Novell®

Connector™

Rev: 01

www.novell.com

June 29, 2007

Audit 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 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.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such 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 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 other countries.

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

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see 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

Sentinel 6 may contain the following third-party technologies:

- 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/
- ANTLR. For more information, disclaimers and restrictions, see http://www.antlr.org
- Boost, Copyright © 1999, http://Boost.org
- BSF, licensed by the Apache Software Foundation Copyright © 1999-2004. For more information, disclaimers and restrictions see http://xml.apache.org/dist/LICENSE.txt.
- Bouncy Castle, Copyright © 2000-2004, the Legion of Bouncy Castle. For more information, disclaimers and restrictions see http://www.bouncycastle.org
- Checkpoint. Copyright © Check Point Software Technologies Ltd.
- Concurrent, utility package. Copyright © Doug Lea. Used without CopyOnWriteArrayList and ConcurrentReaderHashMap classes.
- Crypto++ Compilation. Copyright © 1995-2003, Wei Dai, incorporating the following copyrighted work: mars.cpp by Brian Gladman and Sean Woods. For more information, disclaimers and restrictions see http://www.eskimo.com/
- Crystal Reports Developer and Crystal Reports Server. Copyright © 2004 Business Objects Software Limited
- DataDirect Technologies Corp. Copyright © 1991-2003
- edpFTPj, licensed under the Lesser GNU Public License. For more information, disclaimers and restrictions see http://www.enterprisedt.com/products/edtftpj/purchase.html
- Enhydra Shark, licensed under the Lesser General Public License available at: http://shark.objectweb.org/license.html
- Esper. Copyright 2005-2006, Codehaus.
- ICEsoft ICEbrowser. ICEsoft Technologies, Inc. Copyright © 2003-2004
- ILOG, Inc. Copyright © 1999-2004
- Installshield Universal. Copyright © 1996–2005, Macrovision Corporation and/or Macrovision Europe Ltd
- Java 2 Platform, Standard Edition. Copyright © Sun Microsystems, Inc. For more information, disclaimers and restrictions see http://java.sun.com/j2se/1.4.2/j2re-1_4_2_10-license.txt

  The Java 2 Platform may also contain the following third-party products:

  - CoolServlets © 1999
  - DES and 3xDES © 2000 by Jef Poskanzer
  - Crimson © 1999-2000 The Apache Software Foundation
  - Xalan J2 © 1999-2000 The Apache Software Foundation
  - NSIS 1.0j © 1999-2000 Nullsoft, Inc

- Eastman Kodak Company © 1992
- Lucinda, a registered trademark or trademark of Bigelow and Holmes
- Taligent, Inc
- IBM, some portions available at: http://oss.software.ibm.com/icu4j/

For more information regarding these third-party technologies and their associated disclaimers and restrictions, see: http://java.sun.com/j2se/1.4.2/j2se-1_4_2-thirdpartylicensereadme.txt

- 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
- JavaMail. Copyright © Sun Microsystems, Inc. For more information, disclaimers and restrictions see http://www.java.sun.com/products/javamail/downloads/index.html
- Java Ace, by Douglas C. Schmidt and his research group at Washington University and 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
- 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
- Java Network Launching Protocol (JNLP). Copyright © Sun Microsystems, Inc. For more information, disclaimers and restrictions, please see http://www.java.sun.com/products/javawebstart/download-jnlp.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
- JIDE. Copyright © 2002 to 2005, JIDE Software, Inc.
- JLDAP. Copyright 1998-2005 The OpenLDAP Foundation. All rights reserved. Portions Copyright (C) 1999 - 2003 Novell, Inc. All Rights Reserved.
- jTDS 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
- Monarch Charts. Copyright © 2005, Singleton Labs
- Net-SNMP. Portions of the code are copyrighted by various entities, which reserve all rights. Copyright © 1989, 1991, 1992 by Carnegie Mellon University; Copyright © 1996, 1998 to 2000, the Regents of the University of California; Copyright © 2001 to 2003 Networks Associates Technology, Inc.; Copyright © 2001 to 2003, Cambridge Broadband, Ltd.; Copyright © 2003 Sun Microsystems, Inc. and Copyright © 2003 to 2004, Sparta, Inc. For more information, disclaimers and restrictions, see http://net-SNMP.sourceforge.net
- The OpenSSL Project. Copyright © 1998-2004. The Open SSL Project. For more information, disclaimers and restrictions, see http://www.openssl.org
- Oracle Help for Java. Copyright © 1994-2006, Oracle Corporation
- RoboHELP Office. Copyright © Adobe Systems Incorporated, formerly Macromedia.
- SecurityNexus. Copyright © 2003 to 2006. SecurityNexus, LLC. All rights reserved.
- 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/
- Sonic Software Corporation. Copyright © 2003-2004. The SSC software contains security software licensed from RSA Security, Inc
- Tinyxml. For more information, disclaimers and restrictions see http://grinninglizard.com/tinyxmldocs/index.html
- SecurityNexus. Copyright © 2003 to 2006. SecurityNexus, LLC. All rights reserved.
- 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

