Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

Configuration Guide for Oracle SYSDBA Audit Multiple Folder 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 SYSDBA Audit Multiple Folder SmartConnector

Configuration Guide for Oracle SYSDBA Audit Multiple Folder SmartConnector

This guide provides information for installing the SmartConnector for Oracle SYSDBA Audit Multiple Folder and configuring the device for event collection. Event collection from Windows platforms is not supported.

Because the Oracle database does not allow the destination for audit file output to be configured in Windows (this output is sent to the Windows Event Log), this SmartConnector is not supported for installation on Windows operating systems. Use the SmartConnector to collect Oracle Audit events from Windows systems.

This SmartConnectors also logs SYSDBA login/logout behavior; the SmartConnector for Oracle Audit DB does not.

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

For complete information about Oracle database auditing, see the *Oracle Database Security Guide* for your database version.

Configuration

Oracle Auditing

ArcSight SmartConnectors support the following types of auditing:

- Standard auditing
- Administrator auditing

Standard Auditing

Use standard auditing for SQL statements, privileges, schemas, objects, and network and multi-tier activity. Standard audit records are written to either of the following locations:

SYS.AUD$ system table: You can view the contents of this table by querying the DBA_ AUDIT_TRAIL data dictionary view, or the DBA_COMMON_AUDIT_TRAIL view.

Operating System files: The AUDIT_TRAIL initialization parameter controls how standard audit trail records are written.

Administrator Auditing

On UNIX systems, you can monitor the activities of system administrators (user SYS, and users connecting with the SYSDBA or SYSOPER privilege) by using the Syslog Audit Trail, in addition to the Operating System Audit Trail. Syslog is another destination audit trail, similar to operating system files, XML format files, and database tables.

To control how administrator audit files are written, set the following initialization parameters:

AUDIT_SYS_OPERATIONS parameter: Enables or disables administrator auditing. Setting it to TRUE records system administrator activities in the operating system file that contains the audit trail.

AUDIT_SYSLOG_LEVEL parameter: When the AUDIT_TRAIL parameter is set to OS, writes SYS and standard operating system audit records to the system audit log using the syslog utility.

Activities Always Audited

Regardless of whether database auditing is enabled, Oracle Database *always* audits certain database-related operations and writes them to the operating system audit file. The operating system audit file captures the complete archived messages for these types of activities. This includes the following operations:

- **Administrative privilege connections to the database instance:** An audit record is generated that lists the operating system user connecting to Oracle Database as SYSOPER or SYSDBA. This provides for accountability of users with administrative privileges.
- **Database startup:** An audit record is generated that lists the operating system user starting the instance, the user terminal identifier, and the date-and-time stamp. This data is stored in the Operating System Audit Trail because the Database Audit Trail is not available until after the startup has successfully completed.
- **Database shutdown:** An audit record is generated that lists the operating system user shutting down the instance, the user terminal identifier, and the date-and-time stamp. You can set the location of this file by using the AUDIT_FILE_DEST initialization parameter.

Audit Trails

Standard Audit Trail

In standard auditing, SQL statements, privileges, schema objects, and network activity are audited. Audit the objects in your own schemas using the AUDIT statement. To disable auditing of an object, use the NOAUDIT statement. No additional privileges are needed to perform this task. Users can run AUDIT statements to set auditing options regardless of the AUDIT_TRAIL parameter setting. If auditing has been disabled, the next time it is enabled, Oracle Database will record the auditing activities set by the AUDIT statements.

Note the following:

- To audit objects in another schema, the `AUDIT ANY` system privilege is required.
- To audit system privileges, the `AUDIT SYSTEM` privilege is required.

- If the O7_DICTIONARY_ACCESSIBILITY initialization parameter has been set to FALSE (the default), only users who have the SYSDBA privilege can audit objects in the SYS schema.

Operating System Audit Trail

As an alternative to creating standard audit records in the DBA_AUDIT_TRAIL (SYS.AUD$ table), you can create standard audit records in operating system files.

