CA Nimsoft Monitor

Probe Guide for Active Directory Events

adevl v1.5 series

Legal Notices

Warranty

The material contained in this document is provided "as is," and is subject to being changed, without notice, in future editions. Further, to the maximum extent permitted by applicable law, Nimsoft LLC disclaims all warranties, either express or implied, with regard to this manual and any information contained herein, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Nimsoft LLC shall not be liable for errors or for incidental or consequential damages in connection with the furnishing, use, or performance of this document or of any information contained herein. Should Nimsoft LLC and the user have a separate written agreement with warranty terms covering the material in this document that conflict with these terms, the warranty terms in the separate agreement shall control.

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

No part of this manual may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Nimsoft LLC as governed by United States and international copyright laws.

Restricted Rights Legend

If software is for use in the performance of a U.S. Government prime contract or subcontract, Software is delivered and licensed as "Commercial computer software" as defined in DFAR 252.227-7014 (June 1995), or as a "commercial item" as defined in FAR 2.101(a) or as "Restricted computer software" as defined in FAR 52.227-19 (June 1987) or any equivalent agency regulation or contract clause. Use, duplication or disclosure of Software is subject to Nimsoft LLC's standard commercial license terms, and non-DOD Departments and Agencies of the U.S. Government will receive no greater than Restricted Rights as defined in FAR 52.227-19(c)(1-2) (June 1987). U.S. Government users will receive no greater than Limited Rights as defined in FAR 52.227-14 (June 1987) or DFAR 252.227-7015 (b)(2) (November 1995), as applicable in any technical data.

Trademarks

Nimsoft is a trademark of CA.

Adobe®, Acrobat®, Acrobat Reader®, and Acrobat Exchange® are registered trademarks of Adobe Systems Incorporated.

Intel® and Pentium® are U.S. registered trademarks of Intel Corporation.

Java(TM) is a U.S. trademark of Sun Microsystems, Inc.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Netscape(TM) is a U.S. trademark of Netscape Communications Corporation.

Oracle® is a U.S. registered trademark of Oracle Corporation, Redwood City, California.

UNIX® is a registered trademark of the Open Group.

ITIL® is a Registered Trade Mark of the Office of Government Commerce in the United Kingdom and other countries.

All other trademarks, trade names, service marks and logos referenced herein belong to their respective companies.

For information on licensed and public domain software, see the *Nimsoft Monitor Third-Party Licenses and Terms of Use* document at: http://docs.nimsoft.com/prodhelp/en_US/Library/index.htm?toc.htm?1981724.html.

Contact CA Nimsoft

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?
1.5	September 2013	Initial Web-based GUI version of this probe. (Previous versions of this probe are configured using Infrastructure Manager).

Chapter 1: Overview

The Active Directory Events probe generates alerts based on messages from the NT event logs associated with Active Directory. The probe monitors the event logs Directory Service, Application, DNS Server and File Replication Service for new messages and generates alarm messages according to your setup. You can set up the probe to trigger an alarm each time a log event occurs in windows, which will activate it immediately every time a new message is put into the event log. Alternatively, you can choose to check the event log for new messages at fixed time intervals, which will reduces the system load generated by the probe.

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 Active Directory Events 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 adevl probe

The Release Notes for the adevl 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 Active Directory Events 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 Active Directory Events probe.

Chapter 2: Configuration Details

The Active Directory Events probe is configured by defining one or more profiles, identifying a set of criteria for event log messages and how they are configured. This probe allows you to define actions to be done on different event log messages. This probe is configured to generate alerts that are based on messages from the NT event logs associated with Active Directory.

This section contains the following topics:

adevl Node

This node allows you to view and configure the alarm properties of the Active Directory Events probe. You can configure the properties of the alarm messages when the event messages are issued. You can also view and configure the list of event messages of the current event.

Navigation: adevl

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

adevl > Probe Information

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

adevl > Properties

This section allows you to configure the alarm message properties that are based on the event messages. You can also configure the log properties of the Active Directory Events probe.

- Description Delimiter: Used to add any character, including special characters, to replace the existing character as delimiter.

- Remove Recurring Delimiter: Removes the repetition of delimiter.

  Default: Not selected

- Run Type
  - Poll: Specifies the time interval for checking the probe at regular intervals.

    Default: 30

  - Event: Specifies that the trigger is issued each time a new message arrives in the event log.

    Default: 20

- Default post subject: Specifies the default message subject of the event log messages when they are posted.
- Column prefix: Defines that the prefix entered in this field is sent with each field name when an event is posted.
- Log File: Defines the log file where the probe logs information about its internal activity.

  Default: adevl.log

- Log Level: Defines how much information is written to the log file.

  Default: 3-info

- Maximum Events to fetch: Specifies the maximum number of events that are fetched from the event log.
- Fetch alarms on configurator startup: Fetches all alarms at configuration start-up.

  Default: Selected

adevl > Event Log Status

This section allows you to configure the messages in the event log.

Exclude Node

This node allows you to configure the profiles that are excluded from the Active Directory Events probe. You can also configure the event selection criteria for the excluded profile.

