MasterScope SystemManager G
EventCorrelationCmd
Batch Registration of the Monitoring Definitions
Operation Procedure Manual

Revision History

Edition	Chapter/Section	Details
First Edition	–	–

Table of contents

1. Preface

This document is an operation procedure manual that is used to perform the batch registration for the monitoring definitions of the event correlation by using a command on the manager in the MasterScope SystemManager G.

2. Supported OS

The supported OS is the same as that of the MasterScope SystemManager G manager.

3. Functional outline

The event correlation provides a function which analyzes whether the received message matches the specified rule, and issues a message that triggers the action performed depending on the analyzed result.

This function is used to import/export the rule definition and the group definition by using a command line on the manager.

The definition of the event correlation comprises two types of definition files; hierarchy definition file and rule definition file.

- The hierarchy definition file is a definition file that defines the event correlation group or rule hierarchy structure. The rule definition file is applied to every single rule that is defined in the hierarchy definition file.
- The rule definition file is a definition file that defines the rule monitoring condition that is defined to a rule defined in the hierarchy definition file, input/output event conditions, filter conditions and others.

3.1 Procedure of the batch import for the monitoring definition of the event correlation

Follow the procedure below to perform the batch import for the monitoring definition of the event correlation:

1. Create a hierarchy definition file and a category definition file with editor and others.

Or, export the event correlation settings by the EventCorrelationCmd EXPORT command, and then edit the output hierarchy definition file and the rule definition file with editor and others.

[Related item]

Hierarchy definition file

Rule definition file

EventCorrelationCmd EXPORT

2. Check the syntax of the hierarchy definition file and the rule definition file, and convert them to the object files.

[Related item]

EventCorrelationCmd SU

3. Import the object files that were converted by the "EventCorrelationCmd SU" command to the event correlation to apply.

[Related item]

EventCorrelationCmd IMPORT

4. Command Reference

■ EventCorrelationCmd command

This command can be used to define the rule monitoring definition of the event correlation, and to import/export the I/O event conditions, filter conditions, and others.

[Related item]

EventCorrelationCmd SU

EventCorrelationCmd IMPORT

EventCorrelationCmd EXPORT

4.1 EventCorrelationCmd SU

This command is used to check the syntax of the hierarchy definition file and the rule definition file, and to convert them to the object file.

- ■ This command exists on the machine where the manager is installed.
- ■ For the UNIX manager (HP-UX, Linux), execute it using an account that has root authority.

[Path]

Windows manager

<Manager Installation Directory>¥Manager¥bin¥EventCorrelationCmd.exe

UNIX manager (HP-UX, Linux)

<Manager Installation Directory>/Manager/bin/EventCorrelationCmd.exe

[Specification method]

EventCorrelationCmd.exe SU <SourceFile> [ObjectFile]

[Description]

This command is used to check the syntax of the hierarchy definition file and the rule definition file that are specified by argument <SoruceFile>, and to convert them into the object files on the manager. The object file name is specified by an absolute path by using argument [ObjectFile].

If the requisite parameter is omitted or is invalid, the usage is displayed. If an object file already exists in the path specified by <ObjectFile>, it is overwritten.

[Argument]

SourceFile	Specifies the name of the hierarchy definition file to be converted by using an absolute path. The file name cannot be omitted. Specifies the file output by EventCorrelationCmd EXPORT or the file created by the user.
ObjectFile	Specifies the object file name for which the hierarchy definition file is converted and output by using an absolute path. If it is omitted, an object file with the hierarchy definition file and the ″sgo″ extension is output in an identical directory to the hierarchy definition file.

[Return value]

0 is returned on success.

When the execution fails, a message is output to the standard output and the following values are returned according to the error details.

Return value	Details
1	Error in specifying an argument Specify the correct argument according to the displayed Help.
5	Failed to write into a file. Writing the file of the output target failed. Check the disc free space of the output destination or check whether the file attribute is read only. Contact the developer with the contents of "DetailCode: <Error detail code>" attached that is a standard output when problems cannot be solved.
6	The object file that was specified by argument <ObjectFile> has already existed. Specify an object file that has not existed by using argument <ObjectFile>.
7	The definition file that was specified by argument <SourceFile> does not exist. Specify a definition file that exists by using argument <SourceFile>.
8	Error in the format of the definition file Check the error detail, the line number where the format is incorrect, and the contents to correct the definition file.

[Note]

■ When the path for the arguments <SourceFile> and <ObjectFile> are specified as arguments including spaces, for example C: Program Files, it is required to enclose the path with double quotations ("").

■ The respective types of commands must be executed with Administrator authority. Start the command prompt with Administrator authority for Windows Server 2008 or later versions.

■ To execute these commands on the UNIX (HP-UX, Linux) manager, the following preparations are required.

- Library path setting
  Add the following path to environment variable LD_LIBRARY_PATH:

  /opt/UMF/Operations/Manager/bin

■ Specify UTF-8 for the locale of the execution environment.

[Related item]

Hierarchy definition file

Rule definition file

EventCorrelationCmd IMPORT

4.2 EventCorrelationCmd IMPORT

This command is used to import the object files that were converted by the ″EventCorrelationCmd SU″ command, to the event correlation view.

- ■ This command exists on the machine where the manager is installed.
- ■ For the UNIX manager (HP-UX, Linux), execute it using an account that has a root authority.

[Path]

Windows manager

<Manager Installation Directory>¥Manager¥bin¥EventCorrelationCmd.exe

UNIX manager (HP-UX, Linux)

<Manager Installation Directory>/Manager/bin/EventCorrelationCmd.exe

[Specification method]

EventCorrelationCmd.exe IMPORT [-N NodeID] <ObjectFile>

[Description]

This command is used to import the object files that were specified by argument <ObjectFile> to the event correlation view.

If a parameter is invalid, the usage is displayed.

[Argument]

-N NodeID	Specify the node ID of the group or rule to be imported when you want to update all of the rule definitions or rule (s) under the specified group under the event correlation. The node ID is the one which is displayed as the group ID or rule ID of the property view on the right of the screen when the group or rule node in the event correlation view is selected. Import fails when the node ID of a node that does not exist under the event correlation view. When ″00000000″ is specified for the node ID or when this parameter is omitted, all of the groups and rules under the event correlation view are the target to be imported.
ObjectFile	Specifies the object file name that is converted by the ″EventCorrelationCmd SU″ command by using an absolute path. The file name cannot be omitted.

[Return value]

0 is returned on success.

When the execution fails, a message is output to the standard output and the following values are returned according to the error details.

Return value	Details
1	Error in specifying an argument Specify the correct argument according to the displayed Help.
3	Fails to establish communication with manager Check that the manager is started up, and execute the command under the state where the manager is started up.
4	Failed in acquiring the definition mode Check whether the definition mode is acquired in the monitoring terminal. In addition, check whether there is any import/export currently being executed.
7	The specified file does not exist. Specify an existing file by using an argument.
9	The specified node ID does not exist. Specify an existing node ID by an argument.

