MasterScope SystemManager G Ver8.0.0
Cloud Service (AWS) Monitoring Function
User's Guide

July 2018

NEC Corporation

1. Microsoft, Windows, and Windows Server are registered trademarks of Microsoft Corporation in the United States of America and other countries. Other Microsoft products mentioned in this guide are also registered trademarks of Microsoft Corporation in the United States of America and other countries.
2. Amazon and AWS are trademarks or registered trademarks of Amazon.com, Inc. in the United States of America and other countries.
3. Other product names, company names, and proper nouns mentioned in this document are trademarks or registered trademarks of their respective companies.
4. The TM and ® marks are not included in the text or figures of this document.
5. The specifications or designs of windows shown in this document are subject to change without notice to improve the product.

Contents

Chapter 1 About This Document 1

Chapter 2 About Cloud Service (AWS) Monitoring 2

Chapter 3 System Requirements 3

Chapter 4 Installation 4

4.1 Installing a remote monitoring agent 4

4.2 Registering a license 4

Chapter 5 Monitoring Setup 5

5.1 Adding a host to be monitored 5

5.1.1 Adding the remote monitoring agent 5

5.1.2 Specifying the authentication information for cloud service (AWS) monitoring 6

5.1.3 Moving the monitoring target (AWS) to the topology view 13

5.2 Setting up performance monitoring 14

5.2.1 Specifying the resource subject to performance monitoring 14

5.2.2 Specifying the instance subject to performance monitoring 15

5.2.3 Specifying the counter subject to performance monitoring 16

5.2.4 Cautions 17

5.3 Setting up cloud event monitoring 18

5.3.1 Defining cloud event monitoring filters 18

5.3.2 Defining extraction conditions for cloud event monitoring 21

5.3.3 Changing information added to an event reported to message monitoring 25

5.3.4 Specifying options for cloud event monitoring 26

5.3.5 Displaying the content of the current event 28

5.4 Importing and exporting cloud service (AWS) monitoring definitions 31

Chapter 6 Uninstallation 32

6.1 Uninstalling a remote monitoring agent 32

6.2 Deleting settings from AWS 32

6.2.1 Deleting the CloudWatch event rule 32

6.2.2 Deleting the SQS queue 33

Chapter 7 Frequently Asked Questions 34

7.1 Cannot connect to AWS 34

7.1.1 Check the proxy server settings. 34

7.2 Events not displayed for cloud event monitoring 34

7.2.1 Check the settings of Amazon Web Services. 34

7.2.2 Changing the AWS CloudWatch event rule name or SQS queue name 35

7.3 Getting an event other than the EC2 instance status change in cloud event monitoring 36

7.3.1 Adding an AWS CloudWatch event rule 36

7.3.2 Adding an analysis rule for the added event 36

7.4 Restarting the remote monitoring agent 39

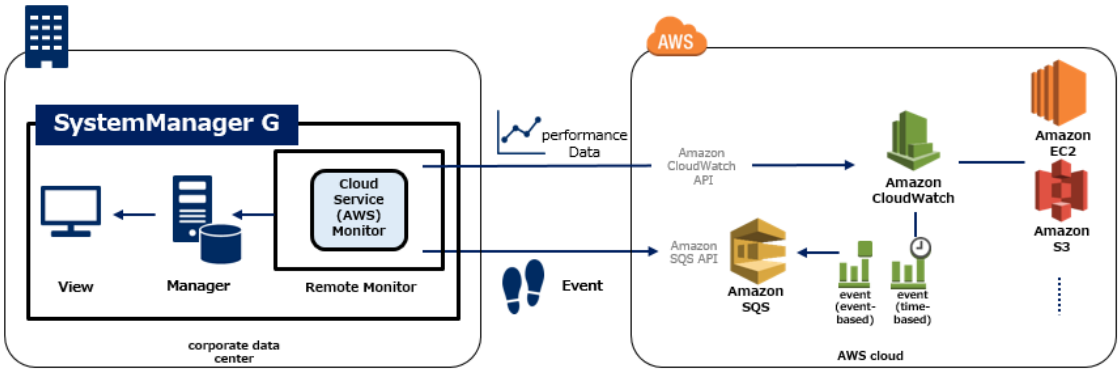
Chapter 8 Cautions 40

8.1 Creation of authentication information 40
8.2 Time of the remote monitoring agent 40
Chapter 9 Message List 41
9.1 AWS authentication messages 41
9.2 EC2 instance status change event 41

Chapter 1 About This Document

This document describes the setting procedures for monitoring Amazon Web Services by using the cloud service (AWS) monitoring functions of MasterScope SystemManager G.

Chapter 2 About Cloud Service (AWS) Monitoring



The cloud monitoring service (AWS) provides the following functions.

1. Performance monitoring

   The Amazon CloudWatch function is used to monitor the operation and performance metrics of the resources used in AWS.

2. Cloud event monitoring

   Amazon CloudWatch Events is used to monitor changes in the status of resources.

   In this version, a rule has been automatically added for transferring the EC2 instance status change event to the Simple Queue Service (SQS). Event information is retrieved from the SQS queue and sent as a message.

Chapter 3 System Requirements

■ Windows manager

This function is compatible with a Windows environment manager supported by SystemManager G. It cannot be used with an HP-UX or Linux manager.

■ Windows remote monitoring agent

Supported platforms

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

Required software

The following .Net Framework is required.

- Microsoft .Net Framework 3.5

■ Monitoring targets

The following API versions are supported.

Amazon Web Service	Version	API version
AWS CloudWatch	2013-02-22(1.1.0)	2010-08-01
AWS Simple Queue Service	2016-08-31	2012-11-05

■ Required license

This function is optional. To use this function, purchase the following license:

MasterScope SystemManager G Cloud Monitor for Amazon Web Service

Chapter 4 Installation

In this document, the installation directory of the product is described as follows:

%RemoteAgtInsDir%:	Installation directory of a remote monitoring agent
%RemoteAgtSgDir%:	SG directory of a remote monitoring agent

4.1 Installing a remote monitoring agent

Install a remote monitoring agent.
For information about how to install the product, see the MasterScope Media Release Memo. For detailed information about a remote monitoring agent, see the MasterScope SystemManager G Release Memo.

4.2 Registering a license

Cloud service (AWS) monitoring requires a license.
Register the license key from the monitoring window, and enable it by restarting the manager service. Once you register the license key, a code word application code is generated. Apply for the issuance of a code word, and register the issued code word.

If a license is not registered, the [Account setting detail] dialog box (*) does not show the [AWS] tab. (See “5.1.2 Specifying the authentication information for cloud service (AWS) monitoring.”)

Chapter 5 Monitoring Setup

To set up monitoring, perform the procedure below.

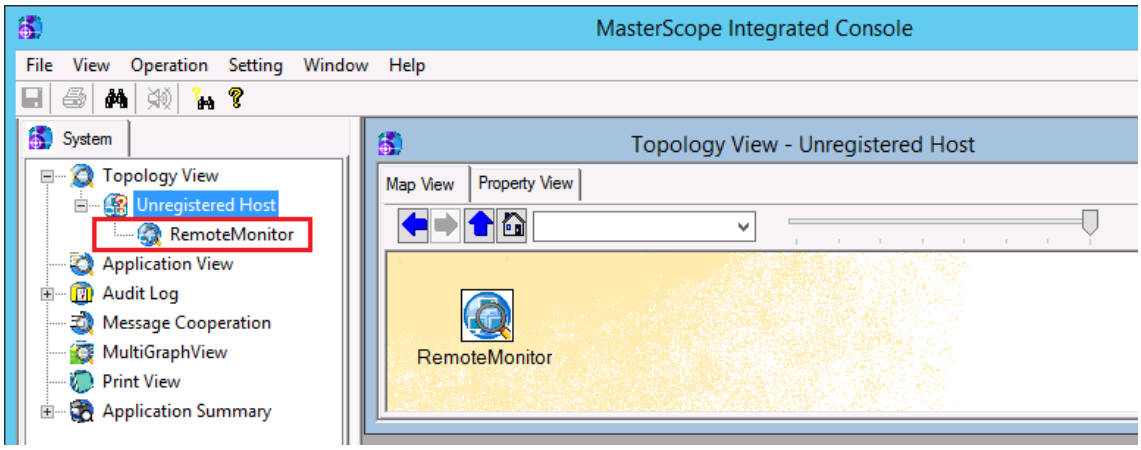
5.1 Adding a host to be monitored

5.1.1 Adding the remote monitoring agent

Open the monitoring window, and add the remote monitoring agent to the topology tree.

The new remote monitoring agent connected to the manager is automatically registered under the [Unregistered Host] group directly under the root node (topology view node).

The agent cannot be defined as a remote host when it is registered in the [Unregistered Host] group. Remote host definition becomes possible when the agent is moved directly under the root node (topology view node) or to a defined host group.



5.1.2 Specifying the authentication information for cloud service (AWS) monitoring

To perform cloud service (AWS) monitoring, the authentication information must be specified when adding a remote host.

1. Set up a proxy server.

   To access AWS via a proxy server, perform proxy server setup.

   If you do not use a proxy server, the setup is not necessary.

   Open the %RemoteAgtSgDir%\VMEventLogBase\CloudMonitoring.ini file.

   The character code of this file is UTF-16.

   Specify the proxy server and port number in the format below.

   ```
   [AWS]
   ProxyHost=proxyserver.xxx.yyy.jp
   ProxyPort=8080
   ```

   - ProxyHost

   Specify the proxy server. (Setting example: proxyserver.xxx.yyy.jp)

   The available characters are as defined in RFC 952. (The server name begins with an alphabetic character (a-z, A-Z) followed by an arbitrary sequence of alphabetic characters (a-z, A-Z), numbers (0-9), periods (.), and/or hyphen signs (-).)

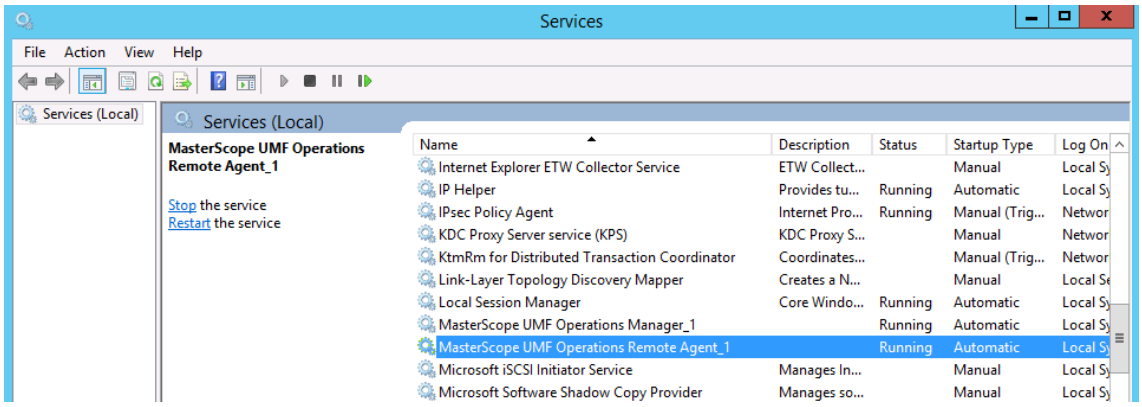
   The length may be up to 1,024 characters.

