CA Unified Infrastructure Management

Probe Guide for Active Directory Events

adevl v2.0 series

Copyright Notice

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?
2.0	September 2014	■ Updated the **Overview**, **adevl Node**, and **<Profile Name> Node** topics. ■ Added the **Software Requirements** and **Known Issues** topics.
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 check the event log for new messages at fixed time intervals, which reduces the system load of the probe.

The Active Directory Events probe now supports the following non-English locales:

- B-Portuguese
- Chinese (traditional and simplified)
- French
- German
- Italian
- Japanese
- Korean
- Spanish

This section contains the following topics:

About This Guide

This guide is for the CA Unified Infrastructure Management Administrator to help understand the configuration of the Active Directory Events probe and provides the following information.

- Overview of the Active Directory Events probe and related documentation for previous probe versions.
- Configuration details of the probe.
- Field information and common procedures for configuring the probe.

Important! Description for the intuitive GUI fields is not 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 Unified Infrastructure Management Probes (http://docs.nimsoft.com/prodhelp/en_US/Probes/ProbeReference/index.htm)

New Features

The probe now supports internationalization for monitoring Active Directory Event logs in various Asian and European locales.

Preconfiguration Requirements

This section contains the preconfiguration requirements for the CA UIM Active Directory Events probe.

Software Requirements

The adevl probe requires the following software environment:

- Nimsoft Monitor Server 7.1 to 7.6 or CA Unified Infrastructure Management 8.0 or later.
- Robot 7.1 or later.
- Probe Provisioning Manager (PPM) probe version 2.38 or later (for Admin Console GUI only).
- Java Virtual Machine 1.6 or later.
- Active Directory installed.

Note: For SOC functionality, NM Server 5.6 or later and UMP 2.5.2 or later is required.

Supported Platforms

Please refer to the Compatibility Support Matrix for the latest information on supported platforms. See also the Support Matrix for 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

The **adevl** node is used to configure the general settings of Active Directory Events probe. These settings are applicable to all monitoring profiles of the probe.

This section contains configuration details specific to the Active Directory Events probe.

Navigation: adevl

Set or modify the following values as required:

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 lets you configure the general properties of the Active Directory Events probe.

- Description Delimiter: defines an ASCII character to replace the existing character as delimiter. Recommendation is to use a special character as delimiter.
- Remove Recurring Delimiter: removes the repetition of delimiter.

  Default: Not selected
- Generate New Metric Id: displays different metric ID when adevl and ntevl probes are deployed on the same robot.
- Run Type: specifies the condition when the probe is triggered for updating the events list. You can select one of the following options:
  - Poll: lets you configure the time interval (in the **Poll interval (Seconds)** field) for fetching the details of new events. Configure the **Alarm Timeout (Seconds)** field for generating an alarm, when the probe is unable to fetch new event details within the specified time limit.

    Default: 30
  - Event: updates the event list when the new event is logged in the event log file. Configure the **Alarm Timeout (Seconds)** field for generating an alarm, when the probe is unable to fetch new event details within the specified time limit.

    Default: 10

- Default post subject: defines the default subject of the alarm messages, which the probe generates. This default post subject can be overridden while creating a monitoring profile.

  Default: adevl

  A subject, which is used internally in CA UIM for alarm messages, cannot be used in this field:

  - alarm
  - alarm_new
  - alarm_update
  - alarm_close
  - alarm_assign
  - alarm_stats
  - QOS_MESSAGE
  - QOS_DEFINITION

  In case, any of the given subject is used then the probe uses the **evl_** as the message subject. If the field is left blank, probe uses adevl as the default post message subject.

  Note: This field only defines the default post message subject, select the **Post Message** option in the **Alarm** section of the *profile name* node for sending the message. You can even override the message subject there.

- Column Prefix: defines a text for appending after each column name of the alarm message.

  Default: evl_

- Log File: defines the log file where the probe logs information about its internal activity.

  Default: adevl.log

- Log File Size (KB): sets the size of the log file.

  Default: 100

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

  Default: 0-fatal

- Maximum Events to fetch: defines the maximum number of latest events that the probe fetches from each event log file and displays in the **Event Log** section. If the field is left blank, the probe displays all the events.

  Default: 1000

  Important! Do not configure the field value to more than 1000 else the probe can stop responding. Refer the **Known Issues** section for more detail.