[Note]

■ When the path for the argument <ObjectFile> is specified as an argument including spaces, for example C: Program Files, it is required to enclose the path with double quotations ("").

■ The respective types of commands must be executed with Administrator authority. Start the command prompt with Administrator authority for Windows Server 2008 or later versions.

■ To execute these commands on the UNIX (HP-UX, Linux) manager, the following preparations are required.

- Library path setting

  Add the following path to the environment variable LD_LIBRARY_PATH:

  /opt/UMF/Operations/Manager/bin

■ Specify UTF-8 for the locale of the execution environment.

[Supplementary]

An execution error occurs in the following cases.

■ The manager is stopped when the command is executed.

■ When the import and export commands are executed at the same time, or when the monitoring screen in the definition mode exists when the command is executed

■ When a file other than the object file that is created by the "EventCorrelationCmd SU" command is specified for the argument <ObjectFile>

[Related item]

EventCorrelationCmd SU

4.3 EventCorrelationCmd EXPORT

The command that is used to export the settings of the event correlation view that was set on the monitoring screen, to the hierarchy definition file and the rule definition file. The hierarchy definition file and category definition file are exported to the specified directory as ″Hierarchy.txt″ and ″Rule_<Rule ID>.txt″, respectively.

* The hierarchy definition file output by EventCorrelationCmd EXPORT and the hierarchy definition file output by BusinessCmd EXPORT both have an identical file name, ″Hierarchy.txt″.

When using the EXPORT command of both of the functions, specify different folders for <OutPutFile Path> of EventCorrelationCmd and <OutPutFile Path> of BusinessCmd.

If EXPORT is performed with the same folder specified, the existing hierarchy definition file is overwritten.

- This command exists on the machine where the manager is installed.
- For the UNIX manager (HP-UX, Linux), execute it using an account that has a root authority.

[Path]

Windows manager

<Manager Installation Directory>¥Manager¥bin¥EventCorrelationCmd.exe

UNIX manager (HP-UX, Linux)

<Manager Installation Directory>/Manager/bin/EventCorrelationCmd.exe

[Specification method]

EventCorrelationCmd.exe EXPORT [-N NodeID] <OutPutFile Path>

[Description]

This command is used to export the currently set event correlation view setting to the directory that is specified for the argument <OutPutFile Path>, to the hierarchy definition file (Hierarchy.txt), and to the rule definition file (Rule_<Rule ID>.txt).

When the argument <NodeID> is specified, the hierarchy definition file is exported to the ″Hierarchy_<NodeID>.txt.″

If a parameter is invalid, the usage is displayed. If the hierarchy definition file and rule definition file already exist in the path specified by <OutPutFile Path>, they are overwritten.

[Argument]

– N NodeID	Specify the node ID of the group or rule to be exported when you want to export all of the rule definitions or the specified rule definition under the specified group under the event correlation view. The node ID is the one which is displayed as the group ID or rule ID of the property view on the right of the screen when the group or rule node in the event correlation view is selected on the monitoring screen. Export fails when the node ID of a node that does not exist under the event correlation view. When "00000000" is specified for the node ID or when this parameter is omitted, all of the groups and rules under the event correlation view are the target to be exported. When "00000000" is specified for the node ID, the hierarchy definition file is "Hierarchy.txt" as in the same manner as when the node ID is omitted.
OutPutFile Path	Specify the directory to which the hierarchy definition file and rule definition file are exported by using the absolute path. More than 200 characters cannot be specified for the path length. The file name cannot be omitted.

[Return value]

0 is returned on success.

When the execution fails, a message is output to the standard output and the following values are returned according to the error details.

Return value	Details
1	Error in specifying an argument Specify the correct argument according to the displayed Help.
3	Fails to establish communication with manager Check that the manager is started up, and execute the command under the state where the manager is started up.
4	Failed in acquiring the definition mode Check whether the definition mode is acquired in the monitoring terminal. In addition, check whether there is any import/export currently being executed.
5	Failed to write into a file. Writing the file of the output target failed. Check the disc free space of the output destination or check whether the file attribute is read only. Contact the developer with the contents of "DetailCode: <Error detail code>" attached that is a standard output when problems cannot be solved.
9	The specified node ID does not exist. Specify an existing node ID by an argument.

12	The character string length of the directory specified for <OutputFile Path> is too long. Specify a path whose length is less than 200 characters.

[Note]

■ The enable (the rule monitoring state after import) of the [RULECATEGORY] section in the hierarchy definition file is not imported upon export. Edit this parameter as needed when you want to update the rule monitoring state or when importing to a different environment.
For details, see “5.2.2 Rule definition”

■ When the path for the argument <OutPutFile Path> is specified as an argument including spaces, for example C: Program Files, it is required to enclose the path with double quotations (“”).

■ The respective types of commands must be executed with Administrator authority. Start the command prompt with Administrator authority for Windows Server 2008 or later versions.

■ To execute these commands on the UNIX (HP-UX, Linux) manager, the following preparations are required.

- Library path setting

  Add the following path to environment variable LD_LIBRARY_PATH:

  /opt/UMF/Operations/Manager/bin

■ Specify UTF-8 for the locale of the execution environment.

[Supplementary]

An execution error occurs in the following cases.

■ The manager is stopped when the command is executed.

■ When the import and export commands are executed at the same time, or when the monitoring screen in the definition mode exists when the command is executed

■ When a non-existing directory is specified for the parameter <OutPutFile Path>

■ When the argument <OutPutFile Path> is not a folder specification.

[Related item]

Hierarchy definition file

Rule definition file

5. Hierarchy definition file

In the hierarchy definition file, the definitions of the event correlation group and rule hierarchy structure are described.

When creating a hierarchy definition file, note the following.

■ With respect to the character code and line feed character in the file, specify UTF-16 (without BOM) and the CR+LF line feed character for the Windows manager while specifying UTF-8 (without BOM) and the LF line feed code for the UNIX manager.

■ Indents are added using the tab character in the file description examples in this document to improve readability, however deleting indents does not cause any problems. To add an indent, the tab character and one-byte spaces can be used.

■ The file is composed of a header part and a definition part. On the header part, the product name (SystemManager G) and the function name (EventCorrelation) are described while on the definition part, the descriptions of the definition are described in the section units (from [<Section name>] to [END_<Section name>]).

