Novell®
Sentinel™

6.0

www.novell.com

October 5, 2007

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 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**

Differences between Sentinel 5.x and Sentinel 6 1
Device Configuration 1
Collector Functionality 1

Differences in Functionality **2**

Getting Started 2
Collector Configuration and Operation 2
Offset 2
File All 2
File New 2
New Offset Setting 2
File Rotation 3
File Delimiter 4

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.*

This document instruct users of Sentinel 6 on how to use Collectors written for Sentinel 5.x with *File all* or *File new* connection method with Sentinel 6.0.

This document focuses on the File 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 and previous versions (For more information, see Using 5.x Collectors with Sentinel 6.)
- Creating File connections
- File All connections in Sentinel 5.x (For more information, see the documentation for any 5.x File Collector.)
- File New connections in Sentinel 5.x (For more information, see the documentation for any 5.x File Collector.)

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

Differences between Sentinel 5.x and Sentinel 6

Due to changes in functionality between Sentinel 5.x and Sentinel 6, the following are not valid for Sentinel 6 Collectors and Connectors.

- Port configuration
- Installing the DB Connector
- Information about setting parameters (actual parameter names and values are still valid, but the method for setting them has changed).

Device Configuration

The configuration of devices (including operating systems, network devices, and other applications, that write event data to files for the Collector to read) for Sentinel 6.0 is similar to the device configuration in Sentinel 5.x.

Collector Functionality

The general functionality of the File Collector is similar to Sentinel 6.0 and previous versions. The important update in the File Connector is about implementation and configuration of File All/ file rotation. These updates are discussed in detail in this guide.

The technical implementation of the Collectors has also changed slightly with the release of Sentinel 6.0. In Sentinel 5.x, File Collectors read directly from a file for data as compared to Sentinel 6.0 where Collectors use data maps.

Differences in Functionality

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

Getting Started

Import required Connector and Collector using Event Source Management. The Connectors and Collectors must be located in a directory that can be easily browsed.

For more information on the import process, see Event Source Management in *Sentinel User Guide.*

Collector Configuration and Operation

For more information on major differences in configuration for Sentinel 5.x Collectors that used file connection, see Importing Plug-ins in *SentinelUser Guide and* File Connector documentation that explain configuring Collectors that use the File Connector in Sentinel 6.0 Event Source Management framework.

For Collectors that are already deployed, see the parameters in the Sentinel 5.x Collector when configuring the parameters for the Sentinel 6.0 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 6.0, 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 6.0, 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 when the Event Source is stopped or restarted for any reason.

New Offset Setting

In Sentinel 6.0, 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

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 as the name of the latest file, file rotation can be used to automatically switch reading from the old log file to the new one. In Sentinel 5.x, if the Collector supports file rotation, this is included in the Collector script.

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 6.0 with other arguments, the FileConnector.InputFile argument has been deprecated in Sentinel 6.0 due to the changes related to the creation of Event Source Management.

In Sentinel 5.x, SETCONFIG with FileConnector.InputFile argument was 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)
```

In Sentinel 6.0, file rotation is handled in the File Connector plug-in itself. The procedures for using file rotation are described in the Connector documentation for the File Connector.

You must update any custom Collectors written for Sentinel 5.x that used file rotation to use the File Connector's rotation.

To update a Sentinel 5.x Collector with file rotation to run with Sentinel 6.0:

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 (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> */
   ```

   WARNING:

   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 6.0, download the File Connector from the Novell web site (http://www.novell.com/documentation/sentinel6/) 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. For example:

```
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. For example:

```
0x0D0x0A0x0D0x0A
```

In Sentinel 6.0, 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 6.0 File Connector uses a new line character as the default delimiter (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 this as the record delimiter, no further modification is necessary.

If the record delimiter is not a new line character, you must modify the Connector 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 click *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.

A Revision History

Revision 01

Initial document

July 2007