- yWorks. Copyright © 2003 to 2006, yWorks.

NOTE: As of publication of this documentation, the above links were active. In case you find any of these links broken/inactive, please contact: Novell, Inc., 404 Wyman Street, Suite 500, Waltham, MA 02451 U.S.A.

Contents

About this Guide

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 Collector and Event Source.

Additional Documentation

The other manuals on this product are available at the following URLs:

- http://www.novell.com/documentation/sentinel5
- http://www.novell.com/documentation/sentinel6
- http://support.novell.com/products/sentinel/collectors.html

The additional documentation includes:

- Sentinel User's Guide for Sentinel 6
- Syslog Connector Guide for Sentinel 5
- Audit Collector Guide for Sentinel 5
- Audit Connector Guide for Sentinel 6
- Audit Collector Guide for Sentinel 6
- Documentation for individual Collectors

Documentation Conventions

The following are the conventions used in this manual:

- `ls, --help`: commands, options
- Go to *Start* > *Program Files* > *Control Panel* to perform this action: Multiple actions in a step
- Any references to Sentinel 5.x also apply to Sentinel 4.x. Sentinel 5.x is used for simplicity.
- For more information, refer to *Chapter Name* in *Guide Name*: This is a reference to a chapter/section in another book.

NOTE: Any important notes for the user are mentioned as a Note.

Caution: A Caution indicates information that the user should read to avoid a potentially undesirable result.

Introduction

Sentinel 6 includes an all-new Event Source Management framework for deploying, managing, and troubleshooting event collectors from within the Sentinel console. This framework allows for management of all event collection components from within an intuitive, graphical interface. This GUI replaces functionality previously in the Sentinel Collector Builder and provides a number of new features not available in previous versions of Sentinel.

Collectors and connectors are now created as plug-ins to Sentinel (previously, connector functionality was built into Collector Builder). Collectors and connectors are stored within a central repository in the Sentinel system and are configured and deployed through a simple, wizard based interface. Other ESM features include a collector debugger, the ability to open filters on a single data source with a single mouse click, and integrated right-click actions for analysis and management tasks such as viewing the raw data or creating a Sentinel Active View.

The addition of Event Source Management has led to some differences in how collectors are stored, managed, and deployed within Sentinel. The objective of this document is to instruct users of Sentinel 6 on how to use collectors written for Sentinel 5.x with the Audit connection method with the Sentinel 6 software (including the Event Source Management framework.) This document assumes familiarity with the following topics:

- Importing connectors into Sentinel 6
- Importing collectors into Sentinel 6
- Configuring parameters in Sentinel 6
- General differences between collector management in Sentinel 6 and previous versions (For more information, refer to *Using 5.x Collectors with Sentinel 6..)*

This document focuses on the Audit Connector and the differences between using this connection method in Sentinel 6 and using the Audit Connector with Novell Audit in Sentinel 5.x. In addition to the topics above, this document assumes familiarity with the following topics:

- Sentinel 5.x Audit Collector documentation
- Sentinel 6 Audit Connector documentation
- Installing and configuring the Novell applications that communicate with Novell Audit

NOTE: In this document Audit 5.x connector and Audit 5.x connector are used interchangeably because Audit connections were made through the Audit connector.