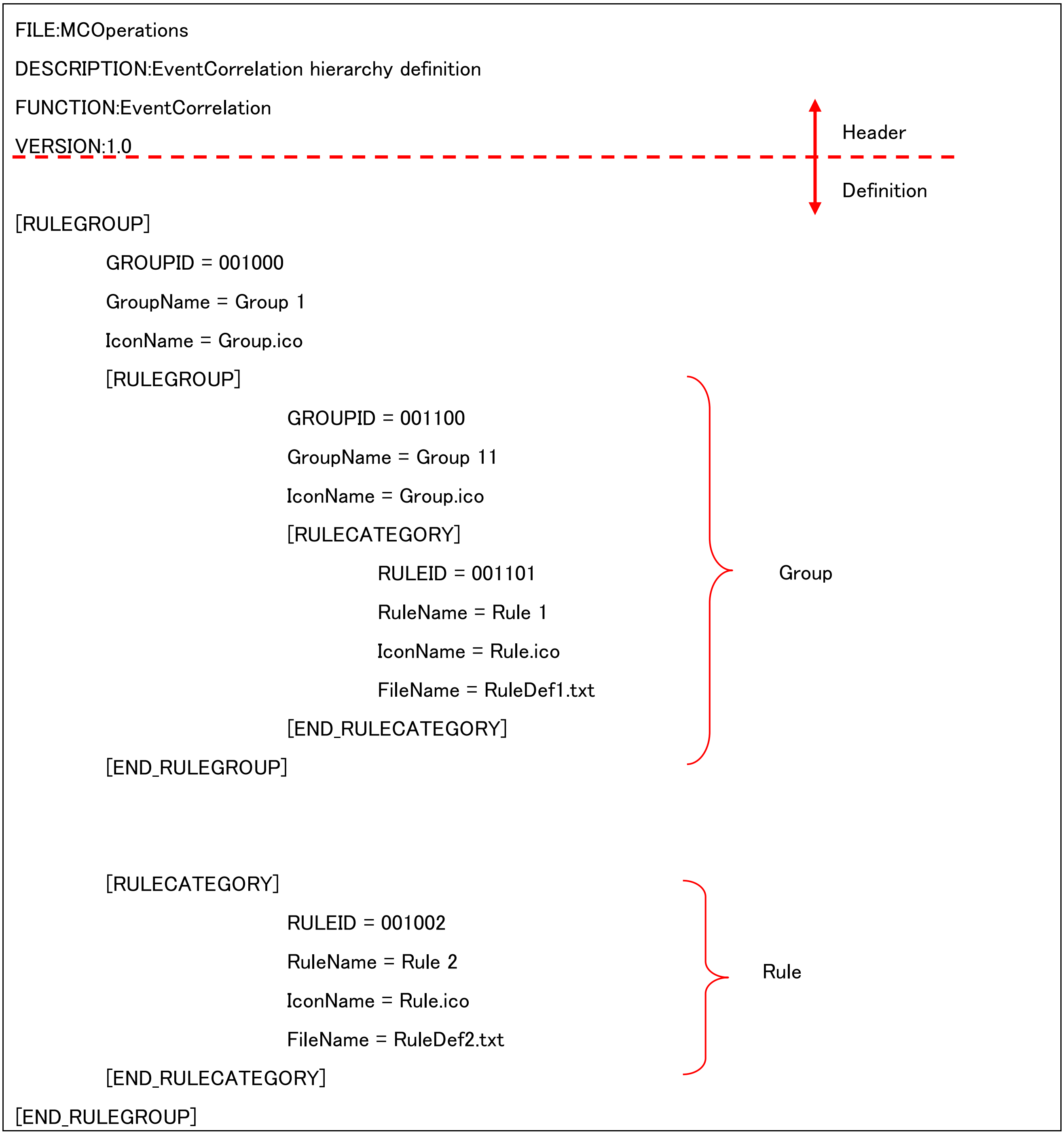
■ The histories that were accumulated in the past by the RULEID before the change cannot be viewed when the RULEID of the hierarchy definition file is changed. Special care shall be taken before the change.

■ For items where [Required] is described in the description of the "Value", the Key=Value line must be described when creating the hierarchy definition file. For items where no [Required] is described, they can be omitted; however, a whole line including the item must be omitted (Value only cannot be omitted when Key only is described).

■ For the comment, "#" must be added at the beginning of a line.

■ For the description of Value for which there is any description about the limit value for setting, the Japanese setting can be set.

[Example of description]



```
FILE:MCOperations
DESCRIPTION:EventCorrelation hierarchy definition
FUNCTION:EventCorrelation
VERSION:1.0

[RULEGROUP]
          GROUPID = 001000
          GroupName = Group 1
          IconName = Group.ico
          [RULEGROUP]
                              GROUPID = 001100
                              GroupName = Group 11
                              IconName = Group.ico
                              [RULECATEGORY]
                                        RULEID = 001101
                                        RuleName = Rule 1
                                        IconName = Rule.ico
                                        FileName = RuleDef1.txt
                              [END_RULECATEGORY]
          [END_RULEGROUP]


          [RULECATEGORY]
                              RULEID = 001002
                              RuleName = Rule 2
                              IconName = Rule.ico
                              FileName = RuleDef2.txt
          [END_RULECATEGORY]
[END_RULEGROUP]
```

5.1 Header part

The character strings in the header part are described as below:

FILE:MCOperations	…Product name (fixed)
DESCRIPTION:EventCorrelation hierarchy definition	…Description (Any description within 256 characters with Japanese descriptions available)
FUNCTION:EventCorrelation	…Function name (fixed)
VERSION:1.0	…File version (fixed)
HIERARCHYINFO:<Information on the export hierarchy> (*1)	
EXPORTNODE:<Specified export node ID> (*1)	

(*1) Information which is output only when argument <NodeID> is specified upon export. This parameter cannot be edited. (It is not required to set and change this parameter.)

5.2 Definition part

5.2.1 Group definition

(1) [RULEGROUP] to [END_RULEGROUP]

In this section, the group definition is described..

For [RULEGROUP], multiple definitions can be described (for the number of groups). This section can be described under the root or under the [RULEGROUP] section.

Key	Value
GROUPID	ID No. for the group definition Specifies a unique ID number for the group in hexadecimal number (0 to 9, and A to F) within the range from 100 through FFFFFFFF. [Required] An ID No. indentical to the ID No. separately specified (for example, RULEID, ConditionID, EventID, FilterID) cannot be specified.
GroupName	Group name Describe the group name by using up to 64 characters. [Required] The name specified here is displayed in the event correlation view tree.
IconName	Icon file name to be used Describe an absolute path that is used as a group icon　by using up to 256 characters. The specified icon file must be located in the machine where the monitoring terminal is installed in advance, or in the machine where the Web monitoring terminal is started up.

5.2.2 Rule definition

(1) [RULECATEGORY] to [END_RULECATEGORY]

In this section, the rule configuration is described.

For [RULECATEGORY], multiple definitions can be described (for the number of categories). This section can be described under the root or under the [RULEGROUP].