   - ProxyPort

   Specify the port number. (Setting example: 8080)

   After changing the settings, restart the remote monitoring agent service.

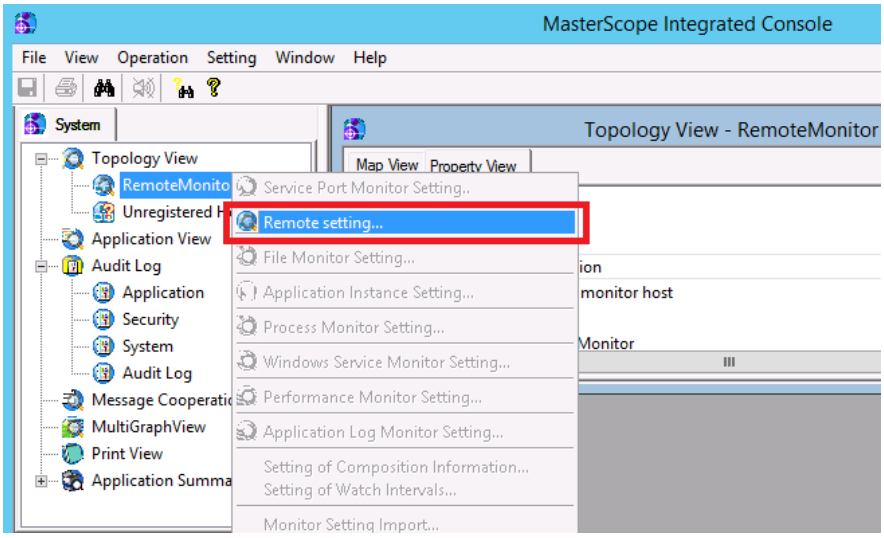
   Choose [Administrative Tools] → [Services] to restart the remote monitoring agent.



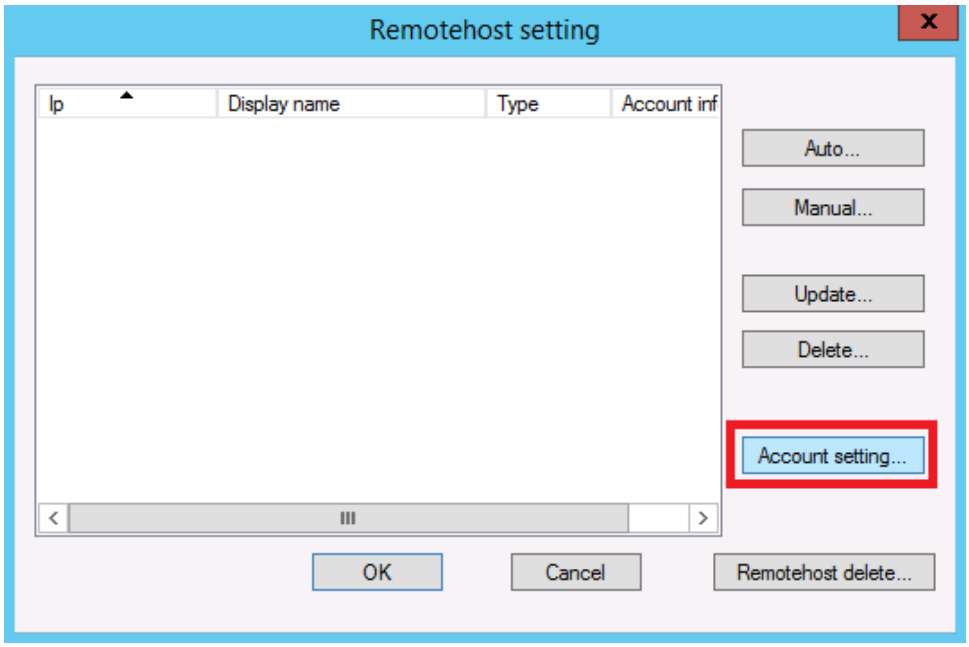
   The service name is “MasterScope UMF Operations Remote Agent_*xxx*_*n*”.

   xxx and *n* differ depending on your environment.

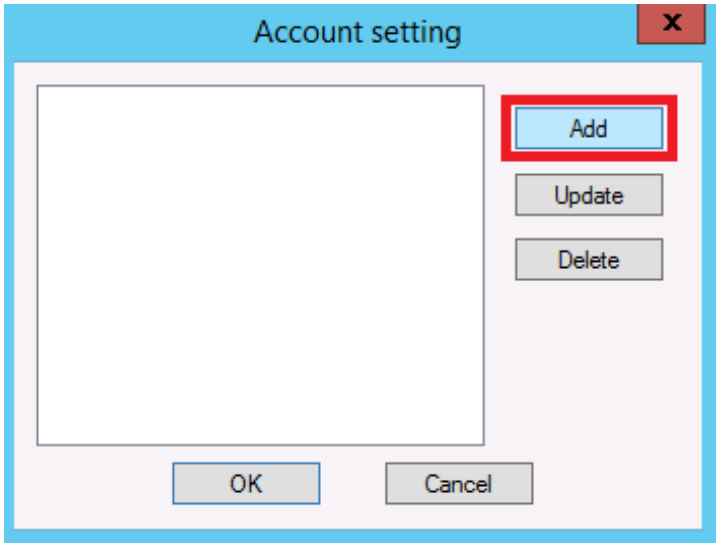
2. Right-click the remote monitoring agent in the topology view, and select [Remote setting] from the resulting menu.



3. When the [Remotehost setting] window is displayed, click [Account setting].

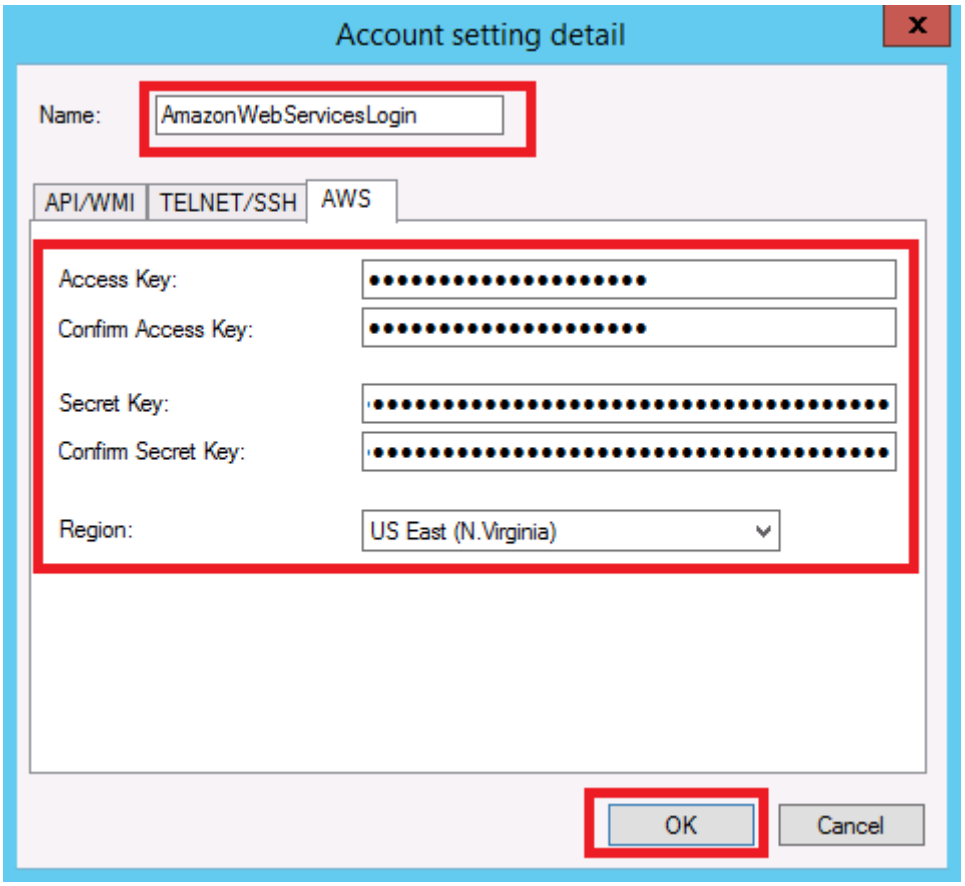


4. When the [Account setting] window is displayed, click [Add].



5. When the [Account setting detail] window is displayed, select the [AWS] tab. Enter the necessary items, and click the [OK] button.

To display the [AWS] tab, it is necessary to register a license for cloud service (AWS) monitoring in advance.



- [Name]

  Specify an arbitrary name for the authentication setting.

- [Access Key]/[Secret Key]

  Specify the access key and secret key created with AWS.

  For details, see the AWS document.

  Managing Access Keys for IAM Users

  http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_access-keys.html

  [Notes]

  ➢ When specifying an access key and secret key for SystemManager G, you can enter the characters shown below.

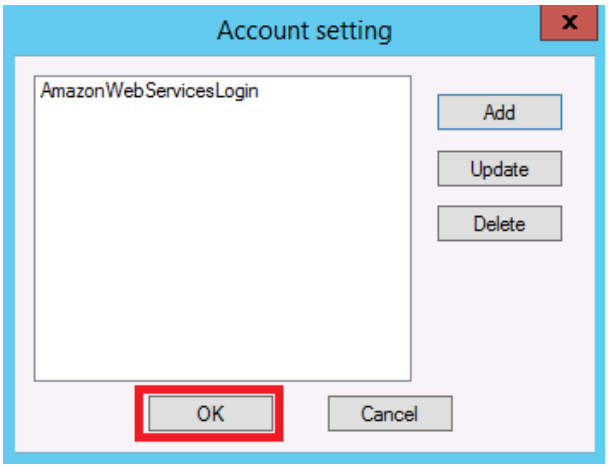
1234567890- ^qwertyuiop@[asdfghjkl;:]zxcvbnm,./!#$%&'()=~|QWERTYUIOP`{ASDFGHJKL+*} ZXCVBNM<>?_"\

  If any character output by Amazon Web Services is not included in the above, contact our maintenance service center.

