Novell® Sentinel™

6.0

October 5, 2007

www.novell.com

Syslog Connector Differences in Sentinel 6

Product Version(s): Requires Sentinel 6.0 or higher

Novell®

Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to any and all parts of Novell software, to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. Please refer to http://www.novell.com/info/exports/ for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at http://www.novell.com/company/legal/patents/ and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
http://www.novell.com

Online Documentation: To access the online documentation for this and other Novell products and to get updates, see http://www.novell.com/documentation.

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Third Party Legal Notices

This product may include the following open source programs that are available under the LGPL license. The text for this license can be found in the Licenses directory.

- edtFTPj-1.2.3 is licensed under the Lesser GNU Public License. For more information, disclaimers and restrictions see http://www.enterprisedt.com/products/edtftpj/purchase.html.
- Esper. Copyright © 2005-2006, Codehaus.
- jTDS-1.2.jar is licensed under the Lesser GNU Public License. For more information, disclaimers and restrictions see http://jtds.sourceforge.net/.
- MDateSelector. Copyright © 2005, Martin Newstead, licensed under the Lesser General Public License. For more information, disclaimers and restrictions see http://web.ukonline.co.uk/mseries.
- Enhydra Shark, licensed under the Lesser General Public License available at: http://shark.objectweb.org/license.html.
- Tagish Java Authentication and Authorization Service Modules, licensed under the Lesser General Public License. For more information, disclaimers and restrictions see http://free.tagish.net/jaas/index.jsp.

This product may include software developed by The Apache Software Foundation (http://www.apache.org/) and licensed under the Apache License, Version 2.0 (the "License"); the text for this license can be found in the Licenses directory or at http://www.apache.org/licenses/LICENSE-2.0. Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

The applicable open source programs are listed below.

- Apache Axis and Apache Tomcat, Copyright © 1999 to 2005, Apache Software Foundation. For more information, disclaimers and restrictions, see http://www.apache.org/licenses/.
- Apache Lucene, Copyright © 1999 to 2005, Apache Software Foundation. For more information, disclaimers and restrictions, see http://www.apache.org/licenses/.
- Bean Scripting Framework (BSF), licensed by the Apache Software Foundation Copyright © 1999-2004. For more information, disclaimers and restrictions see http://xml.apache.org/dist/LICENSE.txt.
- Skin Look and Feel (SkinLF). Copyright © 2000-2006 L2FProd.com. Licensed under the Apache Software License. For more information, disclaimers and restrictions see https://skinlf.dev.java.net/.
- Xalan and Xerces, both of which are licensed by the Apache Software Foundation Copyright © 1999-2004. For more information, disclaimers and restrictions see http://xml.apache.org/dist/LICENSE.txt.

This product may include the following open source programs that are available under the Java license.

- JavaBeans Activation Framework (JAF). Copyright © Sun Microsystems, Inc. For more information, disclaimers and restrictions see http://www.java.sun.com/products/javabeans/glasgow/jaf.html and click download > license.
- Java 2 Platform, Standard Edition. Copyright © Sun Microsystems, Inc. For more information, disclaimers and restrictions see http://java.sun.com/j2se/1.5.0/docs/relnotes/SMICopyright.html.
- JavaMail. Copyright © Sun Microsystems, Inc. For more information, disclaimers and restrictions see http://www.java.sun.com/products/javamail/downloads/index.html and click download > license.

This product may also include the following open source programs.

