ADInsight Copyright © 2007 Mark Russinovich and Bryce Cogswell

Sysinternals - www.sysinternals.com

ADInsight is an advanced monitoring tool for Windows that shows real-time file client-side Active Directory (LDAP - Light-weight Directory Access Protocol) activity. Using ADInsight, you can troubleshoot permissions, performance, and configuration issues that affect ADenabled applications, such as Exchange and SQL Server.

ADInsight uses DLL injection techniques to intercept calls that applications make in the Wldap32.dll library, which is the standard library underlying Active Directory APIs such ldap and ADSI. Unlike network monitoring tools, ADInsight intercepts and interprets all client-side APIs, including those that do not result in transmission to a server. ADInsight monitors any process into which it can load it's tracing DLL, which means that it does not require administrative permissions, however, if run with administrative rights, it will also monitor system processes, including windows services.

ADInsight runs on Windows 2000, Windows XP, Windows Vista, Windows Server 2003, and Windows Server 2008.

Capturing Events

To toggle capture mode on and off, click the **Capture** toolbar button, choose **Capture Events** from the **File** menu, or press **Ctrl+E**. No data is collected when capture mode is off.

✓ Note

By default events are captured when a new connection is made. To change the default capture mode choose Preferences from the **Options** menu and clear **Automatically start to capture after connection**.

Copying an Event

To copy a selected event to the Clipboard, chose **Copy** from the **Edit** menu or press **Ctrl+C**.

Finding Text

To search for an occurrence of text in the Event Pane, click the **Find** toolbar button, choose **Find** on the **Edit** menu, or press **Ctrl+F**. This action opens the **Find** dialog box.



If the text you entered is found in the Event Pane, the matching event will be selected and Auto Scroll will be turned off to keep the line in the window.

- To repeat a search down the event list press the **F3** shortcut key.
- To repeat a search up the event list press the **Shift+F3** shortcut key.

✓ Note

You can search only in columns that are visible in the Event Pane. To set the column display, choose **Select Columns** from the **Options** menu or from the context menu that appears when you right-click on an item.

Clearing the Display

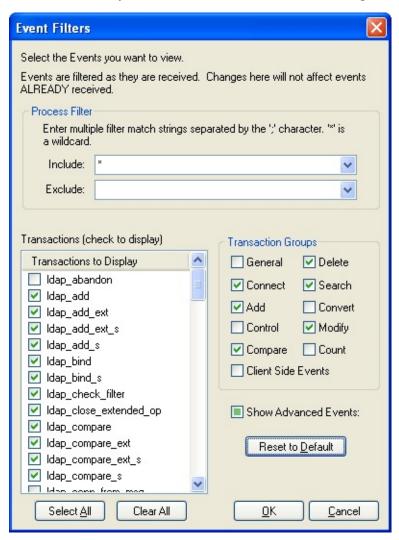
To clear the Event Pane, click the **Clear** toolbar button or choose **Clear Display** from the **Edit** menu.

This action resets the sequence number to 0; it also resets the values displayed in the Time column if relative time is selected.

Filtering the Display

To display or hide processes whose names contain specified text substrings, or to add or exclude selected LDAP transactions, click the **Filter** toolbar button, choose **Event Filter** from the **View** menu, or press **Ctrl+L**.

This action opens the **Event Filters** dialog box.



- To view only processes whose names contain specified substrings, type the text expression in the **Include** list.
- To exclude processes whose names contain specified substrings, type the text expression in the **Exclude** list.

Using Filter Expressions

- You can enter multiple expressions by separating each expression with a semicolon (;).
- Use the Asterisks (*) as a wildcard character.
- Do not include spaces in the expression unless you want the spaces to be part of the filter.
- Filter expressions are a case insensitive.

Selecting Displayed Transactions

- To hide selected LDAP transactions, clear the corresponding check boxes.
- To display events not commonly used for troubleshooting and configuration select Show Advanced Events.

To reset the Include and Exclude expressions and select the default LDAP transaction check boxes, click **Reset to Default**.

