

Novell® Sentinel™

6.0

October 26, 2007

www.novell.com

DB Connector Differences in Sentinel 6

Product Version(s): Requires Sentinel 6.0 or higher

N

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/edtfpj/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.tanukisoft.com/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
Functionality	1
Importing Connectors and Collectors	2
Device Configuration	2
Collector Configuration and Operation	2
JDBC Collectors	2
ODBC Collectors	2
Offset File	3
Special Considerations	5
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 focuses on the Database (DB) 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 6.0 and previous versions.
- Creating database connections
- ODBC connections in Sentinel 5.x (For more information, see the documentation for any 5.x ODBC Collector.)
- JDBC connections in Sentinel 5.x (For more information, see the documentation for any 5.x JDBC Collector.)

These documents can be found at

<http://support.novell.com/products/sentinel/collectors.html>.

For more information, see [“Using 5.x Collectors in Sentinel 6.0”](#). For more information on using Sentinel 6.0, see [Event Source Management](#) in *Sentinel User Guide*.

You can use ODBC or JDBC Connectors. Novell recommends using JDBC Connectors. For more information, see [“JDBC Collectors”](#).

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)

Functionality

The general functionality of the ODBC and JDBC Collectors are similar to Sentinel 6.0 and previous versions. For more information about the functionality of 5.x Collectors, see 5.x documentation for that Collector.

The technical implementation of the Collectors has changed slightly with the release of Sentinel 6.0. In the past, database Collectors used name value pairs to represent the data collected through ODBC or JDBC. New Collectors built for Sentinel 6.0 uses a data map instead. ODBC does not support data maps, so all new Sentinel 6.0 Collectors will be built to use JDBC connections.

Importing Connectors and Collectors

You must import the appropriate Connector and Collector using Event Source Management. For more information on the import process, see [Event Source Management](#) in *Sentinel User 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. For more information, see [“Using 5.x Collectors in Sentinel 6.0”](#).

Collector Configuration and Operation

JDBC Collectors

For more information on Sentinel 5.x Collectors that used JDBC, see [Sentinel User Guide](#). It explains how to import a Collector and Connector. For more information on configuring the JDBC Connector, see the procedures in the specific Database Connector documentation.

For Collectors that are already deployed in your environment, see the parameters in the Sentinel 5.x Collector when configuring the parameters for the Sentinel 6.0 Collector.

For more information on how to use the existing offset file to prevent data overlap between the Sentinel 5.x system and the Sentinel 6 system, see [“Offset File”](#). (If you wish to overlap data between the old system and the upgraded system, you must set the database offset deliberately to an older value, typically a lower row number, in order to manipulate the Collector into collecting older data.)

ODBC Collectors

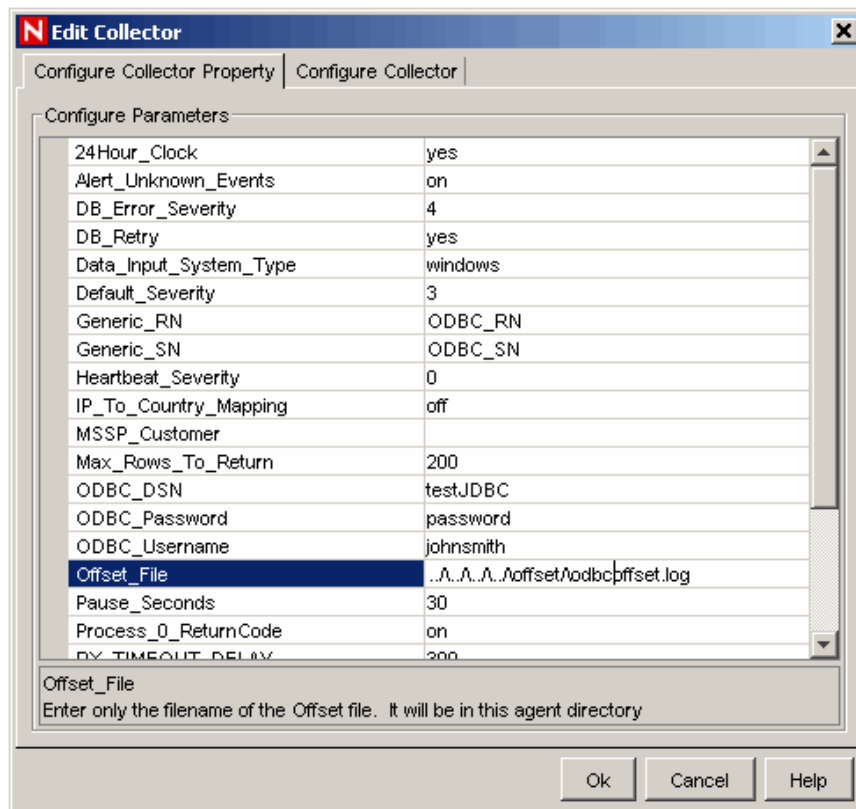
Collectors with ODBC as their connection method use an ODBC data source directly; there is no real Connector. The DBConnector is not necessary for ODBC Collectors.

