Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for eEye Retina Network Security Scanner DB (RTD File)

Configuration Guide

November 30, 2016

Configuration Guide

SmartConnector for eEye Retina Network Security Scanner DB (RTD File)

November 30, 2016

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise Development LP shall not be liable for technical or editorial omissions contained herein. The information contained herein is subject to change without notice. The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only. Hewlett Packard Enterprise Development LP products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices. This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise Development LP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Follow this link to see a complete statement of Hewlett Packard Enterprise Development LP copyrights, trademarks and acknowledgements:
https://www.protect724.hpe.com/docs/DOC-13026.

Revision History

Date	Description
11/30/2016	Updated installation procedure for setting preferred IP address mode.
02/15/2016	Removed ODBC support due to Java 8 implementation; MS Access database is no longer supported.
02/14/2014	Added the “Increase Default Memory Size” section.
09/30/2013	Updated “Create an ODBC Data Source” section and added troubleshooting information regarding connection failure.
05/15/2012	Added new installation procedure.
09/24/2010	Updated versions supported.
02/11/2010	Added support for FIPS Suite B and CEF File transport.
06/30/2009	Global update to installation procedure for FIPS support.
03/27/2009	First release of this SmartConnector.

Contents

SmartConnector for eEye Retina Network Security Scanner DB (RTD File)

This guide provides information for installing the SmartConnector for eEye Retina Network Security Scanner DB (RTD File) and configuring the device for log event collection. eEye Retina Network Security Scanner version 5.0 is supported.

Product Overview

eEye Retina Network Security Scanner identifies known and zero-day vulnerabilities and provides security risk assessment for policy enforcement and regulatory audits.

The SmartConnector for eEye Retina Network Security Scanner DB (RTD File) uses the reports generated by the Network Security Scanner to retrieve host information (such as vulnerabilities, open ports, and URI information) and send it to the ArcSight ESM Manager.

If you encounter the error message "Memory usage in red zone" when running the connector, you can increase the default memory setting. See the section "Increase Memory Size for XML Reports" for details.

Operational Modes

The SmartConnector for eEye Retina Network Security Scanner DB, as with other vulnerability scanners, supports two operational modes:

- **Interactive -**This mode is designed to be used by an operator who requires only certain reports to be sent to ArcSight. In this mode, the SmartConnector reads the contents of the configured folder and presents it in a UI window. The user can select which scan reports are to be sent to the ArcSight ESM Manager. After completing the selections the user can click on the **Send** button to send all the selected scanner reports to ArcSight. The user can simply close (exit) the window when all the desired scans have been sent to ArcSight and the connector will terminate. In this mode, the connector should not be run as a service, only as a stand-alone application.

- **Automatic -** This mode is designed to automatically import the reports from Retina Network Security Scanner to the ArcSight ESM Manager. In this mode, the SmartConnector periodically retrieves the contents of the configured folder and, whenever a new file is detected, automatically processes it and sends it to the ArcSight ESM Manager. The SmartConnector can run as a service in this mode because it is designed to run in unattended mode.

In both modes, the SmartConnector for eEye Retina Network Security Scanner records the file names of the reports that have been sent to the ArcSight ESM Manager; therefore, if you use the interactive mode, the list of files available displays only the files that have not yet been sent to the ArcSight ESM Manager. The same applies for the Automatic mode; only files that are present in the configured folder that have not been sent already are processed.

To run a scanner connector in interactive mode, the connector must be run in standalone mode and not as a service. Automatic mode, however, can be run either standalone or as a service, although the general preference is to run automatic mode as a service.

Configuration

Download and Install a JDBC Driver

During the installation process, you will be directed to leave the wizard and copy the JDBC driver file you download to a SmartConnector folder. For information about and to download the MS SQL Server JDBC Driver, see:

http://msdn.microsoft.com/en-us/sqlserver/aa937724

Different versions of the JDBC driver are required for different SQL Server database versions; be sure to use the correct driver for your database version. The name of the jar file may be different for some JDBC driver versions.

Install the driver.