You can direct audit trail records to an operating system audit trail if the operating system makes an audit trail available to Oracle Database. If not, then Oracle Database writes the audit records to a file outside the database. The target directory varies by platform. On most UNIX platforms, it is $ORACLE_BASE/admin/$DB_UNIQUE_NAME/adump, but for other platforms, check the platform documentation to learn the correct target directory.

Use the AUDIT_FILE_DEST initialization parameter to specify an operating system directory into which the audit trail is written, when the AUDIT_TRAIL initialization parameter is set to OS or to XML. You must set AUDIT_FILE_DEST to a valid directory with permissions restricted to the owner of the Oracle software and the DBA group. Mandatory auditing information also goes into that directory, as do audit records for user SYS if the AUDIT_SYS_OPERATIONS initialization parameter is specified. Change AUDIT_FILE_DEST using the following ALTER SYSTEM statement, which enables the new destination to be effective for all subsequent sessions.

```
ALTER SYSTEM SET AUDIT_FILE_DEST = directory_path DEFERRED;
```

If you do not set the AUDIT_FILE_DEST parameter, Oracle Database places the file in the following default locations:

- **Linux and Solaris:** $ORACLE_BASE/admin/$DB_UNIQUE_NAME/adump

  For example:

  /opt/oracle/app/oracle/admin/orcl/adump

Notes:

- If your operating system supports an audit trail, then its location is operating system-specific. On most UNIX platforms, it is $ORACLE_BASE/admin/$DB_UNIQUE_NAME/adump, but for other platforms, check the platform documentation to learn the correct target directory.
- When the AUDIT_TRAIL initialization parameter is set to XML (or XML,EXTENDED), Oracle Database writes audit records to XML-formatted operating system files. The XML-

format audit records are written to the directory specified by the `AUDIT_FILE_DEST` parameter on all platforms.

Syslog Audit Trail

A potential security vulnerability for an operating system audit trail is that a privileged user, such as a database administrator, can modify or delete database audit records. To minimize this risk, you can audit the activities of system administrators by creating a Syslog Audit Trail.

Syslog is a standard protocol on UNIX-based systems for logging information from different components of a network. Applications call the syslog function to log information to the syslog daemon, which then determines where to log the information. You can configure syslog to log information to a file name `syslog.conf`, to the console, or to a remote, dedicated log host.

Because applications, such as an Oracle process, use the syslog function to log information to the syslog daemon, a privileged user would not have permissions to the file system where syslog messages are logged. For this reason, audit records stored using a Syslog Audit Trail can be more secure than audit records stored using an Operating System Audit Trail.

In addition to restricting permissions to a file system for a privileged user, for a Syslog Audit Trail to be secure, neither privileged users nor the Oracle process should have `root` access to the system where the audit records are written.

Enabling Auditing of Administrative Users

Use the AUDIT_SYS_OPERATIONS initialization parameter to specify whether all users connecting as SYSDBA or SYSOPER are to be audited. For example, the following setting specifies that SYS is to be audited:

```
AUDIT_SYS_OPERATIONS = TRUE
```

The default value, FALSE, disables SYS auditing.

All audit records for SYS are written to the operating system file that contains the audit trail, and not to SYS.AUD$ (also viewable as DBA_AUDIT_TRAIL).

For Solaris, if the AUDIT_FILE_DEST parameter is not specified, the default location is `$ORACLE_HOME/rdbms/audit`.

For other operating systems, see their audit trail documentation.

All SYS-issued SQL statements are audited indiscriminately and regardless of the setting of the AUDIT_TRAIL initialization parameter.

