Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

Configuration Guide for Oracle Unified Audit Trail DB SmartConnector

Document Release Date: February 2022
Software Release Date: February 2022

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

Configuration Guide for Oracle Unified Audit Trail DB SmartConnector

Configuration Guide for Oracle Unified Audit Trail DB SmartConnector

This guide provides information for installing the SmartConnector for Oracle Unified Audit Trail DB and configuring the device for event collection.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight SmartConnectors.

Additional Documentation

The ArcSight SmartConnectors documentation library includes the following resources:

- *Installation Guide for ArcSight SmartConnectors*, which provides detailed information about installing SmartConnectors.
- *Configuration Guides for ArcSight SmartConnectors*, which provides information about configuring SmartConnectors to collect events from different sources.
- *Release Notes for ArcSight SmartConnectors*, which provides information about the latest release

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the documentation site for ArcSight SmartConnectors.

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com.

For specific product issues, contact Micro Focus Customer Care.

Product Overview

In previous releases of Oracle Database, there were separate audit trails for individual components. With Oracle 12c, these are unified into one audit trail, which are viewable from the UNIFIED_AUDIT_TRAIL data dictionary view for single-instance installations or Oracle Database Real Application Clusters environments.

With Unified Auditing and Conditional Auditing, you can configure context-dependent logging to reduce performance overhead and enable more effective analysis of audit logs.

- Conditional Auditing logging policies can minimize log entries to specific events, such as particular SQL statements that include CREATE or ALTER actions that originate from outside specific application servers.
- Unified Auditing lets you run analysis reports on an entire set of audit data in one operation. With a unified audit trail, the audit information is consistently formatted and contains consistent fields.

Configuration

For complete information about Oracle database auditing, see the following topics in the Oracle Database Online Documentation 12c Release 1 *Database Security Guide:*

- "Introduction to Auditing" (https://docs.oracle.com/database/121/DBSEG/auditing.htm#DBSEG1023)
- "Configuring Audit Policies" (https://docs.oracle.com/database/121/DBSEG/audit_config.htm#DBSEG1025

Oracle 8i: Connector Upgrade

With the addition of Oracle 11g support, ArcSight replaced the 10.2.0.1 oracle-jdbc driver in $ARCSIGHT_HOME\current\lib\agent with the oracle-jdbc-11.1.0.6.jar. This driver no longer connects to Oracle 8i databases.

Make sure you do the following, before upgrading the connector:

- Go to $ARCSIGHT_HOME\Current\lib\agent and locate the oracle-jdbc-10.2.0.1.jar file. Copy it to a temporary location.
- After completing connector upgrade and before running the connector, replace the 11.1.0.6.jar file with the 10.2.0.1.jar file.

Installing the SmartConnector

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

Preparing to Install the SmartConnector

Before you install any SmartConnectors, make sure that the Micro Focus ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on ArcSight Documentation.

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on ArcSight Documentation for instructions.

Before installing the SmartConnector, make sure that the following are available:

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

Installing and Configuring the SmartConnector

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant Global Parameters, when prompted.
4. Select **Oracle Unified Audit Trail DB** from the Type drop-down, then click **Next**.
5. Enter the following SmartConnector parameters, then click **Next**.

Parameter	Description
JDBC/ODBC Driver	Select a JDBC Database driver from the drop-down list or accept the default value. The default Oracle JDBC driver provided works with Oracle 9i, 10g, 11g and 12c database versions. If you are using Oracle 8i, see Oracle 8i: Connector Upgrade.
Periodically Change Passwords	Select true to periodically change the password after logging in to the database. The default value is false.

Parameter	Description
Password Changing Interval (in seconds)	If periodically change passwords is set to true, specify the interval at which the password needs to be changed. The default value is 86400 seconds (24 hours).
Desired Length for Generated Passwords	Specify the desired password length for generated passwords or accept the default value of 16.
SSL Connection	Default is 'false'. Change to 'true' for TCPS.
SSL TrustStore Path	Enter the absolute path for the truststore file.
SSL TrustStore Type	Select either JKS (default) or PKCS12 as needed.
SSL TrustStore Password	Enter password for the truststore.
SSL KeyStore Path	Enter the absolute path for the keystore file.
SSL KeyStore Type	Select either JKS (default) or PKCS12 as needed.
SSL KeyStore Password	Enter password for the keystore.

6. Click **Add**, then specify the following information:

Parameter	Description
URL	Enter the URL for the Oracle Database instance being audited in this field starting with the following URL template: jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=<HostName>)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=<sid>))). For example: 'jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS= (PROTOCOL=TCP) (HOST=x.x.x.x or hostname) (PORT=1521)) (CONNECT_DATA= (SERVICE_ NAME=xxxx)))'
User	Enter the name of an Oracle database user having access the database instance.
Password	Enter the password for the Oracle database user.
Frequency	Enter how often, in seconds, the is to poll the Oracle database. The default value is 5.

7. To add more databases, click **Add** and specify the parameters.
8. Click **Export** to export the hoe.st name data you have entered into the table into a CSV file.

9. Click **Import** to select a CSV file to import into the table rather than add the data manually.
10. Select a destination and configure parameters.
11. Specify a name for the connector.
12. If you have selected ArcSight Manager as the destination, 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.
13. Select whether you want to run the connector as a service or in the standalone mode.
14. Complete the installation.
15. Run the SmartConnector.

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

Configuring Start at Date

When you want the connector to start at specific timestamps, the connector requires two timestamps as bind variables; therefore, two values for `startatdate` should be defined. To do this, before running the SmartConnector, open the `agent.properties` file (located at `$ARCSIGHT_HOME\current\user\agent`), and add a second value to the `startatdate` variable as shown in the following example.