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 from the Sentinel Control Center.
2. Create the ODBC Data Source Name. For more information on creating ODBC Data Source, see Collector specific documentation..
3. Log into the Sentinel Control Center with administrative rights or as a user with permission to manage Collectors.
4. Click *Event Source Management > Live View*.

5. Import the Collector. For more information on importing Collectors, see [Event Source Management](#) in *Sentinel User Guide*.
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.



Complete the Collector configuration. Start the Collector. No Connector or Event Source creation is necessary for ODBC Collectors.

For Collectors that are already deployed in your environment, you must see the parameters in the Sentinel 5.x Collector when configuring the parameters for the Sentinel 6.0 Collector.

For more information on how to use the existing offset file to prevent data overlap between the Sentinel 5.x system and the Sentinel 6 system, see [“Offset File”](#). (If you wish to overlap data between the old system and the upgraded system, you must set the database offset deliberately 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

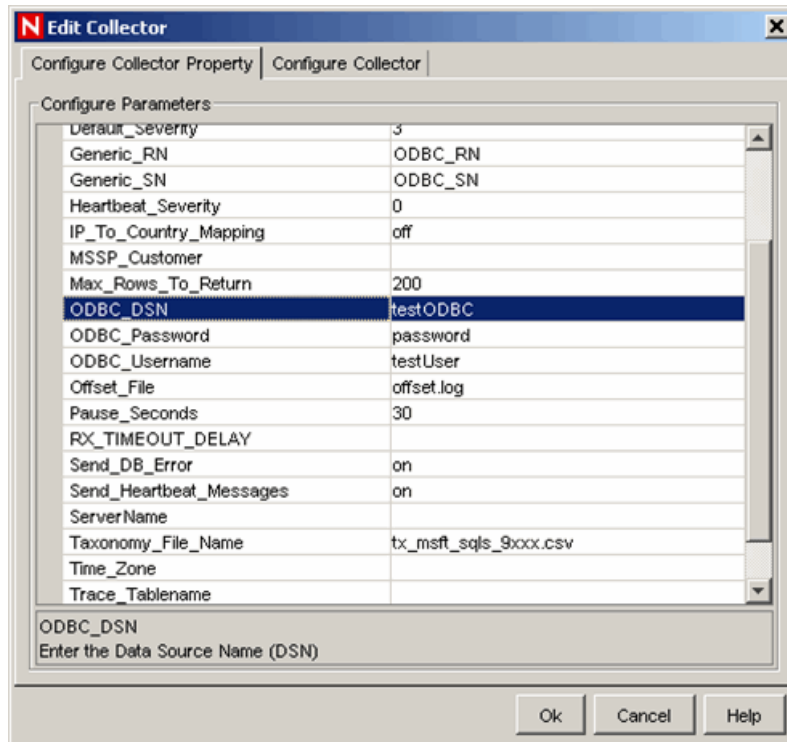
last database query (and the starting point for the next database query). In Sentinel 6.0, the unique row identifier is stored in the database.

However, it is still possible to use older Sentinel ODBC or JDBC Collectors with an offset file using the procedure mentioned below. This method is very similar with the Sentinel 5.x ODBC and JDBC Collectors.. Using the offset value in the existing offset file will ensure that the new Sentinel 6.0 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 under %ESEC_HOME% (for Windows) or \$ESEC_HOME (for UNIX).
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 click *Event Source Management > Live View*.
4. Right-click the Collector in the Event Source Management window and select *Edit*.
5. Create a folder named `offset` under %ESEC_HOME%\data (for Windows) or \$ESEC_HOME/data (for UNIX).
6. 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
```



NOTE: 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 automatically reconnects to the database server if the connection is lost. There are a few reasons the connection might be lost – the database server might 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. Whereas ODBC Collectors can only run on Windows-based Collector Managers.

For these reasons, all new Sentinel 6.0 Collectors will be built using JDBC connections.

A Revision History

Revision 01

Initial document

June 2007