rich Client, Hinemos Web Client and Hinemos Agent via HTTP Proxy.

10.1.1 Connections from Hinemos Client to Hinemos Manager

Set HTTP Proxy settings from Hinemos Client.

1. Specify from Hinemos Client Menu "Client Setup" -> "Setup" -> "Preference" dialog HTTPS Proxy Connection Settings(Refer Figure 10-1).

   HTTP Proxy Host

   Enter an 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

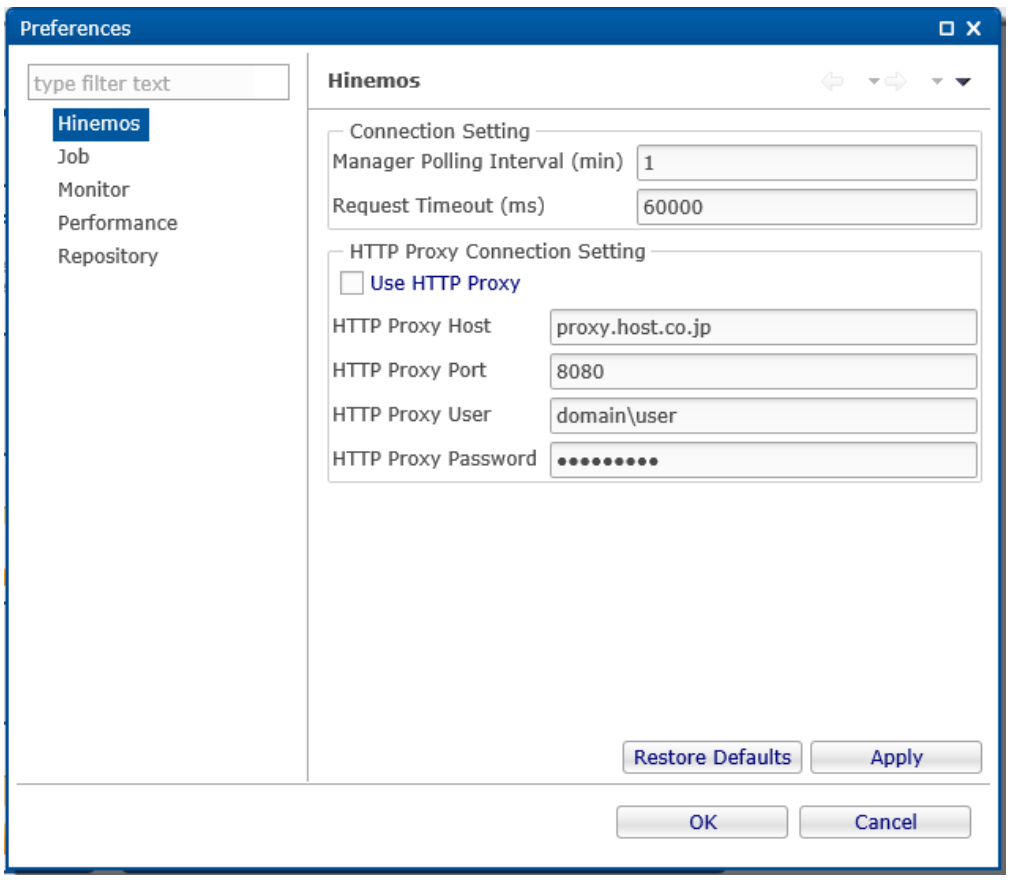

Figure 10-1 Settings of Cconnections in between Components of Hinemos

10.1.2 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
```

Set up 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.

10.2 HTTPS Connection to Hinemos Manager

Hinemos5.0 supports HTTPS communication for both between Hinemos Client and Hinemos Manager and between Hinemos Agent and Hinemos Manager.

10.2.1 Preparing server certificate of Hinemos Manager Server

To connect Hinemos Manager with HTTPS, a server certificate must be created on the Hinemos Manager.

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 .
```

2. Edit openssl.cnf as written below

```
# vi openssl.cnf

[ req ]
# x509_extensions       = v3_ca # The extentions 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 /root/keystore
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. To read a server certificate from Hinemos Manager, select Maintenance perspective of Hinemos Client and open Maintenance [Hinemos Property] view, and change the following parameters:

```
ws.client.address=https://0.0.0.0:8443  ←Change this parameter to connect Hinemos Client with HTTPS.
ws.agent.address=https://0.0.0.0:8444  ←Change this parameter to connect Hinemos Client with HTTPS.
```

The parameters related to HTTPS connection are as follows:

ws.client.address:

Connected address from Hinemos Client to Hinemos Manager

This parameter can select https as a protocol as necessary. When https is selected, the port number is changed to a number different from that for http.

ws.agent.address:

Connected address from Hinemos Agent to Hinemos Manager

This parameter can select https as a protocol as necessary. When https is selected, the port number is changed to a number different from that for http. When https protocol is selected, the setting of connection from all agents to be monitored must be changed to https.

ws.https.keystore.path:

Directory Path of Keystore

ws.https.keystore.password:

Password of the keystore

ws.https.keystore.type:

Type of Keystore

Hinemos Manager must be restarted in order to reflect configuration changes on this property file.

10.2.2 HTTPS Connections from Hinemos Rich Client to Hinemos Manager

Start Hinemos Rich Client, and enter the URL to the "URL to connect" in Connection[Login] dialog.