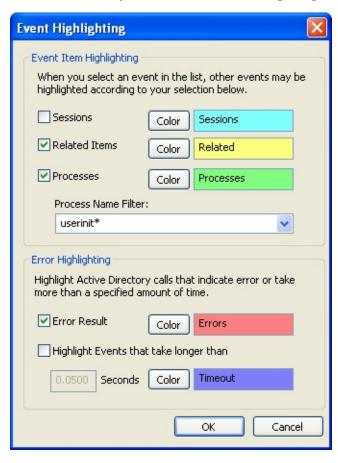
Notes

- Changes in the Event Filters dialog box do not affect items already in the display.
- When you start Insight for Active Directory with a Process Filter applied from a previous session, the Event Filters dialog box will open to confirm your filter settings. To start the console without opening the Filter dialog box, add the -q parameter to your startup command.

Highlighting Events

To set display highlighting properties, choose **Highlight Preferences** on the **Highlight** menu or from the context menu that appears when you right-click on an item in the Event Pane.

This action opens the **Event Highlighting** dialog box.



- To highlight events in the same session handle as the selected item, click **Sessions**.
- To highlight events with the same event handle as the selected item, click **Related Items**.
- To highlight events whose process names contain specified text substrings, click Processes and type the text expression in the Process Name Filter list. Filter expression rules apply to text in the Process Name Filter.
- To highlight events with errors, click **Error Result**.

■ To highlight events with Result Times that are longer than a specified time, click **Highlight Events that take longer than** and type the time in seconds.

To change a highlight color, click the **Color** button corresponding to the highlight option. This action opens the **Highlight Color** dialog box.

To toggle all highlighting on and off, choose **Enable Highlighting** on the **Highlighting** menu.

☑ Note

The **Next** and **Prev** toolbar buttons are disabled when highlighting is disabled or **Error Result** is not selected.

Finding Event Errors

To go to the next error in the Event Pane, click the **Next** toolbar button or choose **Next Event Error** from the context menu that appears when you right-click on an item in the Event Pane.

To go to the previous error in the Event Pane, click the **Prev** toolbar button or choose **Previous Event Error** from the context menu that appears when you right-click on an item in the Event Pane.

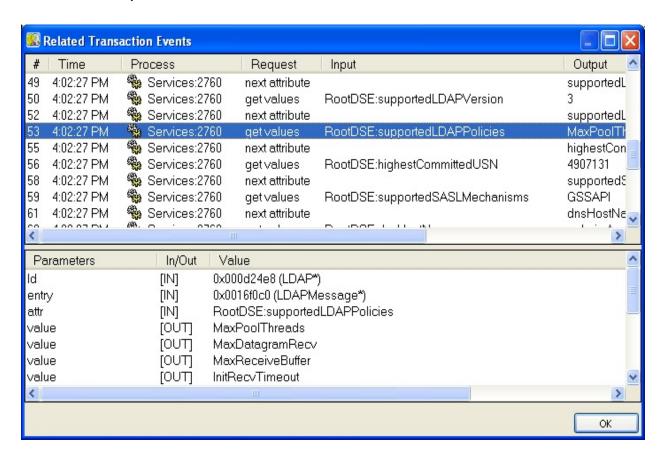
Note

The **Next** and **Prev** toolbar buttons are disabled when highlighting is off, when Error Result in the **Event Highlighting** dialog box is not selected, or when no item is selected in the Event Pane.

Viewing Related Events

To view a list of events with the same event handle as the selected item, choose **View Related Events** on the **View** menu or on the context menu that appears when you right-click on the item.

This action opens the **Related Transaction Events** window.



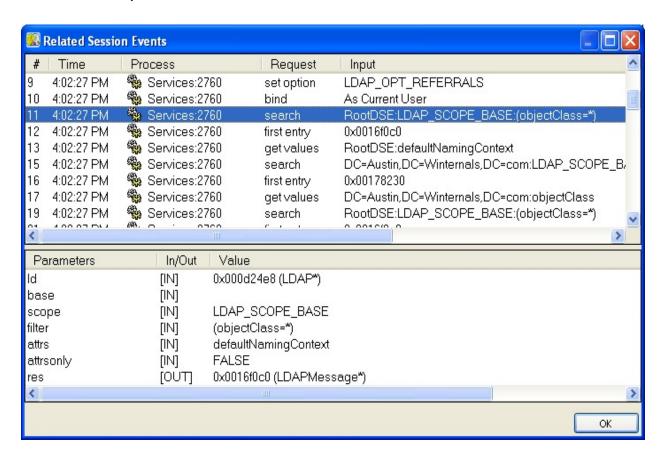
Note

Columns that appear in the window correspond to the columns visible in the Event Pane. To add or remove columns, choose **Select Columns** from the **Options** menu or from the context menu that appears when you right-click on an item.

