Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

Configuration Guide for Oracle Audit Vault 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 Audit Vault DB SmartConnector

Configuration Guide for Oracle Audit Vault DB SmartConnector

This guide provides information for installing the SmartConnector for Oracle Audit Vault 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

Oracle Audit Vault is an enterprise-wide audit solution that consolidates, detects, monitors, alerts, and reports on audit data for security auditing and compliance. Oracle Audit Vault consolidates audit data and critical events into a centralized and secure audit warehouse.

Configuration

For complete information about Oracle Audit Vault, see the *Oracle Audit Vault Administrator's Guide* and the *Oracle Audit Vault Auditor's Guide*. The *Oracle Audit Vault Auditor's Guide* explains how Oracle Audit Vault auditors can use the Audit Vault Console to audit data in Oracle and Microsoft SQL Server databases. The *Oracle Audit Vault Administrator's Guide* provides usage information for Audit Vault administrators who perform administrative tasks on an Audit Vault system.

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:

1. Go to $ARCSIGHT_HOME\Current\lib\agent and locate the oracle-jdbc-10.2.0.1.jar file. Copy it to a temporary location.
2. 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 Connector

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. Exit the installation wizard.
4. Select **Oracle Audit Vault DB** from the Type drop-down, then click **Next**
5. Enter the following SmartConnector parameters, then click **Next**.

Parameter	Description
Oracle Audit Vault JDBC 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 8i, 10g, and 11g database versions. If you are using Oracle 8i, see "Oracle 8i: Connector Upgrade" in the Configuration section of this guide.

Parameter	Description
Oracle Audit Vault Database URL	Enter the URL for the Oracle Database instance being audited in this field (for example, 'jdbc:oracle:thin:@<hostname>:<port>:<sid>').
	You can connect to a database in an RAC setup, using 'jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP) (SERVICE_NAME=DATABASE_SERVICENAME)))'. For example:
	'jdbc:oracle:thin:@(DESCRIPTION= (ADDRESS LIST= (ADDRESS= (PROTOCOL=TCP) (HOST=x.x.x.x) (PORT=1521))) (CONNECT_DATA= (SERVICE_NAME=xxxx) (SERVER=DEDICATED)))'
Oracle Audit Vault Database User	Enter the name of an Oracle database user having access to the database instance.
Oracle Audit Vault Database Password	Enter the password for the Oracle Audit Vault database user.

6. Select a destination and configure parameters.
7. Specify a name for the connector.
8. 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.
9. Select whether you want to run the connector as a service or in the standalone mode.
10. Complete the installation.
11. Run the SmartConnector.

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

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 Audit Vault DB Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Connector Severity	High = 2; Medium = 1
Destination Address	SOURCE_HOSTIP
Destination Host Name	SOURCE_HOST
Destination User Name	USERNAME
Device Custom Date 1	ALERTTIME
Device Custom Number 1	PROCESS#
Device Custom Number 2	EVENT_STATUS
Device Custom String 1	ALERTNAME
Device Custom String 2	SOURCE_NAME
Device Custom String 3	TARGET_OWNER
Device Custom String 4	_DB_URL
Device Custom String 5	OSUSER_NAME
Device Custom String 6	ALERTRULE
Device Event Class ID	All of (EVENT_ID,'|', EVENT_STATUS)
Device Host Name	_DB_HOST
Device Product	'Audit Vault'
Device Receipt Time	AVTIME
Device Severity	ALERT_SEVERITY
Device Vendor	'Oracle'
External ID	ALERT_SEQUENCE

ArcSight ESM Field	Device-Specific Field
File Name	TARGET_OBJECT
Message	One of (ALERTDESC, EVENTDESC)
Name	EVENT_NAME
Source Address	CLIENT_HOSTIP
Source Host Name	CLIENT_HOST

Oracle Audit Vault DB 12.2.x Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Destination Address	HOST_IP
Destination Host Name	HOST_NAME
Destination User Name	TARGET_OWNER
Device Action	ACTION_TAKEN
Device Custom Date 1	ALERTTIME
Device Custom Number 1	ALERT_RAISED;
Device Custom Number 2	MONITORING_POINT_ID
Device Custom String 1	ALERT_NAME
Device Custom String 2	SECURED_TARGET_NAME
Device Custom String 3	SECURED_TARGET_TYPE
Device Custom String 4	THREAT_SEVERITY
Device Custom String 5	POLICY_NAME
Device Custom String 6	ALERT_RULE
Device Event Category	LOG_CAUSE
Device Event Class ID	(EVENT_NAME,"|",EVENT_STATUS)
Device Host Name	_DB_HOST
Device Product	Audit Vault and Database Firewall
Device Receipt Time	AV_ALERT_TIMESTAMP
Device Severity	ALERT_SEVERITY

ArcSight ESM Field	Device-Specific Field
Device Vendor	Oracle
Event Outcome	EVENT_STATUS
File Name	TARGET_OBJECT
File Type	TARGET_TYPE
Message	(DESCRIPTION,"|",ERROR_MESSAGE)
Name	EVENT_NAME
Reason	ERROR_CODE
Request Client Application	CLIENT_PROGRAM
Request Context	COMMAND_PARAM
Request Cookies	_DB_URL
Request Method	COMMAND_CLASS
Request Url	COMMAND_TEXT
Source User Privileges	USER_NAME
Start Time	EVENT_TIME

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 Audit Vault 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!