- ANTLR. For more information, disclaimers and restrictions, see http://www.antlr.org.
- Boost. Copyright © 1999, Boost.org.
- Concurrent, utility package. Copyright © Doug Lea. Used without CopyOnWriteArrayList and ConcurrentReaderHashMap classes.
- Java Ace, by Douglas C. Schmidt and his research group at Washington University. Copyright © 1993-2005. For more information, disclaimers and restrictions see http://www.cs.wustl.edu/~schmidt/ACE-copying.html and http://www.cs.wustl.edu/~pjain/java/ace/JACE-copying.html.
- Java Service Wrapper. Portions copyrighted as follows: Copyright © 1999, 2004 Tanuki Software and Copyright © 2001 Silver Egg Technology. For more information, disclaimers and restrictions, see http://wrapper.tanukisoftware.org/doc/english/license.html.
- JLDAP. Copyright 1998-2005 The OpenLDAP Foundation. All rights reserved. Portions Copyright © 1999 - 2003 Novell, Inc. All Rights Reserved.
- OpenSSL, by the OpenSSL Project. Copyright © 1998-2004. For more information, disclaimers and restrictions, see http://www.openssl.org.
- Rhino. Usage is subject to Mozilla Public License 1.1. For more information, see http://www.mozilla.org/rhino/.
- Tao (with ACE wrappers) by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine and Vanderbilt University. Copyright © 1993-2005. For more information, disclaimers and restrictions see http://www.cs.wustl.edu/~schmidt/ACE-copying.html and http://www.cs.wustl.edu/~pjain/java/ace/JACE-copying.html.
- Tinyxml. For more information, disclaimers and restrictions see http://grinninglizard.com/tinyxmldocs/index.html.

NOTE: As of the publication of this documentation, the above links were active. In the event you find that any of the above links are broken or the linked web pages are inactive, please contact Novell, Inc., 404 Wyman Street, Suite 500, Waltham, MA 02451 U.S.A.

Preface

This manual gives you a general understanding of this Connector and the differences between this connection method in Sentinel 6 and previous versions of Sentinel. It is intended mainly for the system administrators to configure the Connector, to establish connection between Collectors and Event Source.

Additional Stopgap documentation available on Novell Web Portal are:

- Sentinel 6.0 Syslog Connector Guide
- Sentinel 6.0 Audit Connector Guide
- Sentinel 6.0 DB Connector Guide
- Sentinel 6.0 File Connector Guide
- Sentinel 6.0 WMI Connector Guide
- Using 5.x Collectors in Sentinel 6.0

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation and enter your comments there.

Additional Documentation

The other manuals on this product are available at http://www.novell.com/documentation.

For additional documentation to install and use Connectors and Collectors, see Sentinel User Guide.

Documentation Conventions

Notes and Cautions

NOTE: Notes provide additional information that may be useful.

WARNING:

Warning provides additional information that may keep you away from performing tasks that may cause damage or loss of data.

Commands

Commands appear in courier font. For example:

```
useradd –g dba –d /export/home/oracle –m –s /bin/csh
oracle
```

References

- For more information, see “Section Name” (if in the same Chapter).
- For more information, see Chapter number, “Chapter Name” (if in the same Guide).
- For more information, see Section Name in Chapter Name, *Guide Name* (if in a different Guide).

Other References

The following manuals are available with the Sentinel install CDs.

- Sentinel Install Guide
- Sentinel User Guide
- Sentinel Collector Builder User Guide
- Sentinel User Reference Guide
- Sentinel 3rd Party Integration Guide
- Release Notes

Contacting Novell

- Website: http://www.novell.com
- Novell Technical Support: http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup
- Self Support: http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog
- Patch Download Site: http://download.novell.com/index.jsp
- 24x7 support: http://www.novell.com/company/contact.html
- For Collectors/Connectors/Reports/Correlation/Hotfixes/TIDS: http://support.novell.com/products/sentinel

Contents

Introduction

Sentinel 6.0 provides a graphical Event Source Management framework which helps in deploying, managing, and troubleshooting Collectors within the Sentinel console. This framework replaces functionality previously in the Sentinel Collector Builder and provides new features.

The addition of Event Source Management has led to some differences in how the Collectors are stored, managed and deployed within Sentinel. For more information, see Event Source Management in *Sentinel User Guide*.

This document focuses on the Syslog Connector and the differences between using this connection method in Sentinel 6.0 and previous versions.

This guide assumes that you are familiar with:

- Importing Connectors into Sentinel 6.0
- Importing Collectors into Sentinel 6.0
- Configuring parameters in Sentinel 6.0
- General differences between Collector Management in Sentinel 6.0 and previous versions.

These documents can be found at http://support.novell.com/products/sentinel/collectors.html.

For more information, see "Using 5.x Collectors in Sentinel 6.0". For more information on using Sentinel 6.0, see Event Source Management in *Sentinel User Guide*.