Key	Value
RULEID	ID No. for the rule definition Specifies a unique ID number for the rule in 3-to-8 digit hexadecimal number (0 to 9, and A to F) within the range from 100 through FFFFFFFF. [Required] An ID No. indentical to the ID No. separately specified (for example, GROUPID, ConditionID, EventID, FilterID) cannot be specified. Precautions: The histories that were accumulated in the past by the RULEID before the change cannot be viewed when the RULEID of the hierarchy definition file is changed. Special care shall be taken before the change.
RuleName	Rule name Describe the rule name by using up to 64 characters. [Required] The name specified here is displayed in the event correlation view tree.
IconName	Icon file name to be used Describe an absolute path that is used as a rule icon by using up to 256 characters. The specified icon file must be located in the machine where the monitoring terminal is installed in advance, or in the machine where the Web monitoring terminal is started up.
FileName	File name of the rule definition file Describe the file name of the rule definition file in which the definition for this rule is described by using up to 256 characters. [Required] Specify an absolute path or a relative path from the path where the hierarchy definition file is located.
Update	Enabling/disabling of the rule definition update 0: Disable 1: Enable * This is set by default. Specify disabled when you do not want to perform update by importing another rule definition because there is not any change in the rule definition. Monitoring the rules that do not perform update is available during the import. The monitoring rule is temporarily disabled during the import when "Update" is enabled. Therefore, the rules that are monitored before the import are all reset. Note that resources cannot be utilized during the import when "Update" is disabled, resulting in delay of the monitoring.

Key	Value
Enable	Rule monitoring state after the import 0: Disable 1: Enable 2. To retain the state ＊ This is set by default (while it is enabled in the case of adding new rules). Specify the rule monitoring state (Enable/disable) after the import.

6. Rule definition file

This rule comprises the monitoring conditions and output events, and the settings about the individual conditions, for example, input events, are included in the monitoring conditions. Judgment is made according to the monitoring conditions for the defined rule, and then the rule generates an output event specified when the rule is established.

Monitoring condition, output event, monitoring key, and others are defined in the rule definition file.

When creating a rule definition file, note the following.

- ■ The rule definition file must be stored in an identical directory to the one where the hierarchy definition file is located.
- ■ With respect to the character code and line feed character in the file, specify UTF-16 (without BOM) and the CR+LF line feed character for the Windows manager while specifying UTF-8 (without BOM) and the LF line feed code for the UNIX manager.
- ■ Indents are added using the tab character in the file description examples in this document to improve readability, however deleting indents does not cause any problems. To add an indent, the tab character and one-byte spaces can be used.
- ■ The file is composed of a header part and a definition part. On the header part, product name (SystemManager G) and the function name (EventCorrelation) are described while on the definition part, the descriptions of the definition are described in section units.
- ■ For items where [Required] is described in the description of the "Value", the Key=Value line must be described when creating the hierarchy definition file. For items where no [Required] is described, they can be omitted; however, a whole line including the item must be omitted (Value only cannot be omitted when Key only is described).
- ■ For the comment, "#" must be added at the beginning of a line.
- ■ For the description of Value for which there is any description about the limit value for setting, the Japanese setting can be set.

[Example of description]

```
FILE:MCOperations
DESCRIPTION:EventCorrelation category definition
FUNCTION:EventCorrelation
VERSION:1.0

[RULE]
        RuleType = 0
        SameMonitorKey = 0
        [MONITORKEY]
                MonitorKeyName = Monitor key 1
                [COMPOSITIONGROUP]
                        CompositionGroupName = Constituent group 1
                        Component = a
                        Component = b
                [END_COMPOSITIONGROUP]
        [END_MONITORKEY]
        [CONDITION]
                CombinationType = 1
                ConditionID = 10001
                ConditionName = Occurrence condition1
                ConditionType = 3
                [INPUTEVENT]
                        EventID = 20001
                        EventName = Input event
                        [EXTRACTION_KEY]
                                MonitorKeyName = Monitor key 1
                                KeyRef = $MESSAGETEXT$
                                KeyType = 3
                                KeyStart =agent=
                                KeyEnd =)
                        [END_EXTRACTION_KEY]
                [END_INPUTEVENT]
```

Header

Definition

Monitoring key

Occurrence condition 1
(Prerequisites of
occurrence condition 2)

```
            [CONDITION]
                CombinationType = 1
                ConditionID = 10002
                ConditionName = Occurrence condition 2
                ConditionType = 3
                [INPUTEVENT]                                   Occurrence
                    EventID = 20002                            condition 2
                    EventName =   Input event                  (Occurrence
                    [EXTRACTION_KEY]                           condition 1
                        MonitorKeyName = Monitor key 1         connection
                        KeyRef = $MESSAGETEXT$                 condition)
                        KeyType = 3
                        KeyStart =agent=
                        KeyEnd =)
                    [END_EXTRACTION_KEY]
                [END_INPUTEVENT]
            [END_CONDITION]
    [END_CONDITION]
    [OUTPUTEVENT]
        EventID = 30001
        OutputEventType = 1
        QuoteNode = 1
        QuoteApplication= 1                                    Output event
        EventCategory = EventCorrelation
        MessageText = Abnormal event occurs in ServerA.
    [END_OUTPUTEVENT]
[END_RULE]
```

6.1 Header part

The character strings in the header part are described as below:

FILE:MCOperations	…Product name (fixed)
DESCRIPTION:EventCorrelation rule definition	…Description (Any description within 256 characters with Japanese descriptions available)
FUNCTION:EventCorrelation	…Function name (fixed)
VERSION:1.0	…File version (fixed)

6.2 Definition part

6.2.1 Rule definition

(1) [RULE]to [END_RULE]

Root section. This section describes the rule type and identical key monitoring in parallel (ON/OFF).

Multiple [RULE]s cannot be described in the rule definition file.

Key	Value
RuleType	Describe the rule type in numeric value. 0: Occurrence rule (To monitor the condition triggered by the input event occurrence) * This is set by default. 1: Deterrence rule (To deter the notice on the event)
SameMonitorKey	Describe whether to perform identical event monitoring in parallel, in the numeric value. 0: Do not perform * This is set by default. 1: Perform monitoring * Monitoring in parallel cannot be specified when settings other than ″Occurrence″ and ″Time″ are defined in the rule monitoring conditions.

6.2.2 Monitoring key name definition

(1) [MONITORKEY] to [END_MONITORKEY]

This section describes the monitoring key name that is extracted from the event message by specifying a character string.

This section can be described directly under the [RULE] section.

Multiple keys can be described for [MONITORKEY] (for the number of monitoring keys).

Up to 10 keys can be defined as the monitoring keys for a rule definition.

Key	Value
MonitorKeyName	Describe a monitoring key name by using up to 64 characters. [Required] Identical monitoring key names cannot be described under the [RULE] section.

6.2.3 Constituent group definition

(1) [COMPOSITIONGROUP] to [END_COMPOSITIONGROUP]

This section describes the constituent group in which a monitoring key is extracted from the event message by specifying the character string, and then the extracted character string is treated as an identical key.