```
https://[IP address of Hinemos Manager]:8443/HinemosWS/
```

Set the other items in the same manner as when Hinemos Manager is connected with HTTP protocol. As a result, Hinemos Rich Client and Hinemos Manager perform communication encrypted by HTTPS with each other. (Host authentication of HTTPS is not performed.)

10.2.3 HTTPS Connections from Hinemos Web Client to Hinemos Manager

Access Hinemos Web Client from browser and specify the following as the URL to which Hinemos Manager is to be connected:

```
https://[IP address of Hinemos Manager]:8443/HinemosWS/
```

Set the other items in the same manner as when Hinemos Manager is connected with HTTP protocol. As a result, Hinemos Web Client and Hinemos Manager perform communication encrypted by HTTPS with each other. (Host authentication of HTTPS is not performed.)

10.2.4 HTTPS Connections to Hinemos Manager from Hinemos Agent

Agent's setting file

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

Modify these as follows:

```
managerAddress=https://[IP address of Hinemos Manager]:8443/HinemosWS/
```

The Hinemos Agent must be restarted after changing the settings. As a result, Hinemos Agent and Hinemos Manager perform communication encrypted by HTTPS with each other.

10.2.5 Authenticating Host When Hinemos Rich Client is Connected to Hinemos Manager with HTTPS

Perform the following setting if it is necessary to authenticate the host of Hinemos Manager at the connection destination when the Hinemos Manager is accessed from Hinemos Rich Client with HTTPS protocol:

Place the server.crt created in steps written in 10.2.1 Preparing server certificate of Hinemos Manager Server to a terminal where Hinemos Rich 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 32-bit environment. When executing the command in 64-bit environment, change "Program Files" to "Program Files (x86)")

```
>C:\Users>"C:\Program Files\Hinemos\Client5.0.0\eclipse-rcp\jre\bin\keytool.exe" -import -alias hinemos
 -file "C:\tmp\server.crt" -keystore "C:\tmp\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. Modify the startup script of Hinemos Rich Client.

   Modify the start scripts (client_start.vbs and client_clean_start.vbs) that are in the directory to which Hinemos Rich Client is installed.

```
(Before modification)
  ...
  strCmdLine = strCmdLine & strVmArgs & eclipseLocale & "-Dorg.apache.commons.logging.Log= ...(Omitted)...
  ' strCmdLine = strCmdLine & " -Dhttps.hostVerify=true"
  ' strCmdLine = strCmdLine & " -Djavax.net.ssl.trustStore=C:\tmp\cacerts"
  ' strCmdLine = strCmdLine & " -Djavax.net.ssl.trustStorePassword=changeit"
  objWshShell.CurrentDirectory = strExecFolder
  ...

(After modification)
  ...
  strCmdLine = strCmdLine & strVmArgs & eclipseLocale & "-Dorg.apache.commons.logging.Log= ...(Omitted)...
  strCmdLine = strCmdLine & " -Dhttps.hostVerify=true"                        ← Undo Comment Out
  strCmdLine = strCmdLine & " -Djavax.net.ssl.trustStore=C:\tmp\cacerts"    ← Undo Comment Out
  strCmdLine = strCmdLine & " -Djavax.net.ssl.trustStorePassword=changeit" ← Undo Comment Out
  objWshShell.CurrentDirectory = strExecFolder
  ...
```

   Specify the following environment variables:

   https.hostVerify:

   This variable authenticates the host when it is true. If it is not set, false is assumed (host is not authenticated) for the operation.

   javax.net.ssl.trustStore:

   This variable specifies the file path of a trust store file.

   javax.net.ssl.trustStorePassword:

   This variable specifies the password of a trust store file.

4. Start the Client by using modified client_start.vbbs and connect it with HTTPS.

   When the client started by using modified client_start.vbs is used, the host is authenticated if the Hinemos Rich Client is connected to Hinemos Manager with HTTPS.

10.2.6 Authenticating Host when Hinemos Web Client is connected to Hinemos Manager with HTTPS

Make the following setting if the host of Hinemos Manager at the connection destination needs to be authenticated when Hinemos Web Client is connected to the Hinemos Manager with HTTPS protocol:

Place the server.crt created in steps written in 10.2.1 Preparing server certificate of Hinemos Manager Server to a terminal where Hinemos Web Client is installed. (In this document, server.crt will be placed in /opt/hinemos/etc/ssl/.)

1. Execute the following command on the server to which Hinemos Web Client is installed:

```
# mkdir /opt/hinemos_web/conf/ssl
# keytool -import -import -alias hinemos -file /opt/hinemos/etc/ssl/server.crt -keystore /opt/hinemos_web/conf/ssl/cacer

Enter keystore password:(Enter changeit)
Input the new password again: (Input changeit if asked.)

Owner: O=Default Company Ltd, L=Default City, C=XX
Issure: O=Default Company Ltd, L=Default City, C=XX

(Omitted)

Trust this certificate? [No]: Yes
Certificate was added to keystore
```

2. Edit the setting file for Hinemos Web Client.

   Edit /opt/hinemos_web/conf/hinemos_web.cfg.

```
(Before editing)
  ...
  ### JVM - HTTPS HostVerify
  #export JVM_SSL_OPTS="-Dhttps.hostVerify=true -Djavax.net.ssl.trustStore=
    /opt/hinemos_web/conf/ssl/cacerts -Djavax.net.ssl.trustStorePassword=changeit"

(After editing)
  ...
  ### JVM - HTTPS HostVerify
  export JVM_SSL_OPTS="-Dhttps.hostVerify=true -Djavax.net.ssl.trustStore=
    /opt/hinemos_web/conf/ssl/cacerts -Djavax.net.ssl.trustStorePassword=changeit"

   ↑Undo Comment Out
```

   Specify the following environment variables:

   https.hostVerify:

   This variable authenticates the host when it is true. If it is not set, false is assumed (host is not authenticated) for the operation.

   javax.net.ssl.trustStore:

   This variable specifies the file path of a trust store file.

   javax.net.ssl.trustStorePassword:

   This variable specifies the password of a trust store file.

