Novell®

Connector™

Rev: 01

www.novell.com

June 29, 2007

DBConnector 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.

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 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....1
Additional Documentation....1
Documentation Conventions....1
Introduction....2
Outdated Sections of the 5.x Documentation....2
Collector Functionality....3
Getting Started....3
Device Configuration....3
Collector Configuration and Operation....3
  JDBC Collectors....3
  ODBC Collectors....3
  Offset File....5
Special Considerations....6
Revision History....7
  Revision 01....7

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
- Database (DB) Connector Guide for Sentinel 5
- Database (DB) Connector 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 ODBC or JDBC 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 in 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 database (DB) 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 database connections
- ODBC connections in Sentinel 5.x (For more information, refer to the documentation for any 5.x ODBC collector.)
- JDBC connections in Sentinel 5.x (For more information, refer to the documentation for any 5.x JDBC collector.)

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

In Sentinel 6, there is an option to use ODBC or JDBC option. The JDBC connector is preferred, for reasons that are explained later in this document, but both connection types will be explained in this document.

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 DBconnector
- Information about setting parameters (actual parameter names and values are still valid, but the method for setting them has changed)

Collector Functionality

From an end user perspective, the general functionality of the ODBC and JDBC collectors is basically the same in Sentinel 6 and previous versions. For more information about the functionality of the collectors, refer to the 5.x documentation for that collector.

The technical implementation of the collectors has changed slightly with the release of Sentinel 6. In the past, database collectors used name value pairs to represent the data collected via ODBC or JDBC. New collectors built for Sentinel 6 use a data map instead. ODBC does not support data maps, so all new Sentinel 6 collectors will be built to use JDBC connections.

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 the *Event Source Management* chapter in the *Sentinel User's Guide*.

Device Configuration

The configuration of devices (in this case, the database server) for Sentinel 6 is the same as configuration of devices in Sentinel 5.x.

Collector Configuration and Operation

JDBC Collectors

For Sentinel 5.x collectors that used JDBC, 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 Database Connector documentation that explain how to configure the JDBC connector.

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.

In addition, please refer to the *Offset File* section below for information on how to use the existing offset file to prevent data overlap between the Sentinel 5.x system and the Sentinel 6 system. (If data overlap between the old system and the upgraded system is desirable, the database offset may be deliberately set to an older value, typically a lower row number, in order to manipulate the collector into collecting older data.)

ODBC Collectors

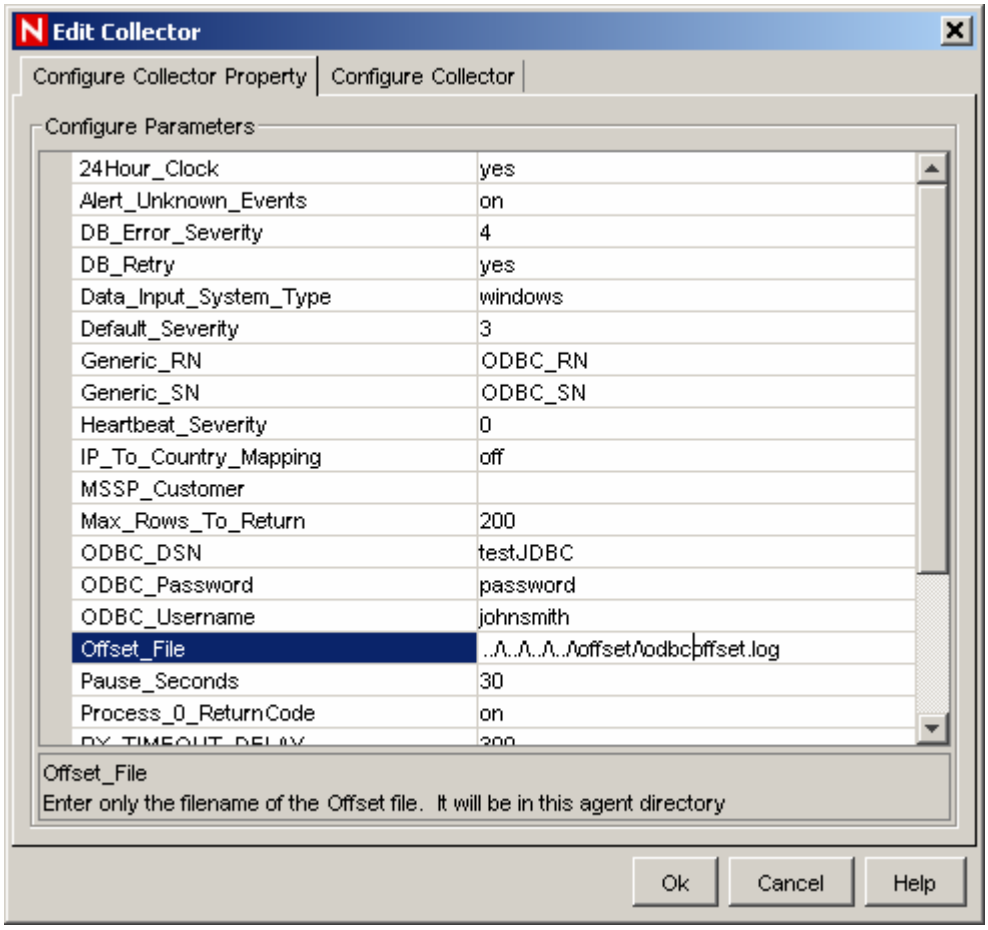
Collectors with ODBC as their connection method use an ODBC data source directly; there is no real connector. The DBConnector is not necessary for ODBC collectors.