Differences between Sentinel 5.x and Sentinel 6

The general functionality of the Syslog Connector is the same in Sentinel 6 and previous versions of Sentinel. There are two components to the Connector:

- Syslog Server/Proxy: This component listens on a TCP or UDP port for Syslog messages.
- Syslog Connector: This client component registers to the server for all messages (or for filtered messages).

NOTE: References to the Syslog Connector in the Sentinel 6 documentation are equivalent to the Syslog Connector Client or Syslog Client in Sentinel 5.x documentation.

For more information on 5.x Syslog Connector, see Sentinel Collector 5.x documentation that supports Syslog connection method.

Differences in Functionality

There are multiple differences in functionality between the Syslog Connector for Sentinel 5.x and Sentinel 6.

- Syslog in Sentinel 5.x listens on TCP and UDP ports at the same time for the Syslog messages from sources.
- Syslog in Sentinel 6 listens on only one port. This port can be TCP, UDP, or SSL.
- Syslog in Sentinel 6 adds support for SSL connections to the source device.

- Syslog in Sentinel 5.x listens over a dedicated port for connections from Syslog Clients. It was invoked using `-Connector <port number>` because the Syslog Server and the Client component could be running on different machines and thus on different JVM's.
- Syslog in Sentinel 6 does not use a socket to send messages between the Syslog Server and the Syslog Connector. Instead, messages are sent as callbacks. The Server and the Connector component run on the same machine using the same JVM.
- The Syslog Connector in Sentinel 5.x supports events from Novell applications that implement Novell's Audit API.
- The Syslog Connector in Sentinel 6 is exclusively for Syslog messages. To collect events from Novell audit applications that implement the Audit API, there is a Sentinel 6 Audit Connector. This Connector differences are described in Audit Connector Differences in Sentinel 6.0 documentation.

Syslog Server/Proxy Configuration

The Collector and Syslog Connector should be imported into Event Source Management using the procedures in the Event Source Management in *Sentinel User Guide*. During the import, there are several configuration options in Sentinel 6 that replace configuration options in Sentinel 5.x.

In Sentinel 5.x, configuration options for the Syslog Server could be stored in a file called syslog.conf, located in %ESEC_HOME%\wizard\syslog\config or $ESEC_HOME/wizard/syslog/config. This file is used when Syslog Server starts up if the Syslog Server is configured as a service. Alternatively, the same commands could be used if starting the Syslog Server from a command line.

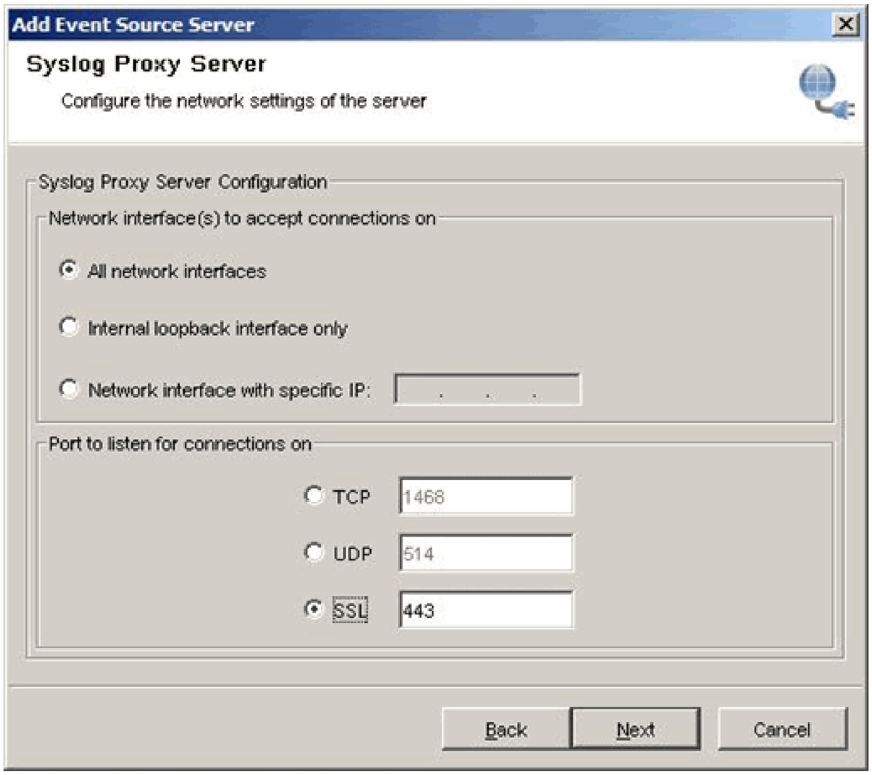
In Sentinel 6, options for the Syslog Server are configured in the Event Source Management interface as properties of the Event Source Server.

