

CA Nimsoft Monitor

Probe Guide for Cisco Nexus Monitoring

cisco_nexus v1.0 series



CA Nimsoft Monitor Copyright Notice

This online help system (the "System") is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This System may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This System is confidential and proprietary information of CA and protected by the copyright laws of the United States and international treaties. This System may not be disclosed by you or used for any purpose other than as may be permitted in a separate agreement between you and CA governing your use of the CA software to which the System relates (the "CA Software"). Such agreement is not modified in any way by the terms of this notice.

Notwithstanding the foregoing, if you are a licensed user of the CA Software you may make one copy of the System for internal use by you and your employees, provided that all CA copyright notices and legends are affixed to the reproduced copy.

The right to make a copy of the System is limited to the period during which the license for the CA Software remains in full force and effect. Should the license terminate for any reason, it shall be your responsibility to certify in writing to CA that all copies and partial copies of the System have been destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS SYSTEM "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS SYSTEM, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The manufacturer of this System is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2014 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Legal information on third-party and public domain software used in the Nimsoft Monitor solution is documented in *Nimsoft Monitor Third-Party Licenses and Terms of Use* (http://docs.nimsoft.com/prodhelp/en_US/Library/Legal.html).

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

Chapter 1: Overview	7
About This Guide	7
Related Documentation	7
Release Summary	7
Chapter 2: Configuration Details	9
Configuration Overview	9
Create Resource Profiles	9
Configuration for Utilization Values	11
Apply Monitoring	11
Configure Dynamic Alarm Thresholds	14
Chapter 3: Probe GUI Reference	15
Tree Hierarchy	15
Tree Icons	15
Cisco Nexus Monitoring Node	16
Profiles Node	17
Chapter 4: Probe Metrics	19
Chapter 5: Known Issues	21

Documentation Changes

This table describes the version history for this document.

Version	Date	What's New?
1.0	05/2014	Special release.

Chapter 1: Overview

The Cisco Nexus Monitoring probe monitors the health and performance of Cisco Nexus switches running Cisco NX-OS software. The probe is capable of monitoring one or more NX-OS devices.

This section contains the following topics:

[About This Guide](#) (see page 7)

[Related Documentation](#) (see page 7)

[Release Summary](#) (see page 7)

About This Guide

This guide is for the CA Nimsoft Monitor Administrator to help understand the configuration of the Cisco Nexus Monitoring probe.

Related Documentation

For related information that may be of interest, see the following material:

Related Documentation

Documentation for other versions of the cisco_nexus probe

The [Release Notes](#) for the cisco_nexus 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)

Release Summary

Please 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 cisco_nexus probe.

Chapter 2: Configuration Details

This section contains configuration details specific to the Cisco Nexus Monitoring probe.

This section contains the following topics:

- [Configuration Overview](#) (see page 9)
- [Create Resource Profiles](#) (see page 9)
- [Configuration for Utilization Values](#) (see page 11)
- [Apply Monitoring](#) (see page 11)

Configuration Overview

At a high level, configuring the Cisco Nexus Monitoring probe consists of the following steps:

1. Add a Resource profile for each Cisco NX-OS enabled device you want to monitor.
2. Add monitors to the appropriate system components and configure monitor data.

The following sections describe how to do each of these tasks.

- [Create Resource Profiles](#) (see page 9)
- [Apply Monitoring](#) (see page 11)

Create Resource Profiles

A resource profile contains the settings needed for the Cisco Nexus Monitoring probe to connect to a Cisco NX-OS device. Create a profile for each device you want to monitor. Once you create a Resource profile, the Resource is added to the tree, and the tree hierarchy is automatically populated with the device components.

Follow these steps:

1. Click the **Options** icon next to the Cisco Nexus Monitoring node in the tree.
2. Click the **Add New Profile** option.
3. Update the field information:

Fields to know:

Hostname

The hostname or IP address of the IBM server you want to monitor.

Active

Select this checkbox to activate monitoring of the resource.

Port

The SSH port for the target system.

Interval (secs)

The time to wait for connection to establish.

Username

A valid username to be used by the probe to log on to the IBM server.

Password

A valid password to be used by the probe to log on the IBM server.

Alarm Message

The alarm message to be sent if the resource does not respond.

4. Click **Submit**.

The profile is created and appears in the tree.

Configuration for Utilization Values

By default the cisco_nexus probe is set for the maximum number of MAC addresses and VLANs for the type of Nexus switch. It might be necessary to adjust these values to correctly calculate your percent utilization metrics. You can change these default values in raw config. The changes become effective after you restart the probe.