Viewing Related Session Events

To view a list of events with the same LDAP session handle as the selected item, choose **View Session Events** on the **View** menu or on the context menu that appears when you right-click on the item.

This action opens the **Related Session Events** window.



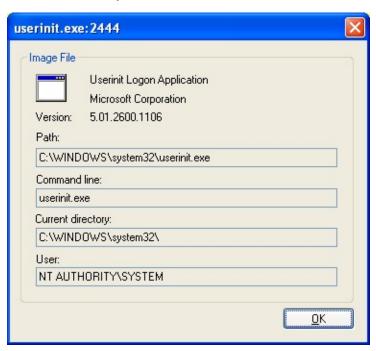
Note

Columns that appear in the window correspond to the columns visible in the Event Pane. To add or remove columns, choose **Select Columns** from the **Options** menu or from the context menu that appears when you right-click on an item.

Viewing Process Information

To view information about the process making an LDAP call, choose **Process Information** from the context menu that appears when you right-click on an item in the Event Pane.

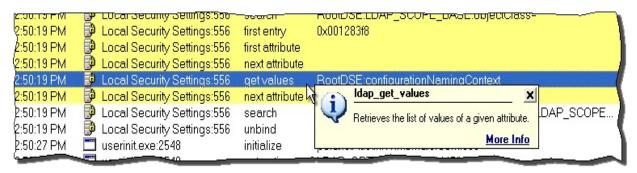
This action opens the **Process Information** window.



Viewing Event Information

To view summary information about an LDAP function that appears in the Request column, double-click an item in the Event Pane or choose **Event Information** from the context menu that appears when you right-click.

This action opens a pop-up dialog box that displays the full name and description of the function.



To view detailed diagnostic information about the LDAP function, click the **More Info** hyperlink. This action opens a browser window with information from the MSDN Library Web site.

Setting Time Display Options

To toggle the **Time** column display between clock time and relative time, choose **Clock Time** from the **Options** menu or press **Ctrl+T**.

- When clock time is selected you can toggle the **Time** column display to show or hide milliseconds by choosing **Show Milliseconds** from the **Options** menu.
- You can toggle the number of decimal places displayed in the Time and Duration columns by choosing Show Simple Time from the Options menu. Simple time is displayed in the Time column only when relative time is selected.

Setting Auto Scroll

By default the display scrolls to automatically show new activity.

To toggle Auto Scroll off and on, click the **Scroll** toolbar button, choose **Auto Scroll** on the **View** menu or press **Ctrl+A**.

✓ Note

Turning off Auto Scroll temporarily sets the History Depth to an unlimited number of lines so that new items will continue to appear in the display.

Setting History Depth

By default older lines are discarded from the event list to stay within a specified History depth. To change History depth, click the **History** toolbar button, choose **History Depth** on the **View** menu, or press **Ctrl+H**.

This action opens the **Event List History Depth** dialog box.



- Type or select a new value in the **History Depth** box or click **Default** to restore the default value of 50,000 lines.
- Type or select **0** in the History Depth box to retain an unlimited number of lines in the display.

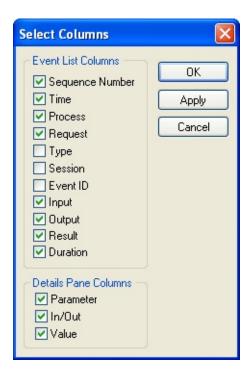
✓ Note

Turning off Auto Scroll temporarily sets the History Depth to an unlimited number of lines so that new items will continue to appear in the display.

Setting the Column Display

To select the columns that appear in the display, choose **Select Columns** from the **Options** menu or from the context menu that appears when you right-click on an item in the Event Pane.

