CA Nimsoft Monitor

Probe Guide for AWS Monitoring

aws v2.0 series

CA Nimsoft Monitor Copyright Notice

Contact CA

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

Send comments or questions about CA Technologies Nimsoft product documentation to nimsoft.techpubs@ca.com.

To provide feedback about general CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Documentation Changes

This table describes the version history for this document.

Version	Date	What's New?
2.0	June 2014	Documentation on the first Admin Console GUI enabled version of the AWS Monitoring probe.

Chapter 1: Overview

The Amazon Web Services (AWS) probe remotely monitors the health and performance counters of various AWS services over a cloud network. The probe lets you create profiles that monitor your AWS user account. The probe fetches all the service data from the AWS and lets you configure various monitoring parameters on each service. Based on the configured parameters, the probe generates Quality of Service (QoS) data and issues status alarms.

The AWS provides a decentralized IT infrastructure to multiple organizations. You can create an account on the AWS cloud and can use its services as per your IT infrastructure requirements. The various capabilities of AWS include storage, web-scale computing, database access, and messaging.

Note: The current version is accessible only through Admin Console GUI.

The CA Nimsoft AWS Monitoring probe provides monitoring of the following AWS services:

- Health: the probe monitors the overall health status of the AWS services for a specific geographical location. Alarms are generated in case any service is unavailable.
- Amazon S3: this service provides an interface for storing and fetching data at any time instance. The probe generates QoS data based on the time consumed in storing and retrieving files.
- Amazon Elastic Compute Cloud (EC2): this service provides a flexible web-scale computing interface. The probe generates QoS data based on the performance of various instances that are using the AWS services.

Important! Amazon can charge the AWS account which the probe uses to monitor the AWS services. You must consider this while configuring the probe for monitoring various AWS services.

This section contains the following topics:

About This Guide

This guide is for the CA Nimsoft Monitor Administrator to help understand the configuration of the AWS Monitoring probe and provides the following information:

- Overview of the AWS Monitoring probe and related documentation for previous probe versions.
- Configuration details of the probe.
- Field information and common procedures for configuring the probe.

Important! Description for the intuitive GUI fields is not included in the document.

Related Documentation

Related Documentation

Documentation for other versions of the aws probe

The Release Notes for the aws probe

User documentation for the Admin Console

Monitor Metrics Reference Information for CA Nimsoft Probes (http://docs.nimsoft.com/prodhelp/en_US/Probes/ProbeReference/index.htm)

Preconfiguration Requirements

This section contains the preconfiguration requirements for the Nimsoft AWS Monitoring probe.

- You must have an account on AWS with valid credentials, such as, **Access Key** and **Secret Access Key**.
- Download the AWS SDK library **aws-java-sdk-version.jar** version 1.7.12 or higher from http://aws.amazon.com/sdkforjava/
- If you have been using a probe version prior to version 2.01 then you must manually transfer the existing configurations to the new version.
- You must remove all the versions of the aws probe that are older than version 2.01 as upgrade to version 2.01 is not supported.

Note: You must have subscription of the EC2 service so that the AWS Monitoring probe can access the AWS resource.

Software Requirements

The probe requires:

- One or more Amazon AWS accounts and subscription to the EC2 service.
- Java 1.6 or higher. (on the robot machine, where the probe runs)

The aws probe version 2.0x has the following requirements along with the above mentioned requirements:

- NMS version 7.6 or later.
- Probe Provisioning Manager (PPM) probe version 2.34 and later.
- AWS SDK library **aws-java-sdk-version.jar** version 1.7.12 or higher from http://aws.amazon.com/sdkforjava/

  Note: The AWS SDK library must be placed at the NMS robot machine where the aws probe is installed.

Important! The aws probe is accessible only through the Admin Console GUI as the Infrastructure Manager (IM) GUI is no longer available.