- Select Log Files: lets you select the log files, which the probe monitors. Select a log file from the **Available** list and add it to the **Selected** list.

  Default:

- Output Encoding: specifies the character encoding for generating alarms and QoS messages when the probe is deployed in a non-English locale.

  Default: blank

- System Encoding: specifies the system and output encoding where the probe is installed.

  Default: blank

  Note: The probe auto-detects the system and output encoding when these field values are blank. However, the recommendation is to specify the appropriate encoding in the fields. You can use UTF-8, UTF-16BE, UTF-16LE, UTF-32BE, UTF-32LE, Shift_JIS, ISO-2022-JP, ISO-2022-CN, ISO-2022-KR, GB18030, GB2312, Big5, EUC-JP, EUC-KR, ISO-8859-1, ISO-8859-2, windows-1250, and windows-1252 encodings.

- Alarm List Size: defines the buffer size for storing the event details that match the monitoring profile criteria. This field is useful when a profile generates an alarm when a certain number of events are found. For example, a monitoring profile generates an alarm when the matching events count reaches 50. Since the event count is up to 49; probe keeps the events detail in the buffer.

  Default: 1000

- WMI Query Timeout: defines the time-out interval of WMI query for fetching the monitoring data. The probe uses WMI queries when hosted on operating systems earlier than Windows Server 2008.

  Default: 1

  Note: The WMI service must be enabled on the host system for this option to work.

- WMI Timeout Interval: specifies the unit of WMI query time-out interval.

  Default: Seconds

adevl > Subsystems Configuration

This section lets you define a different alarm subsystem ID for each monitored log file. Use the New button and define the new subsystem ID by configuring the following fields:

- Subsystem Key: defines a subsystem key for the appropriate log file. This key must be identical to the corresponding log file name, contain only small characters, and the slash (/) character is replaced with $$. For example, the key is **microsoft-iis-configuration$$administrative** for the **Microsoft-IIS-Configuration/Administrative** log file.
- Subsystem Value: defines a different alarm subsystem ID for each monitored log file. The recommendation is to use the default subsystem ID pattern (1.1.11.1.X) for other log files too. This pattern is mandatory to view the metric details under the **Event Log** node of the Unified Management Portal (UMP).

  You can also define an appropriate name of newly defined subsystem value in the **nas** probe, else subsystem value is displayed as is on UMP.

The default configuration of the probe monitors dns, filerep, and directory log files, with the following subsystem IDs:

- 2.1.2
- 2.1.2
- 2.1.2

Important! Do not delete or modify any of the default subsystem IDs.

adevl > Language String Configuration

This section lets you configure the various non-English event severity strings with appropriate severities in English. If not configured, the probe displays the event severity as Information on the probe GUI. The reason is that Windows returns event severity string in specific locales and the probe cannot compare these values with equivalent English string. For example, if your Windows is in the **French** locale, then define **Erreur** in the **Error** field.

Note: The Language String Configuration is applicable when the probe is deployed on Windows Vista or Windows Server 2008 R2 or a later version.

adevl > Event Log Status

This section displays a list of events in a grid for one of the selected log files. Select a grid row and the corresponding event details with XML view are displayed on the screen.

Note: Use the **Options** icon of the adevl node and specify the log file for displaying the events list in this **Event Log** grid. By default, the probe displays the **Application** events.

The **Actions** drop-down list provides you the following options:

- **Clear Log:** deletes the log from the list.

- **New Profile:** creates a monitoring profile for the selected event log. Refer the *profile name* node for the field descriptions and other related information.
- **Exclude Profile:** creates an exclude profile for the selected event log. Refer the *exclude profile name* node for the field descriptions and other related information.

<Host Name> Node

The *host name* node is used to identify the host of the system, on which the probe is deployed. This node does not contain any field or section and is used for classifying the exclude and monitoring profiles.

Exclude Node

The **Exclude** node is used to create a profile for excluding the events from monitoring by the probe. This node does not contain any field or section, but contains only child nodes where each child node is a different exclude profile.

Navigation: adevl > Exclude

Set the following values as required:

Exclude > Add Exclude Profile

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

<Exclude Profile> Node

The *exclude profile* node is used to define the event selection criteria. The Active Directory Events excludes the matching events from monitoring.

Note: This node is referred to as *exclude profile* in this document and is user-configurable.