Device Configuration

There are many different source devices that may connect to the Audit. The configuration of those devices for collecting data using Sentinel should not be different for 5.x and 6.x.

Collector/Connector Functionality

In Sentinel 5.x, connections to Novell Audit API-instrumented applications were made using the Audit Connector. In Sentinel 6, there is an Audit Connector designed specifically for this purpose.

The general functionality of the Audit connector is the same in Sentinel 6 as in Sentinel 5.x. There are two components to the connector:

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

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

Differences in Functionality

There are several differences in functionality between the Audit Connector for Sentinel 5.x and Sentinel 6.

- In Sentinel 5.x, Audit listens over a dedicated port for connections from Audit Clients. It was invoked using -connector <port number> because the Audit Server and Audit component could be running on different machines and thus on different JVM's.
- In Sentinel 6, Audit does not use a socket to send messages between the Audit Server and the Audit Connector. Instead, messages are sent as callbacks. The Server and the Connector component run on the same machine using the same JVM.
- In Sentinel 5.x, filtering for events coming from the platform agent using the Audit connector can be configured manually by creating event configuration files (in XML format) in a dedicated folder before starting the Audit Server.
- In Sentinel 6, the Audit Connector can retrieve event filtering information from eDirectory.

NOTE: This option is only available if the Secure Logging Server (SLS) has already been installed and configured for Novell Audit and if that information has been stored in eDirectory. If this is not true, the Audit Connector will retrieve all events without filtering.

Audit Server/Proxy Configuration

The collector and Audit 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 Audit 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 Audit Server starts up if the Audit Server is configured as a service. Alternatively, the same commands could be used if starting the Audit Server from a command line.

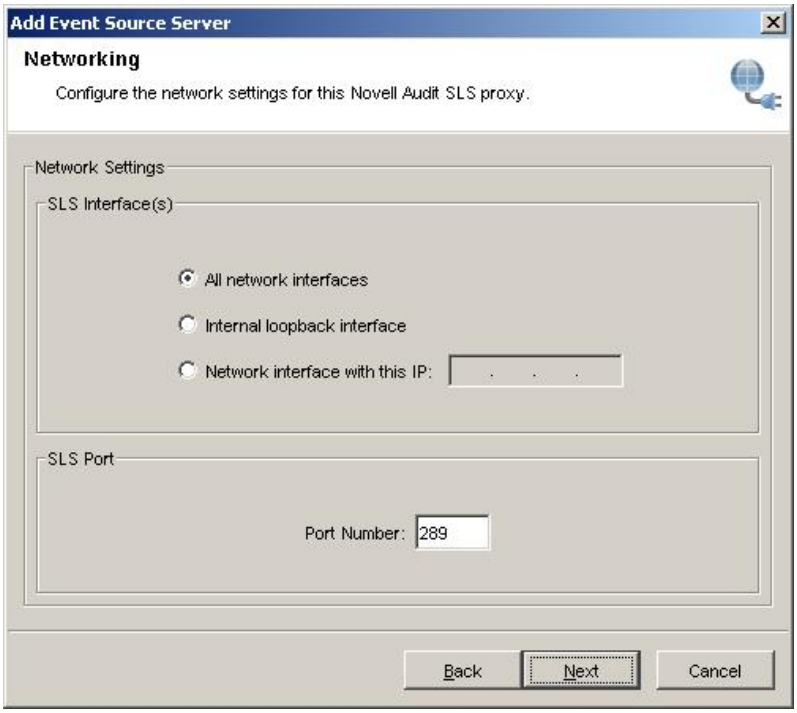
In Sentinel 6, options for the Audit Server are configured in the Event Source Management interface as properties of the Event Source Server.

Novell Audit Connection

In Sentinel 5.x, connections to Novell Audit were configured in the Syslog.conf file, located in %ESEC_HOME%\wizard\Audit\config or $ESEC_HOME/wizard/Audit/config. This was done using the –`audit` option:

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

In Sentinel 6, the new Audit Event Source Server configuration wizard has the following screen, which gives the option to configure the port on which the Server will be listening.