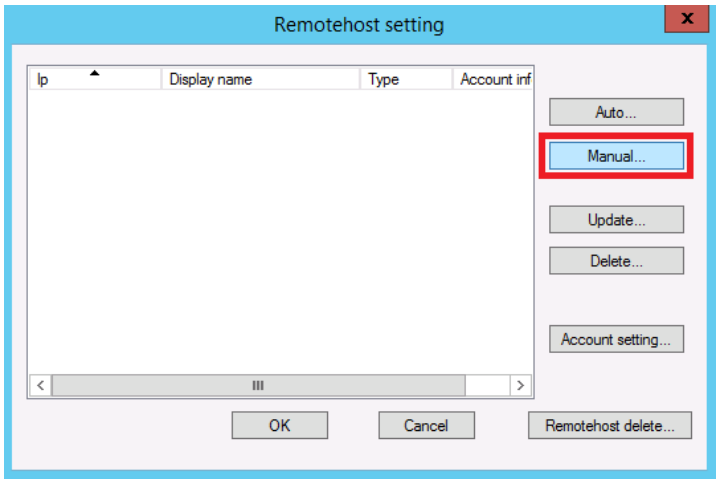
- [Region]

  Select the AWS region.

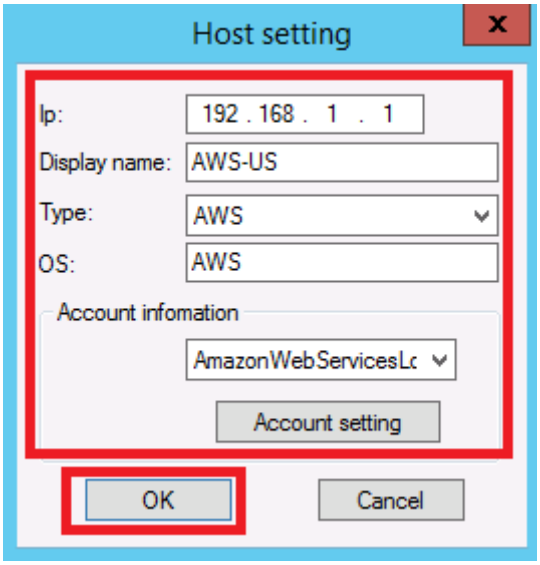
6. When the [Account setting] window is displayed, click the [OK] button.



7. When the [Remotehost setting] window is displayed, click the [Manual] button.



8. When the [Manual] window is displayed, enter the connection information and click the [OK] button.



- [Ip]

Specify the AWS host to be monitored.

This IP address is not used for the actual communication. Specify a value that is not identical to the IP address of any other remote host to be monitored.

- [Display name]

Specify the node name to be displayed in the topology view, by using up to 64 characters. This item must always be specified. The available characters are single-byte alphanumeric characters, hyphens (-), underscores (_), at signs (@), and periods (.).

The same node name that is already registered in the topology view cannot be specified.

If you specify a character string that is reserved for the system or not acceptable as a file or directory name, the host may fail to be monitored normally.

- [Type]

Select [AWS] from the pull-down list.

- [OS]

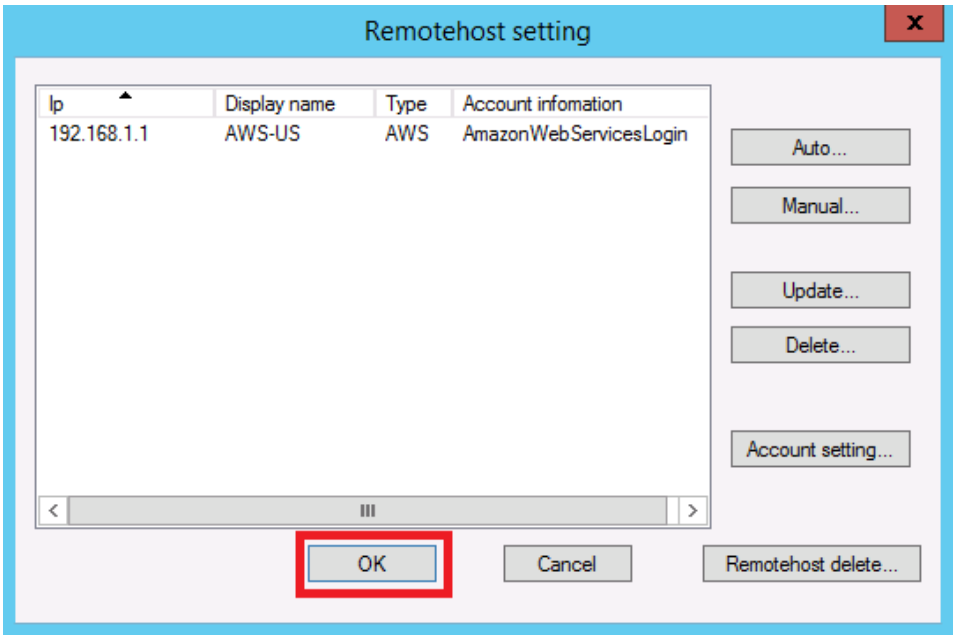
Specify the OS name by using up to 128 characters. This item is optional.

- [Account setting]

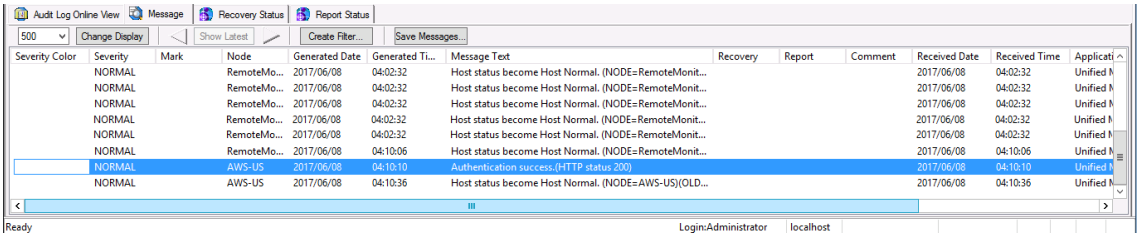
Select the registered authentication information to be used for remote host monitoring.

Select the authentication information created in step 5.

9. When the [Remotehost setting] window is displayed, click the [OK] button.

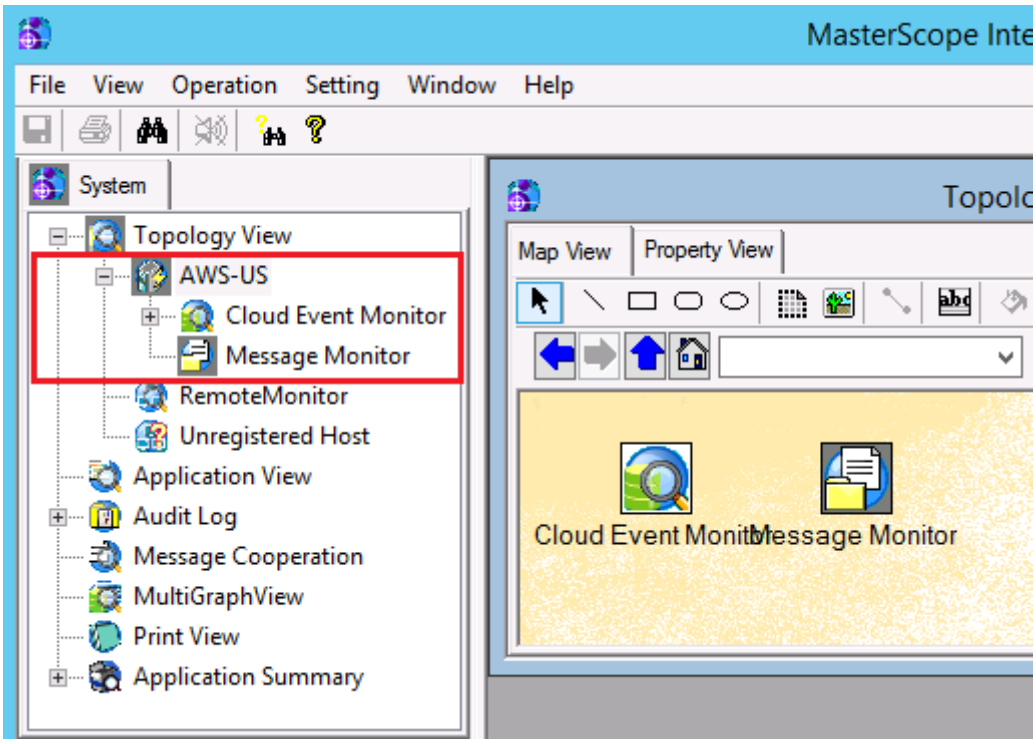


If the host is successfully authenticated, “Authentication success.” is displayed in the message view.



5.1.3 Moving the monitoring target (AWS) to the topology view

If successfully authenticated, the monitored node is connected under the [Unregistered Host] node in the topology view. Move it under the topology view.



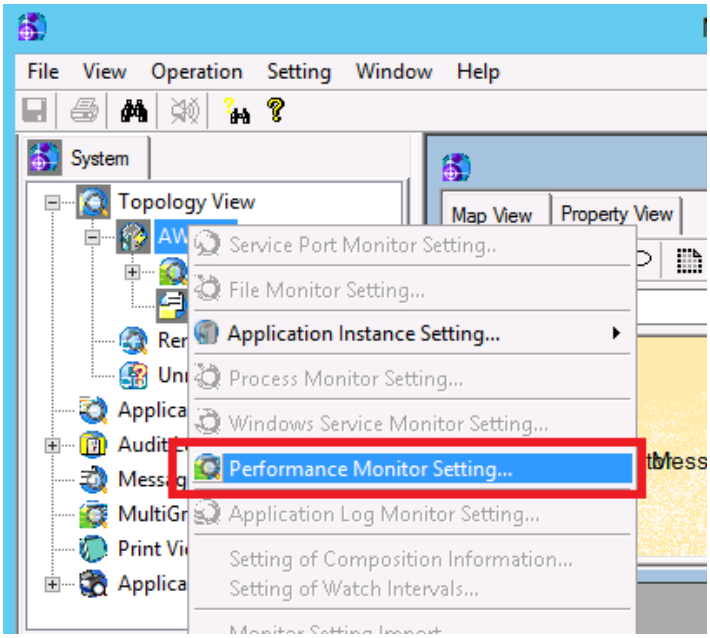
5.2 Setting up performance monitoring

Set up the object to be monitored (resource, instance, or counter) in the same way as the performance monitoring setup for remote host monitoring.