Navigation: adevl > Exclude

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

Exclude > Add Exclude Profile

This section allows you to create and activate an exclude profile.

<Exclude Profile> Node

This node allows you to configure the properties of the Event Selection Criteria of the exclude profiles.

Note: All the profiles, appearing as child nodes, under the Excludes Node is user-configurable. Hence, they are referred to as *exclude profile* throughout this document.

Navigation: adevl > Exclude > *exclude profile*

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

***exclude profile* > Event Selection Criteria**

This section allows you to configure the properties of the event selection criteria of the exclude profile.

- Active: Activates the exclude profile.

  Default: Selected

- Log: Specifies the log for which the event log is monitored.

  Default: *

- Computer: Defines the event if the computer name matches event.

  Default: *

- Source: Defines the source from where the event is logged.

  Default: *

- Severity: Specifies the filter for the event if this field matches the severity in the event log.

- User: Specifies the filter for the event if this field matches the user in the event log.

- Category: Defines the filter for the event if this field matches category in the event log.

- Event ID: Defines the filter for the event if this field matches event ID in the event log.

- Message String: Defines the filter for the event if this field matches message string in the event log.

  Default: *

Profiles Node

This node allows you to create the monitoring profile for the Active Directory Events probe. You can also configure the event selection criteria and set the QoS conditions.

Navigation: adevl > Profiles

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

Profiles > Add New Profile

This section allows you to create and activate a monitoring profile.

<Profile Name> Node

This node allows you to configure the event selection criteria of the exclude profiles. You can also configure the QoS settings of the Active Directory Events probe.

Note: All the profiles, appearing as child nodes, under the **Profiles** Node is user-configurable. Hence, they are referred to as *profile name* throughout this document.

Navigation: adevl > Profiles > *profile name*

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

***profile name* > Event Selection Criteria**

This section allows you to configure the properties of the event selection criteria of the exclude profile.

- No propagation of events: Makes the event selection criteria of this profile unavailable for all other profiles.

  Default: Not Selected

- Log: Specifies the log from the drop-down menu for which the event log is monitored.

  Default: *

- Computer: Defines the event if the computer name matches event.

  Default: *

- Source/Publisher: Defines the source from where the event is logged.

  Default: *

- Severity: Specifies the filter for the event if this field matches severity in the event log.

- User: Specifies the filter for the event if this field matches user in the event log.

  Default: *

- Category: Defines the filter for the event if this field matches category in the event log.

  Default: *

- Event ID: Defines the filter for the event if this field matches event ID in the event log.

  Default: *

- Message String: Defines the filter for the event if this field matches message string in the event log.

  Default: *

- Run Command on match: Enables **Command Executable** and **Command Arguments** fields.
- Command executable: Specifies the command to run if an event has the selected criteria.
- Command arguments: Specifies the optional command parameters that are used to run the command in case an event occurs has the selected criteria.

***profile name* > QoS**

This section allows you to configure the QoS properties of the Active Directory Events probe.

- QoS Name: Defines the QoS name for event log.
- Units: Defines the unit value for the QoS.
- Metric Type Id: Defines the unique id for the QoS.
- Publishing Data: Triggers the generation of QoS.
- Publishing Alarms: Triggers the generation of alarms.
- Time interval (in seconds): Specifies the time interval for the detection of the event.
- Alarm Message: Defines an alarm message for the selected profile. You can use variables in the messages.
- Level: Specifies the severity level of the generation of QoSalarms.
- Set Suppression Key: Activates the suppression of message for avoiding the creation of multiple instances of the same alarm event.
- Time Frame(Value): Specifies the time interval for the monitoring of the events.
- Event Count: Specifies the number of times the alarm is generated when the events are monitored.
- Post message: Posts the event log message as a Nimsoft message.
- Post Message Subject: Defines a custom message for the profile.

***profile name* > Variables**

This section allows you to define one or more variables for each profile. You can define any number of variables on a profile.

Note: The name for two variables cannot be the same.

- Name: Defines the name of the variable.
- Source Line: Enables the **Source Line Value** field.
- Source Line Value: Defines the value of the variable at which, the threshold alarm is defined.
- From Character Position: Specifies the position of the character from where the source line is defined to extract the variable.

- Source From Position
  - Column: Specifies the position in the column where the source line is defined.
  - From Character Position: Specifies the position of the character in the source line.
  - Match Expression: Enables the correct position in the match expression.
- Operator: Specifies the operator of comparison.
- Threshold: Defines the threshold value for the variable.

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 Active Directory Events probe.

Follow these steps:

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

   The specified section of the Active Directory Events probe is configured.

Add Exclude 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 **Exclude** node.
2. Click the **Add Exclude Profile** option.
3. Update the field information and click **Submit**.

   The profile is saved and you can configure the event selection criteria for the Active Directory Events probe.

Manage Profiles

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 New Profile** option.
3. Update the field information and click **Submit**.

   The profile is saved and you can configure the profile properties to monitor the event log status.

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: adevl QoS Metrics

The following table describes the QoS metrics that can be configured using the Active Directory Events probe.

Monitor Name	Units	Description
QOS_EVL_COUNT	Count	Windows Events