Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

Configuration Guide for Oracle Audit Syslog 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

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Document Revision History

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

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.

To check for recent updates or to verify that you are using the most recent edition of a document, go to ArcSight Product Documentation Community on the Micro Focus Security Community.

Document Changes

Date	Product Version	Description
MM/DD/YYYY	X.X.X.X	Description of change

Contents

SmartConnector for Oracle Audit Syslog 6

Product Overview 7

Configuration 8

Oracle Auditing 8

Configuring Oracle DB Syslog Auditing 9

Configuring for the Syslog SmartConnectors 11

Installing the SmartConnector 14

Preparing to Install Connector 14

Installing and Configuring the SmartConnector 14

Device Event Mapping to ArcSight Fields 18

Oracle Audit SYSDBA Event Mappings to ArcSight ESM Fields 18

Oracle Audit Trail Event Mappings to ArcSight ESM Fields 19

Troubleshooting 21

Send Documentation Feedback 23

SmartConnector for Oracle Audit Syslog

SmartConnector syslog event collection is supported for Oracle database instances running on UNIX platforms only.

This guide provides information for installing the SmartConnector for Oracle Audit Syslog and configuring the device for syslog event collection.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector 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.
- *Configuration Guide for ArcSight SmartConnector Load Balancer*, which provides detailed information about installing Load Balancer.
- *Release Notes for ArcSight SmartConnectors and ArcSight SmartConnector Load Balancer*, 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

This connector is used to monitor auditing though the Syslog Audit Trail, available with Oracle Database versions 10.2 and later, and the Operating System Audit Trail. This guide provides information about the Syslog Audit Trail, Administrator Auditing, and configuring syslog auditing.

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

Note: None of the connector versions support Oracle Multitenancy at this time.

Configuration

Oracle Auditing

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. Syslog is another destination audit trail, similar to operating system files and database tables. On Windows, these activities are recorded in the Windows Event Log, along with other types of activities.

For both UNIX and Windows, 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.

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 the `syslog.conf` file to select the destination, where you want to log the information, whether to a console or to a remote dedicated host.

Note: In this document, the file names `syslog.conf` and `rsyslog.conf` indicate the same syslog configuration file based on the type of OS you are using. `rsyslog.conf` is the file name used in newer operating systems whereas `syslog.conf` is for older operating systems.

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.

Configuring Oracle DB Syslog Auditing

Note: SmartConnector syslog event collection is supported for Oracle database instances running on UNIX platforms only.

To enable syslog auditing, complete the following steps:

1. Switch to the `oracle` user.
2. Enter `sqlplus /nolog`.
3. Enter `connect / as sysdba`.
4. Enter `create pfile=<full_path_to_file.ora> FROM SPFILE="<full path to spfile>`.

   The `<full_path_to_file.ora>` is the location to which the `oracle` user has write access. (For example, `/home/oracle/new.ora`.)

5. Enter `shutdown`.
6. Enter `exit`.
7. Edit the file `full_path_to_file.ora` to add the following lines:

```
*.audit_sys_operations=TRUE
     *.audit_syslog_level='local1.warning'
     *.audit_trail='OS'
```

8. Switch to `root` user to add the audit file destination to the `syslog` configuration file `/etc/syslog.conf`.

   For example, assuming you had set the `AUDIT_SYSLOG_LEVEL` to `local1.warning`, enter the following:

   ```
   local1.warning /var/log/audit.log
   ```

   This setting logs all warning messages to the `/var/log/audit.log` file.
9. Restart the syslog logger:

   ```
   $/etc/rc.d/init.d/syslog restart
   ```

   Now, all audit records will be captured in the file `/var/log/audit.log` through the syslog daemon.
10. Switch back to the `oracle` user.
11. Enter `sqlplus /nolog`.
12. Enter `connect / as sysdba`.
13. **13** Enter `startup pfile=<full_path_to_file.ora>`.