Socket Connections

In Sentinel 5.x, Audit has the following –`connector` option

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

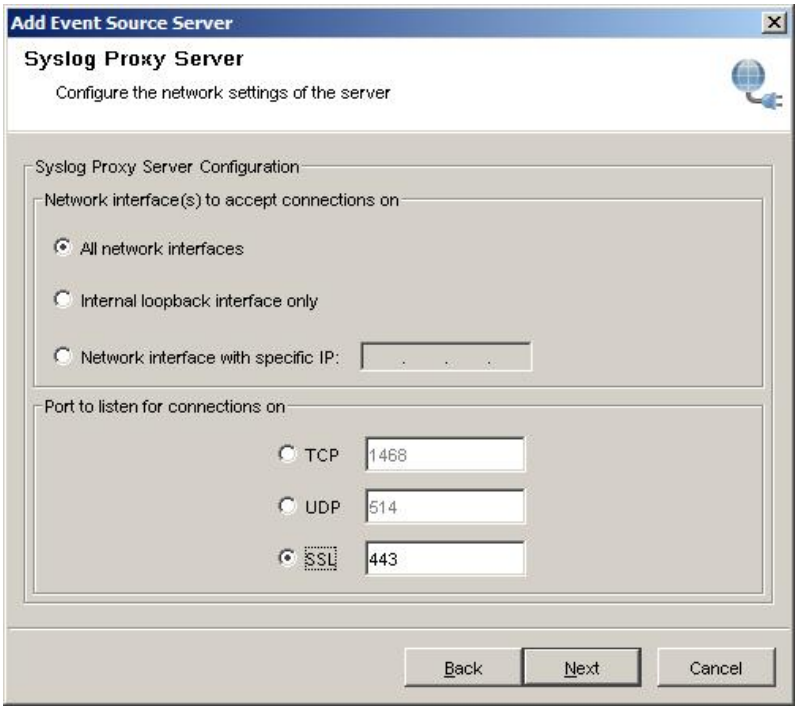
Since in Audit 6.0 the Server and the connector component runs on the same machine (same JVM), there was no need to use socket to send messages from Audit Server to Connector.

