Novell®
Sentinel™

6.0

www.novell.com

October 5, 2007

WMI 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.

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

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 .0 User Guide.*

The focus of this document is to describe usage of Sentinel 5.x Collectors that support WMI 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 in Sentinel 6.0.)
- Windows event log configuration
- Domain accounts in Windows

For more information on using Collectors in Sentinel 6.0, see Event Source Management in *Sentinel 6.0 User Guide*.

Device Configuration

The configuration of various Source Devices (the Windows machines whose event logs will be monitored) for this Collector are similar to the Sentinel 6.0 and previous versions. For more information, see 5.x documentation for a WMI-based Collector.

Collector Functionality

The general functionality of the WMI Connector in Sentinel 6.0 is similar to the previous version. For more information about the functionality of the Collectors, see 5.x documentation for a WMI-based Collector.

Differences in Functionality

There are several configuration differences in the WMI Connector for Sentinel 6.0 detailed below.

Eventlog.exe and Servers.txt

In Sentinel 5.x, eventlog exe is spawned in conjunction with the process Connector. The servers.txt file, a manually created configuration file, indicates which servers to collect data from, log types (application, system, or security), date-time to start collecting data, and a filter to apply to the collected data.

During the Collector's operation, the date-time offset was updated in the servers.txt file to indicate the last data read from each Windows server.

In Sentinel 6.0, you must import Windows Collector and Windows WMI Connector. For more information on importing a Collector, see Event Source Management in *Sentinel 6.0 User Guide*.

You must use servers.txt file for a reference while using the Event Source Management interface. You can create Event Sources that specify the servers to collect data from, log types (application, system, or security), date-time to start collecting data, and a filter to apply to the collected data. The Event Source Management framework will create a configuration file similar to the servers.txt file.

- Server name is entered as a text field while creating a new Event Source.
- Log types can be selected from a drop-down menu.
- One Event Source must be configured in ESM for each server and log type in the original servers.txt file.

In Sentinel 5.x, it was possible to run multiple eventlog.exe instances on the same Collector Manager machine. You must install eventlog.exe on each Collector Manager machine individually.

In the first release of the WMI Connector (r1) for Sentinel 6.0, the Collector Manager can run only one instance of the WMI Connector per machine. The second release (r2) of the WMI Connector enables multiple WMI Connectors per Collector Manager. In both releases of the WMI Connector, all necessary setup of .exe and .jar files on the Collector Manager is handled by the Event Source Management framework when the Connector is configured.

Accounts and Permissions

In Sentinel 5.x, Collector Manager was a distinct service, which is configured to run as a logon account that has permission to access the remote Windows servers. This is necessary in order to receive the events through WMI.

In Sentinel 6.0, the Sentinel Service, which now includes the Collector Manager service, must be configured to run as a logon account that has permission to access the remote Windows servers. This is necessary in order to receive the events through WMI.

Date-Time Offset

In Sentinel 5.x, the date-time offset was updated in the servers.txt file while the Collector was in operation. This offset indicated the last data read from each Windows server.

In Sentinel 6.0, date-time offset is entered when you create a new Event Source. This information is updated in the database as a Connector property during the Collector's operation.

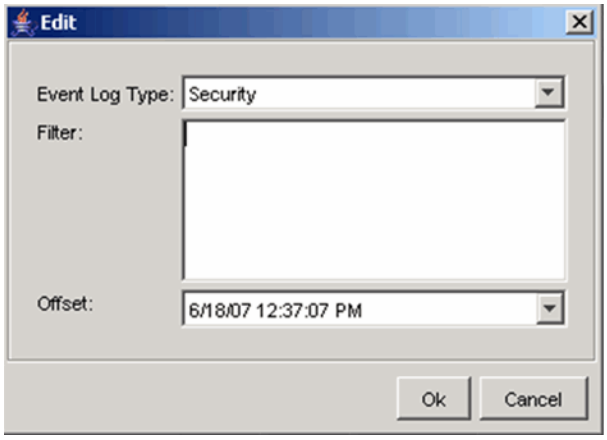
TIP:

Using the date-time offset from servers.txt configuration file(s) from Sentinel 5.x when configuring the Sentinel 6.0 Event Sources will prevent data duplication resulting from the same data being read twice.

Event Filtering

In Sentinel 5.x, the filtering criteria for messages was included in the servers.txt file in WQL (a language similar to SQL but used for WMI queries).

In Sentinel 6.0, the WQL filtering criteria is entered in the ESM interface when you configure an Event Source.



Special Considerations

In Sentinel 6.0, the Event Sources must be unique for the WMI Connector to work properly. The administrator must validate manually that there are no duplicates. If there are duplicates, it may lead to file I/O exception errors.

APPENDIX

A Revision History

Revision 01

Initial Document

June 2007