This section can be described directly under the [MONITORKEY] section.

For [COMPOSITIONGROUP], multiple groups can be described to a monitoring key (for the number of constituent groups).

When Component includes the wildcard specification and a message matches the multiple specifications, correlation is performed for a component that is regarded as a component that belongs to the Component group described first.

(When Component does not include the wildcard specification, the definition order can be ignored.)

Example

```
[COMPOSITIONGROUP]
        CompositionGroupName = Constituent group A
        Wildcard = 1
        Component=Host1*
        Component=Host2*
[END_COMPOSITIONGROUP]
[COMPOSITIONGROUP]
        CompositionGroupName = Constituent group B
        Wildcard = 1
        Component=Host2*
        Component=Host3*
[END_COMPOSITIONGROUP]
```

In the example described above, Host20, Host21, and others match both constituent group A and constituent group B; however, it is assumed and controlled as a component that belongs to constituent group A because it is described first.

Key	Value
CompositionGroupName	Describe a constituent group name by using up to 64 characters. [Required] You cannot specify identical monitoring group names under the [MONITORKEY] where a monitoring key name is defined.
Component	Describe a component name (equipment, host, and others) that is used to extract a monitoring key by using the specified character string and that is treated as an identical key, by using up to 256 characters. The number of components that can be defined in the [COMPOSITIONGROUP] section is up to 10,000. Identical component names cannot be described under the monitoring key. Example When ServerA, ServerB, and ServerC are extracted by the monitoring key and you want to treat them as an identical key, define the component name as described below: [COMPOSITIONGROUP] CompositionGroupName=Identical key group A Component=ServerA Component=ServerB Component=ServerC

Key	Value
Wildcard	Describe in numeric value whether to utilize the wildcard (*) for the component name. 0: Does not specify the wildcard * This is set by default. 1: Specifies the wildcard

6.2.4 Condition definition

(1) [CONDITION] to [END_CONDITION]

This section describes the condition to be monitored.

This section can be described under the [RULE] section or directly under the [CONDITION] section.

Multiple conditions can be described for [CONDITON] (for the number of conditions).

The number of monitoring conditions (excluding AND/OR) can be defined up to 32 when the rule type is an occurrence rule.

Only one monitoring condition can be defined when the rule type is a deterrence rule.

The conditions that can be set by the respective rule types are described below.

- Occurrence rule: ″Occurrence″, ″Number of times″, ″Time″
- Deterrence rule: ″Time deterrence″, ″Period deterrence″
-

In the case of an occurrence rule, conditions in combination can be defined.

Example 1

When the ″Occurrence″ condition A and ″Occurrence″ condition B are combined by the ″AND″ condition

(Rule is established when the condition in combination of conditions A and B.

```
Rule A
  +--″AND″ condition
       +---″Occurrence″ condition A
       +---″Occurrence″ condition B
```

Example 2

In the case of a combination of ″Occurrence″ condition A as a prerequisite for the ″Time″ condition B

(Rule is established when the condition B is established after condition A is established.)

```
Rule A
  +---″Occurrence″ condition A
       +---″Time″ condition B
```

Key	Value
ConditionID	ID No. for the condition definition Specifies a unique ID number for the condition in 3-to-8 digit hexadecimal number (0 to 9, and A to F) within the range from 100 through FFFFFFFF. [Required] An ID No. identical to the ID No. separately specified (for example, GROUPID, RULEID, EventID, FilterID) cannot be specified.
ConditionName	Describe a condition name by using up to 64 characters. [Required] Identical condition names cannot be specified under the [RULE]. * This parameter setting is not necessary when the condition combination type (CombinationType) is "AND" or "OR."
CombinationType	Describe the condition combination type in numeric value. [Required] 1: Condition (this is specified when defining the monitoring conditions, for example, "Occurrence", "Time", "Number of times", "Time deterrence", and others) 2: "AND" condition 3: "OR" condition
ConditionType ConditionType!	Describe the condition combination type as a numeric value. [Required] 1: Time deterrence 2: Period deterrence 3: Occurrence 4: Number of times 5: Time Describe by using ConditionType and ConditionType! when the negative condition is OFF and ON, respectively. Either ConditionType or ConditionType! is described. Note that the negative condition can be used only when the condition type is "Number of times" or "Time."
ResetTime	Describe the elapse time after the condition establishment to reset within the range from 1 to 864000. If it is omitted, reset is not performed after the condition establishment. The description is available only when the condition type is "Occurrence", "Number of times", or "Time".
TimeValue	Specifies the time to continue monitoring from when the input event occurs within the range from 1 to 864000. The description is available only when the condition type is "Occurrence", "Time", or "Time deterrence". The description cannot be omitted when the condition type is "Occurrence", "Time", or "Time deterrence".

Key	Value
CountValue	Describe the number of occurrences of input event within the range from 2 to 65535. The description is available only when the condition type is ″Number of times″. The description cannot be omitted when the condition type is″Number of times″.
BasePoint	Describe the base point of the deterred time for the time deterrence in numeric value. 1: To set the start event as a base point * This is set by default. 2: To set the end event as a base point The description is available only when the condition type is ″Time deterrence″.
EventCountType	Describe the type to be counted as a number of detected events of the period deterrence in numeric value. 1: To count only the input event　* This is set by default. 2: To count all of the events including deterrence start and deterrence end events. The description is available only when the condition type is ″Period deterrence″.

6.2.5 Input event definition

(1) [INPUTEVENT] to [END_INPUTEVENT]

This section describes the filter definition for the message that is the input event for the condition, automatic message check, and mark making.

This section can be described only under the [CONDITION] section.

The definition must be made when (CombinationType) is a ″Condition.″ ″AND/OR″ condition cannot be defined.

Key	Value
EventID	ID No. for the event definition Specifies a unique ID number for the event in 3-to-8 digit hexadecimal number (0 to 9, and A to F) within the range from 100 through FFFFFFFF. [Required] An ID No. indentical to the ID No. separately specified (for example, GROUPID, RULEID, ConditionID, FilterID) cannot be specified.
EventName	Describe the event name by using up to 64 characters. [Required]
OutputEventUse	Describe whether to use the message that was issued as an output event, as an input event in numeric value. 0: Do not use 1: Use * This is set by default.

6.2.6 Monitoring key extraction definition

(1) [EXTRACTION_KEY] to [END_EXTRACTION_KEY]

This section describes the monitoring key extraction condition in order to extract the specified character string from the event (*) message.

This section can be described only under the respective event definition sections.

The monitoring key extraction definition cannot be omitted in the input event in which no prerequisite exists when the monitoring key name ("MONITORKEY") is defined in a rule.