Multiple Audit Clients on One Machine

In Sentinel 5.x, the Audit Connector 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 (for example, 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=-audit
wrapper.app.parameter.4=192.168.0.10:1468
wrapper.app.parameter.5=-connector
wrapper.app.parameter.6=127.0.0.1:9091
```

In Sentinel 6, the Audit 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



Message Buffer Size

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

`-auditQueueSize`	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 10,000.

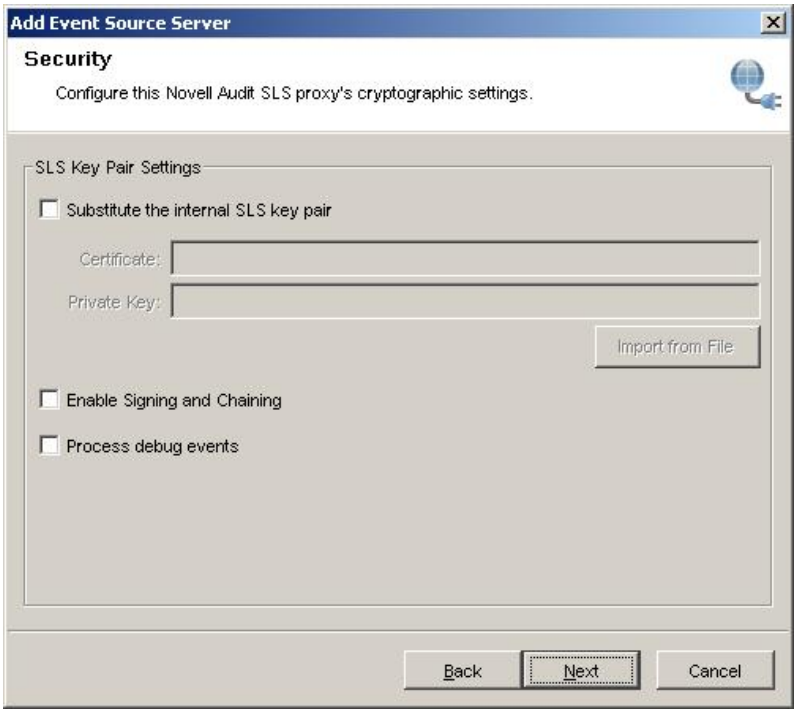
In Sentinel 6, the message buffer size for the Audit Connector is fixed at 10,000.

Certificates

In Sentinel 5.x, the configuration options `-Dsentinel.audit.keystore` and `-Dsentinel.audit.password` are used to configure which keystore and password the Audit Server should use when talking to the Platform Agents.

`-Dsentinel.audit.password`	This property provides the key for the certificate.
`-Dsentinel.audit.keystore`	This property points out to the location of the keystore containing the Audit proxy server certificate

In Sentinel 6.0, the following *Event Source Server* configuration screen allows the user to configure the keystore that the Audit Connector uses when establishing connection with the Platform Agents.



Miscellaneous Options

In Sentinel 5.x, the options `–shared` and `–private` were used to indicate whether the Server should accept Audit 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 Audit Server and the Audit Client run on the same machine (using the same JVM), so this option is not needed.

Audit Client Configuration

As mentioned above, the Collector and Audit 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 Audit Client could set in the Rx/Tx Value during the port configuration for the Audit-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.)

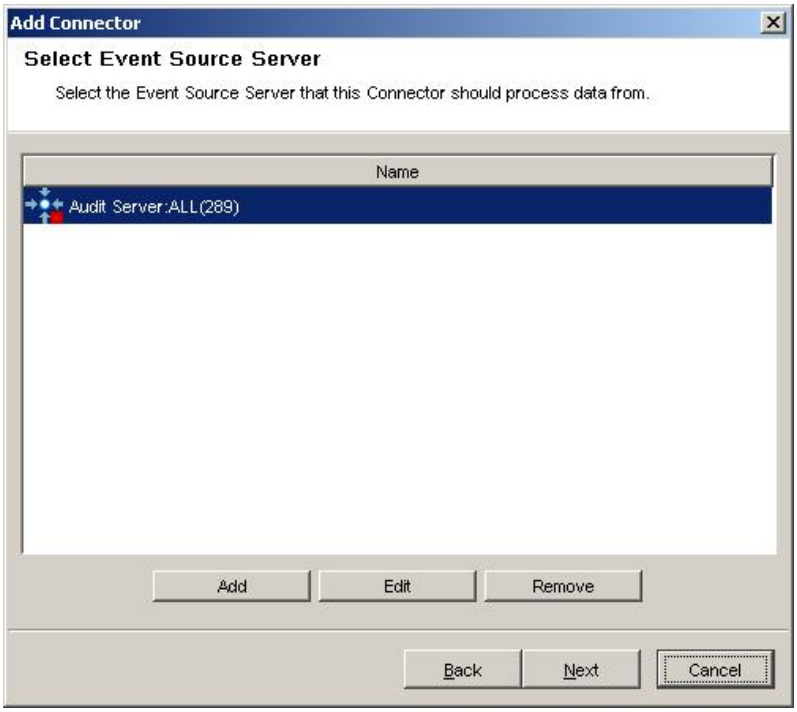
In Sentinel 6, options for the Audit Client are configured in the Event Source Management interface as properties of the Connector and the Event Source.

Audit Proxy Server Connection

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

-proxy <host:port number>	The Audit 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 Audit Connector configuration wizard.



Miscellaneous Options

In Sentinel 5.x, the `–audit` option is used to indicate that the Audit Client should only receive Audit messages, not syslog messages.

`-audit`	Configures the client to accept the binary audit events and parses them to NVP pair. This option is valid only when listening for audit messages from proxy.

In Sentinel 6, the Audit Connector is only used for Audit messages, so there is no equivalent configuration setting.

In Sentinel 5.x, the `-retry` option was used to configure reconnect parameters for the Audit Connector.

`-retry`	Time in milliseconds the client waits before attempting to reconnect to the proxy.

In Sentinel 6, the Audit Server/Proxy and the Audit Connector are always on the same machine, so there is no equivalent configuration setting.

Revision History

Revision 01

Initial Document

June 2007