    Note: The database is not started at this point. The startup pfile is being changed to point to the new file just created and modified. When the database is started, it will read the new parameters and send log messages to the local syslog.
14. To verify that the new parameter was set, enter `show parameter`. The `audit_trail` parameter now should be set to `OS`.
15. Enter `create spfile from pfile=<full_path_to_file.ora>`.
16. Enter `exit`.
17. Restart the database instance:

```
CONNECT SYS / AS SYSOPER
  Enter password: password
  Connected.
  SQL> SHUTDOWN;
  Database closed.
  Database dismounted.
  ORACLE instance shut down.
  SQL> STARTUP;
  ORACLE instance started.
```

Configuring for the Syslog SmartConnectors

The syslog SmartConnectors use a sub-connector architecture that lets them receive and process syslog events from multiple devices. There is a unique regular expression that identifies the device. For example, the same SmartConnector can process events from a Cisco Router and a NetScreen Firewall simultaneously. The SmartConnector inspects all incoming messages and automatically detects the type of device that originated the message.

You can install the syslog SmartConnector as a syslog daemon, pipe, or file connector. You can use the Syslog Deamon, Syslog Deamon NG, or Syslog File connector types depending on your requirement. The Syslog File type SmartConnectors also support Syslog Pipe.

Syslog Daemon SmartConnector

The Syslog Deamon SmartConnector is a syslogd-compatible daemon designed to work in operating systems that have no syslog daemon in their default configuration, such as Microsoft Windows. The SmartConnector for Syslog Daemon implements a UDP receiver on port 514 by default, or can be configured on another port to receive syslog events. You can also configure to use the TCP protocol.

To use the SmartConnector for Syslog Daemon, add the following statement in the *rsyslog.conf* file:

```
*.* @@(remote/local-host-IP):514
```

Example: `local1.warning @@10.0.0.1:514`

- To read all Syslog events, use *.*
- To filter specific events, replace regex with the specific event name.
- For example: *.* @@(remote/local-host-IP):514 and local1.warning @@10.0.0.1:514.
- To send events over a TCP connection, use @@ and to send events over an UDP connection, use @.

If you are running SmartConnector for Syslog Daemon on the same machine as the server, you must provide the IP address of the local host. If you want to forward events to other machines, you must provide the IP address of the same.

Messages longer than 1024 bytes might be split into multiple messages on syslog daemon. No such restriction exists on syslog file or pipe.

Syslog Pipe and File SmartConnectors

When a syslog daemon is already in place and configured to receive syslog messages, an extra line in the syslog configuration file *rsyslog.conf* can be added to write the events to either a file or a system pipe and the ArcSight SmartConnector can be configured to read the events from

it. In this scenario, the ArcSight SmartConnector runs on the same machine as the syslog daemon. The additional configurations for the ArcSight syslog file or syslog pipe SmartConnectors in the system where all Syslog Daemon SmartConnector configurations are done.

The Syslog Pipe SmartConnector is designed to work with an existing syslog daemon. This SmartConnector is especially useful when storage is a factor. In this case, syslogd is configured to write to a named pipe, and the Syslog Pipe SmartConnector reads from it to receive events.

The Syslog File SmartConnector is similar to the Pipe SmartConnector. However, this SmartConnector monitors events written to a syslog file such as messages.log rather than to a system pipe.

Using the SmartConnector for Syslog Pipe or File

This section provides information to set up your existing syslog infrastructure to send events to the ArcSight Syslog Pipe or File SmartConnector.

The standard UNIX implementation of a syslog daemon reads the configuration parameters from the /etc/rsyslog.conf file, which contains specific details about which events to write to files, write to pipes, or send to another host.

For Syslog Pipe:

1. Execute the following command to create a pipe:

   ```
   mkfifo /var/tmp/syspipe
   ```

2. Add one of the following lines depending on your OS to the */etc/rsyslog.conf* file:

   ```
   *.debug  /var/tmp/syspipe
   ```

   or

   ```
   *.debug  |/var/tmp/syspipe
   ```

3. Restart the syslog daemon in one of the following methods:
   Enter the following commands:

   ```
   /etc/init.d/syslogd stop
   /etc/init.d/syslogd start
   ```

   or

   Execute the following command to send a configuration restart signal:

   On RedHat Linux:

   ```
   service syslog restart
   ```

   On Solaris:

```
kill -HUP `cat /var/run/syslog.pid´
```

For Syslog File:

1. Create a file or use the default file into which log messages must be written.
2. Modify the /etc/rsyslog.conf file

   The syslog daemon is forced to reload the configuration and start writing to the pipe.
3. Restart the syslog daemon in one of the following methods:
   a. Restart the syslog daemon in one of the following methods:
   Enter the following commands:

   ```
   /etc/init.d/syslogd stop
   /etc/init.d/syslogd start
   ```

   or

   Execute the following command to send a configuration restart signal:

   On RedHat Linux:

   ```
   service syslog restart
   ```

   On Solaris:

   ```
   kill -HUP `cat /var/run/syslog.pid´
   ```

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. Do one of the following depending on your requirement:

- Select **Syslog Daemon** from the **Type** drop-down:
  a. Click **Next**, the specify the following paramenters:

Parameters	Description
Network port	The SmartConnector for Syslog Daemon listens for syslog events from this port.
IP Address	The SmartConnector for Syslog Daemon listens for syslog events only from this IP address, apart from the default (ALL) to bind to all available IP addresses.
Protocol	Specify whether to read files in batch mode or real-time mode. In batch mode, all files are read from the beginning.
Forwarder	This option applies to Batch Mode only. Specify **None**, **Rename**, or **Delete** as the action to be performed to the file when the connector finishes reading and reaches end of file . For the real-time mode, retain the default value **None**.

  b. **Click Next.**
- Select **Syslog File** from the **Type** drop-down:

a. Click **Next**, the specify the following paramenters:

Parameters	Description
Pipe Absolute Path Name	Specify an absolute path to the pipe, or accept the default value: `/var/tmp/syspipe`.
File Absolute Path Name	Specify the full path name for the file from which this connector will read events. The following are default values: • **Solaris:** `\var\adm\messages` • **Linux:** `\var\log\messages` You can use a wildcard pattern in the file name. In the real-time mode, rotation can occur only if the file is over-written or removed from the folder. The real-time processing mode assumes the following external rotation: • **Date format log rotation:** The device creates a new log at a specified time in the with the naming convention `filename.timestamp.log`. The connector detects the new log and terminates the reader thread to the previous log after the processing is complete. The connector then creates a new reader thread to the new `filename.timestamp.log` and begins processing that file. To enable this log rotation, specify timestap in `yyyy-MM-dd` date format. For example, `filename.yyyy-MM-dd.log` • **Index log rotation:** The device writes to indexed files in the following format: `filename.log.001, filename.log.002, filename.log.003`, and so on. At startup, the connector processes the log with highest index. When the device creates a log with a greater index, the connector terminates the reader thread to the previous log after processing completes, creates a thread to the new log, and begins processing that log. To enable this log rotation, use an index format, as shown in the following example:`filename'%d,1,99,true'.log;` Specifying `true` indicates that the index can be skipped. For example, if 5 appears before 4, processing proceeds with 5 and will not read 4. Use of `true` is optional.
Reading Events Real Time or Batch	Specify whether to read files in batch mode or real-time mode. In batch mode, all files are read from the beginning.
Action Upon Reaching EOF	This option applies to Batch Mode only. Specify **None**, **Rename**, or **Delete** as the action to be performed to the file when the connector finishes reading and reaches end of file . For the real-time mode, retain the default value **None**.
File Extension If Rename Action	This option applies to Batch Mode only. Specify the extension to be added to the file name if the action on reaching the end of file is specified as **Rename**. The default value is **Processed**, which adds a `.processed` extension.