Ports

The ports on which the Syslog Connector listened were configured in the syslog.conf file using the following commands:

`-udp <port>`	Port for listening for UDP messages from devices (default 514)
`-tcp <port>`	Port for listening for TCP connections from devices (default 1468)

In Sentinel 6, this option is configured in Event Source Management (ESM) when adding a new Syslog Event Source Server, for reference see screenshot below:



Add Event Source Server

Syslog Proxy Server

Configure the network settings of the server

Syslog Proxy Server Configuration

Network interface(s) to accept connections on

- ● All network interfaces
- ○ Internal loopback interface only
- ○ Network interface with specific IP: [. . .]

Port to listen for connections on

- ○ TCP 1468
- ○ UDP 514
- ● SSL 443

Novell Audit Connection

In Sentinel 5.x, connections to Novell Audit are configured in the syslog.conf file using the –`audit` option:

`-audit <port>`	Port for listening for messages from Novell Audit (default 289)

In addition, Sentinel 5.x had the following options in the syslog.conf file for Novell Audit:

```
–auditQueueSize
-authentication
-Dsentinel.audit.password
-Dsentinel.audit.keystore
-Dsentinel.audit.configuration
```

In Sentinel 6, there is a special Connector designed for Novell Audit, so these parameters are all irrelevant for the Sentinel 6 Syslog Connector.

Socket Connections

Syslog 5.1.3 has the following –`connector` option

`-connector <port>`	Port for listening for TCP connections from Connectors (default 9091)

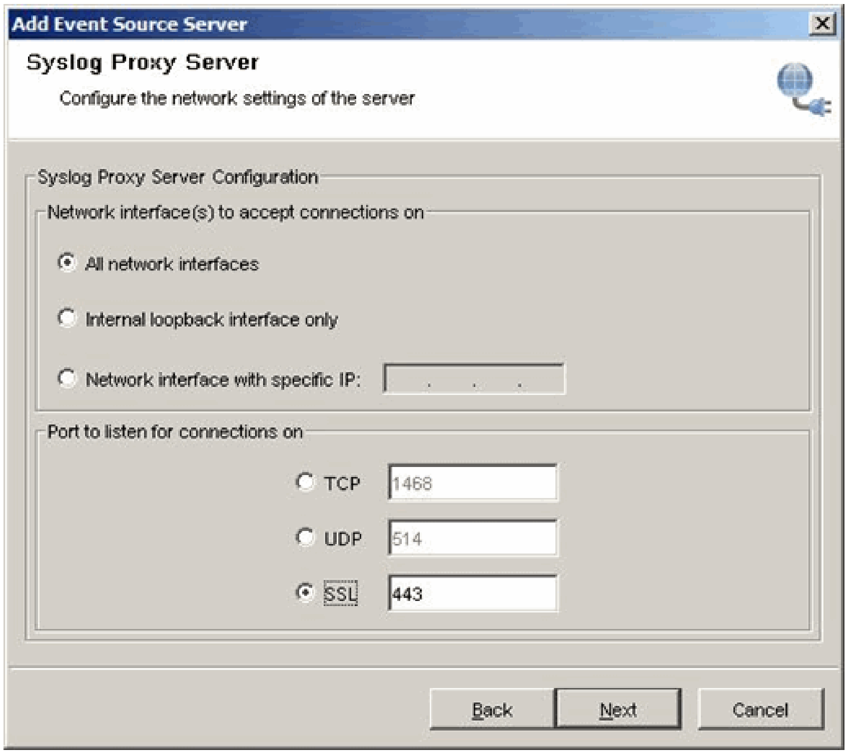
Since in Syslog 6.0 the Server and the Connector component runs on the same machine (same JVM), there was no need to use socket to send messages from Syslog Server to Connector.