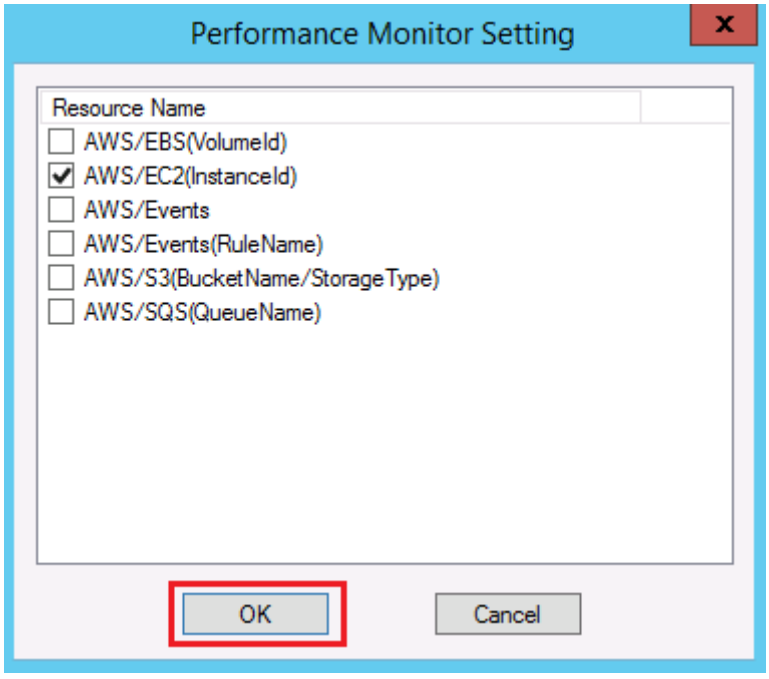
For a detailed window operation method, see also “About performance monitoring” and “About monitoring the performance on a remote host” of SystemManager G Manual (help).

5.2.1 Specifying the resource subject to performance monitoring

1. Right-click the AWS node in the topology view, and choose [Performance Monitor Setting].



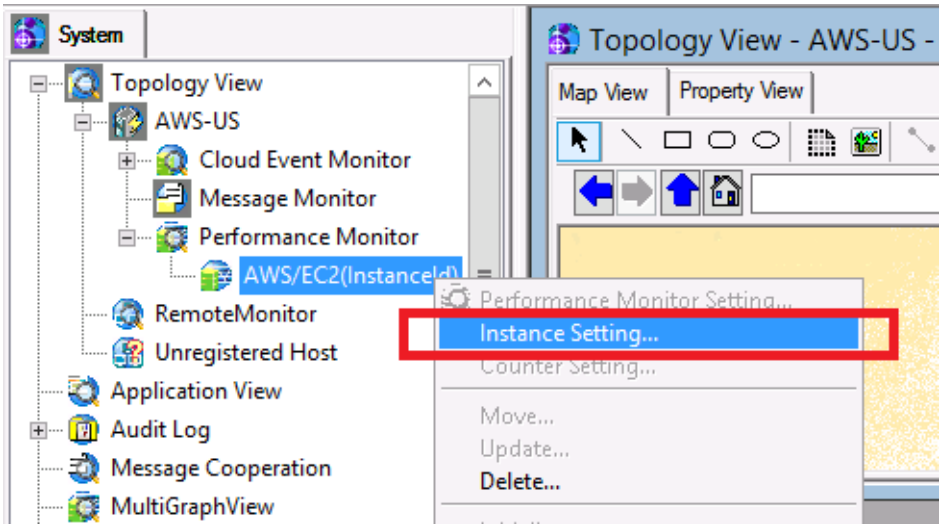
2. [Performance Monitor Setting] lists the namespaces for AWS CloudWatch.
   A namespace is displayed in the format of “namespace(dimension name)”.



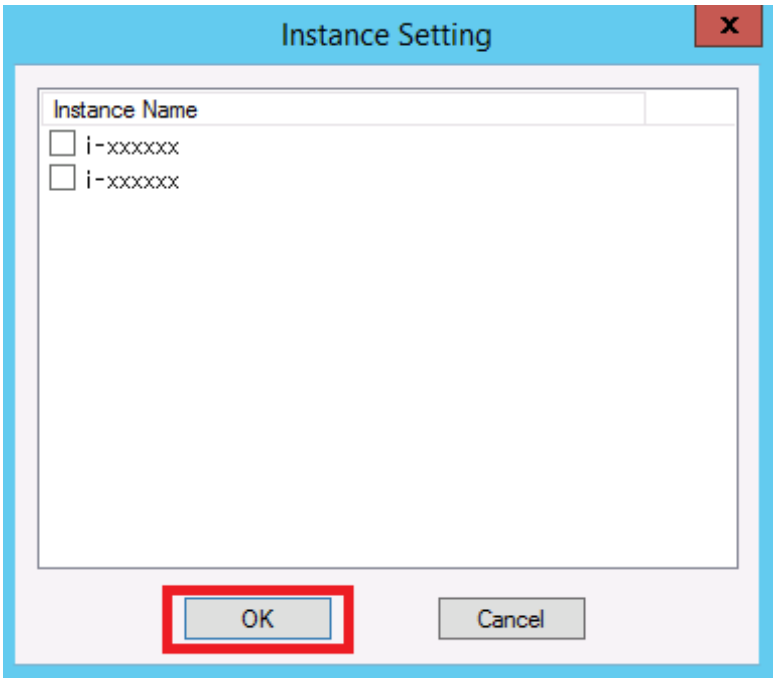
Select the check box of the item to be monitored, and click the [OK] button.

5.2.2 Specifying the instance subject to performance monitoring

1. Right-click the node added using [Performance Monitor Setting], and choose [Instance Setting].



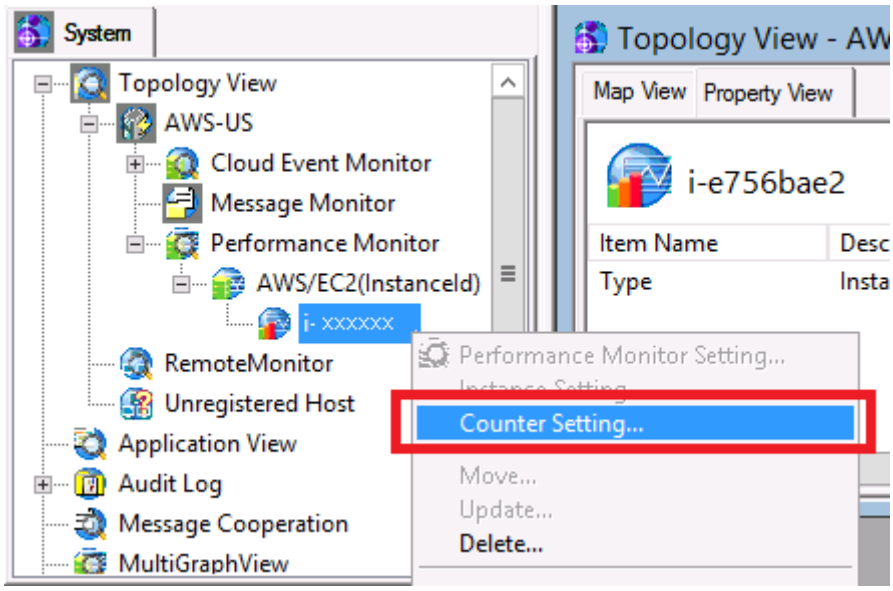
2. [Instance Setting] lists the monitoring targets corresponding to the dimension. In the case of EC2, instance IDs are listed.



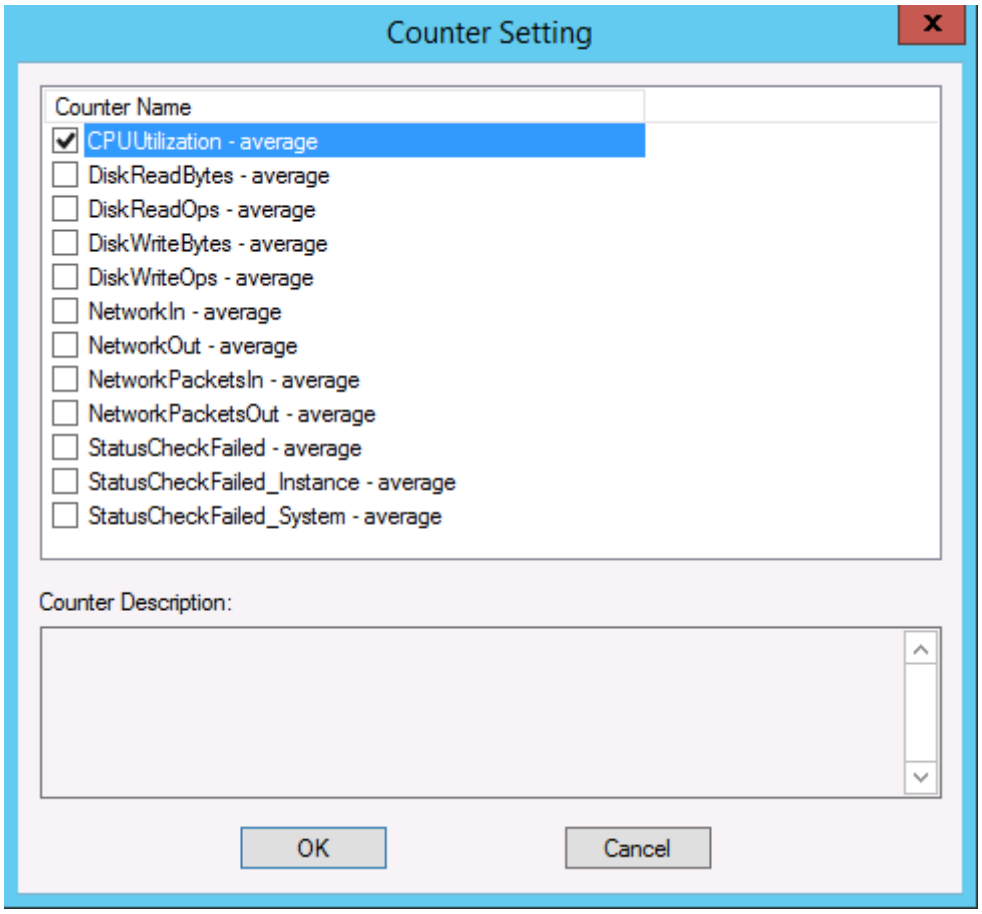
Select the check box of the item to be monitored, and click the [OK] button.

5.2.3 Specifying the counter subject to performance monitoring

1. Right-click the node added using [Instance Setting], and choose [Counter Setting].



2. [Counter Setting] lists the AWS metrics.



Select the check box of the metric to be monitored, and click the [OK] button.

[Notes]

- [Counter Description] is not displayed. See the AWS document.
  http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CW_Support_For_AWS.html

5.2.4 Cautions

1. When you set up the resource, instance, or counter specified with [Performance Monitor Setting], it may take time before the window is displayed because information needs to be acquired from Amazon Web Services.