To use a 5.x ODBC collector with Sentinel 6:

1. Place the ODBC collector (from 4.x or 5.x) in a location that can be browsed to from the Sentinel Control Center.
2. Create the ODBC Data Source Name, as you did for Sentinel 5.x.
3. Log into the Sentinel Control Center as a user with permission to manage Collectors.
4. Go to *Event Source Management > Live View*.

5. Use the instructions in the *Event Source Management* chapter of the *Sentinel User's Guide* to import the collector.
6. Enter the following parameters for the Collector:
   - ODBC_DSN
   - ODBC_Password (not necessary if Windows Authentication is used)
   - ODBC_Username (not necessary if Windows Authentication is used)

NOTE: If you are using Windows Authentication with ODBC, the Sentinel Service must be run as a domain user with permission to read from the source database.



7. Complete the Collector configuration.
8. Start the Collector. Unlike most Sentinel 6 Collectors, no Connector or Event Source creation is necessary for ODBC Collectors.

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.

In addition, please refer to the *Offset File* section below for information on how to use the existing offset file to prevent data overlap between the Sentinel 5.x system and the Sentinel 6 system. (If data overlap between the old system and the upgraded system is desirable, the database offset may be deliberately set to an older value, typically a lower row number, in order to manipulate the collector into collecting older data.)

Offset File

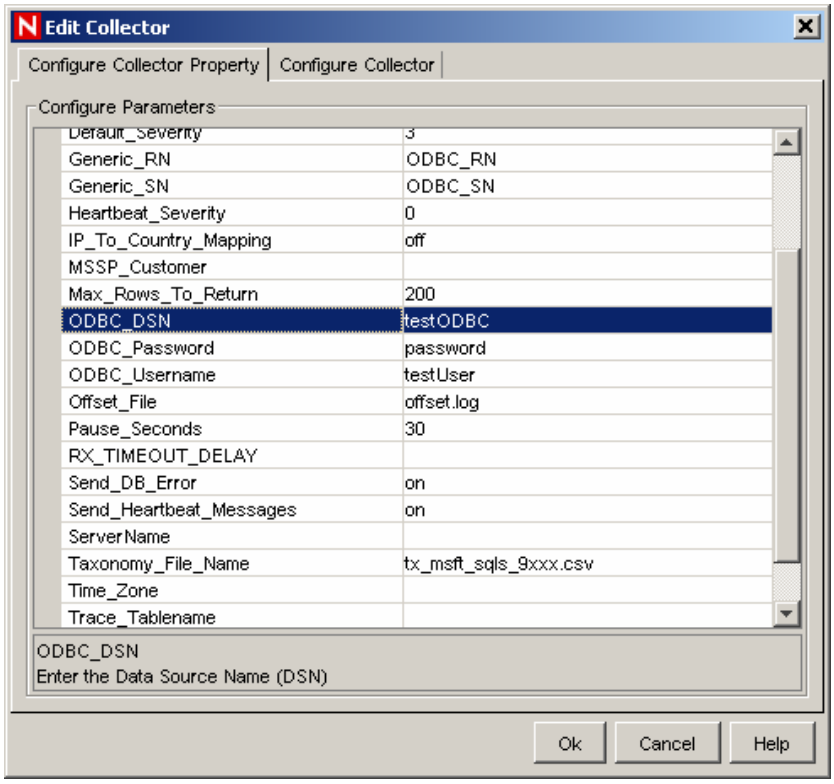
There are changes in how the offset file is configured. In Sentinel 5.x, an offset file is used to record a unique row identifier that indicates the ending point for the last database query (and the starting point for the next database query). In Sentinel 6, the unique row identifier is typically stored in the database instead.

However, it is still possible to use older Sentinel ODBC or JDBC collectors with an offset file using the procedure below. This method is very similar to the way the Sentinel 5.x ODBC and JDBC Collectors worked. Using the offset value in the existing offset file will ensure that the new Sentinel 6 system starts reading data where the Sentinel 5.x system left off.

To use a 5.x database collector with an existing offset file:

1. Create a directory to hold the offset file under %ESEC_HOME% (for Windows) or $ESEC_HOME (for UNIX) directory. In this example, the directory is named *offset*.
2. Copy the existing offset file into the new directory or create a new file with the same value as the value in the existing offset file. The file should have a unique name (such as collectorname_offset.log).
3. Open the Sentinel Control Center and go to *Event Source Management.*
4. Right-click the Collector in the Event Source Management window and choose Edit.
5. On the Configure Collector Property tab, edit the *Offset_File* property with the directory name and file name for the offset file. (In Windows, you must use an escape character "/" before using the backslash "\". For example, the value for Offset _File might be

```
../\../\../\../\offset/\collectorname_offset.log
```



If you have multiple database collectors, each of them should have a corresponding offset file. Each offset file must have a different, unique name.

Special Considerations

JDBC connections are preferred to ODBC connections for several reasons:

- The JDBC connector supports raw data storage in the RxBuffer using a data map. The raw data is stored in the variable `s_raw_message`. This facilitates troubleshooting the collector.
- The JDBC connector can automatically reconnect to the database server if the connection is lost. There are a few reasons the connection might be lost – the database server might be shut down, the network connection might be lost, or the Collector Manager machine or service might be restarted. An ODBC collector would have to be manually restarted in these circumstances.
- The JDBC connector stores the database username and password in encrypted format. ODBC collectors that use SQL Authentication (rather than Windows Authentication) require storing the account name and password in clear text, as shown in the previous graphic. ODBC collectors using Windows Authentication require that the Sentinel Service be run as an account that has permission to read from the source database.
- JDBC collectors can run on Collector Managers on any supported platform. ODBC collectors can only run on Windows-based Collector Managers.

For these reasons, all new Sentinel 6 collectors will be built using JDBC connections.

Revision History

Revision 01

Initial document

June 2007