

CA Nimsoft Monitor

Probe Guide for File and directory checking

dirscan v3.0 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

Chapter 1: Overview	7
About This Guide	7
Related Documentation	7
Preconfiguration Requirements	8
Supported Platforms	8
Chapter 2: Configuration Details	9
dirscan Node	10
Integrated Profile Node	11
Profiles Node	12
Configure a Node	15
Configure Dynamic Alarm Thresholds	16
Add Integrity Profile	17
Add Profile	17
Delete an Integrity Profile	17
Delete Profile	18
Chapter 3: QoS Threshold Metrics	19
dirscan Alert Metrics Default Settings	19
dirscan QoS Metrics	20

Documentation Changes

This table describes the version history for this document.

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

Chapter 1: Overview

The dirscan probe monitors files in specific directories. Alarms can be sent on number of files, age of files, and space used by files.

This section contains the following topics:

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

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

[Preconfiguration Requirements](#) (see page 8)

About This Guide

This guide is for the <cans> Administrator to help understand the configuration of the File and directory checking probe.

This guide contains the following information:

- An overview of the Active Directory Events 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.

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 dirscan probe

The [Release Notes](#) for the dirscan 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 File and directory checking probe.

Supported Platforms

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 dirscan probe.

Chapter 2: Configuration Details

This section describes the configuration concepts and procedures for setting up the File and directory checking probe. This probe is configured to monitor a particular directory.

- Checking that the directory exists,
- Checking that particular files or file types are located in the directory, and
- Checking that the size and age of the files do not exceed expected value.

This section contains the following topics:

[dirscan Node](#) (see page 10)

[Configure a Node](#) (see page 15)

[Configure Dynamic Alarm Thresholds](#) (see page 16)

[Add Integrity Profile](#) (see page 17)

[Add Profile](#) (see page 17)

[Delete an Integrity Profile](#) (see page 17)

[Delete Profile](#) (see page 18)

dirscan Node

This node allows you to configure the log properties of the File and directory checking probe. You can also view the list of alarm messages and their properties.

Navigation: dirscan

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

dirscan > Probe Information

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

dirscan > General Configuration

This section allows you to configure the log properties of the File and directory checking probe.

- Check Interval (seconds): Specifies the time interval at which the directories are scanned.
- Default Message Level: Specifies the level of the alarm message.
- Log Level: Specifies the level of details that are written to the log file.
Default: 0-Fatal
- Log Size (KB): Specifies the size of the file to which the internal probe messages are stored.
- User Name (including domain name): Defines the user name to access the directory or the file. The user name must include the Windows domain name.

dirscan > Message Pool

This section allows you to view the list of alarm messages and their properties.

- Identification Name: Indicates the name of the alarm message.
- Token: Indicates the checkpoint that the probe sets.
- Error Alarm Text: Specifies the text of the alarm message.
- Clear Alarm Text: Specifies the text of the message that is issued after the erroneous values are back within the threshold limits.
- Error Severity: Indicates the severity of the alarm.
- Subsystem string/ID: Indicates the ID of the sub system which issues the alarm.

Integrated Profile Node

This node allows you to create and configure an integrity profile.

Navigation: dirscan > Integrated Profiles

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

Integrated Profiles > Add Profile > Add

This section allows you to create the integrity profile.

- Profile Name: Defines the name of the integrity profile.

<Integrated Profile Name> Node

This node allows you to configure the properties of the integrity profile of the File and directory checking probe. You can also configure the QoS properties of the integrity profile.

Note: The integrity profile is added as the child node under the **Integrity Profiles** node and is user-configurable. Therefore, it is referred to as *integrated profile name* node throughout this document.

Navigation: dirscan > Integrated Profiles > *integrated profile name*

***integrated profile name* > Integrity Profile Information**

This section allows you to configure the properties of the integrity profile.

***integrated profile name* > Quality of Service message**

This section allows you to configure the QoS properties of the alarm message.

