Novell® Sentinel™

6.0

October 5, 2007

www.novell.com

Audit Connector Differences in Sentinel 6

Product Version(s): Requires Sentinel 6.0 or higher

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.

Copyright © 1999-2007 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

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 1

Device Configuration 1
Collector/Connector Functionality 1

Differences in Functionality 2

Audit Messages 2
Filtering Events 2
Audit Server/Proxy Configuration 2
Novell Audit Connection 2
Socket Connections 3
Multiple Audit Clients on One Machine 3
Message Buffer Size 4
Certificates 4
Miscellaneous Options 5
Audit Client Configuration 5
Audit Proxy Server Connection 6
Miscellaneous Options 6

A Revision History A-1

Revision 01 A-1

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.*

The focus of this document is to describe usage of Sentinel 5.x Novell Audit Collectors that support Audit connection method in Sentinel 6.0 framework. 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. For more information, see "Using 5.x Collectors with Sentinel 6.0."

In addition to the topics above, this guide assumes that you are familiar with:

- Sentinel 5.x Audit Collector documentation
- Sentinel 6.0 Audit Connector documentation
- Installing and configuring the Novell applications that communicate with Novell Audit

Device Configuration

There are many different source devices that may connect to the Audit Connector. The configuration of these devices for collecting data using Sentinel is similar in both 5.x and 6.x.

Collector/Connector Functionality

In Sentinel 5.x, Novell Audit API-instrumented applications were connected using the Audit Connector. In Sentinel 6.0, there is an Audit Connector designed specifically for this purpose.

The general functionality of the Audit Connector is similar in both 5.x and 6.x. There are two components of 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 6.0 documentation are equivalent to the Audit Connector Client or Audit Client in Sentinel 5.x documentation.

Differences in Functionality

The several differences in functionality between the Audit Connector for Sentinel 5.x and Sentinel 6.0 are explained below.

Audit Messages

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 may be running on different machines and thus on different JVM's.

In Sentinel 6.0, 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.

Filtering Events

In Sentinel 5.x, filtering for events received 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 6.0, 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 must be imported into Event Source Management. For more information on the procedures, see Event Source Management in *SentinelUser Guide*. During the import, there are several configuration options in Sentinel 6.0 that replaces configuration options in Sentinel 5.x.

In Sentinel 5.x, configuration options for the Audit Server can be stored in a syslog.conf file, located in %ESEC_HOME%\wizard\syslog\config or $ESEC_HOME/wizard/syslog/config. If the Audit Server is configured as a service on your system, syslog.conf will be used when Audit Server starts. Alternatively, you can use the same commands when you start the Audit Server from a command line.

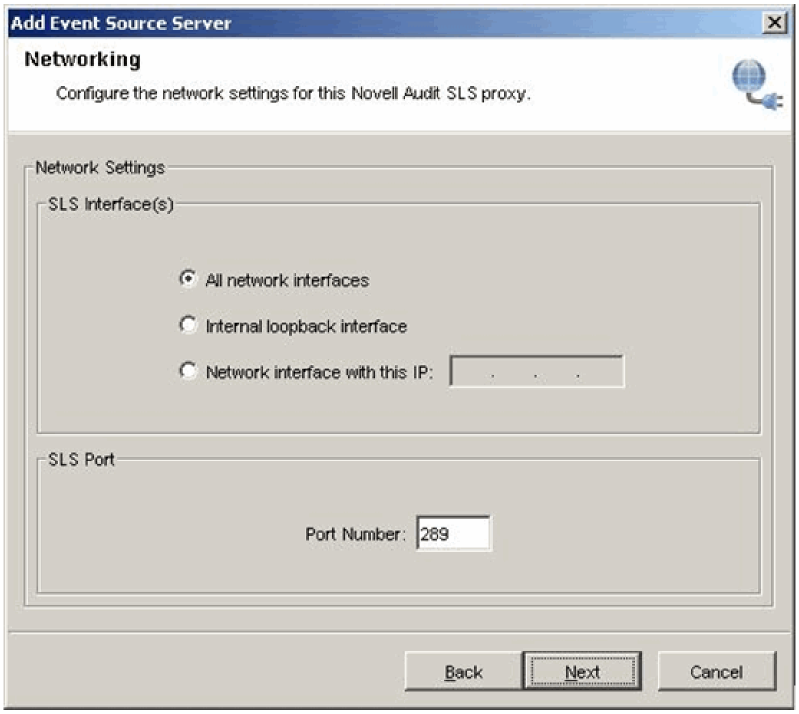
In Sentinel 6.0, options for the Audit Server are configured in the Event Source Management interface as properties of the Event Source Server.