Multiple Syslog Clients on One Machine

In Sentinel 5.x, Syslog could be bound to one specific IP address on a multiple IP machine. In this situation, the port values in the `-connector` parameter can be replaced by `IP address:port` value. For example, a machine with two IP addresses (*e.g.*, 192.168.0.10 and 192.168.0.11) could be set to bind the TCP port with IP 192.168.0.10 and the UDP port with IP 192.168.0.11. In the section of syslog.conf for the Connector port with the local loop back address, the file would be modified to read:

```
wrapper.app.parameter.3=-tcp
wrapper.app.parameter.4=192.168.0.10:1468
wrapper.app.parameter.5=-udp
wrapper.app.parameter.6=192.168.0.11:514
wrapper.app.parameter.7=-connector
wrapper.app.parameter.8=127.0.0.1:9091
```

However, in Sentinel 6, only one type of connection (TCP, UDP, or SSL) is possible per Collector Manager. The Syslog Proxy Server configuration screen provides the option to bind a port to all the IP addresses on the machine or to a particular IP address of that machine.



Add Event Source Server

Syslog Proxy Server

Configure the network settings of the server

Syslog Proxy Server Configuration

Network interface(s) to accept connections on

● All network interfaces

○ Internal loopback interface only

○ Network interface with specific IP: . . .

Port to listen for connections on

○ TCP 1468

○ UDP 514

● SSL 443

Message Buffer Size

In Sentinel 5.x, the message buffer size for Syslog is set using the option `-messageSize` in the `syslog.conf`.

`-messageSize`	Number of messages to be buffered. These messages will be sent again in the case of a temporarily lost connection.

	If the option value is not used or if the option value is less than 0, the value will default to 5000. This option was possible for all clients except Novell Audit.

In Sentinel 6, the message buffer size for the Syslog Connector is fixed at 10,000.

Syslog Server Logging

In Sentinel 5.x, the messages received by the Syslog Server can be logged into a file using the following option in the syslog.conf file:

`-log <file path to log file>`	Name of a log file to append to This option does not apply to Novell Audit.

The Syslog Server in Sentinel 6 does not include this option.

Syslog Client Configuration

As mentioned above, the Collector and Syslog Connector should be imported into Event Source Management using the procedures in the *Event Source Management* chapter of the *Sentinel User's Guide*. During the import, there are several configuration options in Sentinel 6 that replace configuration options in Sentinel 5.x.

In Sentinel 5.x, configuration options for the Syslog Client could set in the Rx/Tx Value during the port configuration for the Syslog-based Collector. For simplicity, they could also be added to a command line in a batch file; the batch file would then be used as the Rx/Tx Value in the port configuration. (This is the recommended method because some commands require double quotations.)

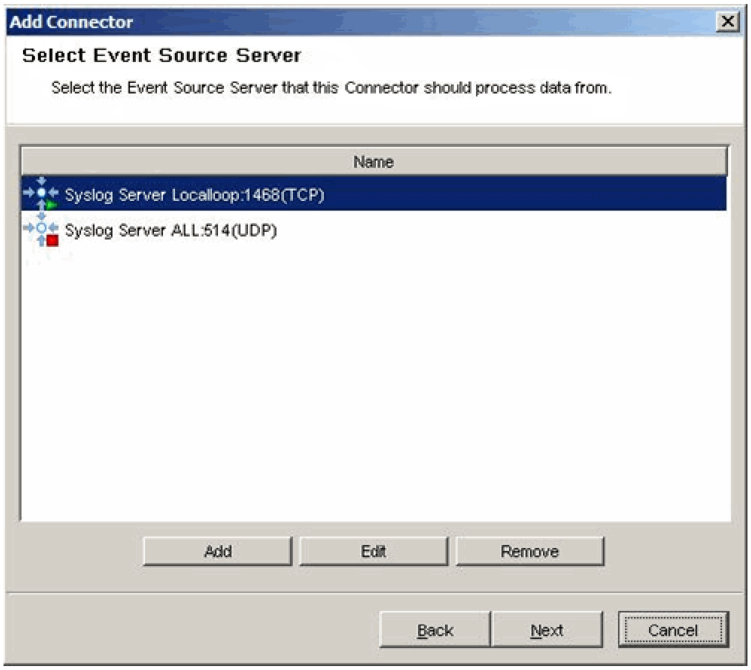
In Sentinel 6, options for the Syslog Client are configured in the Event Source Management interface as properties of the Connector and the Event Source.