2. The resource, instance, and counter displayed by the performance monitoring function for cloud service (AWS) monitoring correspond to the following items of Amazon Web Services.

Name for performance monitoring	AWS
Resource	Namespace(dimension name) When multiple dimension names exist, they are concatenated with a slash (/).
Instance	Item name of each individual dimension When multiple dimensions exist, they are concatenated with a slash (/).
Counter	Metrics

3. Length of an instance name
   If an instance name exceeds 128 characters in length, it is not displayed in the [Instance Setting] dialog box.

4. Interval of performance monitoring
   Cloud service (AWS) monitoring collects performance data from AWS CloudWatch at fixed 5-minute intervals.

5. Detailed monitoring for AWS EC2 instances
   When detailed monitoring for EC2 instances is enabled, performance data displayed at 5-minute intervals on AWS Management Console may be different from the data collected at 5-minute intervals by cloud service (AWS) monitoring if data are collected at different time points.

5.3 Setting up cloud event monitoring

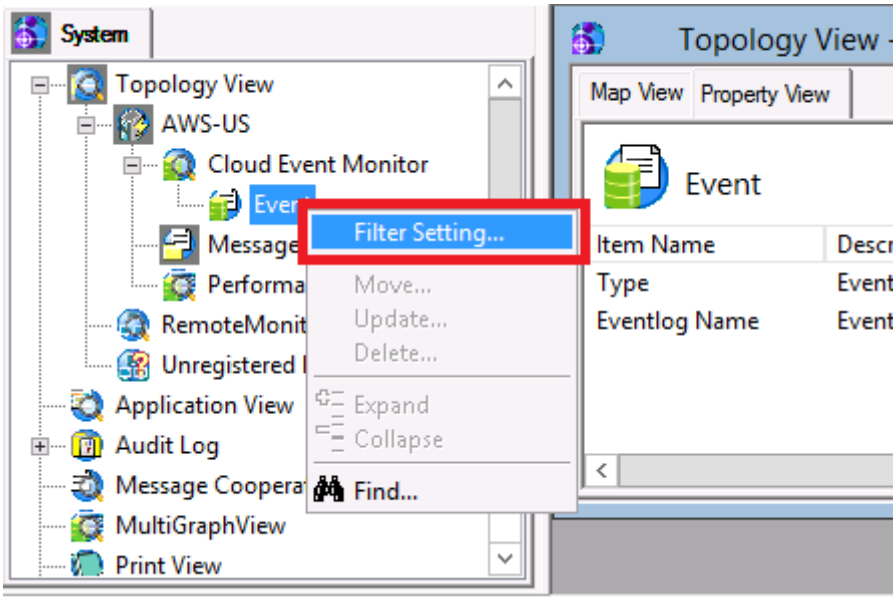
Events that occur on AWS are monitored.

By default, SystemManager G gets the EC2 instance status change event.

If you set a filter, the message monitoring function is notified when a specific event is output. To ensure necessary messages are detected, set filters as necessary in the same way as the event log monitoring setup for remote host monitoring.

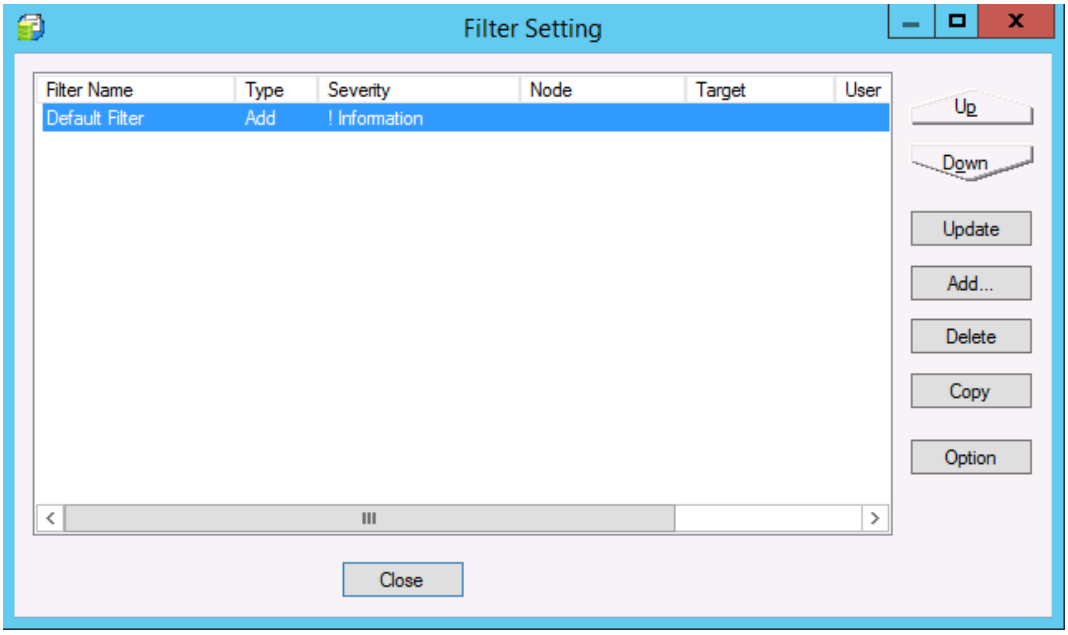
5.3.1 Defining cloud event monitoring filters

Define filters used to extract the events output on AWS to the message monitoring function.



Right-click [Event] of [Cloud Event Monitor] and choose [Filter Setting] from the resulting menu to display the [Filter Setting] dialog box.

For each filter, define a message extraction condition and the information to add when extracting.



The filter list, extraction condition for each filter, and importance to add are displayed. Filtering is processed sequentially from the top of the list to the bottom, and the operation of the filter definition whose condition is matched first is performed. The subsequent filtering processes after the first matched filter definition are not performed. Moreover, no message is reported when none of the filters match the condition.

- [Up] and [Down] buttons

You can change the execution order of the selected filter. The [Up] button switches the position of the selected filter to that of the filter immediately above it, and the [Down] button switches the position of the selected filter to that of the filter immediately below it.

- [Update] button

Redefine the definition details of the currently selected filter. Filter redefinition can also be performed by double-clicking the filter item in the list.

- [Add] button

Add a new filter at the position of the currently selected filter. The positions of the selected filter and subsequent filters are lowered one level each. If you click the [追加] button without selecting any filter, a new filter is added at the bottom.

- [Delete] button

Delete the currently selected filter.

- [Copy] button

Copy the currently selected filter. A filter having the same extraction condition and the same information to add other than the filter name is added at the selected position. The copy source

filter and the subsequent filters are lowered one level each.

- [Option] button

  Open the [Filter Option Setting] dialog box to specify the options for the event log monitoring function.

Immediately after remote host registration, you have [Default Filter] defined.
[Default Filter] is defined to filter the events whose importance is other than [Information] and notify the message monitoring function.

Importance is not set for AWS events.
Cloud event monitoring handles all AWS events as events whose importance is [Information].
To notify the message monitoring function, be sure to set filter definitions.

5.3.2 Defining extraction conditions for cloud event monitoring

Define the conditions for events of the output logs to be notified to message monitoring.

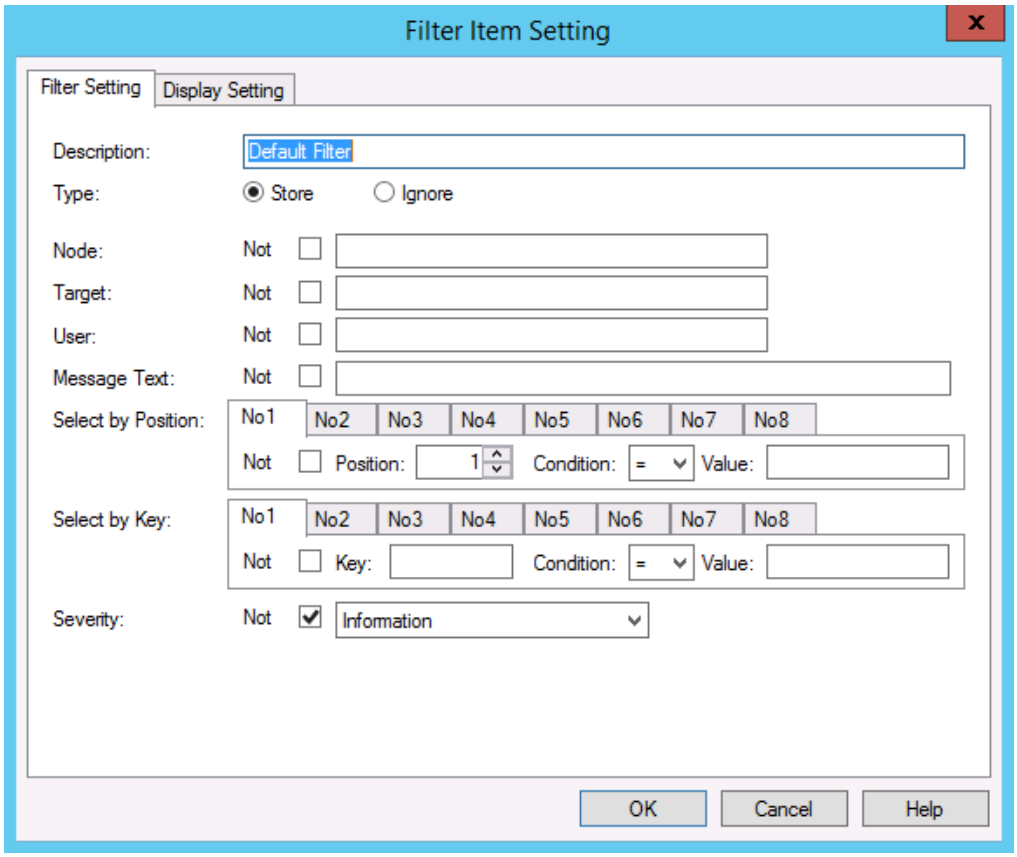
Define the filter extraction conditions in the [Filter Item Setting] dialog box. To display the [Filter Item Setting] dialog box, perform one of the following operations:

- Click the [Add] button in the [Filter Setting] dialog box.
- Select the filter to edit in the [Filter Setting] dialog box, and then click the [Update] button.
- Double-click the filter to edit in the [Filter Setting] dialog box.

When the [Filter Item Setting] dialog box is displayed, enter the extraction conditions in the [Filter Setting] tab and then click the [OK] button.

[Notes]

- When a condition is omitted, that condition is not used (all messages are targeted).
- For a message to be extracted, its content must match all the conditions specified here.
- Commas (,) and double quotation marks (“) cannot be used in this dialog box.



- [Description]

Specify the filter name by using up to 256 characters. The character string specified here is displayed as a filter name of the [Filter Setting] dialog box. [Description] cannot be omitted.

