Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Oracle Audit Syslog

Configuration Guide

April 17, 2017

Configuration Guide

SmartConnector for Oracle Audit Syslog

April 17, 2017

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
04/17/2017	Added mappings for Device Host Name.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
11/17/2015	Added information to Troubleshooting section.
05/15/2015	Added new parameters for Syslog File.
02/16/2015	Added parameter for Syslog Daemon connector configuration.
02/14/2014	Added support for Oracle 12cR1.
02/15/2013	Added mappings for IPv6.
12/21/2012	Added mapping for Reason field to STATUS for both SYSDBA and Audit Trail events.
08/15/2012	Added support for 11gR2
05/15/2012	Added new installation procedure; updated event mappings; added information regarding action split problem.

Contents

SmartConnector for Oracle Audit Syslog

This guide provides information for installing the SmartConnector for Oracle Audit Syslog and configuring the device for syslog event collection. Event collection from Oracle database versions 10g, 11g, 11gR2, and 12cR1 are supported.

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

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.

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 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.

Configuration

Configure Oracle DB Syslog Auditing

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

To enable syslog auditing, follow these 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 Enter `startup pfile=<full_path_to_file.ora>`.

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.
```

Configure the Syslog SmartConnectors

The three ArcSight Syslog SmartConnectors are:

Syslog Daemon
Syslog Pipe
Syslog File

The Syslog Daemon SmartConnector

The Syslog Daemon 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 (configurable) by default that can be used to receive syslog events. Use of the TCP protocol or a different port can be configured manually.

If you are using the SmartConnector for Syslog Daemon, simply start the connector, either as a service or as a process, to start receiving events; no further configuration is needed.

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

The 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 **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.

Configure the Syslog Pipe or File SmartConnector

This section provides information about how 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. First, create a pipe or a file; then modify the **/etc/rsyslog.conf** file to send events to it.

For syslog pipe:

1. Create a pipe by executing the following command:

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

2. Add the following line to your **/etc/rsyslog.conf** file:

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

   or

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

   depending on your operating system.

3. After you have modified the file, restart the syslog daemon either by executing the scripts **/etc/init.d/syslogd stop** and **/etc/init.d/syslogd start**, or by sending a `configuration restart` signal.

   On RedHat Linux, you would execute:

   ```
   service syslog restart
   ```

   On Solaris, you would execute:

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

   This command forces the syslog daemon to reload the configuration and start writing to the pipe you just created.

For syslog file:

Create a file or use the default for the file into which log messages are to be written.

After editing the `/etc/rsyslog.conf` file, be sure to restart the syslog daemon as described above.

When you follow the SmartConnector Installation Wizard, you will be prompted for the absolute path to the syslog file or pipe you created.

Install the SmartConnector

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

Syslog Installation

Install this SmartConnector (on the syslog server or servers identified in the *Configuration* section) using the SmartConnector Installation Wizard appropriate for your operating system. The wizard will guide you through the installation process. When prompted, select one of the following **Syslog** connectors (see *Configure the Syslog SmartConnectors* in this guide for more information):

Syslog Daemon
Syslog Pipe
Syslog File

Because all syslog SmartConnectors are sub-connectors of the main syslog SmartConnector, the name of the specific syslog SmartConnector you are installing is not required during installation.

The syslog daemon connector by default listens on port 514 (configurable) for UDP syslog events; you can configure the port number or use of the TCP protocol manually. The syslog pipe and syslog file connectors read events from a system pipe or file, respectively. Select the one that best fits your syslog infrastructure setup.