b. Click **Next.**

5. Select a destination and configure parameters.
6. Specify a name for the connector.

7. 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.
8. Select whether you want to run the connector as a service or in the standalone mode.
9. Complete the installation.
10. 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 SYSDBA Event Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Additional data	AUTH GRANTEE
Destination Process Name	ProcessId
Destination User Name	DATABASE USER
Destination User Privileges	PRIVILEGE
Device Action	first word from ACTION
Device Custom Number 1	STATUS
Device Custom String 6	CLIENT TERMINAL
Device Event Class Id	first word of ACTION
Device External ID	DBID
Device Host Name	_SYSLOG_SENDER
Device Process Name	Process ID
Device Product	'ORACLESYSDBA'
Device Vendor	'ORACLE'
event.destinationHostName,event.destinationNtDomain	USERHOST
event.fileType	OBJ_PRIVILEGES
event.name,event.deviceAction,event.deviceEventClassId	ACTION NUMBER
event.sourceAddress,event.deviceCustomIPv6Address2, extracted IP address from SES_LABEL (will auto map to Source Host Name)	HOST
event.sourcePort	PORT
event.sourceUserPrivileges	CURRENT_USER
event.transportProtocol	PROTOCOL

ArcSight ESM Field	Device-Specific Field
Message	first word from ACTION
Name	first word from ACTION
Reason	STATUS
Source Host Name	CLIENT TERMINAL
Source User Name	CLIENT USER

Oracle Audit Trail Event Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Additional data	LOGOFF_DEAD
Additional data	LOGOFF_LREAD
Additional data	LOGOFF_LWRIT
Additional data	LOGOFF_PREAD
Additional data	OBJ_CREATOR
Additional data	SESSIONCPU
Additional data	SES_TID
Additional data	STATEMENT
Destination Process Name	ProcessId
Destination User Name	USERID
Destination User Privileges	PRIV_USED
Device Action	ACTION
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom Number 1	RETURNCODE
Device Custom Number 2	SESSIONID
Device Custom Number 3	ENTRYID
Device Custom String 1	COMMENT_TEXT
Device Custom String 2	TERMINAL
Device Custom String 4	SES_LABEL
Device Custom String 5	SES_ACTIONS
Device Event Class Id	ACTION

ArcSight ESM Field	Device-Specific Field
Device External ID	DBID
Device Host Name	_SYSLOG_SENDER
Device Product	'Oracle'
Device Severity	RETURNCODE
Device Vendor	'ORACLE'
File Name	Object name
Name	ACTION
Reason	RETURNCODE
Source Address	extracted IP address from SES_LABEL (will auto map to Source Host Name)
Source User Name	OS_USERID
USERHOST	event.destinationHostName,event.destinationNtDomain

Troubleshooting

Why does connection fail when using JDBC driver?

There is a known Oracle BUG:6051243 that causes our connectors to fail to establish a connection using the JDBC driver when the sqlnet.ora file contains the entry "SQLNET.ALLOWED>LOGON_VERSION=10." The workaround is to use =8 in the sqlnet.ora file, or download patch:67790.

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.

What is causing discrepancies in the audit output?

In some cases, an "action split" problem, which occurs when the field the query is auditing is being displayed in several fields rather than being displayed in one field, is being displayed in several fields. This exists in certain versions of Oracle. It was Oracle fixed this issue in their **audit log files** in newer versions; however, the problem still exists in **audit syslog** in all versions tested. Due to this issue, SmartConnectors for those versions of Oracle do not work.

The following table summarizes versions of Oracle in which our testing shows the action split problem can occur.

Operating System	Oracle DB Version	Audit Log File Action Field Split	Audit Syslog Action Field Split
Linux	10.2.0.1.0	Yes	Yes
Solaris	10.2.0.1.0	Yes	Yes
Linux	10.2.0.5.0	No	Yes
Solaris	10.2.0.5.0	No	Yes
Linux	11.2.0.1.0	No	Yes

How can some of the events generate Device External Id?

If some events are unable to generate Device External IDs, use any of the following methods to generate and re-upload them into ESM or CSV file:

- Get the events from ESM or CSV file which contains blank Device External IDs. Rerun the connector with these events.

- Add the following parameters from the `current/config/agent/agent.defaults.properties` file to the `current/user/agent/agent.properties` file:

```
dstprotector.count=1

dstprotector[0].field=deviceExternalId

dstprotector[0].alternatefield=deviceCustomString6

dstprotector[0].maxsize=100
```

This adds the Device External ID to Device Custom String 6 (DCS6), if it is not used, and sets the **maxsize** value received from Device External ID. You can modify the **maxsize** value as required.

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 Syslog 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!