INTEGRIGY

WHITE PAPER

Integrigy Guide to Oracle Audit Vault

APRIL 2016

INTEGRIGY GUIDE TO ORACLE AUDIT VAULT

Version 1.0 – November 2014
Version 2.0 – April 2016

Authors: Michael A. Miller, CISSP, CISSP-ISSMP, CCSK and Stephen Kost

If you have any questions, comments, or suggestions regarding this document, please send them via e-mail to info@integrigy.com.

Table of Contents

ORACLE AUDIT VAULT

As the Oracle Audit Vault is a purpose built tool for Oracle Security log and audit monitoring, implementing Integrigy's Log and Audit Framework using the Oracle Audit Vault is straight forward. Before installing the Audit Vault, keep in mind that that Oracle Audit Vault is a separately licensed product.

AUDIT VAULT IS A VAULT

Oracle Audit Vault is aptly named; the Oracle Audit Vault is a vault in which data about audit logs is placed, and it is based on two key concepts. First, Oracle Audit Vault is designed to secure data at its source. Second, Oracle Audit Vault is designed to be a data warehouse for audit data.

The Oracle Audit Vault by itself does not generate audit data. Before the Oracle Audit Vault can be used, standard auditing needs to be first enabled in the source databases. Once auditing is enabled in the source databases, the Oracle Audit Vault collects the log and audit data, but does not replicate, copy and/or collect the actual data. This design premise of securing audit data at the source and not replicating it differentiates the Oracle Audit Vault from other centralized logging solutions.

Once log and audit data is generated in source databases, Oracle Audit Vault agents are installed on the source database(s) to collect the log and audit data and send it to the Audit Vault server. By removing the log and audit data from the source system and storing it in the secure Audit Vault server, the integrity of the log and audit can be ensured and proven that it has not been tampered with. The Oracle Audit Vault is designed to be a secure data warehouse of information of log and audit data.

Application Log and Audit Data

For applications, a key advantage to the Audit Vault's secure-at-the-source approach is that the Oracle Audit Vault is transparent. To use the Oracle Audit Vault with applications such as the Oracle E-Business Suite or SAP, standard Oracle database auditing only needs to be enabled on the application log and audit tables. While auditing the application audit tables might seem duplicative, the advantage is that the integrity of the application audit data can be ensured (proven that it has not been tampered with) while not having to replicate or copy the application log and audit data.

For example, the Oracle E-Business Suite has the ability to log user login attempts, both successful and unsuccessful. To protect the E-Business Suite login audit tables, standard Oracle database auditing first needs to be enabled. An Oracle Audit Vault agent will then collect information about the E-Business Suite login audit tables. If any deletes or updates occur to these tables, the Audit Vault would then alert and report the incident. The Audit Vault is transparent to the Oracle E-Business Suite, no patches are required for the Oracle E-Business Suite to be used with the Oracle Audit Vault.