NAS Subsystem ID Requirements

Alarms are classified by their subsystem ID, identifying which part of the system the alarm relates to. These subsystem IDs are kept in a table maintained by the NAS probe. As of the current release, you will have to add the following subsystem IDs manually using the NAS Raw Configuration menu:

Key Name	Value
2.19.	Amazon
2.19.1.	AWS
2.19.1.1.	Resource
2.19.1.2.	ServiceStatus
2.19.1.3.	EC2
2.19.1.4.	S3

To update the Subsystem IDs using Admin Console, follow these steps:

1. In the Admin Console, click the black arrow next to the NAS probe, select **Raw Configure**.
2. Click on the **Subsystems** folder.
3. Click on the New Key Menu item.
4. Enter the Key Name in the Add key window, click **Add.**

   The new key appears in the list of keys with a blank value.
5. Click in the Value column for the newly created key and enter the key value.
6. Repeat this process for all of the required subsystem IDs for your probe.
7. Click **Apply**.

To update the Subsystem IDs using Infrastructure Manager, follow these steps:

1. In Infrastructure Manager, right click on the NAS probe, select **Raw Configure**.
2. Click on the **Subsystems** folder.
3. Click on the **New Key...** button.
4. Enter the Key Name and Value, Click **OK.**
5. Repeat this process for all of the required subsystem IDs for your probe.
6. Click **Apply**.

Alarm Threshold Requirements

The PPM probe maintains a table of subsystem IDs that are mapped to the probes. As of the current release, the subsystem IDs for this probe will default to 1.1.19. If you are using either dynamic or static alarm thresholds, you can change the default entry to the appropriate subsystem ID.

Follow these steps:

1. In the Admin Console, click the black arrow next to the probe, select **Configure**.
2. Select the monitor that you want to modify from the available list.
3. Change the Static and Dynamic **Subsystem (override) fields** to **2.19.1.1.**.
4. Save your settings.

Supported Platforms

Refer to the Nimsoft Compatibility Support Matrix for the latest information on supported platforms. See also the Support Matrix for Nimsoft Probes for additional specific information on the aws probe.

Chapter 2: Configuration Details

The AWS Monitoring probe is configured to create monitoring profiles for accessing AWS resources. The probe fetches the data of EC2 instances and S3 services and provides you with various monitors for generating QoS. You can also configure the health monitors to generate alarms on basis of the availability of services in specific geographical region.

The probe also lets you configure the **Auto Discovery** functionality. If any EC2 instance is added or deleted in the AWS resource, then the **Auto Discovery** functionality updates the list of EC2 instances in the probe.

For the EC2 service, the aws probe lets you enable the following monitors:

- CPU Utilization
- Disk Read
- Disk Write
- Disk Read Operations
- Disk Write Operations
- Network In
- Network Out

For the S3 service, the aws probe lets you enable the following monitors:

- File Read Time
- File Write Time

This section contains the following topics:

aws Node

This node lets you view the probe information and configure the log properties. You can also set the polling interval for **Auto Discovery** functionality and configure the proxy settings.

Note: The **EC2** node and the **S3** node are not visible until you create a monitoring profile. Initially, only the **aws** node and the **AWS Service Health** node are visible.

Navigation: aws

Set or modify the following values as required:

aws > Probe Information

This section provides information about the probe name, probe version, start time of the probe, and the probe vendor.

aws > Probe Setup

This section lets you configure the detail level of the log file. The default value is 3-info.

aws > Auto Discovery

This section lets you set the value of **Discovery Interval (in minutes)**. The **Discovery Interval** specifies the time interval between each time the probe runs the Auto Discovery functionality.

aws > AWS SDK Path

This section lets you define the path of the AWS SDK library for connecting to the AWS cloud. The path specifies the location where you have placed the AWS SDK library file after downloading it.

Note: The AWS SDK library must be placed at the NMS robot machine where the aws probe is installed.

aws > Proxy Settings

This section enables you to connect to the AWS cloud through a proxy server on the network. You need proxy server settings when your network is not an open network.