For software connectors, copy the jar file appropriate for your SQL Server version from the installation folder for the SQL Server JDBC driver to a temporary location; you will copy this file to `$ARCSIGHT_HOME/current/user/agent/lib`, (where `$ARCSIGHT_HOME` refers to the SmartConnector installation folder, such as `c:\ArcSight\SmartConnectors`) after the core SmartConnector software has been installed at step 3 of Install the SmartConnector. Copy only the jar file associated with the version of the driver to be installed to this location.

Add a JDBC Driver to the Connector Appliance/ArcSight Management Center

After downloading and extracting the JDBC driver, upload the driver into the repository and apply it to the appropriate container or containers, as described in this section.

1. From the Connector Appliance/ArcSight Management Center, select **Setup -> Repositories**.
2. Select **JDBC Drivers** from the left pane and click the **JDBC Drivers** tab.
3. Click **Upload to Repository**.
4. From the **Repository File Creation Wizard**, select **Individual Files**, then click **Next**.
5. Retain the default selection and click **Next**.
6. Click **Upload** and locate and select the `.jar` file you downloaded in step 3 of SmartConnector Installation.
7. Click **Submit** to add the specified file to the repository and click **Next** to continue.
8. After adding all files you require, click **Next**.
9. In the **Name** field, enter a descriptive name for the zip file (`JDBCdriver`, for example). Click **Next**.
10. Click **Done** to complete the process; the newly added file is displayed in the **Name** field under **Add Connector JDBC Driver File**.
11. To apply the driver file, select the driver .zip file and click the up arrow to invoke the **Upload Container Files** wizard. Click **Next**.

12 Select the container or containers into which the driver is to be uploaded; click **Next**.

13 Click **Done** to complete the process.

14 Add the connector through the Connector Appliance/ArcSight Management Center interface; see the *Connector Appliance/ArcSight Management Center Online Help* for detailed information. Descriptions of parameters to be entered during connector configuration are provided in the "Install the SmartConnector" section of this guide.

Configure the JDBC Driver and Windows Authentication

This section provides guidance on how to use a JDBC driver with SmartConnectors that connect to Microsoft SQL Servers using Windows Authentication only. As previously described, download the SQL JDBC drivers from Microsoft and install the driver before beginning this procedure.

The JDBC driver does not provide function to supply Windows authentication credentials such as user name and password. In such cases, the applications must use SQL Server Authentication. When installing the connector on a non-Windows platform, configure the Microsoft SQL Server for Mixed Mode Authentication or SQL Server Authentication.

Microsoft Type 4 JDBC drivers (versions 4.0 or later) support integrated authentication. Windows Authentication works only when using one of these drivers. You also will need to add `;integratedSecurity=true` to the JDBC URL entry for the connection to your database.

1 Copy the `sqljdbc_auth.dll` file from the JDBC driver download to the `$ARCSIGHT_HOME\jre\bin directory`. For example, the JDBC driver download path for SQL JDBC driver version 4.0 for 32-bit environment would be `sqljdbc_4.0\enu\auth\x86\sqljdbc_auth.dll` and, for 64-bit environment, `sqljdbc_4.0\enu\auth\x64\sqljdbc_auth.dll`.

When upgrading a connector, the $ARCSIGHT_HOME\jre\bin directory is overwritten; therefore, you will need to copy the authentication file to this folder again after update.

2 Go to `$ARCSIGHT_HOME\current\bin` and double-click `runagentsetup` to continue the SmartConnector installation.

3 When entering the connector parameters, in the **JDBC Database URL** field, append `;integratedSecurity=true` to the end of the URL string.

The following is an example; note that the name or instance of the database configured at installation/audit time should be used.

```
jdbc:sqlserver://mysqlserver:1433;DatabaseName=mydatabase;integratedSecurity=true
```

4 Complete the remaining connector wizard configuration steps.

5 After completing the connector installation, if running on a Windows Server, change the service account to use the Windows account that should login to the database. The Connector will use the account used to start the service, regardless of the account value setting entered in the connector setup process.

Increase Memory Size for XML Reports

The connector cannot process reports that are too lengthy. With the default 256M memory setting, the connector can safely process reports up to 250K in length. If memory is increased to the maximum limit of 1024M, the connector can process reports up to a million lines in length. Longer reports cannot be processed. ArcSight's recommendation for long reports is to split the scan into multiple smaller reports and import them individually.