This action opens the **Select Columns** dialog box.



You can choose any of the following columns to appear in the Event Pane:

Sequence Number	the unique sequence number assigned to an event; gaps in sequence numbers may indicate buffer overflow resulting from heavy activity or filtering that prevents some items from appearing in the display
Time	the time that the event occurred
Process	the name of the process making the LDAP call to the Active Directory
Request	the name of the LDAP function call
Туре	whether the LDAP call is synchronous or asynchronous
Session	the LDAP session handle
Event ID	the LDAP event handle

Input the value passed from the Process to the Active Directory

Output the value passed to the Process from the Active Directory

Result the Result code returned by the function; Success results are not displayed unless

you clear Suppress Success Status on the Options menu

Duration the elapsed time between the call and the result

You can choose any of the following columns to appear in the Details Pane:

Parameter the parameter names for the selected LDAP call

In/Out whether the parameter is being sent or received by the application

Value the value passed to or from the process making the LDAP call

Setting Other Display Options

- To change the font size of items in the display, choose Font on the Options menu.
- Choose Always on Top to keep the window displayed when you switch programs or windows.
- To toggle the Request column between full and simple LDAP function names, click **Show Simple Event Name** on the **Options** menu. Examples of full and simple LDAP function names are:

ldap get values len

Full Name

Simple Name get values length

■ To toggle the display between distinguished and simple names, click **Show Distinguished Name Format** on the **Options** menu. Examples of equivalent distinguished and simple names are:

CN=RCHASE-

Distinguished Name 2K3,CN=Computers,DC=OA,DC=Denver,DC=Addesinc,DC=com

Simple Name OA.Denver.Addesinc.com\Computers\RCHASE-2K3

■ To toggle the display of LDAP filter strings in the Input column and Details Pane between simple format (i.e., prefix notation) and standard format (i.e., infix notation), click **Show Simple LDAP Filters** on the **Options** menu. Examples of equivalent simple and standard format filter strings are:

((NOT((showInAdvancedViewOnly=TRUE)) AND (samAccountType

Simple Format ((name=rchase-2k3*) OR (sAMAccountName=rchase-2k3*)))

Standard Format (&(&(!(showInAdvancedViewOnly=TRUE))(samAccountType=80530)

(name=rchase-2k3*) (sAMAccountName=rchase-2k3*)))

•	To toggle off and on the display of Success status in the Result column, click Suppress Success Status from the Options menu.

Command-Line Options

You can use command-line parameters to set console startup options and to launch the monitoring service from a batch file or command window.

Syntax

```
adinsight [-q] [-o] [-log FileName] [-fi
IncludeString] [-fe ExcludeString] [[-u UserName
-p Password] -r ComputerName]...
```

Parameters

-q

Starts the console without opening the Filter dialog box. By default the Filter dialog box opens at startup if any filters are applied.

-0

Turns off event capture.

-log FileName

Writes activity to a log file without opening the console, where *FileName* is the name of the output file.

–fi

Specifies an Include string for the Filter. Filter expression rules apply to the *IncludeString* text.

-fe

Specifies an Exclude string for the Filter. Filter expression rules apply to the *ExcludeString* text.

-?

Displays help at the command prompt.

Saving Output

To save the contents of the Event Pane as a text file, choose **Save** on the **File** menu or press the **Ctrl+S** shortcut key.

To copy the selected item to the Clipboard, chose **Copy** from the **Edit** menu or press the **Ctrl+C** shortcut key.

✓ Note

You can also save the contents of the Event Pane as HTML formatted reports.