- [Type]

Specify the filter type. If you specify [Store], messages matching this filter are stored in the category. If you specify [Ignore], no message is reported for any log matching this filter and the filtering processing of the subsequent filters is not performed.

- [Node]

Specify the filter condition for the node by using up to 256 characters in the regular expression format. If a negative condition is specified, messages that do not match the regular expression condition are selected.

- [Target] (Target name of the message source)

Specify the filter condition for the target by using up to 128 characters in the regular expression format. If a negative condition is specified, messages that do not match the regular expression condition are selected.

- [User] (User name of the message source)

Specify the filter condition for the user by using up to 128 characters in the regular expression format. If a negative condition is specified, messages that do not match the regular expression condition are selected.

- [Message Text] (Main body of the message)

Specify the filter condition for the message text by using up to 1,024 characters in the regular expression format. If a negative condition is specified, messages that do not match the regular expression condition are selected.

- [Select by Position]

Specify up to 8 search conditions using the position specification in the message text. If a negative condition is specified, messages that do not match the condition are selected.

  - [Position]

    Specify the comparison start position (character number) in the message text in the range between 1 and 1,024.

  - [Condition]

    Specify the comparison condition.

  - [Value]

    Specify the value to compare by using up to 64 characters. The regular expression format cannot be used for [Value].

[Example] To extract messages where the 10th character in the message text is “abnormal”, specify the filter as shown below.

[Position]: 10
[Condition]: =

[Value]: abnormal

- [Select by Key]

Specify up to 8 search conditions using the key specification in the log content. If a negative condition is specified, messages that do not match the condition are selected.

  - [Key]

    Specify the key in the log content by using up to 64 characters.

  - [Condition]

    Specify the comparison condition. When [=] is specified, a regular expression is applied as a comparison value. When a condition other than [=] is specified, a binary comparison with the character string specified for [Value] is performed.

  - [Value]

    Enter the value to compare. When [=] is specified for [条件], specify [比較値] using a regular expression.

  [Example] To extract logs where error_number is 4 or less when the log content includes a character string “error_number = 5” (“5” is variable), specify the filter as shown below.

  [Key]: error_number
  [Condition]: <=
  [Value]: 4

  [Key] and [Value] used for [Select by Key] must be enclosed in separators in the log content. Recognizable separators are one-byte spaces, (,), [,], {, }, <, and >. A character string containing any two-byte space cannot be specified in [Key].

  Example:
  (error_number=1)

  Note that spaces between the key, “=”, and value are ignored.

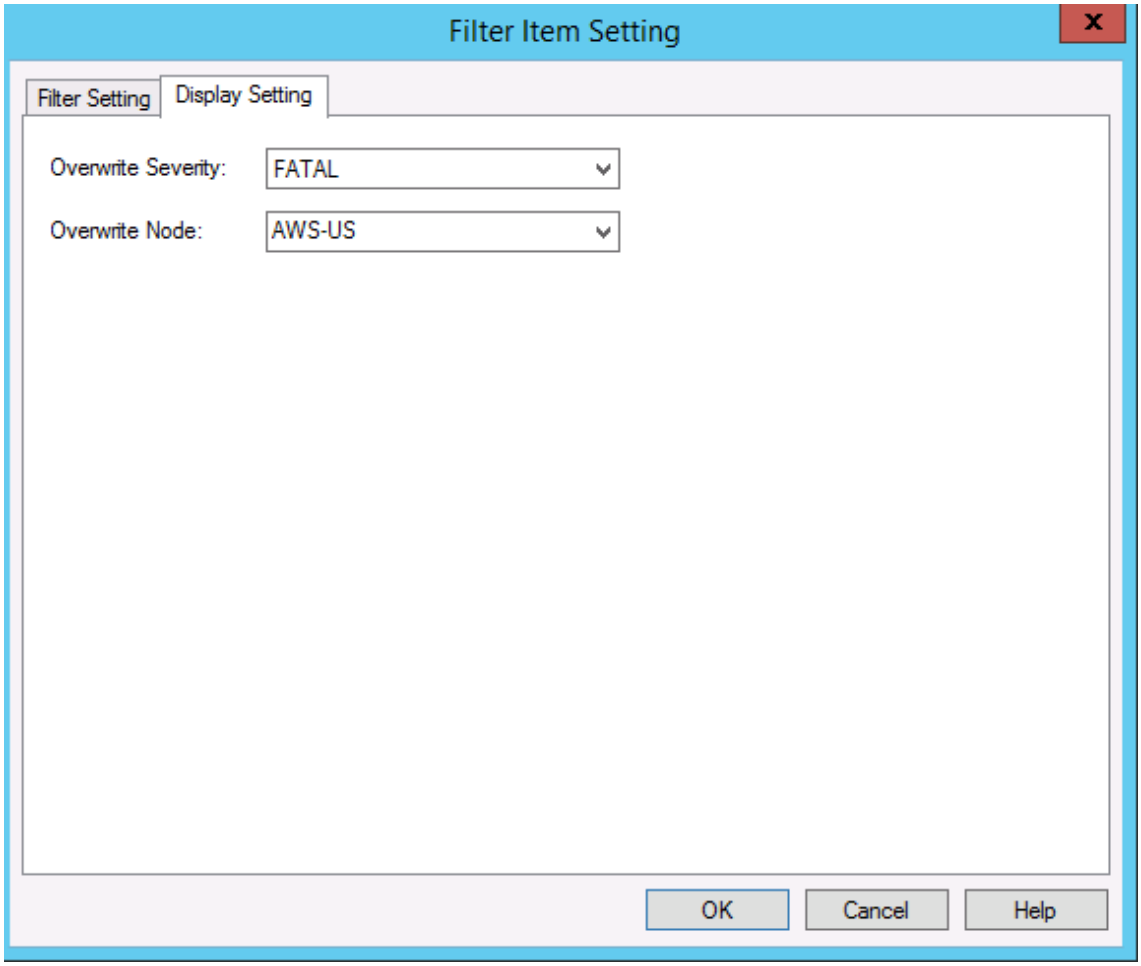
- [Severity]

This item corresponds to [Severity] of the event log. Select a search condition. If a negative condition is specified, messages that do not match the selected condition are targeted.

5.3.3 Changing information added to an event reported to message monitoring

Define the information to add when reporting an extracted event to message monitoring.

In the [Filter Item Setting] dialog box, enter the information to add on the [Display Setting] tab and then click the [OK] button.



- [Overwrite Severity]

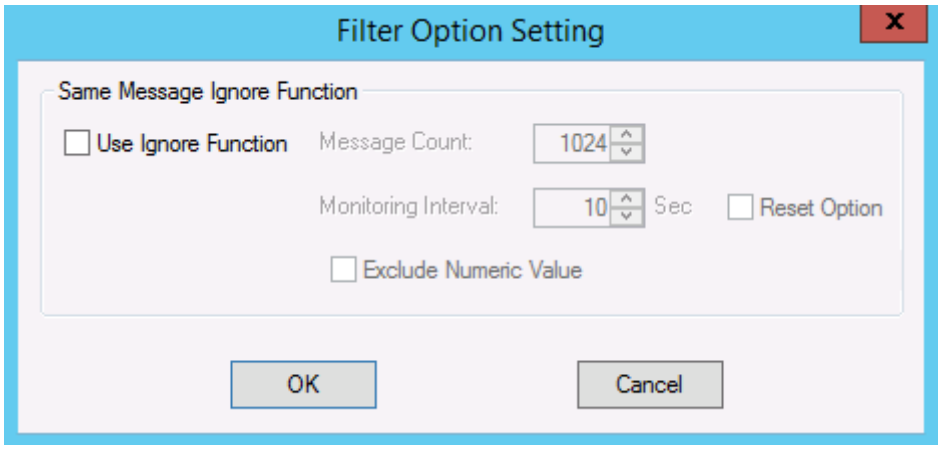
Change the importance of the message matching the filter condition to the specified one. A user mark cannot be used for the importance that can be changed using [Overwrite Severity].

- [Overwrite Node]

Change the node name of the message matching the filter condition to a node name specified by using up to 256 characters.

5.3.4 Specifying options for cloud event monitoring

To define options for cloud event monitoring, click the [Option] button in the [Filter Setting] dialog box. After specifying the options, click the [OK] button.



Same Message Ignore Function

- [Use Ignore function]

  Specify whether or not to report a message when identical events are output in a short period of time. If you select the [Use Ignore function] check box, a message is not reported for any identical log generated in the specified period of time, which helps suppress the number of messages.

- [Message Count]

  Specify the maximum number of logs of the log type for which to suppress the message reporting. Specify a value within the range of 256 to 4,096. The default value is 1,024.

  If the number of suppressed logs exceeds the value specified here, the oldest log (the one whose output has been suppressed for the longest time) is excluded from the suppression target.

- [Monitoring Interval]

  Specify the period during which the message is suppressed, starting from the time when an event is output. Specify a value within the range of 1 to 3,600 seconds. The default value is 10 seconds.

[Example] The following table shows whether or not to report a message and the operation to be performed when the monitoring interval is 1 minute (60 seconds) and events are output as shown below.

Time (Seconds)	Event	Reporting	Operation
000	LOG001	○	LOG001 is added to the suppression target (up to 60 seconds).
010	LOG002	○	LOG002 is added to the suppression target (up to 70 seconds).
020	LOG003	○	LOG003 is added to the suppression target (up to 80 seconds).

Time (Seconds)	Event	Reporting	Operation
030	LOG004	○	LOG004 is added to the suppression target (up to 90 seconds).
040	LOG001	×	A message is not reported because the log is the suppression target.
050	LOG002	×	A message is not reported because the log is the suppression target.
060	LOG004	×	A message is not reported because the log is the suppression target. LOG001 is excluded from the suppression target.
070	LOG001	○	LOG001 is added to the suppression target (up to 130 seconds). LOG002 is excluded from the suppression target.
080	LOG001	×	A message is not reported because the log is the suppression target. LOG003 is excluded from the suppression target.
090	LOG003	○	LOG003 is added to the suppression target (up to 150 seconds). LOG004 is excluded from the suppression target.

- [Reset Option]

  Specify whether or not to reset the period during which to suppress a message if an identical event is output. If you select this check box, the suppression period is reset every time an identical event is output.

[Example] The following table shows whether or not to report a message and the operation to be performed when the monitoring interval is 1 minute (60 seconds), the suppression period is set to be reset, and events are output as shown below.

Time (Seconds)	Event	Reporting	Operation
000	LOG001	○	LOG001 is added to the suppression target (up to 60 seconds).
010	LOG002	○	LOG002 is added to the suppression target (up to 70 seconds).
020	LOG003	○	LOG003 is added to the suppression target (up to 80 seconds).
030	LOG004	○	LOG004 is added to the suppression target (up to 90 seconds).
040	LOG001	×	A message is not reported because the log is the suppression target. The suppression period for LOG001 is reset (up to 100 seconds).