To increase the memory size for stand-alone connectors from the command line, change the following line in `$ARCSIGHT_HOME\current\bin\scripts\connectors.bat` (Windows) or `$ARCSIGHT_HOME/current/bin/scripts/connectors.sh` (Unix)

```
ARCSIGHT_MEMORY_OPTIONS="  -Xms256m -Xmx256m "
```

to

```
ARCSIGHT_MEMORY_OPTIONS="  -Xms1024m -Xmx1024m "
```

To increase the memory size for connectors being run as a service, change the following lines in `user/agent/agent.wrapper.conf` from:

```
wrapper.java.initmemory=256
wrapper.java.maxmemory=256
```

to:

```
wrapper.java.initmemory=1024
wrapper.java.maxmemory=1024
```

To increase the memory size for connectors managed by the Connector Appliance/ArcSight Management Center, the heap size can be set using a container level command.

Install the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.

ArcSight recommends you do not install database connectors on the database server or any mission critical servers as this could cause performance issues.

Prepare to Install Connector

Before you install any SmartConnectors, make sure that the ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger). This configuration guide takes you through the installation process with **ArcSight Manager (encrypted)** as the destination.

For complete product information, read the *Administrator's Guide* as well as the *Installation and Configuration* guide for your ArcSight product before installing a new SmartConnector. If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* for instructions, and start the installation procedure at "Set Global Parameters (optional)" or "Select Connector and Add Parameter Information."

Before installing the SmartConnector, be sure the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

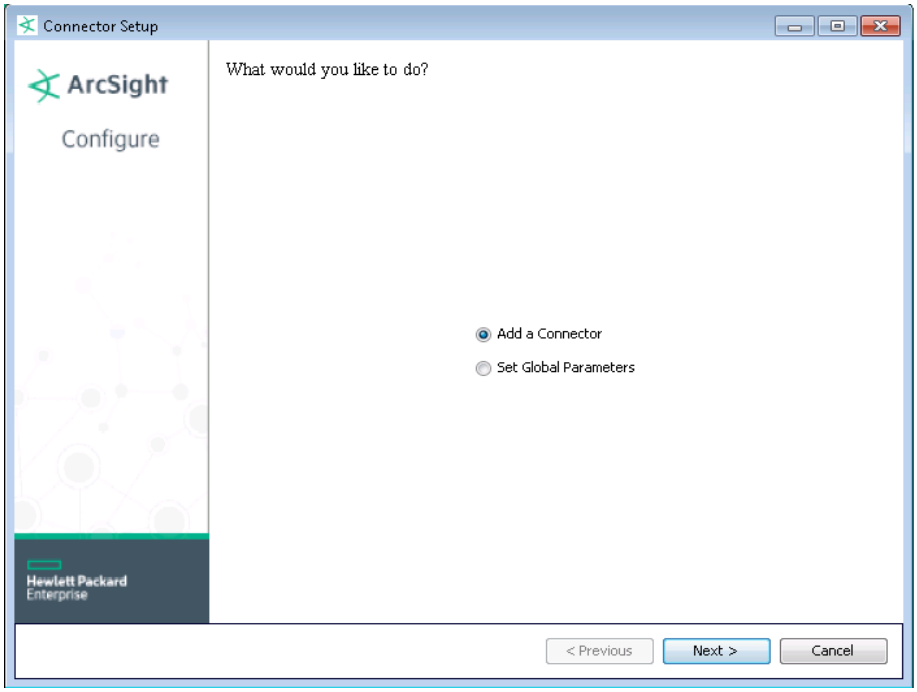
Install Core Software

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the HPE SSO and Protect 724 sites.

1. Download the SmartConnector executable for your operating system from the HPE SSO site.
2. Start the SmartConnector installation and configuration wizard by running the executable.