- Message ID: Specifies the alarm message that is on the detection of a change in the file.
- Command: Defines the action that is taken on the detection of a change in the file.
- File Integrity: Activates the monitoring of one or more specified files for detecting any change.

Profiles Node

This node allows you to create a monitoring profile for the File and directory checking probe.

Navigation: dirscan > Profiles

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

Profiles > Add Profile > Add

This section allows you to create and configure a monitoring profile for the File and directory checking probe.

- Profile Name: Defines the name of the monitoring profile.

<Profile Name> Node

This node allows you to configure the properties of the monitoring profile. You can also configure the properties of the directory or the file that is monitored.

Note: The integrity profile is added as the child node under the **Profiles** node and is user-configurable. Therefore, it is referred to as the *profile name* node throughout this document.

Navigation: dirscan > Profiles > *profile name*

profile name > Profile General Configuration

This section allows you to configure the properties of the monitoring profile.

- **Active:** Activates the monitoring of files and directories.
- **Directory:** Defines the path of the directory that is scanned.
- **Pattern:** Defines the string that is matched in the files that are present in the directory. Those files that match with the pattern are included.
- **Recurse into subdirectories:** Includes the subdirectories of the directory that is scanned.
- **Exclude directory Pattern:** Defines the pattern that is matched with the files for determining the files that are excluded.

profile name > Directory Check

This section allows you to configure the properties of the directory that is scanned.

- **Check Existence of Directory:** Checks the existence of the directory.
- **Message ID:** Specifies the message that is issued when the directory is not found.
- **Automatic Action Command:** Defines the action that is performed when the directory is not found.
- **QoS Directory exists:** Issues the QoS message when the directory is not found.

Note: The current version of the File and directory checking probe does not monitor the directories that are shared on a network.

profile name > Number of Files

This section allows you to configure the properties of files that the monitoring profile scans, concerning the number of files.

- **Expect this value (operator):** Specifies the operator that is used to set the condition for comparing the measured value with the specified value.
- **Expect this value:** Specify the condition for comparing the measured value.
- **Message ID:** Specifies the message that is issued when the specified condition is not met.

- Automatic Action Command: Defines the action that is performed when the specified condition is not met.
- QoS Number of matching files: Issues the QoS message when the specified condition is not met.

***profile name* > Age of File**

This section allows you to configure the properties of the directory that is scanned, concerning the changes in the files that are present in the directory.

- Expect this value: Specify the condition and the value you want the measured value meets. If the specified condition is breached, the alarm message that is selected is issued.
- Unit: Specify the required unit.
- Message ID: Select the alarm message to be issued when the specified condition is breached.
- Automatic action Command: Specify a command to be performed when the specified condition is not met.
- Watch age of: Specifies the age of file can be configured to use the age of the newest file, the oldest file or, each individual file that are found when more than one file match the pattern.
- On creation time: If selected, indicates that the creation time of the file is used while defining threshold.
- Directory changes between each scan: Checks if the directory has changed between each scan. Such a change would happen if a file is created or removed from the directory.
- Directory Age Message ID: The alarm message that is generated when the age of the directory breaches the specified condition.
- Directory age automatic Action Command: Specify a command to be performed when the specified condition is not met.

***profile name* > Space and Size of File**

This section allows you to configure the size properties of the files that are monitored.

- QoS space used by matching files in KiloBytes: Generates the QoS message if the space used by matching file matches the specified space.
- Used Space Operator: Specifies the space condition and unit.
- File space Message ID: Specifies the alarm message that is generated when the file space breaches the specified condition.
- Used space delta Operator: Specify the used space delta condition and unit
- over (cycle): Specify the number of cycles over which the used space delta value is calculated.

- File space Automatic Action Command: Specify a command to be performed when the specified condition is not met.
- File Size Operator: Specify the file size condition and unit.
- File size Message ID: Specifies the alarm message that is generated when the file space breaches the threshold condition.
- File size Automatic Action Command: Specify a command to be performed when the specified condition is not met.
- Watch size of: Specifies the size of file can be configured to use the size of the newest file, the oldest file, or each individual file, when more than one file match the pattern.

