CA Nimsoft Monitor

Probe Guide for DNS Response Monitoring

dns_response v1.6 series

Legal Notices

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

Documentation Changes

This table describes the version history for this document.

Version	Date	What's New?
1.6	September 2013	Initial web-based GUI version of this probe. (Previous versions of this probe are configured using Infrastructure Manager).

Chapter 1: Overview

The Monitor DNS Response Time probe queries your Domain Name Server (DNS) and monitors the response time from the server. The probe can also query the DNS looking for A records (normal hostnames), MX records (mail servers), and NS records (name servers).

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 DNS Response Monitoring probe.

This guide contains the following information:

- An overview of the DNS Response Monitoring probe.
- The related documentation for previous probe versions, release notes, and so on.
- The configuration details of the probe including information for the fields that are required to configure the probe.
- The common procedures that can be used in the probe configuration.
- Field information for the fields, required to configure the probe in the first-time deployment of the probe.

Important! The field description for intuitive terms in the GUI has not been included in the document.

Related Documentation

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

Related Documentation

Documentation for other versions of the dns_response probe

The Release Notes for the dns_response 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 DNS Response Monitoring probe.

Supported Platforms

Refer to the Nimsoft Compatibility Support Matrix for the latest information about supported platforms. See also the Support Matrix for Nimsoft Probes for more specific information about the DNS Response Monitoring probe.

Chapter 2: Configuration Details

You can configure the DNS Response Monitoring probe to query the DNS and to monitor the response times. This probe can also query the DNS looking for A records (normal hostnames), MX records (mail servers), and NS records (name servers).

Navigation: dns_response

Set or modify the following values that are based on your requirement:

dns_response > Probe Information

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

dns_response > General Configuration

This section is used to configure the log properties of the DNS Response Monitoring probe. These settings define the default properties for all the profiles that are created in the DNS Response Monitoring probe.

- Log level: Specifies the level of details that are written to the log file.

  Default: 3 - Info

- Port: Specifies the port number for performing the reverse lookup with the forward lookup from a single profile.

  Default: 1

- Protocol: Specifies the protocol for performing the reverse lookup with the forward lookup from a single profile.

  Default: TCP

- Run Interval (Seconds): Defines the time interval (in seconds) when the profiles are checked.

  Default: 300

dns_response > Message Pool

The **Message Pool** section displays a list of currently configured alarm messages for the DNS Response Monitoring probe. These messages can be used in one or more monitoring profiles in the probe.

- Name: Identifies the name of the message.
- Token: Identifies the token which is used for the internationalization.
- Error: Identifies the alarm message text that is issued on error alarm.
- OK: Identifies the alarm message text that is issued on alarm clear.
- Subsystem: Identifies the subsystem_ID of alarms that defines the source of the alarm.
- Error Token: Identifies the token value of the error message.
- OK Token: Identifies the token value of the clear message.

This section contains the following topics:

dns_response Node

This section contains configuration details specific to the DNS Response Monitoring probe. In this node, you can view the probe information and can configure the log properties of the DNS Response Monitoring probe. You can set the time interval for checking the Domain Name Server (DNS). You can also view the list of alarm messages in the message pool.

Navigation: dns_response

Set or modify the following values that are based on your requirement:

dns_response > Probe Information

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

dns_response > General Configuration

This section allows you to configure the log properties of the probe. You can also specify the time after which the probe checks the DNS that are defined in the activated profiles.

- Log Level: Specifies the level of details that are written to the log file.

  Default: 3 - Info

- Run Interval (Seconds): Specifies the time interval (in seconds) when the monitoring profiles are checked.

  Default: 300

- Clear Alarm on Restart: Clears all probe-related alarms when the probe restarts.

  Default: Not selected

dns_response > Message Pool

This section displays a list of alarm messages that are defined in the DNS Response Monitoring probe. You can select and the message details but cannot add or edit messages to the list. These alarm messages are specified while configuring the monitoring profiles.

Profile-<Profile Name> Node

The Profile-*profile name* node is used to view and update the profile name and domain name that the profile is monitoring.

Note: This node is named as the Profile-*profile name* throughout this document as the profile name is user-configurable.

Navigation: dns_response > Profile-*profile name*

Set or modify the following values that are based on your requirement:

Profile-*profile name* > New Profile

This section is used for managing profile name and domain name that the profile is monitoring.

<Profile Name> Node

This node represents the new profile that is created to monitor the DNS response.

Note: This node is user-configurable. Hence, this node is referred to as the *profile name* node throughout this document.

Network Server Node

The **Network Server** node is used to configure the monitoring properties of the DNS Response Monitoring probe. You can specify various conditions to generate the QoS and alarms.

Navigation: dns_response > Profile-*profile name* > *profile name* > Network Server

Set or modify the following values that are based on your requirement:

Network Server > General Profile Configuration

This section is used to configure the profile-specific monitoring parameters.

- Description: Defines a brief description of the profile. This description is for information only and is not used for any processing.
- Host/Domain: Defines a hostname or domain to be checked.
- Reverse Lookup IP: Defines an IP address for performing the reverse lookup with the forward lookup from a single profile.
- Name Server: Allows you to define the new name server for the current profile.
- Port: Specifies the port number for performing the reverse lookup with the forward lookup from a single profile.

  Default: 1
- Protocol: Specifies the protocol for performing the reverse lookup with the forward lookup from a single profile.

  Default: TCP
- Server Lookup Type: Specifies the server lookup type that the probe supports.