Figure 1 Secure At-Source for Application Log and Audit data

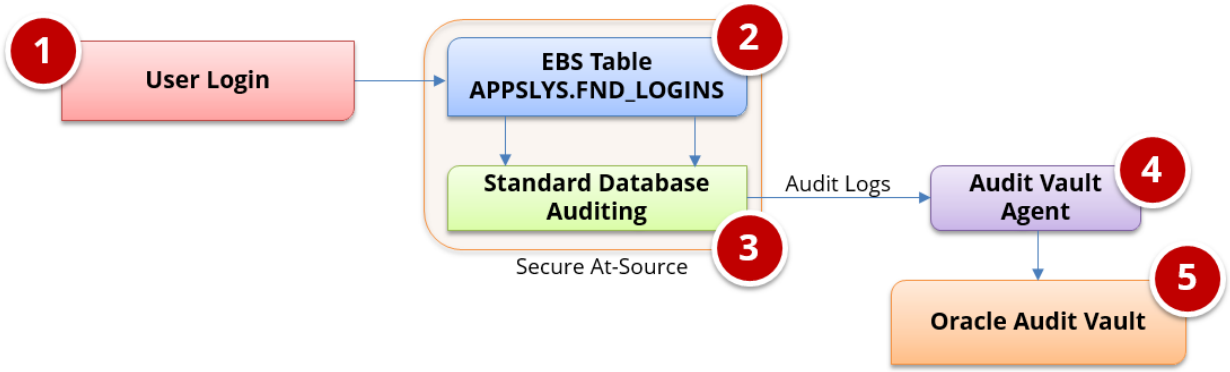
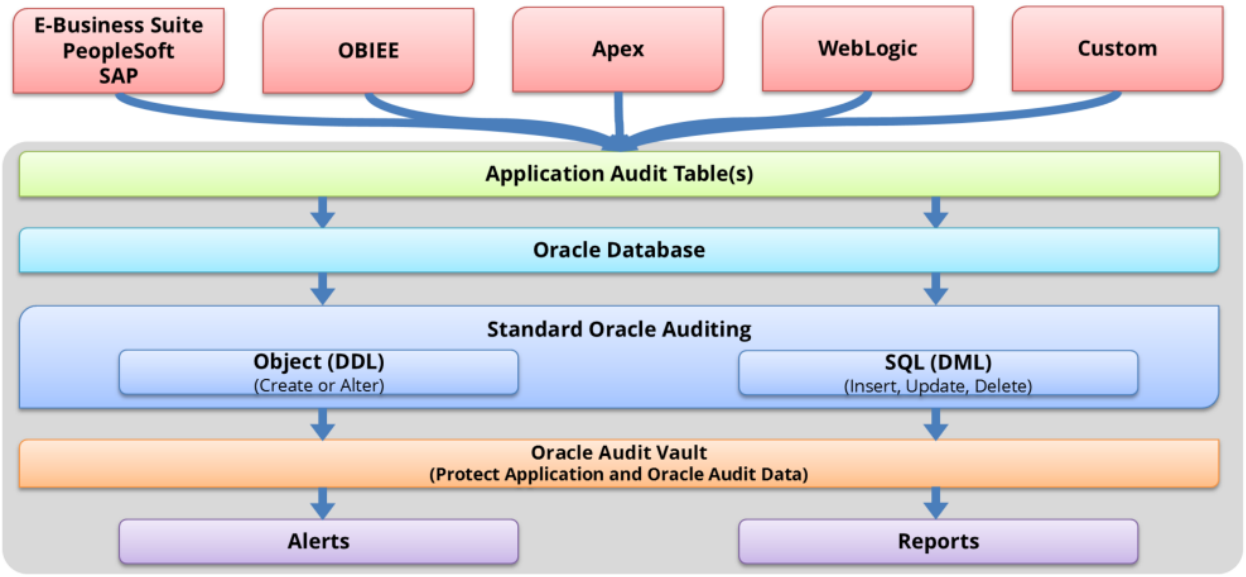


Figure 2 Vault of Log and Audit Data



Audit Vault Categories

Oracle database standard auditing can be defined for the following –

- **SQL statements –** Data Manipulation Language (DML) statements such as when users are attempting to query the database or modify data, using SELECT, INSERT, UPDATE, or DELETE.
- **Database Schema Objects –** Data Definition Language (DDL) statements when users create or modify database structures such as tables or views.
- **Database Privileges –** Audit can be defined for the granting of system privileges, such as SELECT ANY TABLE. With this kind of auditing, Oracle Audit Vault records SQL statements that require the audited privilege to succeed.
- **Fine-grained audit conditions –** Fine Grained Auditing activities stored in `SYS.FGA_LOG$` such as whether an IP address from outside the corporate network is being used or if specific table columns are being modified. For example, when the HR.SALARY table is SELECTED using direct database

connection (not from the application), a condition could be to log the details of result sets where the PROPOSED_SALARY column is greater than $500,000 USD.

- **Redo log data –** Database redo log file data. The redo log files store all changes that occur in the database. Every instance of an Oracle database has an associated redo log to protect the database in case of an instance failure. In Oracle Audit Vault, the capture rule specifies DML and DDL changes that should be checked when Oracle Database scans the database redo log.