Example

In the case of a combination of "Occurrence" condition A as a perquisite for the "Occurrence" condition B

Rule A (with the monitoring key 1 definition)

```
   +--"Occurrence" condition A (* It is required to define the monitoring key 1 extraction in the input event with
the occurrence condition in which no perquisite exists.)
         +---"Occurrence" condition B
```

* The event definition sections in which this section can be defined are listed below:

- [INPUTEVENT] (Input event)
- [RESETEVENT] (Reset event)
- [SUBSEQUENTEVENT] (Following event)
- [SUPPRESS_STARTEVENT] (Deterrence start event)
- [SUPPRESS_ENDEVENT] (Deterrence end event)

Key	Value
MonitorKeyName	Describe a monitoring key name by using up to 64 characters. [Required] Specify a key name identical to the monitoring key name that is described in the [MONITORKEY] section.

Key	Value
KeyRef	Describe the source of monitoring key message extraction by selecting any setting value from below: [Required] $APPLICATION$ Sets the application as a source of the monitoring key extraction. $CREATEDATE$ Sets the occurrence date as a source of the monitoring key extraction. $CREATEDATE$ Sets the occurrence time as a source of the monitoring key extraction. $EVENTCATEGORY$ Sets the event category as a source of the monitoring key extraction. $MESSAGEID$ Sets the message ID as a source of the monitoring key extraction. $MESSAGETEXT$ Sets the message text as a source of the monitoring key extraction. $NODE$ Sets the node as a source of the monitoring key extraction. $OBJECT$ Sets the object as a source of the monitoring key extraction. $SEVERITY$ Sets the severity as a source of the monitoring key extraction. Example KeyRef=$MESSAGETEXT$
KeyType	Describe the method (type) of extracting a monitoring key from the source of extraction. [Required] 1: Extracts all of the character string (All specifications). 2: Extracts by specifying the location of the characters and the number of characters to be extracted (Location specifications). 3: Extracts by specifying the characters in front and behind the character string to be extracted (Key specifications).
KeyPos	Describe the position of the characters of the monitoring key to be extracted from the extraction source in numeric value. [Required*] * It is required only when the extraction method (type) is the position specification.
KeyPosLength	Describe the number of characters of the monitoring key to be extracted from the extraction source in numeric value. [Required*] * It is required only when the extraction method (type) is the position specification.

Key	Value
KeyStart	Describe the character string before the monitoring key to be extracted from the extraction source. [Required*] When it is not specified, the character strings from the first character of the extraction source up to the character string specified by KeyEnd are extracted. When the character string including the single- and double-byte space (s) is specified, the character string is searched for the extraction source including space (s). Example KeyStart =agent In the case above, the character string of the ″Agent″ is compared and the position of the extracted character (s) is searched for. KeyStart =agent In the case above, the character string of the ″Agent″ (including the single-byte space (s) before the agent) is compared and the position of the extracted character (s) is searched for. * When the extraction method (type) is a key specification, either KeyStart or KeyEnd must be described.
KeyEnd	Describe the character string right after the monitoring key to be extracted from the extraction source. [Required*] When there is no specification, the character strings from those specified by KeyStart to the end of the extraction source are extracted. When the character string including the single- and double-byte space (s) is specified, the character string is searched for the extraction source including space (s). * When the extraction method (type) is a key specification, either KeyStart or KeyEnd must be described.

6.2.7 Reset event definition

(1) [RESETEVENT] to [END_RESETEVENT]

This section defines the filter of a message that is the event to reset conditions.

This section can be described only under the [CONDITION] section.

However, the description is only available when the condition type is ″Occurrence″, ″Number of times″, or ″Time″.

Key	Value
EventID	ID No. for the event definition Specifies a unique ID number for the event in 3-to-8 digit hexadecimal number (0 to 9, and A to F) within the range from 100 through FFFFFFFF. [Required] An ID No. indentical to the ID No. separately specified (for example, GROUPID, RULEID, ConditionID, FilterID) cannot be specified.

Key	Value
EventName	Describe the event name by using up to 64 characters. [Required]
OutputEventUse	Describe whether to use the message that was issued as an output event, as a reset event in numeric value. 0: Do not use 1: Use * This is set by default.

6.2.8 Following event definition

(1) [SUBSEQUENTEVENT] to [END_SUBSEQUENTEVENT]

This section defines the filter of a message that is the following event of the time condition.

This section can be described only under the [CONDITION] section.

However, the description is only available when the condition type is "Time". (In the case of the "Time" condition, one or more following event (s) must be defined.)

For this section, multiple definitions are available (for the following number of events).

Key	Value
EventID	ID No. for the event definition Specifies a unique ID number for the event in 3-to-8 digit hexadecimal number (0 to 9, and A to F) within the range from 100 through FFFFFFFF. [Required] An ID No. indentical to the ID No. separately specified (for example, GROUPID, RULEID, ConditionID, FilterID) cannot be specified.
EventName	Describe the event name by using up to 64 characters. [Required]
OutputEventUse	Describe whether to use the message that was issued as an output event, as a following event in numeric value. 0: Do not use 1: Use * This is set by default.

6.2.9 Deterrence start event definition

(1) [SUPPRESS_STARTEVENT] to [END_SUPPRESS_STARTEVENT]

This section defines the filter of a message that is the event to start the deterrence.

This section can be described only under the [CONDITION] section.

This section must be described when the condition type is in "Period deterrence" condition. This section cannot be described when the condition type is "Period deterrence".

Key	Value
EventID	ID No. for the event definition Specifies a unique ID number for the event in 3-to-8 digit hexadecimal number (0 to 9, and A to F) within the range from 100 through FFFFFFFF. [Required] An ID No. indentical to the ID No. separately specified (for example, GROUPID, RULEID, ConditionID, FilterID) cannot be specified.
EventName	Describe the event name by using up to 64 characters. [Required]
OutputEventUse	Describe whether to use the message that was issued as an output event, as a deterrence start event in numeric value. 0: Do not use 1: Use * This is set by default.

6.2.10 Deterrence end event definition

(1) [SUPPRESS_ENDEVENT] to [END_SUPPRESS_ENDEVENT]

This section defines the filter of a message that is the event to end the deterrence.

This section can be described only under the [CONDITION] section.

This section must be described when the condition type is in "Period deterrence" condition. This section cannot be described when the condition type is "Period deterrence."

Key	Value
EventID	ID No. for the event definition Specifies a unique ID number for the event in 3-to-8 digit hexadecimal number (0 to 9, and A to F) within the range from 100 through FFFFFFFF. [Required] An ID No. indentical to the ID No. separately specified (for example, GROUPID, RULEID, ConditionID, FilterID) cannot be specified.
EventName	Describe the event name by using up to 64 characters. [Required]
OutputEventUse	Describe whether to use the message that was issued as an output event, as a deterrence end event in numeric value. 0: Do not use 1: Use * This is set by default.

6.2.11 Output event definition

(1) [OUTPUTEVENT] to [END_OUTPUTEVENT]

This section defines the output event that is notified when the rule is established.