Navigation: adevl > Exclude > *exclude profile*

Set or modify the following values as required:

***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 file from which the probe excludes the events from monitoring. The event log files, which are selected in the adevl node are displayed here. Selecting the * runs the profile on all event logs.

  Default: *

- Computer: defines the computer name on which the event has occurred.

  Default: *

- Source: defines the source from where the event has logged.

  Default: *

- Severity: specifies the severity of the event.

  Default: *

- User: defines the Windows user account for whom the event was generated.

  Default: *

- Category: defines the event category.

  Default: *

- Event ID: defines the unique identification number of the event.

  Default: *

- Message String: defines the message text of the event. You can use the regular expressions for matching the message string.

  Default: *

The events matching the given criteria are excluded from the monitoring profile of the probe.

Profiles Node

The **Profiles** node is used to create a monitoring profile for generating alarms and QoS for the events that match the monitoring criteria. The monitoring profile caters to the monitoring requirements and alerts the user when something unexpected happens. This node does not contain any field or section, but it contains only child nodes where each child node is a different monitoring profile.

Navigation: adevl > Profiles

Set or modify the following values as required:

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: This node is referred to as *profile name* in the document and is user-configurable.

Navigation: adevl > Profiles > *profile name*

Set or modify the following values as required:

profile name **> Event Selection Criteria**

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

- Active: activates the profile.

  Default: Selected

- No propagation of events: excludes an event that matches the selection criteria of one monitoring profile for all other profiles.

  Default: Not Selected

- Log: specifies the log file from which the probe monitors the event. The event log files, which are selected in the adevl node are displayed here. Selecting the * runs the profile on all event logs.

  Default: *

- Computer: defines the computer name on which the event has occurred.

  Default: *

- Source/Publisher: defines the source or the publisher from where the event is logged.

  Default: *

- Severity: specifies the severity of the event.

  Default: *

  Note: The **audit success** and **audit failure** severity options are applicable only for Windows earlier than Vista and 2007. Microsoft has moved these options to the **keyword** field from Windows Vista and 2007 onwards. The severity level of these events is shown as **Informational** in the event viewer. The current implementation of the probe does not support monitoring on basis of the **keyword** field.

- User: defines the Windows user account for whom the event was generated.

  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: defines the executable command when the matching event is found. You can also use the **browse** option and attach a batch file.

- Command arguments: defines the command arguments for executing the command.

- Separator: defines a field separator character for the event message text. This field is useful for segregating the event message text in multiple columns and then uses those column numbers in the **Variables** section. For example, if your event message text is ABCD:EFGH:IJKL:MNOP and the separator is : (colon) then probe segregates the message text in four different columns (0 through 3). You can use these column numbers for fetching the appropriate text to the variable.

  Note: The non-English characters are not supported as a separator.

***profile name* > QoS**

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

- Publish Data: enables profile to generate the QoS.
- Time interval (in seconds): defines the time interval for monitoring the events and generating alarms and QoS.

***profile name* > Alarm**

This section allows you to configure the alarm messages for the monitoring profile of the Active Directory Events probe.

- Publish Alarms: enables the profile to geneaste the alarm message.
- Alarm Message: defines the alarm message to be generated when the event matches the monitoring criteria. You can use following variables in the message text:
  - $profile: Name of the profile for which alarm is generated.
  - $description: User-defined description.
  - $variable: User-defined variable.
  - $source: The source from where the event is logged. For example, [Service Control Manager].
  - $event_id: The ID of the particular event.
  - $category: Category name of the particular event. For example, [Management] and [Disk].
  - $log: The event log name. For example, [System] and [Application].
  - $severity: The event Severity level of the event.
  - $severity_str: The severity code name. For example, [error] and [information].
  - $user: Username of the event.
  - $computer: Host name of the system on which the event is generated.
  - $time_stamp: Date timestamp when the event is generated.
  - $message: Message description available in the event logger.
  - $record_id: The record number which is assigned to the event when the event is logged.
  - $evlData: The data associated with the event. If no data is present, None is added to the message.
- Level: specifies the severity of the alarms. Select the **From Eventlog** option to use the same severity as the event log message.

  Note: The critical level is only supported on the Windows Server 2008.

