CA Nimsoft Monitor

Probe Guide for Active Directory Events

adevl v1.6 series

technologies

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 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 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	August 2014	Updated the document for language and style consistency.
1.6	January 2014	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 (adevl) probe generates alerts based on messages from the NT event logs associated with Active Directory. The probe monitors the event logs of 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 when a log event occurs in windows, which activates 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 reduces the system load of 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: is 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 whenever 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 when this field matches the severity in the event log.

- User: specifies the filter for the event when this field value matches the user in the event log.

- Category: defines the filter for the event when this field matches category in the event log.

- Event ID: defines the filter for the event when this field matches event ID in the event log.

- Message String: defines the filter for the event when 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 list for which the event log is monitored.

  Default: *

- Computer: defines the event when 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 when this field matches severity in the event log.

- User: specifies the filter for the event when this field matches user in the event log.

  Default: *

- Category: defines the filter for the event when this field matches category in the event log.

  Default: *

- Event ID: defines the filter for the event when this field matches event ID in the event log.

  Default: *

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

  Default: *

- Run Command on match: enables the **Command Executable** and the **Command Arguments** fields.
- Command executable: specifies the command to run when 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 the 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 QoS alarms.
- 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