Syslog Proxy Server Connection

In the Sentinel 5.x, the Syslog Connector option –`proxy` is used to specify the Syslog Server that this Connector needs to connect to.

`-proxy <host:port number>`	The Syslog Proxy to connect to, in the format host:port (default is 127.0.0.1:9091)

In Sentinel 6, the proxy server connection is configured on the *Select Event Source Server* screen in the Syslog Connector configuration wizard.



Add Connector

Select Event Source Server

Select the Event Source Server that this Connector should process data from.

Name

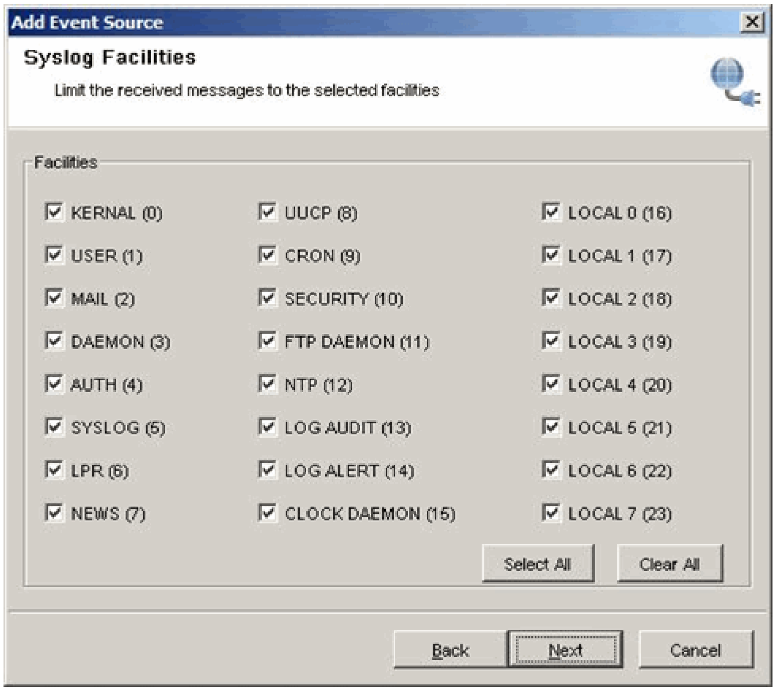
- Syslog Server Localloop:1468(TCP)
- Syslog Server ALL:514(UDP)

Filtering by Syslog Facilities

In Sentinel 5.x, the `–facilities` option is used to specify the types of facilities this Connector is interested in.

`-facilities <facility1,facility2,…>`	Comma separated list of desired facilities (default is all facilities) Not applicable to Novell Audit.

In Sentinel 6, facilities are configured on the *Syslog Facilities* screen in the Syslog Event Source configuration wizard.