   Follow the wizard through the following folder selection tasks and installation of the core connector software:

   Introduction
   Choose Install Folder
   Choose Shortcut Folder
   Pre-Installation Summary
   Installing...
3. When the installation of SmartConnector core component software is finished, the following window is displayed:



Download SQL Server JDBC Driver

To download a Microsoft SQL Server JDBC driver, click **Cancel** to leave the configuration wizard at this point and copy the jar file you downloaded earlier (see "Download and Install a JDBC Driver") to `$ARCSIGHT_HOME/current/user/agent/lib`.

From `$ARCSIGHT_HOME/current/bin`, double-click `runagentsetup` to return to the SmartConnector Configuration Wizard.

Set Global Parameters (optional)

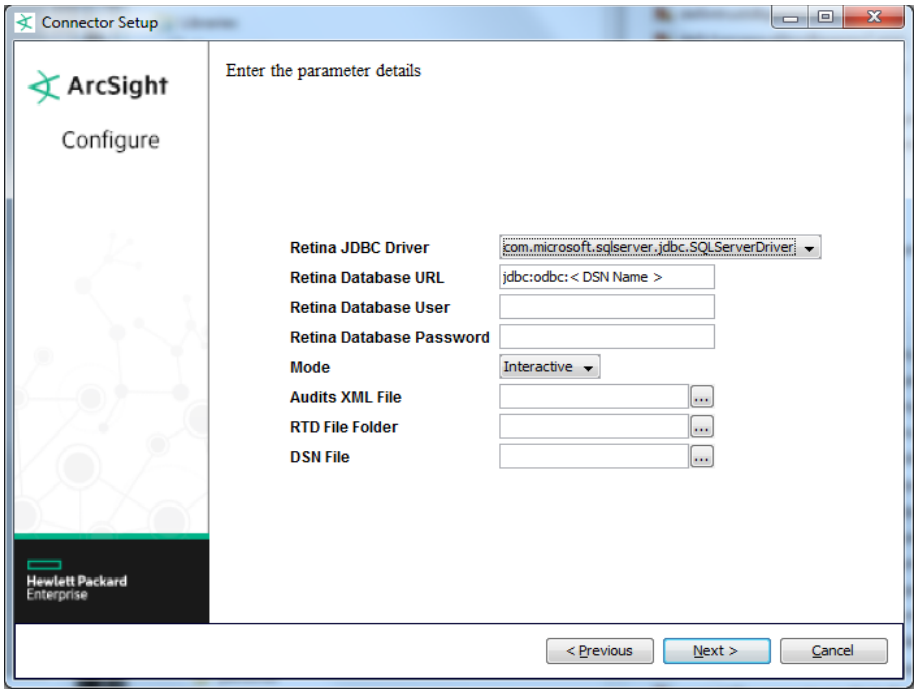
If you choose to perform any of the operations shown in the following table, do so before adding your connector. After installing core software, you can set the following parameters:

Global Parameter	Setting
Set FIPS mode	Set to 'Enable' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disable'.
Set Remote Management	Set to 'Enable' to enable remote management from ArcSight Management Center. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Initially, this value is set to 'Disable'.
Remote management listener port	The remote management device will listen to the port specified in this field. The default port number is 9001.
Preferred IP Version	If both 'IPv4' and'IPv6' IP addresses are available for the local host (the machine on which the connector is installed), you can choose which version is preferred. Otherwise, you will see only one selection. When both values are present, the initial setting is 'IPv4'.

After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to the "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

Select Connector and Add Parameter Information

1. Select **Add a Connector** and click **Next**. If applicable, you can enable FIPS mode and enable remote management later in the wizard after SmartConnector configuration.
2. Select **eEye Retina Network Security Scanner DB (RTD File)** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Retina JDBC Driver	Enter 'com.microsoft.sqlserver.jdbc.SQLServerDriver' (Microsoft SQL Server 2005 JDBC driver).
Retina Database URL	Enter 'jdbc:sqlserver://<MS SQL Server Host Name or IP Address>:1443:DatabaseName=<MS SQL Server Database Name>,' substituting actual values for <MS SQL Server Host Name or IP Address> and <MS SQL Server Database Name>.
Retina Database User	Enter the name of the database user (having administrative privilege)
Retina Database Password	Enter the password for the entered database user name.
Mode	Select 'Interactive' or 'Automatic' mode. In 'Interactive' mode, a graphical user interface is displayed showing reports that can be sent to the ArcSight ESM Manager. In 'Automatic' mode, the new reports are sent automatically to the ArcSight ESM Manager. See "Modes of Operation" in this guide for more information.
Audits XML File	Enter the absolute path to the audits xml file.
RTD File Folder	Enter the name of the folder containing the RTD file to be processed.
DSN File	Enter the name of the temporary file to which the DSN points. The connector copies each new RTD file to be processed onto this temporary file and processes them. You can point the DSN to any of your temporary files, or you can use a file that is shipped with the connector ($ARCSIGHT_HOME/system/agent/config/retina_db/ArcSight_Retina5.rtd).

