l’

Novell® Connector™

Rev: 01

July 9, 2007

www.novell.com

File 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 http://www.novell.com/documentation.

This guide provides you information on:

- Overview of this Connector
- Configuring this Connector to establish connection between the Collector and Event Source.
- Testing the connection

The additional documentation available on Collectors:

- Sentinel Control Center User Guide

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 File all or File new 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*.)

For more information about using Sentinel 6, please refer to the Sentinel User's Guide, Chapter 8 on Event Source Management.

This document focuses on the file connector and the differences between using this connection method in Sentinel 6 and previous versions. In addition to the topics above, this document assumes familiarity with the following topics:

- Creating File connections
- File All connections in Sentinel 5.x (For more information, refer to the documentation for any 5.x File collector.)
- File New connections in Sentinel 5.x (For more information, refer to the documentation for any 5.x File collector.)

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

Outdated Sections of the 5.x Documentation

Due to changes in functionality between Sentinel 5.x and Sentinel 6, the following sections of the collector documentation for collectors using the DB connection are no longer relevant:

- Port configuration
- Get Started
- Collector Prerequisites information about installing the file collector.

- Information about setting parameters (actual parameter names and values are still valid)

Please note that not all the above sections exist in all the file collector documents.

Collector Functionality

From an end user perspective, the general functionality of the File collector in Sentinel 6 is basically the same as in Sentinel 5.x and previous versions. For more information about the functionality of the collectors, refer to the 5.x documentation for that collector. The major difference in user perspective is mainly how File All/New is implemented and configured and how the file rotation is configured. This document discusses these two differences in detail.

The technical implementation of the collectors has also changed slightly with the release of Sentinel 6. In Sentinel 5.x, file collectors read directly from a file for data. In Sentinel 6, Collectors use a data map instead.

Getting Started

To get started, import the appropriate connector and collector using Event Source Management. The connector and collectors must be located in a directory that can be browsed to from the Sentinel Control Center machine.

For more information about the import process, refer to *Event Source Management* in the *Sentinel User's Guide*.

Device Configuration

The configuration of devices (devices, including operation systems, network devices, and other applications, that write event data to files for the collector to read) for Sentinel 6 is the same as configuration of devices in Sentinel 5.x.

Collector Configuration and Operation

For Sentinel 5.x collectors that used file connection, the major differences in configuration are covered by the procedures in the *Sentinel User's Guide* that explain how to import a collector and connector and the procedures in the file connector documentation that explain how to configure the file connector in Sentinel 6's Event Source Management framework

For collectors that are already deployed in your environment, you should refer to the parameters in the Sentinel 5.x collector when configuring the parameters for the Sentinel 6 collector.

Offset

There are three options for reading events from a file:

- Read from the beginning of the file
- Read from the last read position
- Read from a specified location in the file

File All

In Sentinel 5.x, the File All option in Collector Builder is used to read from the beginning of a file. In Sentinel 6, this is configured in the Event Source Management interface by setting the file offset to *Beginning of Data.*

File New

In Sentinel 5.x, the File New option in Collector Builder is used to read from the "last read' position in the file, wherever the collector stopped reading on the previous query. In Sentinel 6, this is configured in the Event Source Management interface by not setting a file offset. If there is no file offset, the File Connector will maintain its position and start reading where it left off when the Event Source is stopped or restarted for any reason.

New Offset Setting

In Sentinel 6, you can start reading from a specified position in the file. This new feature is explained in the *File Offset* section of *File Connector*.

File Rotation

In Sentinel 5.x, if the collector supports file rotation, this is included in the collector script. File rotation is used to change the Collector from reading one file to another. For example, if a source device generates a new log file daily, with the current date in the name of the latest file, file rotation can be used to automatically reading switch from the old log file to the new one.

The command typically used to handle file rotation in Sentinel 5.x is SETCONFIG with the FileConnector.InputFile argument. Although SETCONFIG still works in Sentinel 6 with other arguments, the FileConnector.InputFile argument has been deprecated in Sentinel 6 because of changes related to the creation of Event Source Management.

In Sentinel 5.x, SETCONFIG with FileConnector.InputFile argument was usually used to set the input file name for the collector to a variable, which could be changed in the coding logic. For example:

```
SETCONFIG("FileConnector.InputFile", s_InputFile)
```

More detailed collector analysis may be needed for custom collectors written by customers, partners, or consultants.

In Sentinel 6, file rotation is handled in the File Connector plugin itself. The procedures for using file rotation are described in the Connector documentation for the File Connector. Novell is in the process of modifying its Tier 1 collectors that use file rotation. These modified collectors will be posted to the Novell web site as they are updated:

- T1_SYMA_AVxx_1000_LOGF_Bv520
- T1_QUAL_QGRD_045x_LOGF_Bv520
- Microsoft_Windows_NT_4_LOG_520

Any custom collectors written for Sentinel 5.x that used file rotation should also be updated to use the File Connector's rotation.

To update a Sentinel 5.x collector with file rotation to run with Sentinel 6:

1. Open the collector script in Collector Builder.

2. Review the custom collector code to determine which code is used to implement file rotation. This will often (but perhaps not always) include the SETCONFIG command.
3. Comment out the file rotation code in the collector script. For example:

   ```
   /* <File rotation code to be removed> */
   ```

   Caution: Removing code other than the code used to implement file rotation may affect the functionality of the collector.
4. Save the modified collector.
5. Open the Sentinel Control Center and go to *Event Source Management > Live View*.
6. Import the modified collector in the Event Source Management interface.
7. If the File Connector has not already been imported into Sentinel 6, download the File Connector from the Novell web site and import it in the Event Source Management interface.
8. Use the documentation for the File Connector to configure file rotation during the connector import.

File Delimiter

In Sentinel 5.x, the delimiter for a new record was entered in the Rx state of the collector template in Collector Builder. This delimiter indicates when the Collector Manager should consider one record complete and start reading the next record.

Record delimiters are represented in the Rx state in Collector Builder using hexadecimal notation. A common record delimiter is a new line character:

```
0x0A
```

Some devices create log files with multiline records, however; for these devices, the delimiter may be something more complex, such as a carriage return, a new line character, and another carriage return:

```
0x0D0x0A0x0D0x0A
```

In Sentinel 6, the record delimiter is a property of the File Connector and is entered in the Event Source Management interface as part of the configuration of the File Connector. The Sentinel 6 File Connector uses a new line character as the default delimiter as the default (which is actually the new line character in UNIX and a carriage return plus a new line character for Windows). If the source device uses thjs as the record delimiter, no further modification is necessary.

If the record delimiter is not a new line character, the Connector must be modified to use a new record delimiter.

To use a non-default record delimiter:

1. Refer to the device log files or the Rx state value of the 5.x collector to determine the record delimiter.
2. Log into the Sentinel Control Center and go to *Event Source Management > Live View*.
3. Import the Collector and File Connector.
4. When configuring the File Connector, go to the *Connection Mode* tab.

5. Create a new parameter called *Delimiter*.
6. Enter the value for the record delimiter in hexadecimal format. For example: `0x0D0x0A0x0D0x0A`
7. Save the configuration.

Revision History

Revision 01

Initial document

July 2007