The default values for the maximum number of MAC addresses and VLANs in the Setup section are:

- max_dynamic_mac_addresses = 16000
- max_vlans_nexus50xx = 256
- max_vlans_nexus55xx = 3982

The VLAN settings are device dependent. The supported Nexus switches are:

- Nexus 7000 series
- Nexus 5500 series
- Nexus 5000 series

The maximum number of VLANs depend on the types of Nexus switches connected to the resource. The resource is the system you connect to when you create a device profile in the probe.

- If the resource connects to a Nexus 7000 series switch, the maximum number of VLANs is determined automatically by the probe. There is no default setting for this series of Nexus switch.
- If the resource connects to a Nexus 5500 series switch, the probe uses the value for max_vlans_nexus55xx.
- If the resource connects to a Nexus 5000 series switch, the probe uses the value for max_vlans_nexus50xx.

Apply Monitoring

Once you add a resource profile, the components of the resource are displayed in the tree. Click a node in the tree to see any associated monitors for that component. Configure the QoS measurements you want to collect data for, and any alarms or events you want, by modifying the appropriate fields.

Note: Users of CA Nimsoft Monitor Snap can skip this step. The Default configuration is automatically applied when you activate the Cisco Nexus Monitoring probe in Snap.

Follow these steps:

1. Go to Cisco Nexus Monitoring > *profile name* > *resource name*.
2. Click on a device name. It might be necessary to expand the node in the tree to view the monitors and QoS metrics.

The available monitors appear in a table on the right side of the screen.

3. Select the monitor you want to modify in the table.
4. Change monitor settings in the fields below the table.

Fields to know:

QoS Name

The name to be used on the QoS message issued. The field is read-only.

Description

This is a read-only field, describing the monitor.

Units

The unit of the monitored value (for example %, Mbytes etc.). The field is read-only.

Metric Type Id

Identifies a unique Id of the QoS.

Publish Data

Select this option if you want QoS messages to be issued on the monitor.

Publish Alarms

Select this option if you want to activate alarms.

Value Definition

Value to be used for alarming and QoS.

You have the following options:

- Current Value -- The most current value measured will be used.
- Delta Value (Current –Previous) -- The delta value calculated from the current and the previous measured sample will be used.
- Delta Per Second -- The delta value calculated from the samples measured within a second will be used.
- Average Value Last n Samples -- The user specifies a count. The value is then averaged based on the last "count" items.

Number of Samples

The count of items for the Value Definition when set to Average Value Last n Samples .

Operator

The operator to be used when setting the high or low alarm threshold for the measured value. You must select Publish Alarms to enable this setting.

Example:

=> 90 means alarm condition if the measured value is above 90.

= 90 means alarm condition if the measured value is exact 90.

Threshold

The high or low alarm threshold value. An alarm message will be sent if this threshold is exceeded.

Message Name

The alarm message to be issued if the specified high or low threshold value is breached. These messages are kept in the message pool.

5. Click **Save** at the top of the screen.

When the new configuration is loaded, a Success dialog appears.

6. Click **OK**.

The tree is updated with the new configuration.

Configure Dynamic Alarm Thresholds

Dynamic thresholds are configured at the QoS metric level in each probe that publishes an alarm for a QoS metric.

Important! In order to create dynamic alarm thresholds, you must have the `baseline_engine` probe version 2.0 installed on the robot and configured.

Follow these steps for each QoS metric where you want to configure dynamic thresholds:

1. Select a node in the tree to view any associated monitors and QoS metrics.
2. Select the monitor you want to modify in the table.
3. Select the Publish Data and Compute Baseline options to enable the Dynamic Alarm Thresholds section of the configuration.
4. Choose a threshold algorithm. There are three algorithms allowed for dynamic alarm thresholds:

Note: You must indicate the direction for each algorithm, either increasing or decreasing.

- Scalar: Each threshold is a specific value from the computed baseline.
- Percent: Each threshold is a specific percentage of the computed baseline.
- Standard Deviation: Each threshold is a measure of the variation from the computed baseline. A large standard deviation indicates that the data points are far from the computed baseline and a small standard deviation indicates that they are clustered closely around the computed baseline.

Important! To change the subsystem ID, you must have the `baseline_engine` probe version 2.1 installed on the robot and configured.

5. (Optional) If the Subsystem ID listed in the Subsystem (default) field is not correct for your configuration, enter the correct ID in the Subsystem (override) field.
6. Save your settings.

Chapter 3: Probe GUI Reference

This section describes the fields and features of the Cisco Nexus Monitoring probe.

