Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Microsoft Windows Event Log – Unified: Oracle Audit

Supplemental Configuration Guide

November 15, 2013

Supplemental Configuration Guide

SmartConnector for Microsoft Windows Event Log – Unified: Oracle Audit

November 15, 2013

Warranty

Restricted Rights Legend

Revision History

Date	Description
11.15.2013	Added Oracle versions supported.
09/30.2013	Updated “Collect Events from the Event Log” procedure.
06/30/2012	First edition of this configuration guide.

Contents

SmartConnector for Microsoft Windows Event Log – Unified: Oracle Audit

This guide provides information about the SmartConnector for Microsoft Windows Event Log – Unified: Oracle Audit and its event mappings to ArcSight data fields. Oracle database versions 10g and 11g are supported.

The *ArcSight SmartConnector Mappings to Windows Security Events* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for the SmartConnector for Windows Event Log – Unified: Oracle Audit. .

Product Overview

Auditing is a default feature of the Oracle server. The standard audit commands allow all system privileges to be audited along with access at the object level to any table or view on the database for select, delete, insert or update. Audit can be run for either successful or unsuccessful attempts or both. It can be for each individual user or for all users, and it can also be done at the session level or access level. At action level a single record is created per action and at session level one record is created for all audit actions per session.

Configuration

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

Enable Auditing

Database auditing is enabled and disabled by the AUDIT_TRAIL initialization parameter in the database initialization parameter file, `init.ora`. Setting it to `OS` enables database auditing and directs all audit records to an operating system file:

```
AUDIT_TRAIL=OS
```

Audit Administrative Users

Sessions for users who connect as SYS can be fully audited, including all users connecting as SYSDBA or SYSOPER. Use the `AUDIT_SYS_OPERATIONS` initialization parameter to specify whether such users 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.

Connector Installation and Configuration

Follow the installation and configuration procedures in the *SmartConnector Configuration Guide for Microsoft Windows Event Log – Unified*, selecting **Microsoft Windows Event Log – Unified** as the connector to be configured. .

Collect Events from the Event Log

To set up the connector to collect application events:

1. From `$ARCSIGHT_HOME\current\bin`, double-click **runagentsetup.bat**.
2. Select **Modify Connector** on the window displayed and click **Next**.
3. Select **Modify connector parameters** and click **Next**.
4. Select Navigate to the **Modify table parameters** window.
5. To collect events from an application log, modify the **Application** field by selecting **true** for event collection in the Application field and enter **Oracle Audit** in the **Custom Log Names** field.

   You can specify multiple Custom Log Names in a comma-separated format; for example:

   `Oracle Audit, Exchange Auditing`
6. Click **Next** to update the parameters; when you receive the successful update message, click **Next**.
7. Select **Exit** and click **Next** to exit the configuration wizard.
8. Restart the connector for your changes to take effect.

For more information about application event support, see the *SmartConnector Configuration Guide for Microsoft Windows Event Log – Unified*.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See *ArcSight 101* for more information about the ArcSight data fields.

Oracle Windows Event Log Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Source Service Name	EventSource
Device Vendor	'Oracle'

Event ID 4

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Instance Name
Device Product	'Oracle'
Message	'Custom application information'
Name	'Initializing SGA for instance'

Event ID 5

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Instance Name
Device Product	'Oracle'
Message	'Custom application information'
Name	'Initializing SGA for process in instance'

Event ID 8

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Instance Name
Device Product	'Oracle'
Message	'Custom application information'
Name	'Shutdown normal performed on instance'

Event ID 12

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Instance Name
Device Product	'Oracle'
Message	'Custom application information'
Name	'All process in instance stopped'

Oracle Audit SYSDBA Event Mappings to ArcSight ESM Fields

Event ID 34

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 Product	'ORACLESYSDBA'
Device Vendor	'ORACLE'
Message	first word from ACTION
Name	first word from ACTION
Source Host Name	CLIENT TERMINAL
Source User Name	CLIENT USER

Oracle Audit Trail Event Mappings to ArcSight ESM Fields

Event ID 34

ArcSight ESM Field	Device-Specific Field
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

ArcSight ESM Field	Device-Specific Field
Destination Host Name	USERHOST
Destination NT Domain	USERHOST
Destination Process Name	ProcessId
Destination User Name	USERID
Destination User Privileges	PRIV_USED
Device Action	ACTION
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
Device External ID	DBID
Device Product	'Oracle'
Device Severity	RETURNCODE
Device Vendor	'ORACLE'
File Name	Object name
Name	ACTION
Source Address	extracted IP address from SES_LABEL (will auto map to Source Host Name)
Source NT Domain	OSSUSERID
Source User Name	OS_USERID