- Subsystem: defines a custom subsystem ID for overriding the default subsystem ID. For example, you can give the profile name for identifying each alarm source. You can also use variables in this field, which are explained for the **Alarm Message** field.
- Set Suppression Key: activates the message suppression feature to avoid multiple instances of the same alarm event.
- Optional Key: defines a suppression key for the alarm messages, which overrides the default key.
- Time Frame(Value): specifies the time interval for the monitoring of the events.
- Time Frame(Unit): specifies the unit of the time frame value.
- Event Count: defined the number of events and generates alarms when this number breaches the threshold limit.
- Post message: posts the event log message as the alarm.
- Post Message Subject: defines the subject of the alarm. This value overrides the default message subject, which is defined in the **adevl** node.

profile name **> Variables**

This section allows you to define variables with a set of conditions for each profile. These conditions populate the variable value on real time from the selected event log message. These variables are then used for generating the alarm messages.

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 line number of the event log message text.

  Default: 1
- From Character Position: specifies the position of the character from where the source line is defined to extract the variable.

  Default: 1

- Source From Position
  - Column: specifies the position of the column in the source line to extract the value of the variable.
  - From Character Position: specifies the position of the character in the source line to extract the value of the variable.
  - Match Expression: defines the regular expression for extracting value of the variable, whenever the matching text is found in the event log message.

  Note: You can extract variables from the contents inside parentheses in the match expression. Using number 1, refers to the first parenthesis in the expression, using number 2, refers to the second parenthesis in the expression, and so on.
- Operator: specifies the threshold operator for generating an alarm. Select the **RE** option for using the regular expressions.

  Note: The >, <, >=, and <= operators support only integer and float type values. These operators do not work with string values. Only the = operator works with string values.
- Threshold: defines the threshold value for the variable. For example, set the threshold value for column 0 equal to 10 for generating alarm every time the value in column 0 equals 10.

  Default: 1

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. The probe is now ready to monitor the Active Directory Event logs.

How to Configure Alarm Thresholds

Some Quality of Service measurement probes allow you to set different types of alarm thresholds. These threshold options allow you to more broadly control when alarm messages are sent for each QoS probe.

For more information about the different alarm thresholds and their configuration requirements, refer to the *General Probe Configuration* section of the Admin Console Help.

View Event Log Properties

The Active Directory Events lets you view the event log properties on the probe GUI, which helps you in following ways:

- Identify the events, which require monitoring.
- Identify the event properties for monitoring all related events.
- Provide a direct option for creating a monitoring profile where the selected event details are already filled.

Follow these steps:

1. Click the **Options** next to the **adevl** node.
2. Select the **Add Event Log** option.
3. Select the appropriate event log file from the **Event Log** drop-down list.

   Note: The Event Log drop-down displays only those log files, which are selected in the **Properties** section.
4. Click **Submit**.

   The logs of selected event log files are displayed in the **Events** section.
5. Select the appropriate event in the **Events** list and the event details are displayed below the list.
6. Select the **New Profile** option from the **Actions** drop-down list.
7. Define the **New Profile Name** and click **Submit**.

   The new profile appears under the **Profile** node. You can select the *profile name* node and can verify in the **Event Selection** section that event details are already filled.

   Similarly, select the **Exclude Profile** option from the **Actions** drop-down list for creating an exclude profile for the event.

Add Exclude Profile

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

   Important! Do not use slash (/) in the profile name; else the probe trims the profile name from the slash (/) character and discards the profile properties. For example, if the profile name is **My/Profile** then the probe only saves **My** as the profile name.

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.

Regular Expression Construct Rules

Constructing regular expression and pattern matching requires meta characters. The probe must support Perl Compatible Regular Expression (PCRE). It is recommended to use regular expressions within forward slash **(/)**. The following table lists various rules and constructs for creating regex and pattern matching.