- Enable Proxy: lets you use a proxy server for connecting to the AWS cloud.
- IP: defines the IP address of the proxy server.
- Port: specifies the port on the proxy server through which the connection is established.
- Username: defines the user name for accessing the proxy server.

aws > Add New Profile

This section lets you add a profile for monitoring the EC2 and S3 services data. QoS data is generated according to the performance of these services.

- Hostname: defines a unique name for the profile. This field was identified as **Name** in the previous versions of the probe. You can specify the AWS account name as the value for this field.
- Active: activates the profile for service monitoring.
- Interval (secs): specifies the time interval (in seconds) after which the probe collects the data from the AWS cloud for the specific profile.

  Default: 600

  Note: Interval value must be above 5 minutes.
- Alarm Message: specifies the alarm to be generated when the test connection, which the probe establishes, fails.

  Default: ResourceCritical
- Access Key: defines the login credential of the AWS account for accessing the AWS resource.
- Secret Access Key: specifies the additional login credential of the AWS account.

  Note: The probe uses the combination of the **Access Key** and **Secret Access Key** for accessing the AWS resource.

<Profile Name> Node

This node represents the profile which was created to monitor the health and performance of AWS services. Each profile is mapped with an AWS account. You can check the connection between the probe and the AWS resource through the **Verify Selection** button under the **Actions** drop down.

Note: This node is known as *profile name* node in the document and is user-configurable.

Navigation: aws > *profile name*

Refer to the **Add New Profile** section of the **aws Node** topic for field description.

EC2 Node

The AWS EC2 service of a specific region stores the instance data in the **AWS Cloud Watcher**. For a specific profile, the AWS Monitoring probe fetches the data from the Cloud Watcher.

This node lets you configure how the probe interacts with the EC2 service and how it collects data about the instances of the AWS resource. The probe generates QoS based on the instance data which is collected from the Cloud Watcher.

Navigation: aws > *profile name* > EC2

Set or modify the following values as required:

EC2 > EC2 Configurations

This node lets you configure the EC2 service properties.

- Active: activates the addition of instances of the AWS resource.
- Start Time: specifies the time duration (in minutes) for collecting sample values from the Cloud Watcher. The probe starts collecting the values that were calculated in the last specified minutes.
- Statistic: defines the operation to be performed on the sample values that the probe fetches. You can configure the probe to perform the following operations on the fetched values:
  - Calculate minimum value.
  - Calculate maximum value.
  - Calculate the sum of all the values.
  - Calculate the average of all the values.
  - Calculate the number of data samples.
- Period: specifies a numerical value which is used to divide the collected values into samples.

For example, if the **Start Time** is specified as 10 and the **Period** is specified as 2, then the sample values are divided into 5 lots.

<Instance Name> Node

This node represents an instance of the AWS resource. An EC2 instance is a virtual machine (VM). If any region subscribes to the EC2 service, then an instance of EC2 VM is created for that region.

The AWS Monitoring probe monitors the performance counters of the EC2 instances of the AWS resource. All EC2 instances are visible under the EC2 node.

Note: This node is known as *instance name* node in the document and each instance has a unique ID.

Navigation: aws > *profile name* > EC2 > *instance name*

This node has no fields.

<Monitor Name> Node

This node lets you configure the performance counters of the EC2 instances. The AWS Monitoring probe generates QoS data of the EC2 service of a specific region according to the values fetched from the Cloud Watcher.

The performance counters are divided into following categories:

- CPU
- Disk
- Network

Each category is represented as a node under the *instance name* node.

Note: This node is known as *monitor name* node in the document and it represents various EC2 performance counters.

Navigation: aws > *profile name* > EC2 > *instance name* > *monitor name*

Set or modify the following values as required:

***monitor name* > Monitors**

This section lets you configure the performance counters for generating QoS.