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).

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.

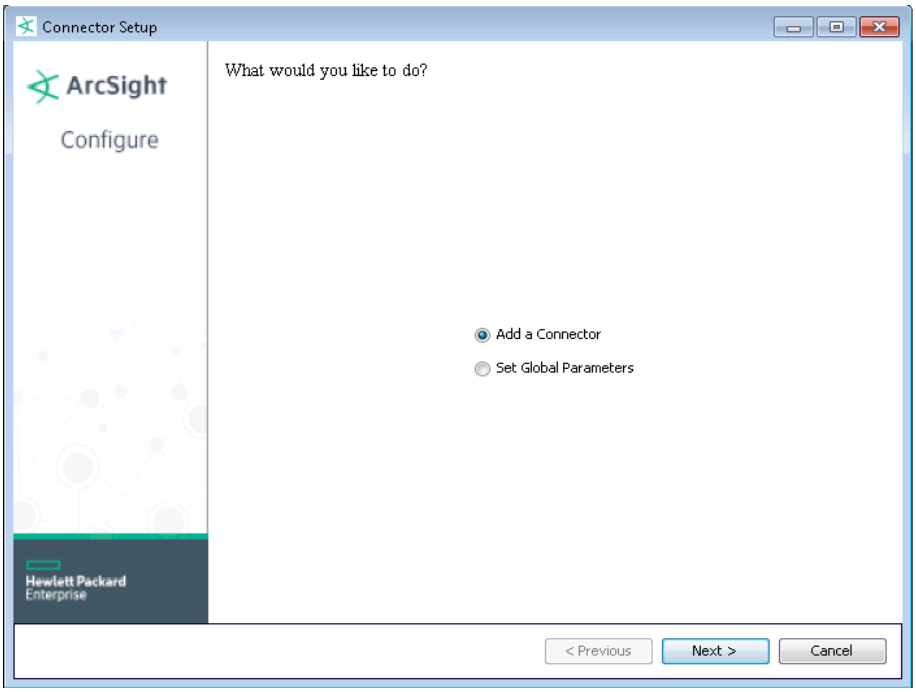
1. Download the SmartConnector executable for your operating system from the HPE SSO site.
2. Start the SmartConnector installation and configuration wizard by running the executable.

When installing a syslog daemon SmartConnector in a UNIX environment, run the executable as 'root' user.

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:



Set Global Parameters (optional)

If you choose to perform any of the operations shown in the following table, do so before adding your connector. 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 **Syslog Daemon, File, or Pipe** and click **Next**.

3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

Syslog Daemon Parameters	*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 (accept the default (ALL) to bind to all available IP addresses).
	Protocol	The SmartConnector for Syslog Daemon uses the selected protocol (UDP or Raw TCP) to receive incoming messages.
	Forwarder	Change this parameter to 'true' only if the events being processed are coming from another SmartConnector sending to a CEF Syslog destination, and that destination also has CEF forwarder mode enabled. That allows attributes of the original connector to be retained in the original agent fields.
Syslog Pipe Parameter	*Pipe Absolute Path Name*	Absolute path to the pipe, or accept the default: /var/tmp/syspipe

Syslog File Parameters	*File Absolute Path Name*	Enter the full path name for the file from which this connector will read events or accept the default: \var\adm\messages (Solaris) or \var\log\messages (Linux).
		A wildcard pattern can be used in the file name; however, in realtime mode, rotation can occur only if the file is over-written or removed from the folder. Realtime processing mode assumes following external rotation.
		For date format log rotation, the device writes to 'filename.timestamp.log' on a daily basis. At a specified time, the device creates a new daily log and begins to write to it. The connector detects the new log and terminates the reader thread to the previous log after 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, use a date format in the file name as shown in the following example:
		`filename'yyyy-MM-dd'.log;`
		For index log rotation, the device writes to indexed files - '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 it is allowed for the index to be skipped; for example, if 5 appears before 4, processing proceeds with 5 and will not read 4, even if 4 appears later. Use of 'true' is optional.

	Reading Events Real Time or Batch	Specify whether file is to be read in batch or realtime mode. For batch mode, all files are read from the beginning. The 'Action Upon Reaching EOF' and 'File Extension if Rename Action' parameters apply for batch mode only.
	Action Upon Reaching EOF	For batch mode, specify 'None', 'Rename', or 'Delete' as the action to be performed to the file when the connector has finished reading and reaches end of file (EOF). For realtime mode, leave the default value of 'None' for this parameter.
	File Extension If Rename Action	For batch mode, specify the extension to be added to the file name if the action upon EOF is 'Rename' or accept the default value of '.processed'.

Select a Destination

1 The next window asks for the destination type; select a destination and click **Next**. For information about the destinations listed, see the *ArcSight SmartConnector User Guide*.

2 Enter values for the destination. For the ArcSight Manager destination, the values you enter for **User** and **Password** should be 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 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.

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

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.

Oracle Audit SYSDBA Event Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
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'
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 Host Name	USERHOST
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

ArcSight ESM Field	Device-Specific Field
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
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

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.

OS	Oracle DB Version	Audit Log File Action Field Split	Audit Syslog Action Field Split
Linux	10.2.0.1.0	Yes	Yes

OS	Oracle DB Version	Audit Log File Action Field Split	Audit Syslog Action Field Split
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