Add Event Source

Syslog Facilities

Limit the received messages to the selected facilities

Facilities

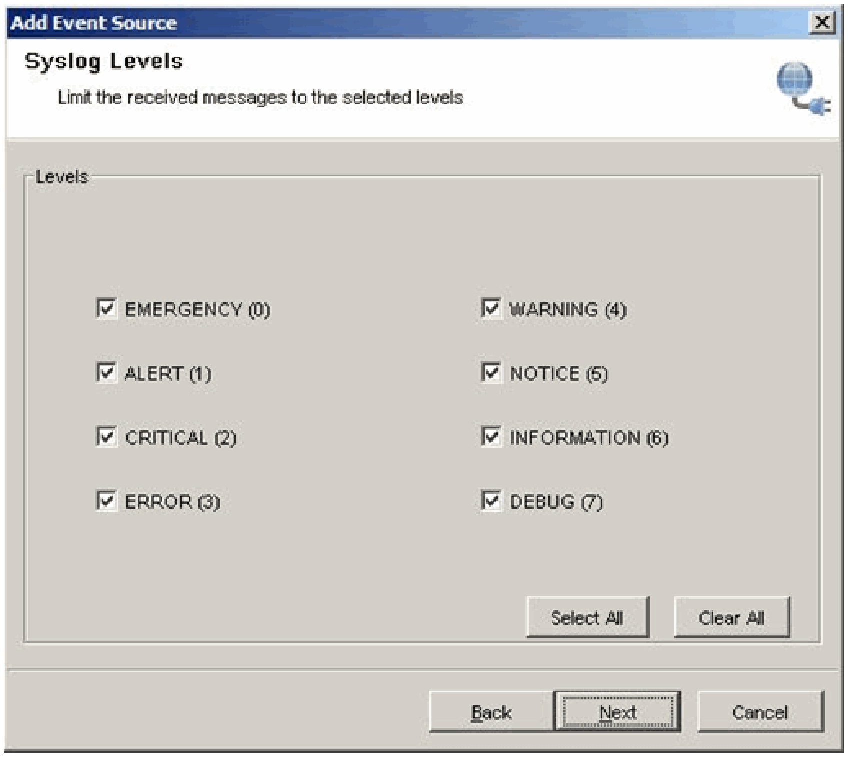
☑ KERNAL (0)
☑ USER (1)
☑ MAIL (2)
☑ DAEMON (3)
☑ AUTH (4)
☑ SYSLOG (5)
☑ LPR (6)
☑ NEWS (7)
☑ UUCP (8)
☑ CRON (9)
☑ SECURITY (10)
☑ FTP DAEMON (11)
☑ NTP (12)
☑ LOG AUDIT (13)
☑ LOG ALERT (14)
☑ CLOCK DAEMON (15)
☑ LOCAL 0 (16)
☑ LOCAL 1 (17)
☑ LOCAL 2 (18)
☑ LOCAL 3 (19)
☑ LOCAL 4 (20)
☑ LOCAL 5 (21)
☑ LOCAL 6 (22)
☑ LOCAL 7 (23)

Filtering by Syslog Levels

In Sentinel 5.x, the option `–levels` is used to specify the levels this Connector is interested in.

`-levels <level1, level2,…>`	Comma separated list of desired severities (default is all levels). Not applicable to Novell Audit.

In Sentinel 6, Syslog levels are configured on the *Syslog Levels* screen in the Syslog Event Source configuration wizard.



Add Event Source

Syslog Levels

Limit the received messages to the selected levels

Levels

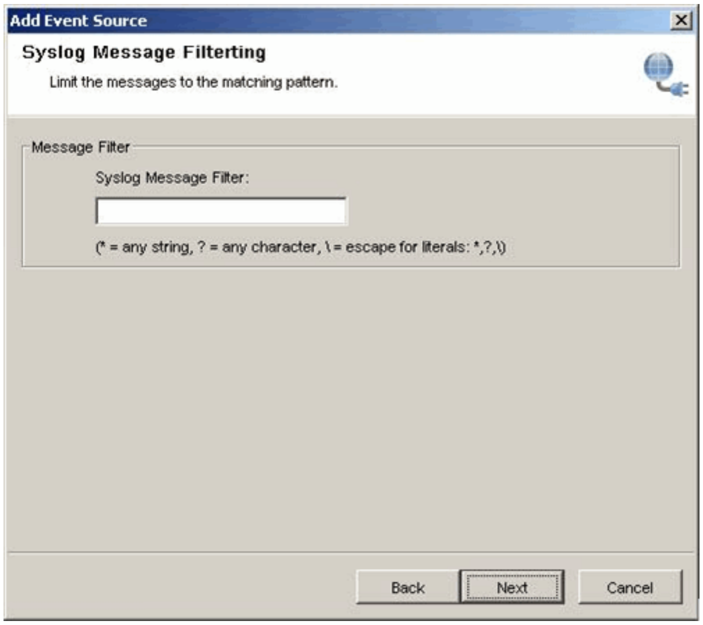
☑ EMERGENCY (0)
☑ ALERT (1)
☑ CRITICAL (2)
☑ ERROR (3)
☑ WARNING (4)
☑ NOTICE (5)
☑ INFORMATION (6)
☑ DEBUG (7)

Filtering by Message Content

In Sentinel 5.x, the option `–body` is used to specify that the Connector is interested in messages that include a specific regular expression.