  Default: Normal IP Address (A)
- Server Lookup Class: Specifies the server lookup class that the probe supports.
- Number of Retries: Specifies the retry attempts for resolving the host or domain name and Reverse Lookup IP. The separate retries are attempted for the **Host/Domain** and the **Reverse Lookup IP**.
- Timeout (Seconds): Specifies the time limit for each request. If you have multiple retries, the cumulative timeout is multiplied by the number of retries.

Network Server > Messages for Alarm Timeout Situations

This section displays a list of alarms for preconfigured timeout situations.

Network Server > Alarm and QoS for Forward Lookup

This section is used to configure alarms and QoS for Forward Lookup. If the threshold value is exceeded, an alarm is issued.

- Enable Forward Lookup Alarm: Allows you to start receiving the Forward Lookup alarms.

  Default: Not Selected

- Forward Lookup alarm Threshold (Milliseconds): Specifies the time limit before issuing the Forward Lookup alarm.

- Enable Forward Lookup Warning: Allows you to start receiving the Forward Lookup warnings.

  Default: Not selected

- Forward Lookup warning Threshold (Milliseconds): Specifies the time limit before issuing the Forward Lookup warning.

- Source used for QoS and Alarm messages (Allow source override): Defines the source of alarm and QoS. If this field is blank, the QoS source is the hostname and alarm source is the IP address of the system.

Network Server > Lookup Failed

This section allows you to generate alarms when the DNS Response Monitoring probe failed to perform the Lookup action.

Network Server > Alarm Time

This section allows you to generate alarms when the response time is greater than the alarm threshold limit.

Network Server > Warning Time

This section allows you to generate alarms when the response time is greater than the warning threshold limit.

Network Server > Parse Error

This section allows you to generate alarms when the DNS Response Monitoring probe is not able to read the response time.

Network Server > DNS Fail

This section allows you to generate alarms when the DNS Server fails to response the DNS Response Monitoring probe.

Network Server > Alarm and QoS for Reverse Lookup

This section is used to configure alarms and QoS for Reverse Lookup. If the threshold value is exceeded, an alarm is issued.

- Enable Reverse Lookup Alarm: Allows you to start receiving the Reverse Lookup alarms.

  Default: Not selected
- Reverse Lookup alarm Threshold (Milliseconds): Specifies the time limit before issuing the Reverse Lookup alarm.
- Enable Reverse Lookup Warning: Allows you to start receiving the Reverse Lookup warnings.

  Default: Not selected
- Reverse Lookup warning Threshold (Milliseconds): Specifies the time limit before issuing the Reverse Lookup warning.
- Source used for QoS and Alarm messages (Allow source override): Defines the source of alarm and QoS. If the field is blank, the QoS source is the hostname and alarm source is the IP address of the system.

Configure a Node

This procedure provides the information to configure a particular section within a node. Each section within the node allows you to configure the properties of the probe for monitoring the DNS servers.

Follow these steps:

1. Select the appropriate navigation path.
2. Update the field information and click **Save**.

   The specified section of the probe is configured. The probe is now ready to monitor the DNS server.

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.

Manage Profiles

A monitoring profile is created to define the DNS server, which the DNS Response Monitoring probe can monitor. The monitoring profile defines the conditions and threshold values for generating QoS and alarms. You can also edit the monitoring parameters, which are based on changing business requirements for catering the changes in monitoring requirements.

Navigation: dns_response

Follow these steps:

1. Click the **Options** icon next to the **dns_response** node in the navigation pane.
2. Click the **Add New Profile** option.
3. Update the field information in the **Add New Profile** dialog and click **Submit**.

   The profile is saved and you can configure the profile properties for monitoring the DNS server.

Delete Profile

You can delete the monitoring profile that is no longer in use. You can also deactivate your monitoring profile, so that whenever a requirement comes again, you are not required to configure all the parameters again.

Navigation: dns_response > Profile-*profile name*

Follow these steps:

1. Click the **Options** icon next to the Profile-*profile name* node in the navigation pane.
2. Click the **Delete Profile** option.
3. Click **Save**.

   The selected profile is removed from the **dns_response** node.

Chapter 3: QoS Threshold Metrics

Many Nimsoft Monitor probes are shipped with the default alarm threshold values. These default values provide an idea about the information to be entered in the fields. These values and are not necessarily recommended best practice values. To aid in tuning thresholds and reducing false-positive alarms, this section describes the QoS metrics and provides the default alarm thresholds.

This section contains the following topics:

dns_response QoS Metrics

The following table describes the QoS metrics that can be configured using the DNS Response Monitoring probe.

Monitor Name	Units	Description
QOS_DNS_RESPONSE	Milliseconds	DNS response
QOS_DNS_RESPONSE_REVERSE	Milliseconds	DNS response

dns_response Alert Metrics Default Settings

The following table describes the default settings for the DNS Response Monitoring probe metrics.

Alert Metric	Error Threshold	Error Severity	Description
LookupFailure	-	Major	Alarms to be issued when DNS lookup of target failed on nameserver for profile.
TimeAlarm	-	Major	Alarms to be issued when DNS lookup time of the target server is breaching the alarm threshold.
TimeWarn	-	Warning	Alarms to be issued when DNS lookup time of the target server is breaching the warning threshold.

Alert Metric	Error Threshold	Error Severity	Description
DNSFailure	-	Major	Alarms to be issued when DNS server for profile does not respond to requests.
ParseError	-	Major	Alarms to be issued when unable to read response time from nameserver for profile.