This section contains the following topics:

[Tree Hierarchy](#) (see page 15)

[Tree Icons](#) (see page 15)

[Cisco Nexus Monitoring Node](#) (see page 16)

[Profiles Node](#) (see page 17)

Tree Hierarchy

Once a Resource profile is added, the components of the Resource are displayed in the tree. Click a node in the tree to see the monitors available for that component. The tree contains a hierarchical representation of the components that exist in the Cisco Nexus environment.

Tree Icons

The icons in the tree indicate the type of object the node contains.

 - Open folder. Organizational node used to group similar objects.

 - The profile icon indicates the status of subcomponent discovery.

 - OK. Discovery of subcomponents is completed.

 - Pending. Discovery of subcomponents is in progress.

 - Unknown.

 - Failed. Discovery of subcomponents failed.

 - A device. Click the triangle next to the folder to collapse it.

Cisco Nexus Monitoring Node

Navigation: Cisco Nexus Monitoring Node

Set or modify the following values based on your requirements.

Cisco Nexus Monitoring > Probe Information

This section displays read-only information about the Cisco Nexus Monitoring probe.

Cisco Nexus Monitoring > Probe Setup

Fields to know:

- Log Level: Select the amount of log information you would like to collect for this probe.

Default: 3 (Recommended)

Cisco Nexus Monitoring > >Add New Profile

You can manually add a device profile.

Fields to know:

Hostname

The hostname or IP address of the IBM server you want to monitor.

Active

Select this checkbox to activate monitoring of the resource.

Port

The SSH port for the target system.

Interval (secs)

The time to wait for connection to establish.

Username

A valid username to be used by the probe to log on to the IBM server.

Password

A valid password to be used by the probe to log on the IBM server.

Alarm Message

The alarm message to be sent if the resource does not respond.

Profiles Node

This section describes how to manage your device configuration. You can modify or delete a device profile, and validate the credentials for each device.

Navigation: Cisco Nexus Monitoring Node > *profile name*

profile name >  > Delete Profile

Select this option to delete the profile.

profile name > **Actions** > **Verify Selection**

Use this section to modify settings for the profile.

profile name > **Resource Setup**

Use this section to modify settings for the profile.

Fields to know:

Hostname

The hostname or IP address of the IBM server you want to monitor.

Active

Select this checkbox to activate monitoring of the resource.

Port

The SSH port for the target system.

Interval (secs)

The time to wait for connection to establish.

Username

A valid username to be used by the probe to log on to the IBM server.

Password

A valid password to be used by the probe to log on the IBM server.

Alarm Message

The alarm message to be sent if the resource does not respond.

Chapter 4: Probe Metrics

The following table describes the metrics that can be configured in the probe.

Resource Entity	Unit	QoS	Description
Host	String	-	The host name.
MAC Addresses	Integer	QOS_MS_MAC_ADDRESS_ACTIVE	The active MAC address table count.
	Integer	QOS_MS_MAC_ADDRESS_TOTAL	The total MAC address table count.
	Percent	QOS_MS_MAC_ADDRESS_UTILIZATION	The percent utilization of MAC addresses.
One GB Ethernet Ports	Integer	QOS_MS_ONE_GB_ETHERNET_PORTS_ACTIVE	The total number of active one GB ethernet ports.
	Integer	QOS_MS_ONE_GB_ETHERNET_PORTS_TOTAL	The total number of one GB ethernet ports.
	Percent	QOS_MS_ONE_GB_ETHERNET_PORTS_UTILIZATION	The percent utilization of one GB ethernet ports.
Port Channels	Integer	QOS_MS_PORT_CHANNELS_ACTIVE	The total number of active port channels.
	Integer	QOS_MS_PORT_CHANNELS_TOTAL	The total number of port channels.
	Percent	QOS_MS_PORT_CHANNELS_UTILIZATION	The percent utilization of port channels.
Resource	Milliseconds	QOS_RESOURCE_RESPONSE_TIME	Response time of data collection from host.
Ten GB Ethernet Ports	Integer	QOS_MS_TEN_GB_ETHERNET_PORTS_ACTIVE	The total number of active ten GB ethernet ports.
	Integer	QOS_MS_TEN_GB_ETHERNET_PORTS_TOTAL	The total number of ten GB ethernet ports.
	Percent	QOS_MS_TEN_GB_ETHERNET_PORTS_UTILIZATION	The percent utilization of ten GB ethernet ports.
VLANs	Integer	QOS_MS_VLANS_ACTIVE	The total number of active VLANs.
	Integer	QOS_MS_VLANS_TOTAL	The total number of VLANs.

	Percent	QOS_MS_VLANS_UTILIZATION	The percent utilization of VLANs.
--	---------	--------------------------	-----------------------------------

Chapter 5: Known Issues

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

No known issues exist at this time.