Note: The performance counters of an EC2 instance are visible in a tabular form. You can select any one counter in the table and can configure its properties.

- QoS Name: indicates the name of performance counter.
- Publish Data: generates the QoS data for the selected counter.

  Note: When you select the **Publish Data** check box, the value of the **Data** column in the table changes from **Off** to **On**.

Similarly, you can configure the other performance counters that are visible under the **CPU**, **Disk,** and **Network** nodes.

S3 Node

The data which is stored in the cloud using the AWS S3 service is segregated into groups that are known as buckets. The aws probe monitors the time which is consumed in storing and retrieving files to and from the bucket, respectively.

This node lets you configure the performance counters for S3 service. The AWS Monitoring probe generates QoS data from the time that is consumed in storing and retrieving files in the AWS resource.

Note: Set the polling interval according to the size of the files that you want to store or retrieve. If the polling interval is too less, then the probe starts fetching data again from the bucket before completing a previous file process. For example, if you want to upload a file of size 1MB then you can set the polling interval as 5 minutes.

Navigation: aws > *profile name* > S3

Set or modify the following values as required:

S3 > S3 Configurations

This section lets you provide details about the file bucket so that the probe can monitor the time consumed in accessing the file bucket.

- Active: enables the monitoring of file bucket access time.
- Bucket Name: defines the name of the file bucket for which the probe monitors the storing and retrieving time.
- File Name: defines the name of the file which is stored or retrieved from the bucket.

S3 > Monitors

This section lets you configure the performance counters for generating QoS.

Note: The performance counters of the S3 service are visible in a tabular form. You can select any one counter in the table and can configure its properties.

- QoS Name: indicates the name of performance counter.
- Publish Data: generates the QoS data for the selected counter.

  Note: When you select the **Publish Data** check box, the value of the **Data** column in the table changes from **Off** to **On**.

AWS Service Health

This node represents the health monitoring service of AWS Monitoring probe. The probe monitors the availability of all the services that AWS cloud provides for a specific geographical location. The probe generates alarms in case any service for a specific region is unavailable. The following alarms are generated after the probe monitors the health of the AWS services:

- Disruption in the service.
- Performance issues.
- Service is operating normally.
- Other information.

Navigation: aws > AWS Service Health

Set or modify the following values as required:

AWS Service Health > Health Configuration

This section enables you to configure the Health Monitoring functionality of the aws probe. The **Health Interval (mins)** field lets you set the time interval, in minutes, during which the probe fetches the health status of the AWS services.

<AWS Region> Node

This node lets you view the list of AWS services that are available for a specific region. You can configure the aws probe for generating alarms for specific AWS services in a region.

Note: This node is known as *AWS region* in the document as this node represents all the geographical locations where AWS provides services.

Navigation: aws > AWS Service Health > *AWS region*

Set or modify the following values as required:

***AWS Region* > AWS Service Status**

This section lets you view the various AWS services that are available for a specific region. You can configure the service properties for generating the alarms in case the service is not available.

Note: The AWS services for the selected region are visible in a tabular form. You can select any one service in the table and can configure its properties.

- Description: indicates the description of the selected service.
- Unit: indicates the unit of the selected service status.
- Metric Type ID: identifies a unique ID for alarm generation.
- Publish Alarms: enables the probe to check the status of the selected service and generate alarms.

  Note: When you select the **Publish Alarms** check box, the value of the **Alarm** column in the table changes from **Off** to **On**.
- Service: indicates the name of the selected service.

Similarly, you can configure the services of the other geographical locations.

Configure a Node

This procedure provides the information to configure a section within a node.

Each section within the node lets you configure the properties of the probe for connecting to the AWS resource and monitoring various AWS services.

Follow these steps:

1. Navigate to the section within a node that you want to configure.
2. Update the field information and click **Save**.

   The specified section of the probe is configured.