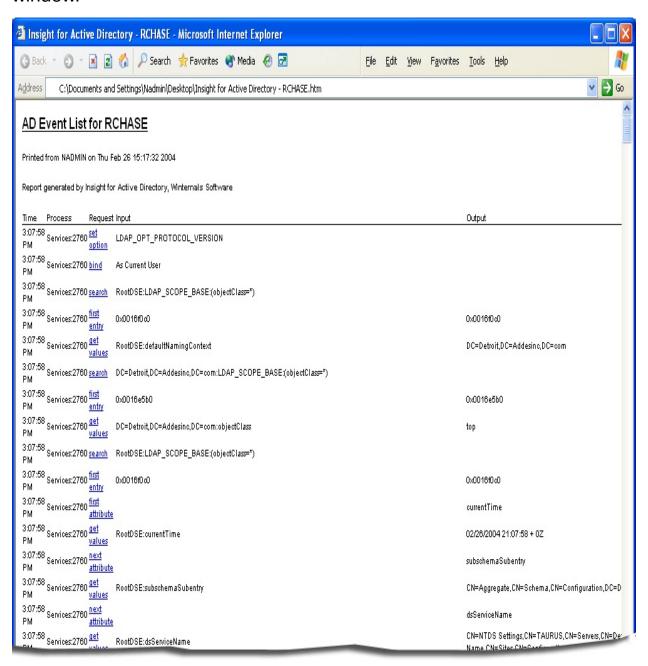
Logging to a File

You can use the command-line $_{-log\ option}$ to write activity to a log file without opening the console.

Viewing Event Reports

To view a report of all items in the Event Pane, choose **Events** from the **HTML Reports** submenu of the **View** menu.

This action opens an HTML-formatted report in your Web browser window.



To view detailed diagnostic information about an LDAP function in the Request column, click the hyperlink. To save the contents of the report,

choose Save As from the File menu of your browser window.

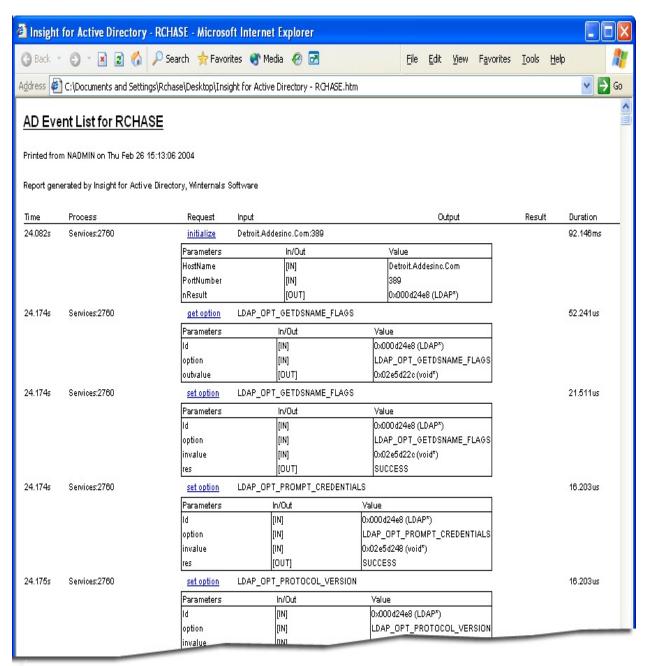
✓ Note

Columns that appear in the report correspond to the columns visible in the Event Pane. To add or remove columns, choose **Select Columns** from the **Options** menu or from the context menu that appears when you right-click on an item.

Viewing Events with Details

To view a report of all items in the Event Pane with corresponding Details Panes, choose **Events with Details** from the **HTML Reports** submenu of the **View** menu.

This action opens an HTML-formatted report in your Web browser window.



To view detailed information about an LDAP function in the Request

column, click the hyperlink. To save the contents of the report, choose **Save As** from the **File** menu of your browser window.

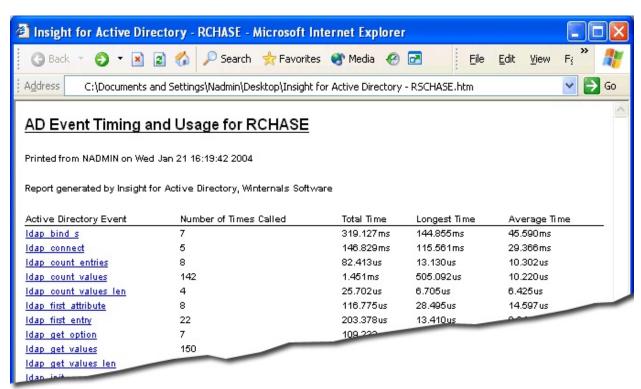
✓ Note

Columns that appear in the report correspond to the columns visible in the Event Pane. To add or remove columns, choose **Select Columns** from the **Options** menu or from the context menu that appears when you right-click on an item.