3. Restart Hinemos Web Client.

   After that, the host of the Manager is authenticated when Hinemos Web Client is connected if HTTPS is specified as the connection destination URL on the Connection[Login] dialog box of Hinemos Web Client.

10.3 Connection to Hinemos Web Client with HTTPS

Hinemos Web Client service supports HTTPS communication from respective browsers.

1. Edit /opt/hinemos_web/conf/server.xml.

```
<!--  ←Comment Out
<Connector port="80" protocol="HTTP/1.1"
         connectionTimeout="20000"
         redirectPort="8443"
         maxThreads="32"
         />
-->   ←Comment Out
<!-- Define a SSL HTTP/1.1 Connector on port 8443
    This connector uses the NIO implementation that requires the JSSE
    style configuration. When using the APR/native implementation, the
    OpenSSL style configuration is required as described in the APR/native
    documentation -->
     ←Undo Comment Out
<Connector port="443" protocol="org.apache.coyote.http11.Http11NioProtocol"
         maxThreads="32" SSLEnabled="true" scheme="https" secure="true"
         clientAuth="false" sslProtocol="TLS"
         keystoreFile="/opt/hinemos_web/.keystore" keystorePass="changeit"
         />
     ←Undo Comment Out
```

2. Create the certificate with following command.

```
keytool -genkey -alias tomcat -keyalg RSA -keystore /opt/hinemos_web/.keystore

Enter keystore password:
Input the new password again:
Enter name.
  [Unknown]: (Press Enter key without entering anything)
Enter company unit name.
  [Unknown]: (Press Enter key without entering anything)
Enter company name.
  [Unknown]: (Press Enter key without entering anything)
Enter city or area name.
  [Unknown]: (Press Enter key without entering anything)
Enter province or county name
  [Unknown]: (Press Enter key without entering anything)
Input a 2-character country number that falls under this unit.
  [Unknown]: (Press Enter key without entering anything)
CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown OK?
  [no]:  (Enter yes)

Input the key password of <tomcat>.
        (Press RETRUN if the password is the same as that for keystore.) (Press Enter key without entering anything)
```

3. The setting will be reflected when Hinemos Web Client service is restarted.

11 Port Setting

11.1 Changing Port of Hinemos Manager

To change the port number of Hinemos manager, select Maintenance perspective of Hinemos Client and open Maintenance [Hinemos Property] view, and change the following parameter:

```
ws.client.address=http://0.0.0.0:8080
ws.agent.address=http://0.0.0.0:8081
```

Set up the following parameters:

- ws.client.address=Connected address from Hinemos Client to Hinemos Manager (Change port)
- ws.agent.address=Connected address from Hinemos Agent to Hinemos Manager (Change port)

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

11.2 Changing Port of Hinemos Web Client Service

To change the port number of Hinemos Web Client, change the following parameters of /opt/hinemos_web/conf/server.xml.

```
<Connector port="80" protocol="HTTP/1.1"
        connectionTimeout="20000"
        redirectPort="8443"
        maxThreads="32"
        />
```

Set up the following parameters:

- port= Port connecting from browser to Hinemos Client service

In order to make the new configuration take effect, you need to restart the Web Client Service.

11.3 Awake Port of Hinemos Agent

Hinemos Agent listens on the awake port (UDP 24005 By default) for requests for updating settings immediately. To change the awake port, use Hinemos Client to modify the value of "Awake Port" in the node properties.

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	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/hinemos.cfg
Output level	—
Rotation	—
Content	PostgreSQL standard output/standard error output

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/9.3/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 Operation 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 setting 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/ thread dump

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

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	Rotate every 10 MB and only the last 5 generations 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 setting file	[Hinemos Agent install directory]\conf\log4j.properties
Output level	priority INFO
Rotation	Rotated every 20Mbyte (last 5 generation including the current log)
Content	Hinemos Agent log

File name	restart.log
Storage directory	[Hinemos Agent install directory]\var\log\
Configured file for log output	—
Output level	—
Rotation	—
Content	Content Hinemos Agent log at the time of restart

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	For java-1.7.0: Rotated every 10MByte and last 5 generation will be kept For java-1.6.0: None
Content	Garbage Collection log of java process

12.6 Changing Log Output and Log Rotation Settings of 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=${hinemos.agent.log.dir}/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\Client5.0
Log setting 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

12.8 List of Hinemos Web Client Log Files

Hinemos Web Client logs are output in log file displayed in Table 12-6.