How to Configure Alarm Thresholds

Some Quality of Service measurement probes allow you to set different types of alarm thresholds. These threshold options allow you to more broadly control when alarm messages are sent for each QoS probe.

For more information about the different alarm thresholds and their configuration requirements, refer to the *General Probe Configuration* section of the Admin Console Help.

Important! Alarm threshold settings are dependent on the baseline_engine probe. If you do not have the correct version of baseline_engine configured, you will not see the additional threshold options.

Configure Static Alarm Thresholds

Important! In order to create static alarm thresholds, you must have the baseline_engine probe version 2.2 installed on the robot and configured.

Static thresholds can be set at the QoS metric level in some of the probes that publish alarms for a QoS metric. For more information about static alarm thresholds, refer to the *How to Configure Static Thresholds* section of the Admin Console Help.

Manage Profiles

The following procedure enables you to add a profile for monitoring the S3 and EC2 services. Each profile represents one AWS resource. There can be multiple instances of an AWS resource.

Follow these steps:

1. Click **Options** next to the **aws** node in the navigation pane.
2. Select **Add New Profile**.
3. Update the field information and click **Submit**.

   The new monitoring profile is visible under the aws node in the navigation pane.

The **Auto Discovery** functionality automatically loads a list of all the instances for the EC2 service.

Delete a Profile

You can delete a profile if you do not want the probe to monitor the performance of a specific AWS resource.

Follow these steps:

1. Click the **Options** icon next to the *profile name* node that you want to delete.
2. Select **Delete Profile**.
3. Click **Save**.

   The monitoring profile is deleted from the resource.

Chapter 3: aws QoS Metrics

The following table describes the checkpoint metrics that can be configured using the AWS Monitoring probe.

The following QoS data is for the AWS S3 service:

Monitor Name	Metric Name	Units	Description
QOS_AWS_FILEREADTIME	File Read Time	Seconds	Time taken to fetch a file from the file bucket.
QOS_AWS_FILEWRITETIME	File Write Time	Seconds	Time taken to store a file in the file bucket.

The following QoS data is for the AWS EC2 service:

Monitor Name	Metric Name	Units	Description
QOS_AWS_CPU_UTILIZATION	CPU Usage	Percent	The percentage of allocated EC2 compute units that are currently in use on the instance. This metric identifies the processing power required to run an application upon a selected instance.
QOS_AWS_DISK_WRITE_BYTES	Data Written	Bytes	This metric is used to determine the volume of the data the application writes onto the hard disk of the instance. This can be used to determine the speed of the application.
QOS_AWS_DISK_READ_BYTES	Data Read	Bytes	This metric is used to determine the volume of the data the application reads from the hard disk of the instance. This can be used to determine the speed of the application.
QOS_AWS_DISK_READ_OPS	Reads	Count	Completed read operations from all ephemeral disks available to the instance. This metric identifies the rate at which an application reads a disk. This can be used to determine the speed in which an application reads data from a hard disk.
QOS_AWS_DISK_WRITE_OPS	Writes	Count	Completed write operations to all ephemeral disks available to the instance. This metric identifies the rate at which an application writes to a hard disk. This can be used to determine the speed in which an application saves data to a hard disk.

QOS_AWS_NETWORK_IN	Total Bytes Received	Bytes	The number of bytes received on all network interfaces by the instance. This metric identifies the volume of incoming network traffic to an application on a single instance.
QOS_AWS_NETWORK_OUT	Total Bytes Sent	Bytes	The number of bytes sent out on all network interfaces by the instance. This metric identifies the volume of outgoing network traffic to an application on a single instance.

Chapter 4: Known Issues

This section contains a list of known issues in this release.

- For S3 service, when the file bucket is empty and the **QOS_FILE_READ_TIME** monitor is activated, the probe should return null entries. Instead, the probe returns valid entries.
- Each time that you save the configuration, the AWS Monitoring probe is restarted and data collection for EC2 and S3 services, starts again.