Viewing Events with Time Results

To view a histogram report of LDAP calls in the Event Pane with Total Time, Longest Time, and Average Time statistics, choose **Event Time Results** from the **HTML Reports** submenu of the **View** menu.

This action opens an HTML-formatted report in your Web browser window.



To view detailed information about an LDAP function, click the hyperlink. To save the contents of the report, choose **Save As** from the **File** menu of your browser window.

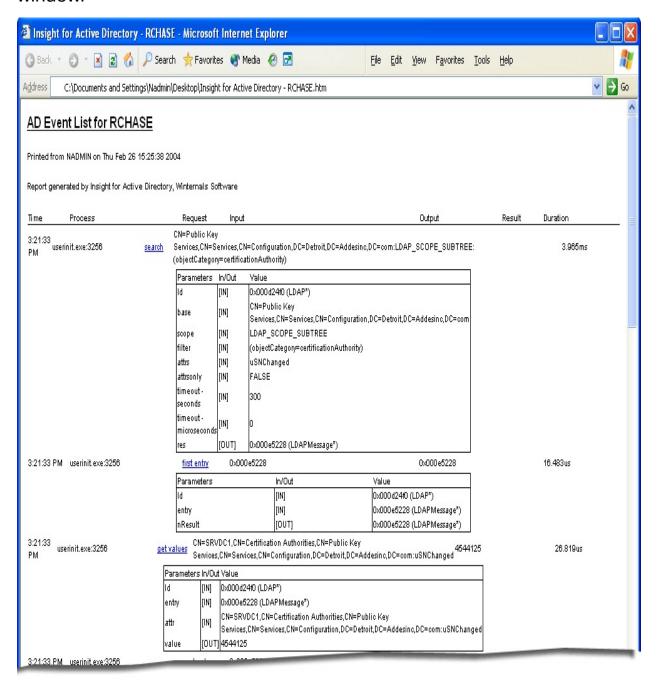
Note

To display uncalled functions, choose Preferences from the **Options** menu and clear **Suppress uncalled functions in reports**.

Viewing Highlighted Events

To view a report of highlighted entries in the Event Pane, choose **Highlighted Events** from the **HTML Reports** submenu of the **View** menu.

This action opens an HTML-formatted report in your Web browser window.



To view detailed information about an LDAP function in the Request column, click the hyperlink. To save the contents of the report, choose **Save As** from the **File** menu of your browser window.

✓ Note

Columns that appear in the report correspond to the columns visible in the Event Pane. To add or remove columns, choose **Select Columns** from the **Options** menu or from the context menu that appears when you right-click on an item.

Change Color Highlighting

You can set color highlighting properties of the display by choosing **Highlight Preferences** from the **Highlight** menu or from the context menu that appears when you right-click on an item in the Event Pane.

Display Only Selected Events

You can display or hide processes whose names contain specified text or add and exclude selected transactions by clicking the **Filter** toolbar button, choosing Event Filter on the **View** menu, or pressing **Ctrl+L**.

Log System Activity

You can use the command-line $_{\text{-log option}}$ to write activity to a log file without opening the console.

Save Events in the Display

You can save the contents of the Event Pane as a text file by choosing **Save** on the **File** menu or pressing **Ctrl+S**.

You can copy a selected item to the Clipboard by choosing **Copy** from the **Edit** menu or pressing **Ctrl+C**.

✓ Note

You can also save the contents of the Event Pane as HTML formatted reports.

View Different Columns in the Display

You can select the columns that appear in the display by choosing select columns from the **Options** menu or from the context menu that appears when you right-click on an item in the Event Pane.

Reporting Bugs

If you encounter a bug please send email to markruss@microsoft.com, including the behavior you observed, the behavior you expected, and steps for reproducing the problem.

Setting Program Preferences

To change the default capture mode when making a new connection, display a tray icon on computers running the monitoring service, change the TCP/IP port number or administrative share name, or display uncalled functions in Events with Time Results reports, choose **Preferences** from the **Options** menu.

This action opens the **Preferences** dialog box.