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 provides the option to configure the port on which the Server will be listening.



Add Event Source Server

Networking

Configure the network settings for this Novell Audit SLS proxy.

Network Settings

SLS Interface(s)

● All network interfaces

○ Internal loopback interface

○ Network interface with this IP: . . .

SLS Port

Port Number: 289

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

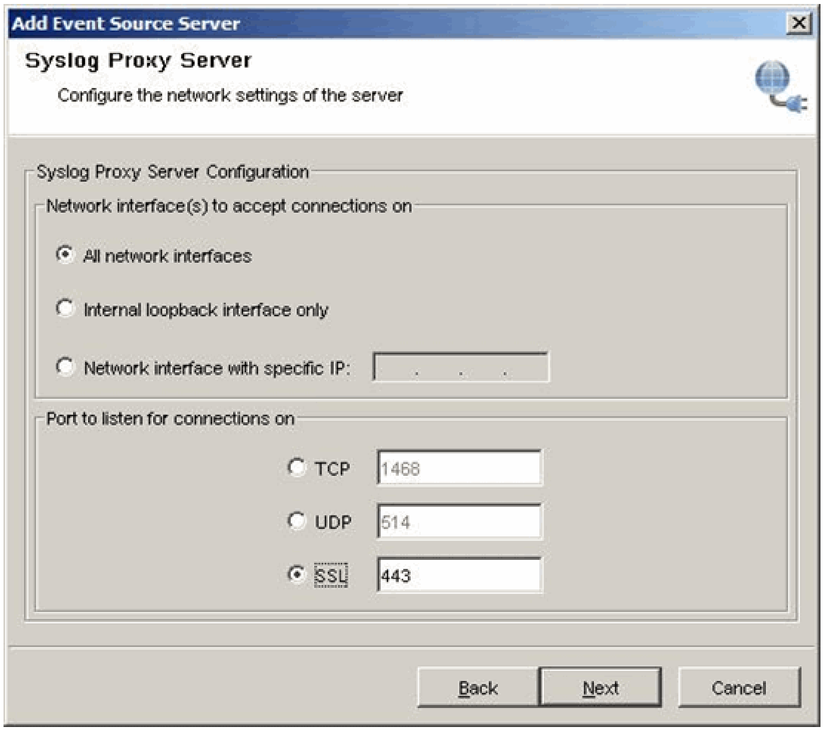
In Sentinel 5.x, the Audit Connector can be bound to one specific IP address on a multiple IP machine. In this situation, the port values in the `-connector` parameter can be replaced by `IP address:port` value. For example, a machine with two IP addresses (for example, 192.168.0.10 and 192.168.0.11) 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 can 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 6.0, 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



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 Audit is set using the option `-auditQueueSize` in the syslog.conf file

`-auditQueueSize`	Number of messages to be buffered. These messages will be resent in case a connection is lost temporarily. If the option value is not used or if the option value is less than 0, the value will default to 10,000.

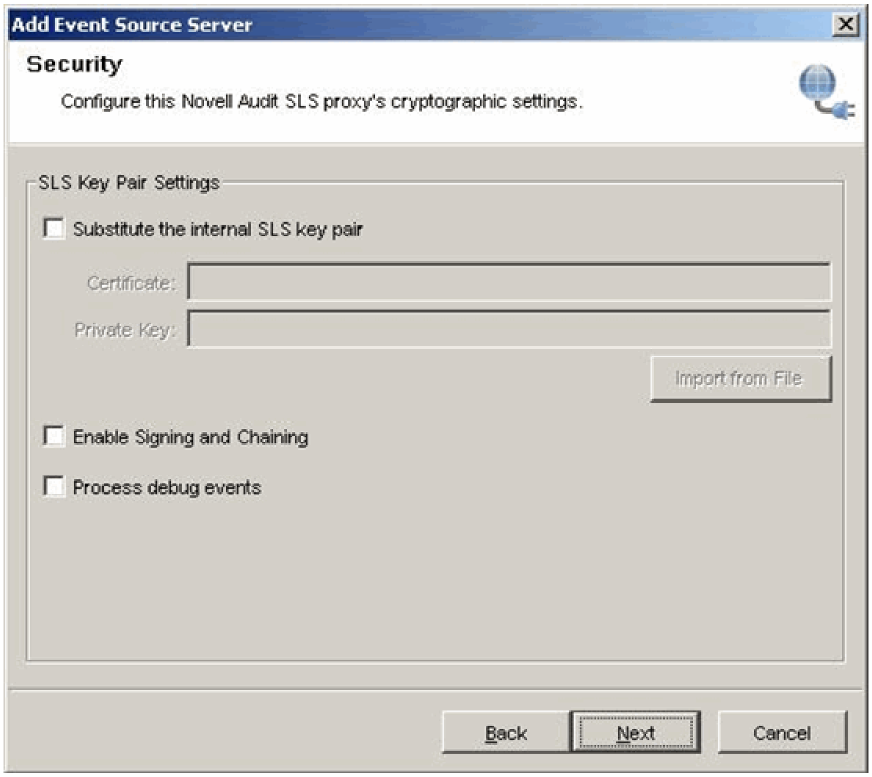
In Sentinel 6.0, the message buffer size for the Audit Connector is fixed at 10,000.