Table 12-6 List of Hinemos Client Log Files

File name	webclient.log
Store directory	/opt/hinemos_web/var/log
Log output setting file	[Hinemos Web Client install directory]\log4j.properties
Output level	—
Rotation	File size 20MByte (Maximum of 5 generations including the current log)
Content	Hinemos Web Client log

File name	catalina.out
Store directory	/ opt/hinemos_web/var/log
Configured file for log output	—
Output level	—
Rotation	Hinemos Web Client Service starts
Content	Hinemos Web Client Service log

File name	catalina.boot.log
Store directory	/ opt/hinemos_web/var/log
Configured file for log output	—
Output level	—
Rotation	—
Content	Hinemos Web Client Service log

File name	gc_webclient.log.*
Store directory	/ opt/hinemos_web/var/log
Configured file for log output	—
Output level	—
Rotation	For java-1.7.0: Rotated every 10MByte and last 5 generation will be kept For java-1.6.0: None
Content	Garbage Collection log of java process

13 List of Hinemos Manager's Configuration Settings

Hinemos Manager's settings are defined in the database. Setting can be added or changed by selecting Maintenance perspective of Hinemos Client and opening Maintenance [Hinemos Property] view.

Table 13-1 Configured Values of INTERNAL Events

Property Name	Description	Data type	Default value
internal.command	If executing a command by INTERNAL event, set " true" for this parameter. If not, set "false"	Truth	false
internal.command.commandline	Executed command triggered by the output of INTERNAL event	String	echo #[GENERATION_DATE] #[MESSAGE] >> /tmp/test.txt
internal.command.priority	priority of INTERNAL events when executing the command	String	info
internal.command.timeout	Timeout vlaue[msec] of a command triggerd by the output of INTERNAL event.	Integer	15000

internal.command.user	Execution user of a command triggered by the output of INTERNAL event.	String	root
internal.event	If INTENAL event to be shown in Monitor[Event] view, set "true" for this parameter. If not, set "false".	Truth	true
internal.event.priority	Priority of INTERNAL event shown in the Monitor[Event] view	String	info
internal.file	If outputting an INTERNAL event to an log file, set "true" for this parameter. If not, set "false".	Truth	true
internal.file.priority	Priority of INTERNAL event when logging out to a log file.	String	info
internal.mail	If sending out INTERNAL event as mail, set "true" for this parameter. If not, set "false".	Truth	false
internal.mail.address	Mail address to send mail when sending out INTERNAL event as a mail.	String	user1@host.domain, user2@host.domain
internal.mail.priority	Priority of INTERNAL events when sending a mail	String	info
internal.syslog	If sending out INTERNAL event as syslog, set "true" for this parameter. If not, set "false".	Truth	false
internal.syslog.facility	Facility when sending out INTERNAL event as syslog	String	daemon
internal.syslog.host	Host to send INTERNAL event as syslog	String	192.168.1.1, 192.168.1.2
internal.syslog.port	Port to send INTERNAL event as syslog	Integer	514
internal.syslog.priority	Priority of INTERNAL event when it is sent out as syslog	String	info
internal.syslog.severity	severity of syslog when sending out INTERNAL event as syslog	String	alert

Table 13-2 Configured Values of the Monitoring Feature

Property Name	Description	Data type	Default value
monitor.sql.jdbc.driver	Number of JDBC drivers used for SQL monitoring	Integer	3
monitor.sql.jdbc.driver.classname.1	Class name of first JDBC driver used for SQL monitoring	String	org.postgresql.Driver
monitor.sql.jdbc.driver.classname.2	Class name of second JDBC driver used for SQL monitoring	String	com.mysql.jdbc.Driver
monitor.sql.jdbc.driver.classname.3	Class name of third JDBC driver used for SQL monitoring	String	oracle.jdbc.driver.OracleDriver
monitor.sql.jdbc.driver.logintimeout.1	Timeout of first JDBC driver used for SQL monitoring [sec]	Integer	30
monitor.sql.jdbc.driver.logintimeout.2	Timeout of second JDBC driver used for SQL monitoring [sec]	Integer	30
monitor.sql.jdbc.driver.logintimeout.3	Timeout of third JDBC driver used for SQL monitoring [sec]	Integer	30
monitor.sql.jdbc.driver.name1	Name displayed on setting dialog for first JDBC driver used for SQL monitoring	String	PostgreSQL
monitor.sql.jdbc.driver.name2	Name displayed on setting dialog for second JDBC driver used for SQL monitoring	String	MySQL
monitor.sql.jdbc.driver.name3	Name displayed on setting dialog for third JDBC driver used for SQL monitoring	String	Oracle