Consider the following SYS session:

```
CONNECT / AS SYSDBA;
 ALTER SYSTEM FLUSH SHARED_POOL;
 UPDATE salary SET base=1000 WHERE name='myname';
```

When SYS auditing is enabled, both the ALTER SYSTEM and UPDATE statements are displayed in the operating system audit file as follows:

```
Thu Jan 24 12:58:00 2002
 ACTION: 'CONNECT'
 DATABASE USER: '/'
 OSPRIV: SYSDBA
 CLIENT USER: jeff
 CLIENT TERMINAL: pts/2
 STATUS: 0

 Thu Jan 24 12:58:00 2002
 ACTION: 'alter system flush shared_pool'
 DATABASE USER: ''
 OSPRIV: SYSDBA
 CLIENT USER: jeff
 CLIENT TERMINAL: pts/2
 STATUS: 0

 Thu Jan 24 12:58:00 2002
 ACTION: 'update salary set base=1000 where name='myname''
 DATABASE USER: ''
 OSPRIV: SYSDBA
 CLIENT USER: jeff
 CLIENT TERMINAL: pts/2
 STATUS: 0
```

Installing the SmartConnector

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

Use OS user **oracle** to install the SmartConnector for correct file permissions to be established.

Connector Appliance/ArcSight Management Center supports mounting for Network File System (NFS) and CIFS (Windows) shares. When you install this connector on one of these devices, establish a CIFS mount on the device before adding the connector. Provide this share name during connector configuration. For more information, see **Remote File Systems** in the Connector Appliance or ArcSight Management Center Administrator's Guide.

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 SYSDBA Audit Multiple Folder** from the **Type** drop-down, then click **Next**.
5. Click **Add**, enter the following SmartConnector parameters, then click **Next**.

Parameter	Description
Folder	Path to and name of the folder containing the Oracle SYSDBA audit logs.
Mode	Select the processing mode: 'batch' or 'realtime'. The default mode is 'realtime.' See "Batch vs. Realtime Mode" for more information.
Encoding	Enter the type of character set encoding used in the audit logs. For example, UTF-8 (8-bit UCS transformation format), UTF-16 (16-bit UCS transformation format)... If this field is left empty, the connector assumes the audit logs are in the default encoding determined by the operating system and locale settings.
Fields	What you specify for this parameter is extracted into the fields whose names you specify (the most common field being the ArcSight Device Host Name event field). When specifying more than one value, separate each field by a comma. When you enter values in this field, you also must enter corresponding Regex (regular expression) parameter values in the Regex field.
Regex	When you enter values for the Fields parameter, enter a regular expression (such as 'audit_(.*?)_\d+.AUD') to be used for extracting fields from the Log File Name. Using java simple date format to create date format file names, example log file names could be:
	audit_ORACLEINST1_20060225.AUD, audit_ORACLEINST2_20060226.AUD
	To extract Oracle Server instance names (which would be ORACLEINST1 and ORACLEINST2 in the sample file names) into the ArcSight deviceHostName event field, enter the expression 'audit_(.*?)_\d+.AUD'.
	Parentheses indicate the logical grouping of part of a regular expression. For each event field you specify for the "Event Fields" parameter, specify an equal number of groupings in the regular expression. (See "Regular Expressions" in the ArcSight FlexConnector Developer's Guide for more information about regular expressions.)
Source	Select the source from which fields are to be extracted (File Name or File Path).
	The following parameters are required for 'realtime' mode; they are used to query the remote Oracle database to determine the current audit files for live Oracle sessions.
Location	Select 'local' or 'remote'. When you select 'local', also fill in the Instance parameter. When you select 'remote', also fill in the URL, User, and Password parameters.
Instance	Enter the database instance in this field when you select 'local' in the Location parameter field.

Parameter	Description
URL	When you select 'remote' as the Location, enter the URL for the Oracle Database instance being audited in this field (for example, jdbc:oracle:thin:@<hostname>:<port>:<sid>). To connect to a database in an RAC setup, use: jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP) (SERVICE_NAME=DATABASE_SERVICENAME)))
User	When you select 'remote' as the Location, enter the name of an Oracle SYSDBA database user having access to the sys.v_$process table.
Password	When you select 'remote' as the Location, enter the password for the Oracle SYSDBA user.