The Audit Vault also supports –

- **Database Vault** – Database Vault settings stored in `DVSYS.AUDIT_TRAIL$` such as Realm audit, factor audit and Rule Audit.
- **System and SYS** – Core changes to the database by privileged users such as DBAs as recorded by `AUDIT_SYS_OPERATIONS`.
- **Stored Procedure Auditing** – Monitor any changes made to PL/SQL and stored procedures. Standard reports are provided to stored procedure operations, deleted and created procedures as well as modification history.

ORACLE AUDIT VAULT COLLECTION AGENTS

Oracle Audit Vault is installed on a server, and collector agents are installed on the hosts running the source databases. These collector agents communicate with the audit vault server.

If the collection agents are not active, no audit data is lost, as long as the source database continues to collect the audit data. When the collection agent is restarted, it will capture the audit data that the source database had collected during the time the collection agent was inactive.

There are three types of agent collectors for Oracle databases. There are other collectors for third-party database vendors such as SAP Sybase, Microsoft SQL-Server, and IBM DB2.

Audit Value Collectors for Oracle Databases*		
Audit Trail Type	**How Enabled**	**Collector Name**
Database audit trail	**For standard audit records:** AUDIT_TRAIL initialization parameter set to: DB or DB, EXTENDED. **For fine-grained audit records:** The audit trail parameter of DBMS_FGA.ADD_POLICY procedure is set to: DBMS_FGA.DB or DBMS_FGA.DB + DBMS_FGA.EXTENDED.	DBAUD

Audit Value Collectors for Oracle Databases*		
Audit Trail Type	**How Enabled**	**Collector Name**
Operating system audit trail	**For standard audit records:** AUDIT_TRAIL initialization parameter is set to: OS, XML, or XML, EXTENDED. For syslog audit trails, AUDIT_TRAIL is set to OS and the AUDIT_SYS_OPERATIONS parameter is set to TRUE. In addition, the AUDIT_SYSLOG_LEVEL parameter must be set. **For fine-grained audit records:** The audit_trail parameter of the DBMS_FGA.ADD_POLICY procedure is set to DBMS_FGA.XML or DBMS_FGA.XML + DBMS_FGA.EXTENDED.	OSAUD
Redo log files	The table that you want to audit must be eligible. See "Creating Capture Rules for Redo Log File Auditing" for more information.	REDO

*Note if using Oracle 12c; the assumption is that Mixed Mode Unified Auditing is being used

ORACLE DATABASE PLUG-IN

The Oracle Audit Vault uses Plug-Ins to define data sources. The following table summarizes several of the important facts about the database plug for Oracle databases –

Oracle Database Plug-In for the Oracle Audit Vault	
Plug-in Specification	**Description**
Plug-in directory	*AGENT_HOME*/av/plugins/com.oracle.av.plugin.oracle
Secured Target Versions	Oracle 10*g*, 11*g*, 12*c* Release 1 (12.1)
Secured Target Platforms	Linux/x86-64 Solaris /x86-64 Solaris /SPARC64 AIX/Power64 Windows /86-64 HP-UX Itanium
Secured Target Location (Connect String)	jdbc:oracle:thin:@//*hostname*:*port*/*service*
AVDF Audit Trail Types	TABLE DIRECTORY TRANSACTION LOG SYSLOG (Linux only) EVENT LOG (Windows only) NETWORK

Oracle Database Plug-In for the Oracle Audit Vault	
Plug-in Specification	**Description**
Audit Trail Location	For TABLE audit trails: sys.aud$, Sys.fga_log$, dvsys.audit_trail$, unified_audit_trail For DIRECTORY audit trails: Full path to the directory containing AUD or XML files. For SYSLOG audit trails: Full path to the directory containing the syslog file. For TRANSACTION LOG, EVENT LOG and NETWORK audit trails: no trail location required.

REPORTS

The Oracle Audit Vault by default installs over one-hundred (100) reports. This includes core audit reports as well as compliance reports.

