A

Novell®

Connector™

Rev: 01

www.novell.com

June 29, 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 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 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
- WMI Connector Guide for Sentinel 6
- Windows Collector Guide for Sentinel 5
- Windows Collector Guide for Sentinel 6

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 WMI 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 WMI 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:

- Windows event log configuration
- Domain accounts in Windows

Device Configuration

The configuration of Source Devices (the Windows machines whose event logs will be monitored) for this collector is the same in Sentinel 6 and previous versions.

Collector Functionality

The general functionality of the WMI connector is the same in Sentinel 6 as in previous versions. For more information about the functionality of the collector, refer to the 5.x documentation for a WMI-based collector.

Collector Configuration and Operation

There are several configuration differences in the WMI connector for Sentinel 6.

Eventlog.exe and Servers.txt

In Sentinel 5.x, eventlog exe is spawned in conjunction with the process connector. It used a manually created configuration file called servers.txt. The servers.txt file indicated 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, the Windows WMI connector should be imported using the instructions in the *Event Source Management* chapter of the *Sentinel User's Guide*. The Windows collector should also be imported.

It would be easiest to set up the Event Sources in Sentinel 6 if you print the servers.txt file and use it 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 for you, similar to the servers.txt file.

- Server name is entered as a text field when you create a new Event Source.
- Log types are selected from a drop-down menu.
- One Event Source should 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. Eventlog.exe had to be installed on each Collector Manager machine individually.

In the first release of the WMI Connector (r1) for Sentinel 6, the Collector Manager can run only one instance of the WMI Connector per machine. The second release (r2) of the WMI Connector will enable 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, 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.

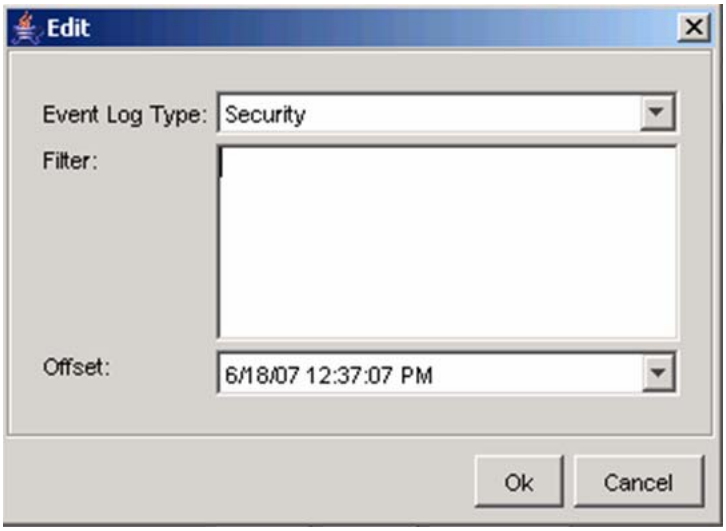
In Sentinel 6, date-time offset is entered when you create a new Event Source. This information is updated in the database as a connector property during the collector's operation.

Using the date-time offset from servers.txt configuration file(s) from Sentinel 5.x when configuring the Sentinel 6 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 very similar to SQL but used for WMI queries).

In Sentinel 6, the WQL filtering criteria is entered in the ESM interface when you configure an Event Source.



Special Considerations

In Sentinel 6, 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.

Revision History

Revision 01

Initial Document

June 2007