monitor.sql.jdbc.driver. properties.1	Additional property of first JDBC driver used for SQL monitoring	String	socketTimeout=3600& tcpKeepAlive=true
monitor.sql.jdbc.driver. properties.2	Additional property of second JDBC driver used for SQL monitoring	String	Undefined
monitor.sql.jdbc.driver. properties.3	Additional property of third JDBC driver used for SQL monitoring	String	Undefined
monitor.log.line.max. length	Maximum string length with the system log monitor's #[LOG_LINE] included [byte]. Syslog messages that exceed this length will be truncated and stored in notification messages.	Integer	256
monitor.common.delete. cascade.perfdata	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"	String	on
monitor.common.report. event.bom	Whether or not to distribute the BOM to the file to the file created by the download feature in the Monitor[Event] view. If the BOM is distributed to the file, set "true". If not, set "false".	Truth	true
monitor.common.report. eventt.count	Maximum number of event information included in the file that occurred with the download feature of Monitor[Event] view	Integer	2000
monitor.common.report. event.format	Time format of the time for the BOM to the file created by the download feature in the Monitor[Event] view	String	yyyy/MM/dd HH:mm:ss
monitor.common.report. event.separator	Column delimiter for the file BOM that occurred with the Monitoring[Event] view download with the Monitoring[Event] view download	String	,
monitor.process.start. second	Time to start tracking process monitor value [sec]	Integer	30
monitor.process.valid. second	Poller collector permissible time [sec]	Integer	50
monitor.snmptrap.listen. address	[Hinemos Manager must be restarted.] Waiting address for java process to receive subject to monitoring and SNMPTRAP	String	0.0.0.0
monitor.snmptrap.listen. port	[Hinemos Manager must be restarted.] Waiting port number of java process to receive subject to monitoring and SNMPTRAP	Integer	162
monitor.snmptrap.org. message.community	true if a community name is output to the original message during SNMPTRAP monitoring; otherwise , false otherwise , false	Truth	true
monitor.snmptrap.org. message.varbind	true if varbind is output to the original message during SNMPTRAP monitoring; otherwise , false	Truth	true
monitor.snmptrap.v3.user	[Hinemos Manager must be restarted.] User of SNMPTRAP of version 3 to be received	String	hinemos
monitor.snmptrap.v3. security.level	Security level of SNMPTRAP of version 3 to be received (noauth_nopriv/auth_nopriv/auth_priv)	String	noauth_nopriv
monitor.snmptrap.v3. auth.password	[Hinemos Manager must be restarted.] Password of version 3 to be received|String	SNMPTRAP	authPassword
monitor.snmptrap.v3. auth.protocol	Authentication protocol (MD5/SHA) of SNMPTRAP of version 3 to be received	String	MD5

monitor.snmptrap.v3.priv. password	Encrypting password of SNMPTRAP of version 3 to be received	String	privPassword
monitor.snmptrap.v3.priv. protocol	[Hinemos Manager must be restarted.] Encrypting protocol (DES/AES) of SNMPTRAP of version 3 to be received	String	DES
monitor.snmptrap.stats. interval	The statistical information is output to a log file when the SNMPTRAP receive count reaches this multiple reaches this multiple	Integer	100
monitor.systemlog.listen. address	[Hinemos Manager must be restarted.] listen address of java process to receive monitored syslog	String	0.0.0.0
monitor.systemlog.listen. port	[Hinemos Manager must be restarted.] Waiting port number of java process to receive monitored syslog	Integer	24514
monitor.systemlog.stats. interval	The statistical information is output to a log file when the syslog receive count reaches this multiple	Integer	Undefined

Table 13-3 Configured Values of the Notification Feature

Property Name	Description	Data type	Default value
notify.log.escalate. manager.hostname	String specified in HOSTNAME section when a syslog is sent by log escalation notification	String	Undefined
notify.log.escalate. manager.protocol	Transfer protocol of log escalation notification (udp, tcp)	String	udp
notify.log.escalate. manager.retry.count	Attempt count of log escalation notification	Integer	1
notify.log.escalate. manager.retry.interval	Interval of retry of log escalation notification [msec]	Integer	10000
notify.command.create. mode	OS platform definition for the command operation of the command notification	String	auto
notify.command.success. exit	Normal value for the command return value of the command notification. It will be notified as an INTERNAL event when other return values.	Integer	0
notify.date.format	(#[GENERATION_DATE]) that can be used in notification	String	yyyy/MM/dd HH:mm:ss

Table 13-4 Configured Values of Mail Notification

Property Name	Description	Data type	Default value
mail.charset.address	Character code of the address of mail notification	String	UTF-8
mail.charset.content	Character code of the main text of mail notification	String	UTF-8
mail.charset.subject	Character code of the subject of mail notification	String	UTF-8
mail.errors.to.address	Destination address of error mail (Error-To)	String	admin@hinemos.com
mail.from.address	Mail address of the sender (From)	String	admin@hinemos.com
mail.from.personal.name	Name of the sender (From)	String	Hinemos Admin
mail.reply.personal.name	Name of reply mail receiver (Reply-To)	String	Hinemos Admin
mail.reply.to.address	Address of reply mail receiver (Reply-To)	String	admin@hinemos.com

mail.transport.tries	Retry count of sending mail	Integer	1
mail.transport.tries. interval	Interval of retry of sending mail [msec]	Integer	10000
mail.transport.password	Password at sending mail	String	password
mail.transport.user	Username at sending mail	String	nobody
mail.smtp.auth	Use of SMTP AUTH	Truth	false
mail.smtp. connectiontimeout	Timeout of connection with SMTP server [msec]	Integer	15000
mail.smtp.host	IP address of SMTP server	String	127.0.0.1
mail.smtp.port	Port number of SMTP server	Integer	25
mail.smtp.timeout	Timeout of request to SMTP server [msec]	Integer	30000
mail.smtp.starttls.enable	Protocol of communication with SMTP server	Truth	false
mail.transport.protocol	which uses SMTP server requiring SSL/TLS(STARTTLS)	String	smtp

Table 13-5 Configured Values of the Performance Feature

Property Name	Description	Data type	Default value
performance.export . encode	Character code of the file created in the export of the performance feature	String	MS932
performance.export.line. separator	New line code of the file created in the export of the performance feature	String	\r\n

Table13-6. Configured Values of the Job Feature

Property Name	Description	Data type	Default value
quartz.dbms.jobStore. misfireThreshold	[Hinemos Manager must be restarted.] Effective period of job to be executed at restarting Hinemos Manager [msec]	Integer	3600000