Audit Reports

The audit reporting bundle installed by the default has the following categories –

- Activity Reports
- Entitlement
- Stored Procedure Audit
- Alerts

The following table lists the audit reports installed by default –

Type	Report	Description
Activity	Activity Overview	Digest of all captured audit events for a specified period of time
Activity	Data Access	Details of audited read access to data for a specified period of time
Activity	Data Modification	Details of audited data modifications for a specified period of time
Activity	Data Modification Before-After Values	Details of audited data modifications for a specified period of time showing before and after values
Activity	Database Schema Changes	Details of audited DDL activity for a specified period of time

Type	Report	Description
Activity	All Activity	Details of all captured audit events for a specified period of time
Activity	Failed Logins	Details of audited failed user logins for a specified period of time
Activity	User Login and Logout	Details of audited successful user logins and logouts for a specified period of time
Activity	Entitlements Changes	Details of audited entitlement related activity for a specified period of time
Activity	Audit Settings Changes	Details of observed user activity targeting audit settings for a specified period of time
Activity	Secured Target Startup and Shutdown	Details of observed startup and shutdown events for a specified period of time
Entitlement	User Accounts	Details of all existing user accounts
Entitlement	User Accounts by Secured Target	User accounts by Secured Target report
Entitlement	User Privileges	Details of audited failed user logins for a specified period of time
Entitlement	User Privileges by Secured Target	User privileges by Secured Target report
Entitlement	User Profiles	Digest of all existing user profiles
Entitlement	User Profiles by Secured Target	User profiles by Secured Target report
Entitlement	Database Roles	Digest of all existing database roles and application roles
Entitlement	Database Roles by Secured Target	Database roles by Secured Target report
Entitlement	System Privileges	Details of all existing system privileges and their allocation to users
Entitlement	System Privileges by Secured Target	System privileges by Secured Target report
Entitlement	Object Privileges	Details of all existing object privileges and their allocation to users
Entitlement	Object Privileges by Secured Target	Object privileges by Secured Target report
Entitlement	Privileged Users	Details of all existing privileged users
Entitlement	Privileged Users by Secured Target	Privileged users by Secured Target report
Stored Procedure Audit	Stored Procedure Activity Overview	Digest of all audited operations on stored procedures for a specified period of time
Stored Procedure Audit	Stored Procedure Modification History	Details of audited stored procedure modifications for a specified period of time
Stored Procedure Audit	Created Stored Procedures	Stored procedures created within a specified period of time

Type	Report	Description
Stored Procedure Audit	Deleted Stored Procedures	Stored procedures deleted within a specified period of time
Stored Procedure Audit	New Stored Procedures	Latest state of stored procedures created within a specified period of time
Alerts	All Alerts	All alerts issued within a specified period of time
Alerts	Critical Alerts	All critical alerts issued within a specified period of time
Alerts	Warning Alerts	All warning alerts issued within a specified period of time

Compliance Reports

The Oracle Audit Vault has seeded reports for the following compliance and legislative requirements – no additional license is required.

- Payment Card Industry (PCI)
- Sarbanes-Oxley Act (SOX)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- United Kingdom Data Protection Act (DPA)

For each compliance statue, following table lists the included reports available –

Compliance Report	Description
Activity Overview	Digest of all captured audit events for a specified period of time
All Activity	Details of all captured audit events for a specified period of time
Audit Settings Changes	Details of observed user activity targeting audit settings for a specified period of time
Created Stored Procedures	Stored procedures created within a specified period of time
Data Access	Details of audited read access to data for a specified period of time
Data Modification	Details of audited data modifications for a specified period of time
Database Schema Changes	Details of audited DDL activity for a specified period of time
Deleted Stored Procedures	Stored procedures deleted within a specified period of time
Entitlements Changes	Details of audited entitlement related activity for a specified period of time
Failed Logins	Details of audited failed user logins for a specified period of time
New Stored Procedures	Latest state of stored procedures created within a specified period of time
Secured Target Startup and Shutdown	Details of observed startup and shutdown events for a specified period of time
Stored Procedure Activity Overview	Digest of all audited operations on stored procedures for a specified period of time

Compliance Report	Description
Stored Procedure Modification History	Details of audited stored procedure modifications for a specified period of time
User Login and Logout	Details of audited successful user logins and logouts for a specified period of time

BI Publisher and Custom Reports

Custom reports can be created in Oracle Audit Vault using Oracle BI Publisher. BI Publisher is an add-on to Microsoft Word and can be used to modify or create new reports.