This section can be described only under the [RULE] section.

In this section, a single occurrence rule, a single deterrence start rule and deterrence end rule can each be defined.

Key	Value
EventID	ID No. for the event definition Specifies a unique ID number for the event in 3-to-8 digit hexadecimal number (0 to 9, and A to F) within the range from 100 through FFFFFFFF. [Required] An ID No. indentical to the ID No. separately specified (for example, GROUPID, RULEID, ConditionID, FilterID) cannot be specified.
OutputEventType	Describe the output message type in numeric value. [Required] 1: Outputs when rule is established. 2: Outputs when the first message of the event of the deterrence target is received. 3: Outputs when the last message of the event of the deterrence target is received. "1" is used for the occurrence rule while "2" and "3" are used for the deterrence rule.
QuoteEvent	Describe the source of quotation in numeric value when the message of the input event is quoted to the output message. 0: Quotes the contents of the input event that is detected first ＊This is set by default. 1: Detects the contents of the input event that is detected last
Severity QuoteSeverity	Describe the ID of the severity of the output message. For details about the severity ID, see "Appendix: Severity ID list". When the severity ID is omitted, "Normal" (SEV_NORMAL) (ID=264) is output. Specify the QuoteSeverity=1 setting when the severity of the input event is quoted. It is not necessary to describe the severity ID when QuoteSeverity=1 is specified.
CreateDateTime	Describe the type of the output message occurrence date to be used in numeric value. 0: Uses the current date and time 1: Uses the input event occurrence date and time ＊This is set by default.
Node QuoteNode	Describe the node name of the output message by using up to 256 characters. When the node name is omitted, the node name of the manager is output. When the node of the input event is quoted, specify QuoteNode=1. It is not necessary to describe the node name when QuoteSeverity=1 is specified.
Application QuoteApplication	Describe the application name of the output message by using up to 256 characters. When the application name is omitted, "Unified Management Framework" is output. Specify the QuoteSeverity=1 setting when the application name of the input event is quoted. It is not necessary to describe the application name when QuoteSeverity=1 is specified.

Key	Value
Object QuoteObject	Describe the object name of the output message by using up to 256 characters. When the object name is omitted, ″System″ is output. When the application name of the input event is quoted, specify QuoteObject =1. It is not necessary to describe the object name when QuoteSeverity=1 is specified.
MessageID QuoteMessageID	Describe the message ID of the output message by using up to 256 characters. When the message ID is omitted, ″00000000″ is output. Specify the QuoteSeverity=1 setting when the message ID of the input event is quoted. It is not necessary to describe the message ID when QuoteMessageID =1 is specified.
EventCategory QuoteEventCategory	Describe the event category name of the output message by using up to 256 characters. When the event category name is omitted, ″Unified Management Framework″ is output. Specify the QuoteEventCategory=1 setting when the event category name of the input event is quoted. It is not necessary to describe the event category name when QuoteEventCategory=1 is specified.
MessageText QuoteMessageText	Describe the message text of the output message by using up to 1024 characters. Specify the QuoteMessageText=1 setting when the message text of the input event is quoted. It is not necessary to describe the message ID when QuoteMessageText=1 is specified. The substitution variable name can be specified for the message text.

Key	Value
SelPos	Up to eight contents that are quoted from the contents of the message text of the input event can be specified with the position specification. They cannot be specified when the quotation from the input event of the message text is specified. Values are described with (<Position>, <Character string length>, ″<Substitution variable name>″). Double quotation ″″″cannot be used for the substitution variable name. <Position> Describe the position from what number of character string to start substitution in the message text within the range from 1 to 1024. <Character string length> Describe the character string length to be replaced for a variable within the range from 1 to 1024. ″<Substitution variable name>″ Describe the variable that replaces the contents to be quoted by using up to 64 characters. Example SelPos = (10, 3, ″CPUVALUE″) SelPos = (20, 2, ″STATUS″)

Key	Value
SelKey	Up to eight key values can be described for the contents that are quoted from the contents of the message text of the input event. Specifying the start key value and the end key value acquires the contents from the next to the start key value up to in front of the end key. They cannot be specified when the quotation from the input event of the message text is specified. Values are described with (″<Start key value>″, ″<End key value>″, ″<Substitution variable name>″). Double quotation, ″″″ cannot be used for the monitoring key value, end key value, and the substitution variable value. ″<Start key value>″ Describe the key value just before the contents that you want to quote from the message text by using up to 64 characters. ″<End key value>″ Describe the key value just after the contents that you want to quote from the message text by using up to 64 characters. ″<Substitution variable name>″ Describe the variable that replaces the contents to be quoted by using up to 64 characters. Example SelKey = (″Server group A″,″Failure″,″SVNNAME″) SelKey = (″Counter″,″Threshold value″,COUNTERNAME″)

6.2.12 Event filter definition

(1) [FILTER] to [END_FILTER]

This section describes the message filter of the respective events (*).

This section can be described only under the respective event definition sections.

Multiple message filters can be described (for the number of filters) in this section. Describe the message filters in ascending order from the one whose execution order is first when the multiple filters are described.

* The event definition sections in which this section can be defined are listed below:

- [INPUTEVENT] (Input event)
- [RESETEVENT] (Reset event)
- [SUBSEQUENTEVENT] (Following event)
- [SUPPRESS_STARTEVENT] (Deterrence start event)
- [SUPPRESS_ENDEVENT] (Deterrence end event)

When describing this section, note the following.

″!″, which indicates negation must be specified just before “=” as in “Key!=Value” continuously If space (s) is included, they are assumed as a part of the key.

Commas　(,)　and　double quotation marks (“) cannot be used in this dialog box.

Key	Value
FilterID	ID No. for the filter definition Specifies a unique ID number for the filter in 3-to-8 digit hexadecimal number (0 to 9, and A to F) within the range from 100 through FFFFFFFF. [Required] An ID No. indentical to the ID No. separately specified (for example, GROUPID, RULEID, ConditionID, EventID) cannot be specified.
FilterName	Describe the filter name by using up to 256 characters. [Required]
Severity Severity!	Describe the ID of severity. For details about the severity ID, see ″Appendix: Severity ID list″. Describe Severity when [Negation] is OFF, and Severity! when [Negation] is ON. Either Severity or Severity! is described.
Category Category!	Describe the filter condition to the category by using up to 32 characters in the regular expression format. Describe Category when [Negation] is OFF, and Category! when [Negation] is ON. Either Category or Category! is described.
Node Node!	Describe the filter condition to the node name by using up to 256 characters in the regular expression format. Describe Node when [Negation] is OFF, and Node! when [Negation] is ON. Either Node or Node! is described.
Application Application!	Describe the filter condition to the application name by using up to 128 characters in the regular expression format. Describe Application when [Negation] is OFF, and Application! when [Negation] is ON. Either Application or Application! is described.
Object Object!	Describe the filter condition to the object name by using up to 128 characters in the regular expression format. Describe Object when [Negation] is OFF, and Object! when [Negation] is ON. Either Object or Object! is described.
MessageID MessageID!	Describe the filter condition to the message ID by using up to 128 characters in the regular expression format. Describe MessageID when [Negation] is OFF, and MessageID! when [Negation] is ON. Either MessageID or MessageID! is described.