Table13-7. Configured Values of the Repository Feature

Property Name	Description	Data type	Default value
repository.device.search. interval	Execution interval of automatic device search [min]. Automatic device search is invalid if 0.	Integer	5
repository.device.search. verbose	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.	Truth	true
repository.device.search. prop.device.cpu	Set true to enable Auto Device Search on CPU information (Node properties > Device > CPU List), or false to disable.	Truth	true
repository.device.search. prop.device.memory	Set true to enable Auto Device Search on memory information (Node properties > Device > Memory List), or false to disable.	Truth	true
repository.device.search. prop.device.nic	Set true to enable Auto Device Search on NIC information (Node properties > Device > NIC List), or false to disable.	Truth	true
repository.device.search. prop.device.disk	Set true to enable Auto Device Search on disk information (Node properties > Device > Disk List), or false to disable.	Truth	true

repository.device.search.prop.device.filesystem	Set true to enable Auto Device Search on file system information (Node properties > Device > File System List), or false to disable.	Truth	true
repository.device.search.prop.device.general	Set true to enable Auto Device Search on genearl device information (Node properties > Device > General Device List), or false to disable.	Truth	true
repository.device.search.prop.basic.hardware	Set true to enable Auto Device Search on hardware information (Node properties > Basic Server Information > Hardware), or false to disable.	Truth	true
repository.device.search.prop.basic.network	Set true to enable Auto Device Search on network information (Node properties > Basic Server Information > Network), or false to disable.	Truth	true
repository.device.search.prop.basic.os	Set true to enable Auto Device Search on OS information (Node properties > Basic Server Information > OS), or false to disable.	Truth	true
repository.device.search.prop.basic.agent	Set true to enable Auto Device Search on Agent information (Node properties > Basic Server Information > Hinemos Agent), or false to disable.	Truth	true

Table 13-8 Configured Values of the Self-check Feature

Property Name	Description	Data type	Default value
selfcheck.alert.threshold	Number of errors detected before the notification	Integer	3
selfcheck.interval	[Hinemos Manager must be restarted.] Time interval to check status of internal component [sec]	Integer	150
selfcheck.monitoring.asynctask.queue	Set true if enabling cue check of asynchronous processing. Set false if disabling this setting.	Truth	true
selfcheck.monitoring.asynctask.queue.list	Name and maximum number of messages of cue checked asynchronous processing	String	(Note 2)
selfcheck.monitoring.db	Set true if enabling access check to database. Set false if disabling this setting.	Truth	true
selfcheck.monitoring.db.validationquery	SQL used to check access to the database	String	SELECT 1 FOR UPDATE
selfcheck.monitoring.filesystem.usage	Set true if enabling the free filesystem space checking. Set false if disabling this setting.	Truth	false
selfcheck.monitoring.filesystem.usage.list	Checking threshold of fres filesystem space of Hinemos Manager Can be specified by delimiting with half width comma. Filesystem usage of "/" directory is monitored with its threshold of 50% with its original settings.	String	/:50
selfcheck.monitoring.job.runningsession	Set true if checking the number of running job session. Set false if disabling this setting.	Truth	true
selfcheck.monitoring.job.runningsession.threshold	Upper threshold of the number of job session	Integer	1000
selfcheck.monitoring.jvm.freeheap	Set true if enabling check of free memory space of Java VM. Set false if disabling this setting.	Truth	true
selfcheck.monitoring.jvm.freeheap.threshold	Threshold of free memory space of Java VM[MByte]	Integer	32
selfcheck.monitoring.scheduler.delay	Set true if enabling scheduler check. Set false if disabling this setting.	Truth	true

selfcheck.monitoring. scheduler.delay.threshold	Upper threshold of delay time [sec] to determine the delay of scheduler.	Integer	300
selfcheck.monitoring. snmptrap.queue	Set true if enabling internal cue check of SNMPTRAP monitoring Set false if disabling this setting.	Truth	true
selfcheck.monitoring. snmptrap.queue.threshold	Maximum number of messages of internal cue of SNMPTRAP monitoring	Integer	10000
selfcheck.monitoring. swapout	Set true if enabling swapout checking. Set false if disabling this setting.	Truth	false
selfcheck.monitoring. systemlog.queue	Set true if enabling internal cue check of system log monitoring. Set false if disabling this setting.	Truth	true
selfcheck.monitoring. systemlog.queue. threshold	Maximum number of messages of internal cue of system log monitoring	Integer	10000
selfcheck.monitoring. table.size	Set true if enabling size check of internal table. Set false if disabling this setting.	Truth	true
selfcheck.monitoring. table.size.list	Upper threshold of table size and table name to be checked	String	(Note 3)
selfcheck.monitoring. thread.activity	Set true if enabling delaying thread check. Set false if disabling this setting.	Truth	true
selfcheck.monitoring. thread.activity.threshold	Upper threshold of delaying time of delaying thread[sec]	Integer	300
selfcheck.monitoring.ws. queue	Set true if enabling access cue check of Web Service Set false if disabling this setting.	Truth	true
selfcheck.monitoring.ws. queue.threshold	Maximum number of messages of access cue of Web Service	Integer	10000
selfcheck.snmp. community	Community name used for SNMP polling to Manager itself (127.0.0.1)	String	public
selfcheck.snmp.port	Port number usedfor SNMP polling to Manager itself (127.0.0.1)	Integer	161
selfcheck.snmp.retries	etry count used for SNMP polling to Manager itself (127.0.0.1)	Integer	3
selfcheck.snmp.timeout	Timeout[sec] used for SNMP polling to Manager itself (127.0.0.1)	Integer	3000
selfcheck.snmp.version	Version (1/2c) used for SNMP polling to Manager itself (127.0.0.1)	String	2c
selfcheck.starup.delay	[Hinemos Manager must be restarted.] Time to start self check [sec]	Integer	90
selfcheck.threadpool.size	Number of threads used for self check feature	Integer	4

