Your Question

Article: 00098
Question:
What are the Record object properties and the additional fields available for advanced treatment in Net Report?

Net Report Answer

The Article is made up of three sections:

- **Introduction:** gives the context in which Record Object Properties and Additional properties should be understood.
- **Section 1:** Record Object Properties.
- **Section 2:** Record Object Additional Fields.

Introduction

When a Net Report agent parses a log line, it generates a message using the Net Report Extensible Log Report Format (NELRF) that is sent to the Net Report Universal Log Analyser (ULA). A NELRF contains properties and fields.

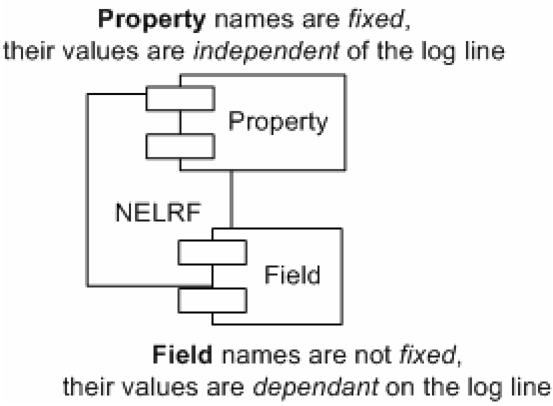
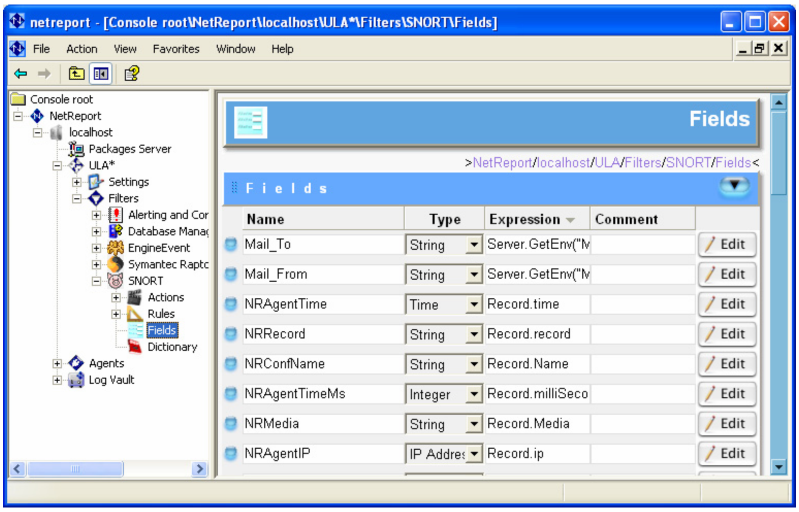

Property names are *fixed*,
their values are *independent* of the log line
Property
NELRF
Field
Field names are not *fixed*,
their values are *dependant* on the log line

Figure 1: NELRF Properties and Fields

Property names are fixed and their values do not dependent on the log line they are at the base of every NELRF. Field names are dependant on the log type and their values are dependant on the log lines.

For Flat File and Syslog agents, the field names are defined by the user via the regular expressions. For other agents, such as the WMI (Windows Management Instrumentation) agent the fields are defined by the means by which the log lines are obtained. However, depending on the agent, sometimes, the agent in question adds additional fields for advanced treatment. A typical example of such additional fields is the file name field.

To treat data contained in a NELRF, the user must access it via the Fields screen in the Net Report Management Console.



Name	Type	Expression	Comment	
Mail_To	String	Server.GetEnv("M		Edit
Mail_From	String	Server.GetEnv("M		Edit
NRAgentTime	Time	Record.time		Edit
NRRecord	String	Record.record		Edit
NRConfName	String	Record.Name		Edit
NRAgentTimeMs	Integer	Record.milliSeco		Edit
NRMedia	String	Record.Media		Edit
NRAgentIP	IP Addres	Record.ip		Edit

Figure 2: Net Report Management Console Fields Screen

Data contained in a NELRF can be accessed via the Record object. In general, the Record contains Properties and Fields.

As any other VBS object property, the properties are invoked using the syntax: Record.propertyname. The user can access the NELRF property values via Record Properties. The Record Object has certain additional properties that are not defined in the NELRF, such as the xml property (.xml). The values of the fields contained in the NELRF which can be accessed by using the following syntax: Record("fieldname").

This article discusses the Record object properties as well as the additional fields that may be added via the agents for advanced treatment.

Section 1: Record Object Properties

Properties can be invoked by using the "." Syntax. The user can access these properties by using the following Expressions:

Expression	Description
Record.name	Name of the agent configuration that has parsed the log line. Which appears in a NELRF as _name*.
Record.type	Name of the destination filter. Which appears in a NELRF as _type*.
Record.time	Date when the agent received the log in Universal Time Coordinate (UTC) Time. Which appears in a NELRF as _time*.
Record.milliseconds	Milliseconds of the Date when the agent received the log extracted from the _time property of the NELRF.
Record.ip	First IP address of the Net Report Agent computer. Which appears in a NELRF as _ip*.
Record.media	Type of media or log format (for example Syslog, Flat File). Which appears in a nelrf as _media*.
Record.record	either - **The Original log line (Flat File).** Which appears in a NELRF as _record*. - **The Syslog message (Syslog)** and log information using the following format: **<date> <sender ip> <original syslog message>**

	- A simplified NELRF (WMI, LEA, Radius, etc): a simplified NERLF only includes the IP and Time properties.
Record.xml	Returns the whole NELRF message.

*The NELRF syntax adds an underscore "_" in front of each property.

Section 2: Record Additional Object Fields

Fields are added by the agent to provide advanced treatment. These fields can be invoked by using the Record("fieldname"), for example, Record("filename") returns the name of the log file (Flat File) or IP of the syslog sender (Syslog). These fields are not defined for all agents. Please note that fields are case sensitive.

Expression	Description
Record("filename")	Name of the log file (Flat File) or IP of the syslog sender (Syslog).
Record("_srctimezone")	Timezone used. Which appears in a NELRF as __srctimezone.
Record("_srccountry")	Country source used by the time field. Which appears in a NELRF as __srccountry.
Record("_srcadjustdaylight")	For Daylight Saving Time (DST) adjustments. Which appears in a NELRF as __srcadjustdaylight.