Select a Destination

1 The next window asks for the destination type; make sure **ArcSight Manager (encrypted)** is selected and click **Next**. (For information about this destination or any of the other destinations listed, see the *ArcSight SmartConnector User Guide*.)

2 Enter values for the **Manager Host Name**, **Manager Port**, **User** and **Password** required parameters. This is the same ArcSight user name and password you created during the ArcSight Manager installation. Click **Next**.

3 Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**. The connector starts the registration process.

4 The certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. (If you select **Do not import the certificate to connector from destination**, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.

Complete Installation and Configuration

1 Review the **Add Connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.

2 The wizard now prompts you to choose whether you want to run the SmartConnector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, select **Leave as a standalone application**, click **Next**, and continue with step 5.

3 If you chose to run the connector as a service, with **Install as a service** selected, click **Next**. The wizard prompts you to define service parameters. Enter values for **Service Internal Name** and **Service Display Name** and select **Yes** or **No** for **Start the service automatically**. The **Install Service Summary** window is displayed when you click **Next**.

4 Click **Next** on the summary window.

5 To complete the installation, choose **Exit** and Click **Next**.

For some SmartConnectors, a system restart is required before the configuration settings you made take effect. If a **System Restart** window is displayed, read the information and initiate the system restart operation.

Save any work on your computer or desktop and shut down any other running applications (including the ArcSight Console, if it is running), then shut down the system.

For instructions about upgrading the connector or modifying parameters, see the *SmartConnector User Guide*.

When using Windows authentication, after completing the connector installation, if running on a Windows Server, change the service account to use the Windows account that should log in to the database. The connector will use the account used to start the service, regardless of the account value setting entered in the connector setup process.

Run the SmartConnector

SmartConnectors can be installed and run in stand-alone mode, on Windows platforms as a Windows service, or on UNIX platforms as a UNIX daemon, depending upon the platform supported. On Windows platforms, SmartConnectors also can be run using shortcuts and optional Start menu entries.

If the connector is installed in stand-alone mode, it must be started manually and is not automatically active when a host is restarted. If installed as a service or daemon, the connector runs automatically

when the host is restarted. For information about connectors running as services or daemons, see the *ArcSight SmartConnector User Guide*.

To run all SmartConnectors installed in stand-alone mode on a particular host, open a command window, go to `$ARCSIGHT_HOME\current\bin` and run: `arcsight connectors`

To view the SmartConnector log, read the file `$ARCSIGHT_HOME\current\logs\agent.log`; to stop all SmartConnectors, enter `Ctrl+C` in the command window.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

eEye Retina Vulnerability Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
ArcSight Severity - High	evice Severity = 7, 8, or 9
ArcSight Severity - Low	Device Severity = 1, 2, or 3
ArcSight Severity - Medium	Device Severity = 4, 5, or 6
Category Technique	Vulnerability
Destination Address	IP
Destination Host Name	HOSTNAME
Destination Mac Address	MACADDR
Device Address	Requester IP
Device Custom String 1	Display Field
Device Custom String 2	Path 1
Device Custom String 3	Path 2
Device Custom String 4	Path 3
Device Mac Address	Requester Mac
Device Product	'Retina Network Security Scanner'
Device Receipt Time	dtsScanEnd (yyyy-MM-dd HH:mm:ss)
Device Severity	Risk
Device Vendor	'eEye'
Name	Vulnerability

eEye Retina Open Ports Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Application Protocol	Display Field
ArcSight Severity - High	evice Severity = 7, 8, or 9
ArcSight Severity - Low	Device Severity = 1, 2, or 3
ArcSight Severity - Medium	Device Severity = 4, 5, or 6
Category Technique	Open Ports
Destination Address	IP
Destination Host Name	HOSTNAME
Destination Mac Address	MACADDR