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 communicating 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.

You can configure the keystore that the Audit Connector uses when establishing connection with the Platform Agents using the following *Event Source Server configuration* screen.



Add Event Source Server

Security

Configure this Novell Audit SLS proxy's cryptographic settings.

SLS Key Pair Settings

□ Substitute the internal SLS key pair

Certificate:

Private Key:

□ Enable Signing and Chaining

□ Process debug events

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 6.0, the Audit Server and the Audit Client both run on the same machine (using the same JVM), so this option is not required anymore.

Audit Client Configuration

The Collector and Audit Connector can be imported using Event Source Management functionality in Sentinel 6.0. For more information on the procedures, see Event Source Management in *SentinelUser 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 can be set in the Rx/Tx Value during the port configuration for the Audit-based Collector. For simplicity, they can 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.)

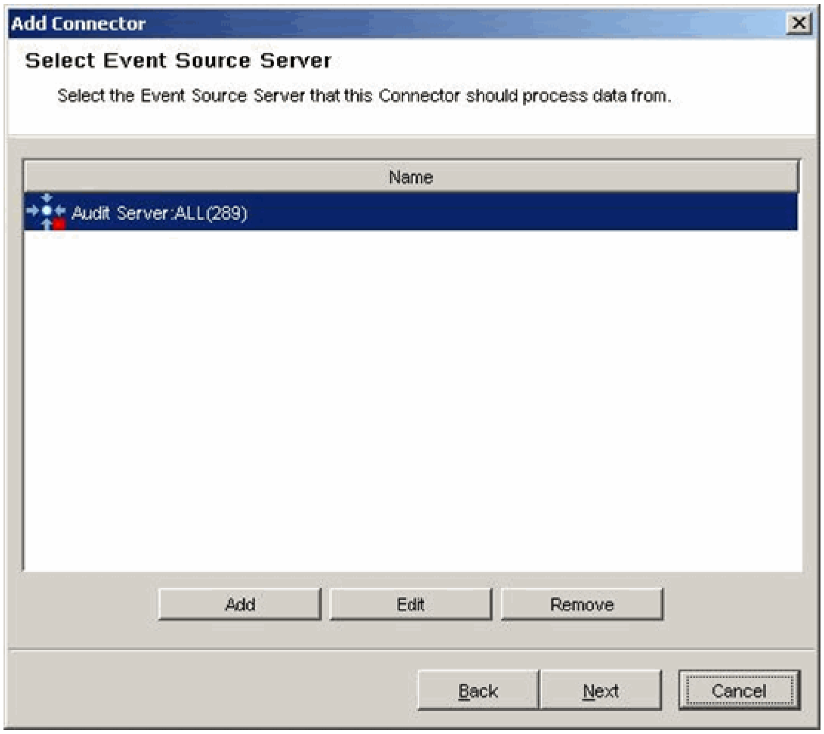
In Sentinel 6.0, options for the Audit Client are configured in the Event Source Management interface as properties of the Connector and the Event Source.

Audit Proxy Server Connection

In the Sentinel 5.x, the Audit Connector option `–proxy` is used to specify the Audit Server to which this Connector is required to be connected.

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

In Sentinel 6.0, the proxy server connection is configured on the *Select Event Source Server* screen in the Audit Connector configuration wizard.



Add Connector

Select Event Source Server

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

Name
Audit Server:ALL(289)

Miscellaneous Options

In Sentinel 5.x, the `–audit` option is used to indicate that the Audit Client must 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 6.0, 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 6.0, the Audit Server/Proxy and the Audit Connector are always on the same machine, so there is no equivalent configuration setting.

APPENDIX

A Revision History

Revision 01

Initial Document

June 2007