Time (Seconds)	Event	Reporting	Operation
050	LOG002	×	A message is not reported because the log is the suppression target. The suppression period for LOG002 is reset (up to 110 seconds).
060	LOG004	×	A message is not reported because the log is the suppression target. The suppression period for LOG004 is reset (up to 120 seconds).
070	LOG001	×	A message is not reported because the log is the suppression target. The suppression period for LOG001 is reset (up to 130 seconds).
080	LOG001	×	A message is not reported because the log is the suppression target. The suppression period for LOG001 is reset (up to 140 seconds). LOG003 is excluded from the suppression target.
090	LOG003	○	LOG003 is added to the suppression target (up to 150 seconds).

- [Exclude Numeric Value]

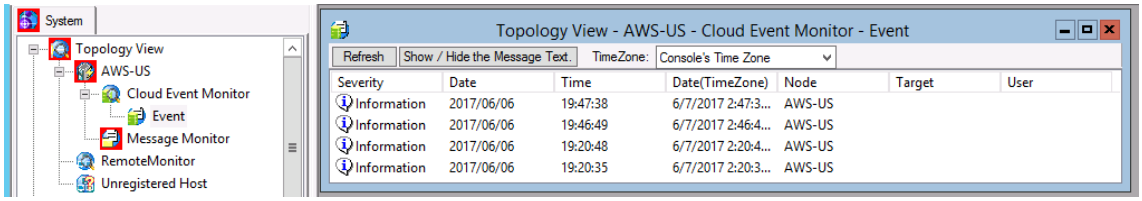
  If you select this check box, an event is recognized as an identical one and suppressed when its log content differs only in numeric values. This option is useful when the content of an event includes occurrence times, etc.

[Example]

When “2017/12/12 error = 0” and “2017/5/12 error = 1” are compared, both are recognized as “// error =” after the numeric values are excluded and, therefore, they are considered an identical message.

5.3.5 Displaying the content of the current event

Double-click the [Event] node in the tree view.



- [Refresh] button

  Updates the displayed content.

- [Show / Hide the Message Text] button

  Displays (or hides) the pane that displays the message text of the selected log at the bottom of

the list.

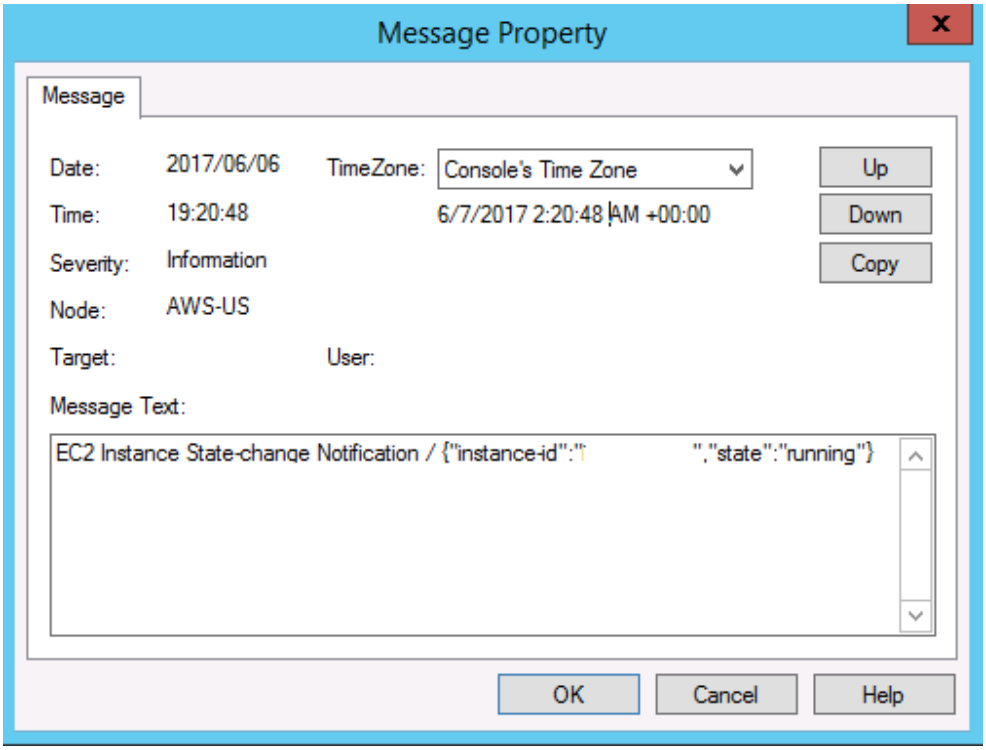
Up to 1,024 characters can be displayed in the message of an event. Excess characters are not displayed.

- [TimeZone]

You can have the [Date(TimeZone)] column display dates and times according to the time zone you specify.

  - [Console's Time Zone: Dates and times are displayed according to the time zone of the machine on which you have the monitoring window opened.
  - [Manager's Time Zone]: Dates and times are displayed according to the time zone of the machine on which you are running the manager service.

Double-clicking an event in the list displays the property dialog box of the event log.



- [TimeZone]

  You can have the [Date(TimeZone)] column display dates and times according to the time zone you specify.

  - [Console's Time Zone]: Dates and times are displayed according to the time zone of the machine on which you have the monitoring window opened.
  - [Manager's Time Zone]: Dates and times are displayed according to the time zone of the machine on which you are running the manager service.

- [Up] and [Down] buttons

  Switch the log whose properties are displayed. Click the [Up] button to display the log immediately above the current one in the list and the [Down] button to display the log

immediately below the current one in the list.

- [Copy] button

  Copy the content of the log to the clipboard.

[Notes]

- The display function for cloud event monitoring displays all event logs, regardless of the event log filter settings.
- If the number of monitored event logs exceeds 1,000, the latest 1,000 logs are displayed.

5.4 Importing and exporting cloud service (AWS) monitoring definitions

You can import and export the performance monitoring settings and cloud event monitoring settings for cloud service (AWS) monitoring, as with an ordinary agent.
For the procedures, see the following items of SystemManager G Help.

- Importing a definition file containing agent monitoring definitions
- Exporting agent monitoring definitions to create a definition file

When exported, the definition file is output with one of the names shown below.

Service name	Definition file name
Topology View	Topology.txt
Message Monitor	MessageView.txt
Performance Monitor	Performance.txt
Hyper visor Monitor (Cloud Event Monitor)	VMEventLog.txt

[Notes]

- In performance monitoring for cloud service (AWS) monitoring, the instance name includes information unique to the connection destination. You cannot apply exported information to another remote agent. To import the information to another remote agent, unselect the [Performance Monitor] check box in the [Import Service] dialog box.
- Cloud Event Monitor is showed as Hyper visor Monitor.

Chapter 6 Uninstallation

6.1 Uninstalling a remote monitoring agent

Uninstall a remote monitoring agent.

For information about how to uninstall the product, see the MasterScope Media Release Memo. For detailed information about a remote monitoring agent, see the MasterScope SystemManager G Release Memo.

6.2 Deleting settings from AWS

SystemManager G adds a rule to the AWS CloudWatch event and a queue to AWS SQS (Simple Queue Service). The settings shown below are added.

Service name	Name
AWS CloudWatch	NEC_SYSMGRG_EVENT_RULE
AWS SQS	NEC_SYSMGRG_EVENT_QUEUE

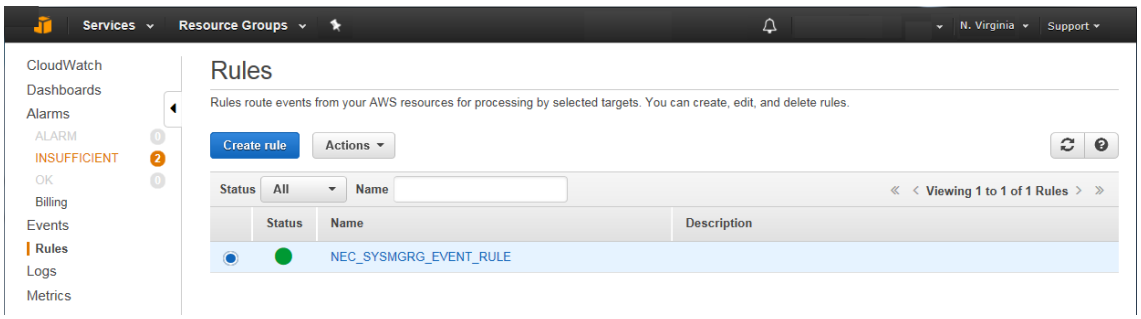
Log in to AWS, and delete the above settings.

If you have renamed the settings as described in”7.2.2Changing the AWS CloudWatch event rule name or SQS queue name”, delete the settings having the new names.

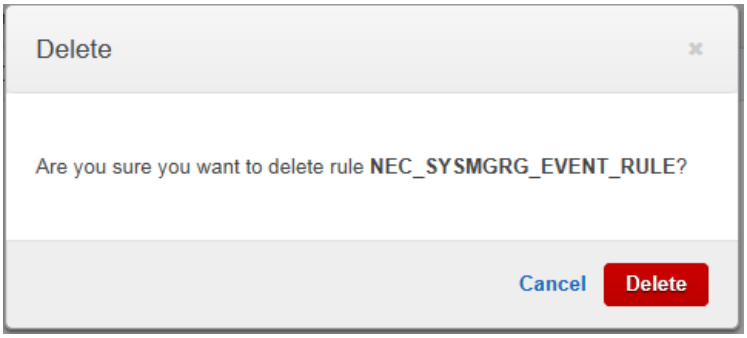
Delete these settings after uninstalling the remote monitoring agent.

6.2.1 Deleting the CloudWatch event rule

1. Select the target event from the CloudWatch Events Rules, and choose [Actions] → [Delete].



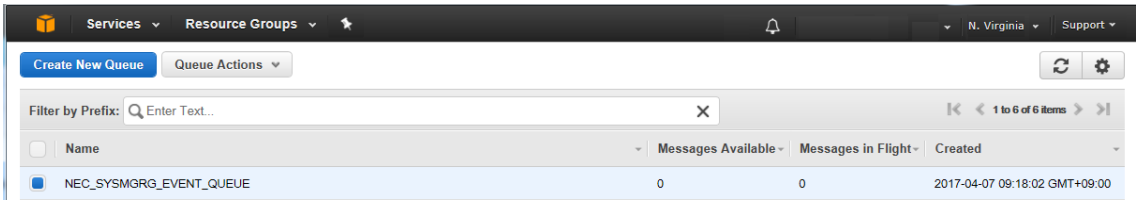
2. When the confirmation dialog box is displayed, choose [Delete].