For example, change:

```
agents[0].oracledatabases[0].startatdate=04/22/2011 14:40:40
```

to:

```
 agents[0].oracledatabases[0].startatdate=04/22/2011 14:40:40,04/22/2011
14:40:40
```

Save your changes.

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.

Oracle Unified Audit Trail 12c Database Field Mappings

ArcSight ESM Field	Device-Specific Field
Destination Address	One of(Extract from COMMENT_TEXT,HOST)
Destination Host Name	HOST_NAME
Destination Port	_DB_PORT
Destination User Name	One of (USERNAME, TARGET_USER)
Destination User Privileges	One of (USED_PRIVILEGE, PRIVILEGE)
Device Action	ACTION_NAME
Device Address	One of(Extract from COMMENT_TEXT, HOST)
Device Custom Floating Point 1	SID (Session ID)
Device Custom Number 1	INSTANCEID
Device Custom Number 2	ERROR_CODE
Device Custom Number 3	ENTRYID
Device Custom String 1	COMMENT_TEXT
Device Custom String 2	GRANTEE (Privilege)
Device Custom String 3	POLICIES
Device Custom String 4	_DB_URL
Device Custom String 5	ACTION_OBJECT_NAME
Device Custom String 6	RULE_SET_NAME
Device Event Category	AUDIT_TYPE
Device Event Class ID	One of (ACTION, '|', RETURN_CODE)
Device External ID	_DB_NAME

ArcSight ESM Field	Device-Specific Field
Device Host Name	_DB_HOST
Device Process Name	OS_PROCESS
Device Product	'Unified Audit Trail'
Device Vendor	'Oracle'
Device Version	VERSION
File ID	SQL_BINDS
File Name	All of (SCHEMA, OBJECT_NAME)
Message	One of (SQL_TEXT, DV_COMMENT)
Name	ACTION_NAME
Old File Hash	__concatenate(DBID,_DB_PORT,_DB_DRIVER)
Old File Name	All of (DBID, _DB_PORT, _DB_DRIVER)
Old File Path	COMMENT_TEXT
Reason	RETURN_CODE
Request Client Application	CLIENT_PROGRAM_NAME
Source Address	One of(Extract from COMMENT_TEXT,HOST)
Source Host Name	One of(Extract from COMMENT_TEXT,USERHOST)
Source Port	One of(Extract from COMMENT_TEXT, Extract from AUTHENTICATION_ TYPE)
Source Service Name	TERMINAL
Source User Name	OS_USERNAME
Transport Protocol	One of(Extract from COMMENT_TEXT, Extract from AUTHENTICATION_ TYPE)

Troubleshooting

Can I use JDBC with SSL to make a connection using TCPS protocol?

First, in the connector installation parameters screen, set the SSL connection to 'true'. Then, set other SSL-related parameters accordingly, including the truststore and keystore paths, types, and passwords. That information is available from your DB administrator.

Next, on the connector side, you need to add the connection URL with parameters:

jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=**TCPS**)(HOST=<server>)(PORT=<port>))(CONNECT_DATA=(SERVICE_NAME=<sid>)))

Note that in the DB connection URL, the value for PROTOCOL changes from 'TCP' to 'TCPS'.

You will also need to configure the connection on database server. Refer to Oracle documentation for information about that side of the connection.

I receive an SSL v3 error message when setting up the connector.

After entering the database connection information for TCPS in the Device Details screen, an error message might occur if your database connection uses the SSL v3 protocol. It will say: "Server chose SSL v3, but that protocol version is not enabled or supported by the client." This error message occurs because Oracle, for security reason, does not recommend using SSL v3.

Microfocus ArcSight does not recommend configuring your server to use SSLv3. If SSLv3 is required, enable SSLv3 in the connector JRE. Go to current\jre\lib\security, edit java.security, and comment out the line: `jdk.tls.disabledAlgorithms=SSLv3`

I receive Oracle error messages associated with a parser.

The connector parser oracle_unified_audit_trail.sdktbdatabase.properties results in Oracle errors:

- ORA-00942
- ORA-22835

To fix the ORA-00942 error:

- Grant read access on `sys.unified_audit_trails` to arcsight
- Grant select on `sys.all_audited_system_actions` to arcsight

To fix ORA-22835 (to limit the text fields size to 4000), the Oracle admin must add the two lines shown below to the following query:

```
SUBSTR(SQL_BINDS,1,4000) AS SQL_BINDS,

SUBSTR(SQL_TEXT,1,4000) AS SQL_TEXT,
```

The changes are shown in bold below.

```
CREATE OR REPLACE VIEW ARCSIGHT.UNIFIED_AUDIT_TRAIL
 AS SELECT
 ACTION_NAME, ADDITIONAL_INFO, APPLICATION_CONTEXTS,
   AUDIT_OPTION, AUDIT_TYPE, AUTHENTICATION_TYPE,
   CLIENT_IDENTIFIER, CLIENT_PROGRAM_NAME, DBID,
   .
   (Lines deleted for brevity)
   .
   RMAN_SESSION_STAMP, ROLE, SCN,
   SESSIONID,
   SUBSTR(SQL_BINDS,1,4000) AS SQL_BINDS,
   SUBSTR(SQL_TEXT,1,4000) AS SQL_TEXT,
   STATEMENT_ID, SYSTEM_PRIVILEGE, SYSTEM_PRIVILEGE_USED,
   TARGET_USER, TERMINAL, TRANSACTION_ID,
   .
   (Lines deleted for brevity)
   .
   XS_USER_NAME
FROM SYS.UNIFIED_AUDIT_TRAIL;
```

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Configuration Guide for Oracle Unified Audit Trail DB SmartConnector (SmartConnectors 8.3.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Documentation-Feedback@microfocus.com.

We appreciate your feedback!