***profile name* > Read response time**

This section allows you to configure the QoS properties of the monitoring profile concerning the time in scanning the files.

- Expect this value : Specifies the condition and unit of the time for checking the specified file.
Note: When specifying read response time, the response time is calculated from reading the first one Mb of the file. If no file specified, the largest file in the directory is scanned for the quality of service response time.
- Message ID: Specifies the alarm message that is generated when the specified condition is breached.
- Command: Specifies the action to be performed when the specified condition is not met.
- Watch: Specifies the required option that is used to compare the response time with the specified value for generating alarms.
- QoS Read Response time of largest file in Bytes per Seconds: Generates QoS message when the read response time of largest file matches the specified response time.

Configure a Node

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

Each section within the node allows you to configure the properties of the File and directory checking probe.

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.

Add Integrity Profile

You can add an integrity profile which is displayed as a child node under the **Integrity Profiles** node.

Follow these steps:

1. Click the **Options** icon beside the **Integrity Profiles** node.
2. Click the **Add Profile** option.
3. Update the field information and click **Submit**.

The profile is saved and you can configure the event selection criteria for the File and directory checking probe.

Add Profile

You can add a monitoring profile which is displayed as a child node under the **Profiles** node.

Follow these steps:

1. Click the **Options** icon beside the **Profiles** node.
2. Click the **Add Profile** option.
3. Update the field information and click **Submit**.

The profile is saved and you can configure the event selection criteria for the File and directory checking probe.

Delete an Integrity Profile

If you no longer want the probe to monitor the directories and files, you can delete the integrity profile.

Follow these steps:

1. Click the **Options** icon beside the *integrity profile name* node.
2. Click the **Delete Profile** option.

The profile is deleted.

Delete Profile

If you no longer want the probe to monitor the event log messages, you can delete the monitoring profile.

Follow these steps:

1. Click the **Options** icon beside the *profile name* node.
2. Click the **Delete Profile** option.

The profile is deleted.

Chapter 3: QoS Threshold Metrics

Many Nimsoft Monitor probes ship with default QoS threshold values set. The default threshold values provide an idea of the type of values to be entered in the fields 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 QoS thresholds.

This section contains the following topics:

[dirscan Alert Metrics Default Settings](#) (see page 19)

[dirscan QoS Metrics](#) (see page 20)

dirscan Alert Metrics Default Settings

This section contains the alert metrics default settings for the File and directory checking probe.

QoS Metric	Warning Threshold	Warning Severity	Error Threshold	Error Severity	Description
FileSizeAlarm	None	None	None	Major	Alarm for file size
FileNumberAlarm	None	None	None	Major	Alarm for file number
FileSpaceAlarm	None	None	None	Major	Alarm for file space
FileDeltaSpaceAlarm	None	None	None	Major	Alarm for delta change in space used by files
FileAgeAlarm	None	None	None	Major	Alarm for file age
ResponseTimeAlarm	None	None	None	Major	Alarm for response time
FileIntegrityAlarm	None	None	None	Major	Alarm for file integrity
DirectoryCheckAlarm	None	None	None	Major	Alarm for Directory existence
FileError	None	None	None	Major	Alarm for File existence
DirAge	None	None	None	Major	Alarm for File Age

dirscan QoS Metrics

This section contains the QoS metrics for the *File and directory checking* probe.

Monitor Name	Units	Description
QOS_DIR_AGE	Seconds	Age of oldest matching file
QOS_DIR_EXISTS	Boolean	Directory exists
QOS_DIR_NUMBER	Files	Number of matching files
QOS_DIR_RESPONSE_TIME	Bytes per second	File Response
QOS_DIR_SPACE	Kilobytes	Space used by matching files
QOS_FILE_INTEGRITY	Boolean	File Integrity Check