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

(Note 2) NotifyStatusTaskFactory:10000,NotifyEventTaskFactory:10000,NotifyMailTaskFactory:10000,NotifyCommandTaskFactory:10000,NotifyLogEscalationTaskFactory:10000, NotifyJobTaskFactory:10000

(Note 3) log.cc_event_log:5120:MBYTE,log.cc_calculated_data:20480:MBYTE,log.cc_job_session:100000:COUNT

Table 13-9 Configured Values for Connection of Hinemos Manager

Property Name	Description	Data type	Default value
ws.client.address	[A restart is required to Hinemos Manager] IP address where Hinemos Manager waits for connection from Client	String	http://0.0.0.0:8080

ws.agent.address	[A restart is required to Hinemos Manager] IP address where Hinemos Manager waits for connection from Agent	String	http://0.0.0.0:8081
ws.https.keystore.password	[A restart is required to Hinemos Manager] Password of the keystore	String	hinemos
ws.https.keystore.path	[A restart is required to Hinemos Manager] Directory path of keystore	String	/root/keystore
ws.https.keystore.type	Type of the keystore	String	PKCS12
ws.https.protocol	[A restart is required to Hinemos Manager] Secure protocol of HTTPS	String	TLS

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 with property editor.)

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 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 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[monitor.message.length]

Property	monitor.message.length
Property name	Maximum bytes of message monitored by Logfile Monitor/Windows Event Monitor
Description	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[job.history.period]

Property	job.history.period
Property name	Maximum lifetime 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[job.message.length]

Property	job.message.length
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[job.stream.charset]

Property	job.stream.charset
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[job.command.mode]

Property	job.command.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[job.filecheck.interval]

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

Parameter[job.filecheck.sender.tries]

Property	job.filecheck.sender.tries
Property name	Maximum attempt count for send processing of the results of job file check
Description	Maximum attempt count for send processing of the results of job file check
Data type	Integer
Default value	15

Parameter[job.filecheck.sender.interval]

Property	job.filecheck.sender.tries
Property name	Interval for send processing of the results of job file check
Description	Interval for send processing of the results of job file check (msec)
Data type	Integer
Default value	60000

Parameter[root.public.key]

Property	root.public.key
Property name	Public key of node to which a file is transferred by a job
Description	Public key of node to which a file is transferred by a job
Data type	String
Default value	Not defined

Parameter[root.authorized.keys.path]

Property	root.authorized.keys.path
Property name	Path of authorized_keys of node from which a file is transferred by a job
Description	Path of authorized_keys of node from which a file is transferred by a job
Data type	String
Default value	/root/.ssh/authorized_keys

Parameter[monitor.logfile.filter.interval]

Property	monitor.logfile.filter.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[monitor.logfile.filter.filesizecheck.period]

Property	monitor.logfile.filter.filesizecheck.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[monitor.logfile.filter.fileheadcheck.period]

Property	monitor.logfile.filter.fileheadcheck.period
Property name	File first part check period setting (seconds)
Description	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[monitor.logfile.filter.fileheadercheck.size]

Property	monitor.logfile.filter.fileheadercheck.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[monitor.logfile.filter.maxsize]

Property	monitor.logfile.filter.maxsize
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[monitor.logfile.syslog.priority]

Property	monitor.logfile.syslog.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	info

Parameter[monitor.logfile.syslog.program]

Property	monitor.logfile.syslog.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[monitor.logfile.forwarding.queue.maxsize]

Property	monitor.logfile.forwarding.queue.maxsize
Property name	Maximum number of messages in internal queue for log file monitoring
Description	Maximum number of messages in internal queue for log file monitoring
Data type	Integer
Default value	5000

Parameter[monitor.logfile.forwarding.transport.maxsize]

Property	monitor.logfile.forwarding.transport.maxsize
Property name	Transmission division unit for processing to transmit result of log file monitoring
Description	Upper-limit number of messages that can be transmitted at once by processing to transmit result of log file monitoring. If the number of messages in the internal cue is greater than the set value, transmission processing is divided.
Data type	Integer
Default value	100

Parameter[monitor.logfile.forwarding.transport.maxtries]

Property	monitor.logfile.forwarding.transport.maxtries
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	900

Parameter[monitor.logfile.forwarding.transport.interval.size]

Property	monitor.logfile.forwarding.transport.interval.size
Property name	Trigger (number of messages) for trying processing to transmit result of log file monitoring

Description	Number of messages that triggers trying processing to transmit result of log file monitoring The result transmission processing will be executed when the number of messages stored in the internal cue since the previous result transmission processing reaches the set value.
Data type	Integer
Default value	15

Parameter[monitor.logfile.forwarding.transport.interval.msec]

Property	monitor.logfile.forwarding.transport.interval.msec
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	1000

Parameter[monitor.logfile.random.access.file]

Property	monitor.logfile.random.access.file
Property name	Method of rotating log file monitoring on Windows environment
Description	By specifying “windows” for this parameter to monitor the log file on Windows environment, the mv method that renames a specific log will be supported when logs are rotated.
Data type	String
Default value	Linux Agent : linux, WindowsAgent : windows