S. No.	Meta Character	Description	Examples for expression enclosed with "/"	Examples for expression enclosed without "/"
1.	**[ ] Square Brackets**	Matches one character within square brackets at once.	■ **[12]:** matches first for **1** and if not found, matches for **2** in the target string. ■ **[0123456789] :** matches any character in the range **0** to **9** in the target string.	**[12]:** matches for 12 in the target string.
2.	**- Dash**	Defines range for the target string when used within square brackets. For example, **[0123456789]** can be written as **[0-9]**.	**[0-9A-C]:** matches for **0** to **9** and **A** to **C** (but not **a** to **c**) in the target string.	**[0-9A-C]:** matches the entire string **[0-9A-C]** with the target string.
3.	**^ Circum flex or Caret**	Negates the expression when used within square brackets.	■ **[^Ff]:** matches for anything except upper or lower case of **F.** ■ **[^a-z]:** matches for anything except lower case **a** to **z**.	**[^Ff]:** matches the entire string **[^Ff]** with the target string.
4.	**^ Circum flex or Caret**	Matches the target string only at the beginning.	**^Moz:** matches for string beginning with Moz (Mozilla).	**^Moz:** matches the entire string with the target string.

5.	**$ Dollar**	Matches the target string only at the end.	**fox$:** matches for *silver fox.*	**fox$:** matches the entire string with the target string.
6.	**. Period**	Matches any character(s) following the expression.	**ton.:** matches for *tons*, *tone*, and *tonneau* but not *wanton*.	**ton.:** matches the entire string with the target string.
7.	**? Question**	Matches the target string when the preceding character occurs for zero times or once.	**colou?r:** matches for *color* (u is found 0 times) and *colour* (u is found 1 time).	**colou?r:** matches the entire string with the target string.
8.	*** Asterisk**	Matches the target string when the preceding character occurs for zero times or more.	**tre*:** matches for *tree* (e is found 2 times), *tread* (e is found 1 time), and *trough* (e is found 0 times).	**tre*:** matches the entire string with the target string.
9.	**+ Plus or Addition**	Matches the target string when the preceding character occurs for once or more.	**tre*:** matches for *tree* (e is found 2 times), *tread* (e is found 1 time), but not *trough* (e is found 0 times).	**tre*:** matches the entire string with the target string.
	{n}	Matches the target string when the preceding character occurs **n** times exactly.	**[0-9]{3}-[0-9]{4}:** matches for 123-4567.	**[0-9]{3}-[0-9]{4}:** matches the entire string with the target string.
11.	**{n,m}**	Matches the target string when the preceding character occurs at least **n** times but not more than **m** times.	**ba{2,3}b:** matches for *baaband*, *baaab* but not *bab* or *baaaab*.	**ba{2,3}b:** matches the entire string with the target string.
12.	**{n, }**	Matches the target string when the preceding character occurs at least **n** times.	**ba{2,}b:** matches for *baab*, *baaab*, and *baaaab* but not *bab*.	**ba{2,}b:** matches the entire string with the target string.
13.	**\\ Escape Sequence**	Matches meta characters with literal.	**\\\\nimsoft:** matches for *nimsoft*.	**\\nimsoft:** matches the entire string with the target string.

14.	**/ Forward Slash**	Matches meta characters with literal.	**//C/:** matches for **/C** in target string **/CATech**.	**/C:** matches the entire string with the target string.
15.	"**(**" or "**)**"	Matches meta characters with literal.	**\(s\):** matches for (s) in the target string window(s).	**(s):** matches the entire string with the target string.

Note: The probe does not support **/s** for adding space in a regular expression.

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	Returns the number of matching events found by the monitoring profile.

Chapter 4: Known Issues

The Active Directory Events probe has the following limitations:

With NMS 7.6 or earlier:

- The **Raw Configure** GUI of the probe is not supported for non-English locales because it can corrupt the entire probe configuration file.
- The probe GUI can stop responding when the **Maximum Events to Fetch** field value is more than 1000. In case the probe GUI has already stopped responding; follow these steps:
  1. Open the IM probe GUI.
  2. Update value of this field to 1000 or less (under the **Properties** tab).
  3. Restart the probe.
- The probe does not support forwarding events monitoring.

With CA UIM 8.0 onwards:

- The probe GUI can stop responding when the **Maximum Events to Fetch** field value is more than 1000. In case, the probe GUI has already stopped responding; follow these steps:
  1. Open the **Raw Configure** GUI.
  2. Update value of the **fetch_number** key (under **setup** section) to 1000 or less.
  3. Restart the probe.

With all NMS or CA UIM Versions:

- The probe does not support forwarding events monitoring.
- Localization is not supported on Windows ia64 platform.
- Do not use same profile name for ntevl and adevl probes, when deployed on same robot.
- Use either IM GUI or AC GUI of the probe to avoid any unexpected issues that can occur during probe configuration.