For example, to modify a new report, to meet specific corporate or internal audit needs, download a standard Oracle Audit Vault report that is similar (Auditor -> Reports -> Custom Reports -> Uploaded Reports). Click on the icon to download both the template and the report definition and load both files into BI Publisher.

Once complete, upload the report definition to the same location (Auditor -> Reports -> Custom Reports -> Uploaded Reports).

REMEDY TICKET SYSTEM INTEGRATION

Oracle Audit Vault 12c includes a standard interface for BMC Remedy ticketing systems. You can configure the Oracle Audit Vault to connect to BMC Remedy Action Request (AR) System Server 7.x. This connection enables the Oracle Audit Vault to raise trouble tickets in response to Audit Vault alerts.

Only one Remedy server can be configured for each Oracle Audit Vault installation. After the interface has been configured, an Audit Vault auditor needs to create templates to map and handle the details of the alert. Refer to the Oracle Audit Vault Administrator's Guide Release 10.3, E23571-08, Oracle Corporation, August 2014, section 3.6 http://docs.oracle.com/cd/E23574_01/admin.103/e23571.pdf.

HP ARCSIGHT INTEGRATION

HP's ArcSight Security Information Event Management (SIEM) system is a centralized system for logging, analyzing, and managing messages from different sources. Oracle Audit Vault can forward messages to ArcSight SIEM.

No additional software is needed to integrate with ArcSight. Integration is done through configurations in the Audit Vault Server console.

Messages sent to the ArcSight SIEM Server are independent of any other messages sent from the Audit Vault (e.g., other Syslog feeds).

There are three categories of messages sent –

- **System** - syslog messages from subcomponents of the Audit Vault Sever
- **Info** - specific change logging from the Database Firewall component of Oracle AVDF
- **Debug** - a category that should only be used under the direction of Oracle Support

OTHER KEY FEATURES

Several standard features of the Oracle database should be kept in mind when considering what alerts and correlations are possible when combining Oracle database and application log and audit data.

Client Identifier

Default Oracle database auditing stores the database username but not the application username. In order to pull the application username into the audit logs, the CLIENT IDENTIFIER attribute needs to be set for the application session which is connecting to the database. The CLIENT_IDENTIFIER is a predefined attribute of the built-in application context namespace, USERENV, and can be used to capture the application user name for use with global application context, or it can be used independently.

CLIENT IDENTIFIER is set using the DBMS_SESSION.SET_IDENTIFIER procedure to store the application username. The CLIENT IDENTIFIER attribute is one the same as V$SESSION.CLIENT_IDENTIFIER. Once set you can query V$SESSION or `SELECT SYS_CONTEXT('USERENV','CLIENT_IDENTIFIER') FROM DUAL.`

The table below offers several examples of how CLIENT_IDENTIFIER is used. For each example, for Level 3 alerts, consider how the value of CLIENT_IDENTIFIER could be used along with network usernames, enterprise applications usernames as well as security and electronic door system activity logs.

Oracle CLIENT_IDENTIFIER	
Application	**Example of how used**
E-Business Suite	As of Release 12, the Oracle E-Business Suite automatically sets and updates CLIENT_IDENTIFIER to the FND_USER.USERNAME of the user logged on. Prior to Release 12, follow Support Note How to add DBMS_SESSION.SET_IDENTIFIER(FND_GLOBAL.USER_NAME) to FND_GLOBAL.APPS_INITIALIZE procedure (Doc ID 1130254.1)
PeopleSoft	Starting with PeopleTools 8.50, the PSOPRID is now additionally set in the Oracle database CLIENT_IDENTIFIER attribute.
SAP	With SAP version 7.10 above, the SAP user name is stored in the CLIENT_IDENTIFIER.
Oracle Business Intelligence Enterprise Edition(OBIEE)	When querying an Oracle database using OBIEE the connection pool username is passed to the database. To also pass the middle-tier username, set the user identifier on the session. To do this in OBIEE, open the RPD, edit the connection pool settings and create a new connection script to run at connect time. Add the following line to the connect script: CALL DBMS_SESSION.SET_IDENTIFIER('VALUEOF(NQ_SESSION.USER)')