Key	Value
MessageText MessageText!	Describe the filter condition to the message text by using up to 1024 characters in the regular expression format. Describe MessageText when [Negation] is OFF, and MessageText! when [Negation] is ON. Either MessageText or MessageText! is described.
SelPos SelPos!	Up to 8 search conditions using the position specification in the message text can be described. Describe SelPos when [Negation] is OFF, and SelPos! when [Negation] is ON. Value is specified in the format of (<Position>, “<Comparison value>”, <Condition>). <Position> Specify the target of comparison from what number of the characters in the message text, or describe within the range from 1 to 1024. ″<Comparison value>″ Describe the value to be compared by using up to 64 characters. The comparison value shall be enclosed with the double quotations. The regular expression format cannot be used for the comparison value. <Condition> Any of the =, <>, >=, >, <=, < shall be described for the comparison value. When ″=″ is specified, matched values are compared while ″<>″ is specified, unmatched values are compared, and then when others are specified, binary values (character codes) are compared. Up to 8 keys including SelPos and SelPos! can be described as shown below: SelPos = (10,″Error″,=) SelPos!= (20,″Manager″,=) SelPos = (30,″Administrator″,=) Only keys can be specified as shown below: In the example below, the second setting has no definition. SelPos = (10,″Error″,=) SelPos = SelPos = (30,″Administrator″,=)

Key	Value
SelKey SelKey!	Up to eight search criteria by the key specification in the message text can be described. Describe SelKey when [Negation] is OFF, and SelKey! when [Negation] is ON. The value is specified in the format of (<Key value>, “<Comparison value>”, <Condition>). <Key value> Describe the key in the message text by using up to 64 characters. ″<Comparison value>″ Describe the values to be compared by using up to 64 characters. The comparison value shall be enclosed with double quotation marks. The regular expression format cannot be used for the comparison value. <Condition> Any of the =, <>, >=, >, <=, < shall be described for the comparison value. When ″=″ is specified, matched values are compared while ″<>″ is specified, unmatched values are compared, and then when others are specified, binary values (character codes) are compared. [Key value] and [Comparison value] used for [key specification] must be enclosed in separators in the message. Recognizable separators are one-byte space, double-byte space, (,), [,], {, }, < and >. Up to 8 keys including SelKey and SelKey! can be described as shown below: SelKey = (error_number,″2″,>=) SelKey!= (count,″0″,=) SelKey = (max,″8″,<=)

7. Precautions

- The import/export function cannot be used in the monitoring terminal/manager of the version prior to MasterScope MISSION CRITICAL OPERATIONS Ver4.2.0. Upgrade the version of all of the monitoring terminals and managers when those with the version prior to MasterScope MISSION CRITICAL OPERATIONS Ver4.2.0 are used. When the import function is performed in the monitoring terminal/manager of the version prior to MasterScope MISSION CRITICAL OPERATIONS Ver4.2.0, incorrect operation of the monitoring terminal and the manager, and damage on the monitoring definition file may possibly occur. In that case, reinstall the product, or perform restoration from the backup file.
- It is recommended to back up the monitoring definition file before performing the import function.
- The rule definition file to be imported must be stored in an identical directory to that where the hierarchy definition file is located.
- When importing, delete the existing definition by replacing them with that to be imported. However, information on the existing rule history is retained when the existing definition and the definition ID (GROUPID or RULEID) to be imported match.
- The option setting or information on the map view cannot be set or output by using the import/export function.
- The export function does not output the monitoring key definition when the setting is not set to enable. (The monitoring key definition is not output even if it is set in the "Monitor key setting" when the "Each Monitor key is monitored in parallel" checkbox of the monitoring option in the rule setting is not checked.)
- The order of the groups and rules that are output by the export function may not match the display on the monitoring function. (The order is sorted in the alphabetical order of the names when displaying them on the monitoring screen.)
- The file that was used to import and the file that is output by the export function do not always match even the file is exported immediately after it has been imported.

8. Appendix: Severity ID List

[System severity]

Severity display name (default)	Severity internal name	Severity ID
STOP	SEV_STOP	256
FATAL	SEV_FATAL	257
CRITICAL	SEV_CRITICAL	258
MAJOR	SEV_MAJOR	259
MINOR	SEV_MINOR	260
WARNING	SEV_WARNING	261
UNKNOWN	SEV_UNKNOWN	262
NOMESSAGE	SEV_NOMESSAGE	263
NORMAL	SEV_NORMAL	264
PROCESSSTOP	SEV_PROCESSSTOP	265
SERVICESTOP	SEV_SERVICESTOP	266
PERFUPERROR	SEV_PERFUPERROR	267
PERFLOWERROR	SEV_PERFLOWERROR	268
HOSTEMPTY	SEV_HOSTEMPTY	269
PERFUPWARNING	SEV_PERFUPWARNING	270
PERFLOWWARNING	SEV_PERFLOWWARNING	271
PROCESSUNKNOWN	SEV_PROCESSUNKNOWN	272
SERVICEUNKNOWN	SEV_SERVICEUNKNOWN	273
PERFUNKNOWN	SEV_PERFUNKNOWN	274
PROCESSRUN	SEV_PROCESSRUN	275
SERVICERUN	SEV_SERVICERUN	276
PERFNORMAL	SEV_PERFNORMAL	277
HOSTNORMAL	SEV_HOSTNORMAL	278
PROCESSUPERROR	SEV_PROCESSUPERROR	279
FORCEEND	SEV_FORCEEND	280
DELAY	SEV_DELAY	281
CONDSTOP	SEV_CONDSTOP	282
EXECUTING	SEV_EXECUTING	283
NOTEXEC	SEV_NOTEXEC	284
CONFIRMATION	SEV_CONFIRMATION	285
UNMANAGED	SEV_UNMANAGED	286

[User severity]

Severity internal name	Severity ID
USER1 … USER32	512 … 543

* The importance ID of the user importance USERn (n=1, 2, ..., 32) is 511+n.

[Mark severity]

Severity display name (default)	Severity internal name	Severity ID
MARK1	MARK1	768
MARK2	MARK2	769
MARK3	MARK3	770
	… MARK128	… 895

* The severity ID of the mark severity MARKn (n=1,2,…,128) is 767+n.

* With respect to MARK1 through MARK3, ″ MARK1″, ″ MARK2″, and ″ MARK3″ are set by default; however, edit and use MARK* as needed for use from the [Option Setting]–[Priority Setting.