6. In Multitenant Architecture, each PDB stores its logs in separate folders, add those folders here.
7. Click **Export** to export the host name data you have entered into the able into a CSV file.
8. Click **Import** to select a CSV file to import into the table rather than add the data manually.
9. Select a destination and configure parameters.
10. Specify a name for the connector.
11. 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.
12. Select whether you want to run the connector as a service or in the standalone mode.
13. Complete the installation.
14. 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 SYSDBA Audit Header Field Mappings

ArcSight ESM Field	Device-Specific Field
Action Number	Additional data
Additional Data	actionDetail
Additional Data	COMMENT_TEXT
Additional Data	LOGOFF_DEAD
Additional Data	LOGOFF_LREAD
Additional Data	LOGOFF_LWRITE
Additional Data	LOGOFF_PREAD
Additional Data	OBJ_CREATOR
Additional Data	SESSIONCPU
Additional Data	SES_TID
Additional Data	STATEMENT
Additional Data	USERHOST
Client Address	event.sourceAddress
Current_User	event.sourceUserPrivileges
Destination Host Name	Node name
Destination Process Name	Unix process pid
Destination User Name	One of (DATABASE USER, USERID)
Destination User Privileges	One of (PRIVILEGE, PRIV$USED)
Device Action	ACTION
Device Custom Floating Point 1	SESSIONID
Device Custom Number 1	STATUS

ArcSight ESM Field	Device-Specific Field
Device Custom Number 2	DBID
Device Custom Number 3	ENTRYID
Device Custom String 1	Oracle Home
Device Custom String 2	Log File
Device Custom String 3	Instance Name
Device Custom String 4	One of (OS Type | SES$LABEL)
Device Custom String 5	One of (OS Version | SES$ACTIONS)
Device Custom String 6	One of (Terminal | CLIENT TERMINAL)
Device Event Class Id	One of (ACTION, both (ACTION, RETURNCODE))
Device Host Name	Image
Device Process Name	Image
Device Product	'ORACLESYSDBA'
Device Receipt Time	timestamp
Device Vendor	'ORACLE'
Device Version	version
File Name	OBJ$NAME
Host	event.sourceAddress,event.deviceCustomIPv6Address2, extracted IP address from SES_LABEL (will auto map to Source Host Name)
Name	ACTION
Port	event.sourcePort
Protocol	event.transportProtocol
Reason	One of (STATUS | RETURNCODE)
Source Address	Source address
Source Host Name	One of (TERMINAL, CLIENT TERMINAL)
Source Service Name	CLIENT TERMINAL
Source User Name	One of (CLIENT USER, OS$USERID)

Troubleshooting

Why are portions of the raw event truncated?

Different UNIX operating systems implement the syslog() call in different ways. This results in Oracle audit records to be written in different formats. For raw audit events from Oracle with ACTION fields, the connector can parse only the first message into an ArcSight event. The truncated portions of the raw event will be missing.

Why use the OS user oracle to install this SmartConnector?

Only the Oracle user has permission to read the Oracle SYSDBA audit log file that is generated. If the Oracle user does the installation, you need not manually modify permissions.

Why do SmartConnector event files disappear after they are processed?

The SmartConnector for Oracle SYSDBA Audit moves processed event files to the backup folder, under the audit folder (by default, the folder name is **arcsight**) to keep the folder clean and to ensure that IDs are not duplicated. Because Oracle SYSDBA audit log naming is based upon the data obtained, a duplicate ID is possible over a long period of time, which would cause duplicate events to be sent to the ArcSight ESM Manager. Note that once the files are moved to the backup directory, the contents of the backup folder are no longer needed by the SmartConnector.

How is it possible to get an ora err code using the shutdown command, but still the status field is 0?

This behavior can be described as an Oracle bug. The status field does not always reflect the level. But if a remote login fails, you will get code 1017 in this field, which may be interesting to investigate.

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 SYSDBA Audit Multiple Folder 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!