ArcSight ESM Field	Device-Specific Field
Destination Port	TCP or UDP
Device Address	Requester IP
Device Event Category	Open Ports
Device Mac Address	Requester Mac
Device Product	'Retina Network Security Scanner'
Device Receipt Time	dtsScanEnd (yyyy-MM-dd HH:mm:ss)
Device Vendor	'eEye'
File Path	Asset category URI
Name	Open Ports
Transport Protocol	TCP or UDP

eEye Retina Operating System URI Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Category Technique	URI
Destination Address	IP
Destination Host Name	HOSTNAME
Destination Mac Address	MACADDR
Device Address	Requester IP
Device Custom String 1	Value Field
Device Mac Address	Requester Mac
Device Product	'Retina Network Security Scanner'
Device Receipt Time	dtsScanEnd (yyyy-MM-dd HH:mm:ss)
Device Vendor	'eEye'
File Path	Asset category URI for the operating system
Name	Operating System

Troubleshooting

"What do I do when the connector can't reconnect to the MS SQL Server database?"

In some cases, connectors using MS SQL Server databases are unable to reconnect to the database after losing and reacquiring network connection. Restarting the connector will resolve this problem.

"How do I deploy SQL Server Native Client?"

When deploying an application that is dependent on SQL Server Native Client, you will need to redistribute SQL Server Native Client with your application. Unlike Microsoft Data Access Components (MDAC), which is now a component of the operating system, SQL Server Native Client is a component of SQL Server. Therefore, it is important to install SQL Server Native Client in your development environment and redistribute SQL Server Native Client with your application.

The SQL Server Native Client redistributable installation program, named sqlncli.msi, is available on the SQL Server installation media and is available as one of the SQL Server Feature Pack components on

the Microsoft Download site. For more information about deploying SQL Server Native Client with your application, see "Deploying Applications with SQL Server Native Client" available from Microsoft.

"Why does my connection to SQL Server fail/hang?"

Oracle has released Java 6 update 30 (6u30) that behaves differently from JRE 6u29, causing possible database connection problems for SQL Server database connectors using JDBC connection. These connection problems can occur with JRE 1.6.0_29 (6u29) and later versions.

Microsoft recommends using JRE 6u30 (and above) instead of JRE 6u29. Apply the "SQL Server 2008 R2 Service Pack 1 Cumulative Update 6" patch to the SQL server if you are experiencing connection failures or hangs.

"Why am I receiving the message 'Login failed for user 'sqluser'. The user is not associated with a trusted SQL Server connection."

Only Microsoft JDBC driver v4 or later support integrated authentication. The driver also does not provide function to supply Windows authentication credentials such as user name and password. In such cases, the applications must use SQL Server Authentication. When installing the connector on a non-Windows platform, configure the Microsoft SQL Server for Mixed Mode Authentication or SQL Server Authentication.

"How can I keep the connector from becoming clogged with events after being shut down for awhile?"

If the connector is shut down for some time on an active database, a lot of events can accumulate that can clog the connector on restart. The `preservestate` parameter can be used to avoid this situation. This parameter is enabled (true) by default. Setting `preservestate` to disabled (false) in the `agent.properties` file allows the connector to skip the old events and start from real time. The `agent.properties` file is located in the `$ARCSIGHT_HOME\current\user\agent` folder. Restart the connector for your change to take effect.

"What do I do when I receive "Connector parameters did not pass the verification with error ..." message?"

You may not have the correct version of jar file. When you download the JDBC driver, the version of the jar file depends on the version of JRE the Connector uses. Versions 7.1.2 and later use JRE 1.7 and require sqljdbc41.jar. Prior versions of the connector that run JRE 1.6 require sqljdbc4.jar.