`-body <regular expression>`	Regular Expression string found in the desired message bodies. Not applicable to Novell Audit.

In Sentinel 6, regular expressions are configured on the *Syslog Message Filtering* screen in the Event Source configuration wizard.



Add Event Source

Syslog Message Filterting

Limit the messages to the matching pattern.

Message Filter

Syslog Message Filter:

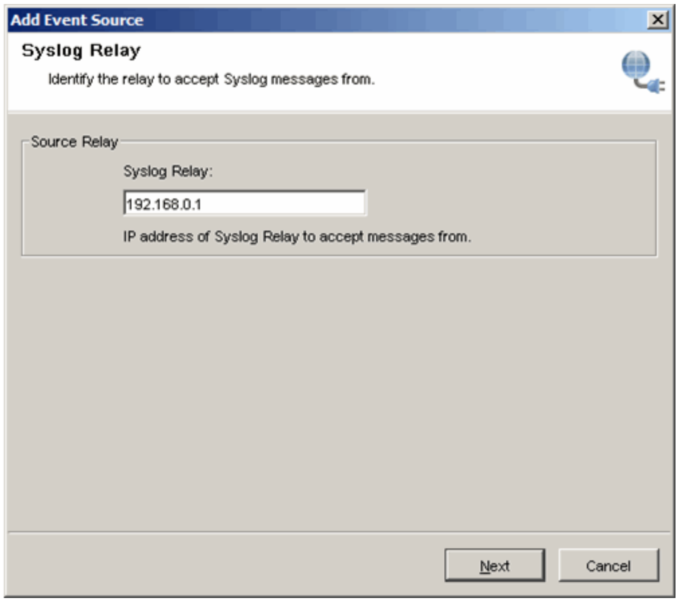
(* = any string, ? = any character, \ = escape for literals: *,?,\)

Filtering by Source IP

In Sentinel 5.x, the option `–sender` is used to specify that the Connector is interested in message originating at a particular IP address.

`-sender <Source IP1[/integer subnet mask], Source IP2[/integer subnet mask],…>`	Comma separated list of desired senders (default is all senders). Not applicable to Novell Audit.

In Sentinel 6, the IP addresses from which the Syslog Connector is interested in receiving messages are configured on the *Syslog Relay* screen in the Event Source configuration wizard.



Add Event Source

Syslog Relay

Identify the relay to accept Syslog messages from.

Source Relay

Syslog Relay: 192.168.0.1

IP address of Syslog Relay to accept messages from.

Syslog Client Message Logging

In Sentinel 5.x, the messages received by the Syslog Connector Client can be logged into a file using the following option:

`-log <file path to log file>`	Name of a log file to append to

In Sentinel 6, the Syslog Connector Client does not include an equivalent option.

Miscellaneous Options

In Sentinel 5.x, the options `–shared` and `–private` were used to indicate whether the Server should accept Syslog Client connections from a remote machine.

`-private`	Accepts Connector connections only from the local machine (default option)
`-shared`	Accepts Connector connections from local and remote machines.

In Sentinel 6, the Syslog Server and Syslog Client run on the same machine (using the same JVM), so this option is not needed.

In addition to the changes described above, several options from the Sentinel 5.x Syslog Connector do not have an equivalent in Sentinel 6. These 5.x options are described below:

`-host < IP1[/integer subnet mask]|Hostname1 | Hostname Regex1, IP2[/integer subnet mask`	Comma separated list of desired hosts (default is all hosts). Not applicable to Novell Audit.
`-retry`	Time in milliseconds the client waits before attempting to reconnect to the proxy. No longer relevant in Sentinel 6 because the Syslog Server/Proxy and Syslog Connector are always on the same machine.

APPENDIX

A Revision History

Revision 01

Initial Document

June 2007