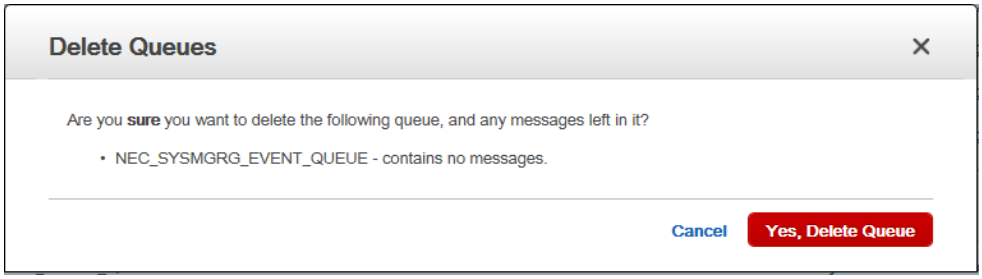
If the AWS specifications have been changed, see the AWS document.

6.2.2 Deleting the SQS queue

1. Select the target queue from the SQS service, and choose [Queue Actions] → [Delete Queue].



2. When the confirmation dialog box is displayed, choose [Yes, Delete Queue].



If the AWS specifications have been changed, see the AWS document.

Chapter 7 Frequently Asked Questions

7.1 Cannot connect to AWS

7.1.1 Check the proxy server settings.

If you connect to the Internet from within your internal network, the connection may be established via a relay server. In this case, set up the proxy server as instructed in “5.1.2 Specifying the authentication information for cloud service (AWS) monitoring.”

7.2 Events not displayed for cloud event monitoring

7.2.1 Check the settings of Amazon Web Services.

SystemManager G adds a rule to the AWS CloudWatch event and a queue to the AWS Simple Queue Service (SQS). The settings shown below are added.

Service name	Name/setting
AWS CloudWatch	NEC_SYSMGRG_EVENT_RULE

	Event pattern:
	{
	"source": [
	"aws.ec2"
	],
	"detail-type": [
	"EC2 Instance State-change Notification"
	]
	}

AWS SQS	NEC_SYSMGRG_EVENT_QUEUE
	Access right: Effect: Allow Principal: Everybody Action: sqs:SendMessage Condition: ArnEquals aws:SourceArn: "arn:aws:events:Region: User:rule/NEC_ SYSMGRG_EVENT_RULE"

Check whether there is already a rule or queue having the same name.

If there is no such rule or queue, restart the remote monitoring agent. After restarting the agent, make the above check again.
If a same name is set, it may conflict with the existing one. In that case, change the name as instructed in the next section.

7.2.2 Changing the AWS CloudWatch event rule name or SQS queue name

1. Open the %RemoteAgtSgDir%\VMEventLogBase\CloudMonitoring.ini file.

   Change the event rule name or SQS queue name as follows:

   ```
   [AWSEvent]
   EventRuleName=NEC_SYSMGRG_EVENT_RULE2
   EventSQSName=NEC_SYSMGRG_EVENT_QUEUE2
   ```

   EventRuleName

   Set the CloudWatch event rule name.

   EventSQSName

   Set the SQS queue name.

2. After changing the settings, restart the remote monitoring agent service.

   Choose [Administrative Tools] → [Services] to restart the remote monitoring agent.

7.3 Getting an event other than the EC2 instance status change in cloud event monitoring

SystemManager G gets the EC2 instance status change event only.
Before adding any other event, thoroughly check the settings and operation.

7.3.1 Adding an AWS CloudWatch event rule

Log in to AWS, and choose [CloudWatch] → [Events] → [Rules] → [Create rule].
Specify NEC_SYSMGRG_EVENT_QUEUE as the target (the new SQS queue name if the name has been changed).
After adding the rule, check the access right of the SQS queue and see whether the event of the added rule can be received.
For details, see the AWS document.

7.3.2 Adding an analysis rule for the added event

1. Open the %RemoteAgtSgDir%\VMEventLogBase\AWSEventDef.json file.
   Adding an analysis rule as follows:
   (Example)

```
{
"RuleName":"AWS Console Sign In via CloudTrail",
"FilterMember":"source",
"FilterValue":"aws.signin",
"EventTime":"time",
"EventUser":"account",
"EventTarget":"detail.userIdentity.userName",
"EventMessage":["detail.eventName"]
},
```

- RuleName
  Specify a rule name. It must be unique in the JSON file.
  This parameter is required.
  Specify “@DEFAULT” to set the rule as the default rule. The default rule is applied when filter conditions (FilterMember, FilterValue) of all other rules are not matched.
  There is a predefined rule with “@DEFAULT” specified as its RuleName in AWSEventDef.json and it can be deleted or modified.

- FilterMember and FilterValue
  Specify a condition to apply the analysis rule.
  Specify one condition for one rule.
  These parameters are required unless RuleName is “@DEFAULT.”
  These parameters are ignored if RuleName is “@DEFAULT.”
  In the example above, the analysis rule is applied when “source” is assigned to key and “aws.signim” is assigned to value of JSON of an event.

- EventTime

  Event time is obtained from the value for the specified key.

  If this parameter is not specified, the value for “time” key is obtained.

  If parsing the value for the specified key fails, the event is not collected.

  See 【Supported Date Formats】for the supported date formats.

- EventUser

  An event user is obtained from the value for the specified key.

  If this parameter is not specified, the value for “account” key is obtained.

- EventTarget

  An event target is obtained from the value for the specified key.

  If this parameter is not specified, the value for “source” key is obtained.

- EventMessage

  Specify an array of message keys. Message texts are obtained from the values for the specified keys.

  When multiple keys are specified, message texts are concatenated with ‘/’ as a separator.

  If EventMessage is not specified or “@ALL” is specified, the whole JSON is obtained.

  The max length of a message text is 1024 characters. If it excesses the max length, the first 1024 characters of the text are obtained.

[Supported Date Formats]

ISO8601 basic format is not supported and parsing a date string in the format (ex. 20180512T220643+0000) will fail.

ISO8601 extended format and RFC 1123 format are supported.

Supported formats are listed in the following table.

Type	Specified String Example
ISO8601 Extended Format	2018-05-12T22:06:43+00:00
	2018-05-12T22:06:43.0123456+00:00
	2018-05-12T22:06+00:00
	2018-05-12T22:06:43Z
	2018-05-12T22:06:43+0900
	2018-05-12T22:06:43-06
	2018-05-12T22:06:43
RFC1123 Format	Mon, 15 Jun 2009 20:45:30 GMT
	15 Jun 2009 20:45:30 GMT

	Mon, 15 Jun 2009 20:45 GMT
	15 Jun 2009 20:45 GMT
	Mon, 15 Jun 2009 20:45:30 Z
	Mon, 15 Jun 2009 20:45:30 +0000
	Mon, 15 Jun 2009 20:45:30 -0600
	Mon, 15 Jun 2009 20:45:30

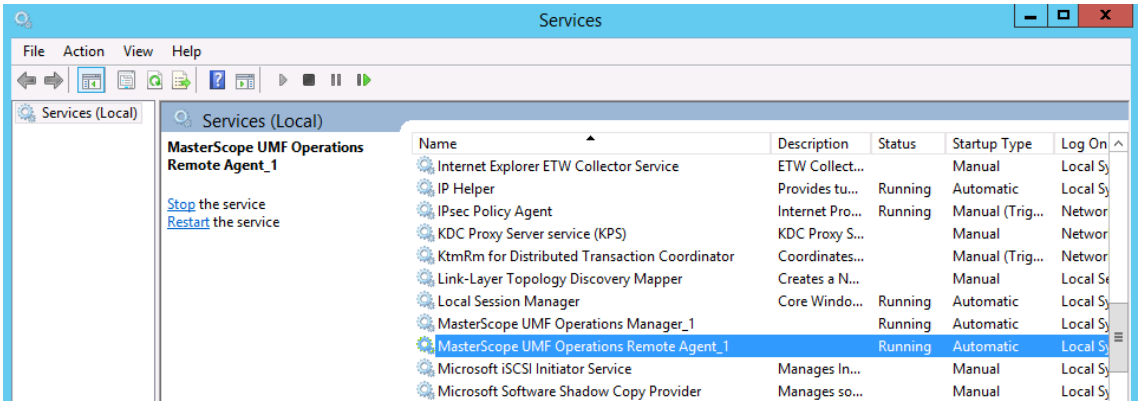
[Notes]

- The format of the AWSEventDef.json file is subject to change without prior notice.
- If the definition of this file is invalid (the JSON format is invalid), the event may fail to be read. Before editing this file, be sure to back it up.
- Checking the JSON format for the event that occurs in AWS is your responsibility. A sample is displayed in [Event Pattern Preview] for AWS CloudWatch rule creation.

2. After changing the settings, restart the remote monitoring agent service.
   Choose [Administrative Tools] → [Services] to restart the remote monitoring agent.

7.4 Restarting the remote monitoring agent

Choose [Administrative Tools] → [Services].



The service name of the remote monitoring agent is as follows:

MasterScope UMF Operations Remote Agent_*xxx*_*n*

xxx and *n* differ depending on your environment.

Chapter 8 Cautions

8.1 Creation of authentication information

You cannot use the AWS authentication information by adding it to the existing authentication information created before the cloud service (AWS) monitoring license is enabled.
Create new authentication information after enabling the license.

8.2 Time of the remote monitoring agent

Set the clock of the machine in which to install the remote monitoring agent to the correct time. If the time is incorrect, the cloud service (AWS) monitoring function does not work normally.

Chapter 9 Message List

The messages reported to the message monitoring function are listed below.

9.1 AWS authentication messages

Importance	Normal
Message text	Authentication success.(HTTP status *n*)
Application	Unified Management Framework
Object	AWS Authentication
Message ID	01870001
Category	Unified Management Framework
Meaning	Login to AWS succeeded. *n*: Displays the HTTP status.

Importance	Abnormal
Message text	Authentication failed.(*message*)(HTTP status *n*)
Application	Unified Management Framework
Object	AWS Authentication
Message ID	01870002
Category	Unified Management Framework
Meaning	Login to AWS failed. *message*: Displays the error message returned from AWS. *n*: Displays the HTTP status.

9.2 EC2 instance status change event

This message is displayed when events are transferred to the message monitoring function.

Importance	Normal
Message text	EC2 Instance State-change Notification / {"instance-id":"*instance*","state":"*status*"}
Application	Unified Management Framework
Object	AWS Event
Message ID	00000000
Category	Event
Meaning	Reports a change in the EC2 instance status. *instance*: Displays the EC2 instance ID. *status*: Displays the status of the EC2 instance. (*)

(*) For details, see the AWS document.

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-lifecycle.html