Parameter[monitor.custom.thread]

Property	monitor.custom.thread
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[monitor.custom.command.mode]

Property	monitor.custom.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[monitor.custom.bufferr]

Property	monitor.custom.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[monitor.custom.charset]

Property	monitor.custom.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[monitor.custom.lineseparato]

Property	monitor.custom.lineseparato
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[monitor.custom.forwarding.queue.maxsize]

Property	monitor.custom.forwarding.queue.maxsize
Property name	Maximum number of messages of internal cue for custom monitoring
Description	Maximum number of messages of internal cue for custom monitoring
Data type	Integer
Default value	5000

Parameter[monitor.custom.forwarding.transport.maxsize]

Property	monitor.custom.forwarding.transport.maxsize
Property name	Transmission division unit for processing to transmit result of custom monitoring
Description	Upper-limit number of messages that can be transmitted at once by custom monitoring result transmission processing. Transmission processing is divided if the number of messages in the internal cue is greater than the set value.
Data type	Integer
Default value	100

Parameter[monitor.custom.forwarding.transport.maxtries]

Property	monitor.custom.forwarding.transport.maxtries
Property name	Maximum attempt count for send processing of the results of custom monitoring
Description	Maximum attempt count for send processing of the results of custom monitoring
Data type	Integer
Default value	900

Parameter[monitor.custom.forwarding.transport.interval.size]

Property	monitor.custom.forwarding.transport.interval.size
Property name	Trigger (number of messages) for trying processing to transmit result of custom monitoring
Description	Number of messages that triggers trying processing to transmit result of custom monitoring. The result transmission processing will be executed when the number of messages stored in the internal cue since the previous result transmission processing reaches the set value.
Data type	Integer
Default value	15

Parameter[monitor.custom.forwarding.transport.interval.msec]

Property	monitor.custom.forwarding.transport.interval.msec
Property name	Interval for send processing of the results of custom monitoring(msec)
Description	Interval for send processing of the results of custom monitoring(msec)
Data type	Integer
Default value	1000

Parameter[monitor.winevent.filter.interval]

Property	monitor.winevent.filter.interval
Property name	Monitoring interval of Windows Event Monitor
Description	Monitoring interval of Windows Event Monitor(msec)
Data type	Integer
Default value	10000

Parameter[monitor.winevent.filter.timeout]

Property	monitor.winevent.filter.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[monitor.winevent.buffer]

Property	monitor.winevent.buffer
Property name	Buffer size of Windows Event monitor
Description	Description Command timeout of event retrieving command for Windows Event Monitor(msec).
Data type	Integer
Default value	1000000

Parameter[monitor.winevent.maxevents]

Property	monitor.winevent.maxevents
Property name	Maximum event log collected by event log retrieving command.
Description	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	-1

Parameter[monitor.winevent.mode]

Property	monitor.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

Othe	auto : automatically decided by OS (With Windows Server 2008/2012, Windows 7, 8, or 8.1: wevtutil) 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[monitor.winevent.forwarding.queue.maxsize]

Property	monitor.winevent.forwarding.queue.maxsize
Property name	Maximum number of messages in internal cue for Windows Event Monitor
Description	Maximum number of messages in internal cue for Windows Event Monitor
Data type	Integer
Default value	5000

Parameter[monitor.winevent.forwarding.transport.maxsize]

Property	monitor.winevent.forwarding.transport.maxsize
Property name	Transmission division unit for processing to transmit result of Windows Event Monitor
Description	Upper-limit number of messages that can be transmitted at once by Windows event monitoring result transmission processing. If the number of messages in the internal cue is greater than the set value, transmission processing is divided.
Data type	Integer
Default value	100

Parameter[monitor.winevent.forwarding.transport.maxtries]

Property	monitor.winevent.forwarding.transport.maxtries
Property name	Maximum attempt count for send processing of the results of Windows Event Monitor
Description	Maximum attempt count for send processing of the results of Windows Event Monitor
Data type	Integer
Default value	900

Parameter[monitor.winevent.forwarding.transport.interval.size]

Property	monitor.winevent.forwarding.transport.interval.size
Property name	Trigger (number of messages) for trying processing to transmit result of Windows Event Monitor
Description	Number of messages that triggers trying processing to transmit result of Windows Event Monitor. The result transmission processing will be executed when the number of messages stored in the internal cue since the previous result transmission processing reaches the set value.
Data type	Integer
Default value	15

Parameter[monitor.winevent.forwarding.transport.interval.msec]

Property	monitor.winevent.forwarding.transport.interval.msec
Property name	Interval for send processing of the results of Windows Event Monitor(msec)
Description	Interval for send processing of the results of Windows Event Monitor(msec)

Data type	Integer
Default value	1000

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

Property	monitor.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[monitor.winevent.gt.char.replace]

Property	monitor.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[monitor.winevent.lt.char.replace]

Property	monitor.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>:8081/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 (msec)
Description	Timeout time when connecting to the Hinemos Manager(msec)
Data type	Integer
Default value	10000

Parameter[request.timeout]

Property	request.timeout
Property name	Receive timeout from the Hinemos Manager (msec)
Description	Timeout time when receiving from the Hinemos Manager(msec)
Data type	Integer
Default value	60000

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

15 ChangeLog

ChangeLog

Version	Date	Details
1st Edition	06/01/2015	First release
2nd Edition	09/18/2015	Second release