Database Link Usage

A database link is a one-way connection between two databases. Starting with Oracle version 11.2.0.3, database session information now can report additional information for those sessions involving database links. As often database links are created between databases of different security profiles; it is important to note that it is now able to log session activity that includes the details of the database link:

DBLINK_INFO returns the source of a database link. Specifically, it returns a string of the form:

SOURCE_GLOBAL_NAME=*dblink_src_global_name*, DBLINK_NAME=*dblink_name*,
SOURCE_AUDIT_SESSIONID=*dblink_src_audit_sessionid*
where:

- *dblink_src_global_name* is the unique global name of the source database
- *dblink_name* is the name of the database link on the source database
- *dblink_src_audit_sessionid* is the audit session ID of the session on the source database that initiated the connection to the remote database using *dblink_name*

You can verify DBLINK_INFO:

- Oracle 12c provides a DBLINK_INFO column in `SYS.UNIFIED_AUDIT_TRAIL`.
- `SELECT SYS_CONTEXT('USERENV','DBLINK_INFO') FROM DUAL`

Last Login

Tracking when database users last logged in is a common compliance requirement. This is required in order to reconcile users and cull stale users. New with Oracle12c, Oracle provides this information for database users. The system table `SYS.DBA_USERS` has a column, last_login.

Example:

```
select username, account_status, common, last_login
from sys.dba_users
order by last_login asc;
```

Username	Account_Status	Common	Last_Login
C##INTEGRIGY	OPEN	YES	05-AUG-14 12.46.52.000000000 PM AMERICA/NEW_YORK
C##INTEGRIGY_TEST_2	OPEN	YES	02-SEP-14 12.29.04.000000000 PM AMERICA/NEW_YORK
XS$NULL	EXPIRED & LOCKED	YES	02-SEP-14 12.35.56.000000000 PM AMERICA/NEW_YORK
SYSTEM	OPEN	YES	04-SEP-14 05.03.53.000000000 PM AMERICA/NEW_YORK

INTEGRIGY LOG AND AUDIT FRAMEWORK WITH ORACLE AUDIT VAULT

Integrigy's Log and Audit Framework can be easily implemented using the Oracle Audit Vault. The high-level summary is a follows –

Level 1

Enable database auditing as directed by the Integrigy Framework Level 1 requirements.

Level 2

1. Install the Oracle Audit Vault. If already installed, it is highly recommended to perform a health check as described in Audit Vault Server Configuration Report and Health Check Script (Doc ID 1360138.1).
2. Configure Oracle database to use Syslog per Integrigy Framework Level 2 requirements. Set the database initialization parameter AUDIT_TRAIL parameter to equal 'OS' and AUDIT_FILE_DEST parameter to desired file in the directory specification. Last set the initialization parameter AUDIT_SYSLOG_LEVEL to 'LOCAL1.WARNING' to generate Syslog formatted log files.
3. Install and activate the Oracle Audit Vault collector agent OSAUD for operating system files. Collect Syslog formatted logs located by the AUDIT_FILE_DEST parameter.

Level 3

Protect application log and audit tables by creating standard database audit policies and adding these new policies the Audit Vault Collectors. Create database alerts based on correlations between standard database events and application audit logs.

Oracle E-Business Suite Example

To use the Oracle Audit Vault with the Oracle E-Business Suite, no additional patches required either for the E-Business Suite or the Oracle database. This is because the Oracle Audit Vault uses only standard Oracle database functionality.

There are two steps for Level 3. The first is to protect the Oracle E-Business Suite audit tables, the second is to build alerts and reports that correlate application and database log information. To protect the E-Business Log and Audit tables, enable standard auditing on them. The second step is to define the Audit Vault alerts and reports.

Below are three examples.

E12 - Protect Application Audit Data
The sign-on audit tables log user logon and navigation activity for the professional forms user interface. This data needs to be protected.

Steps

1. Enable Standard Auditing
2. Create Audit Vault Alert
3. Forward to Alert to Syslog (This feature is available as of Oracle AVDF version 12.1.2)

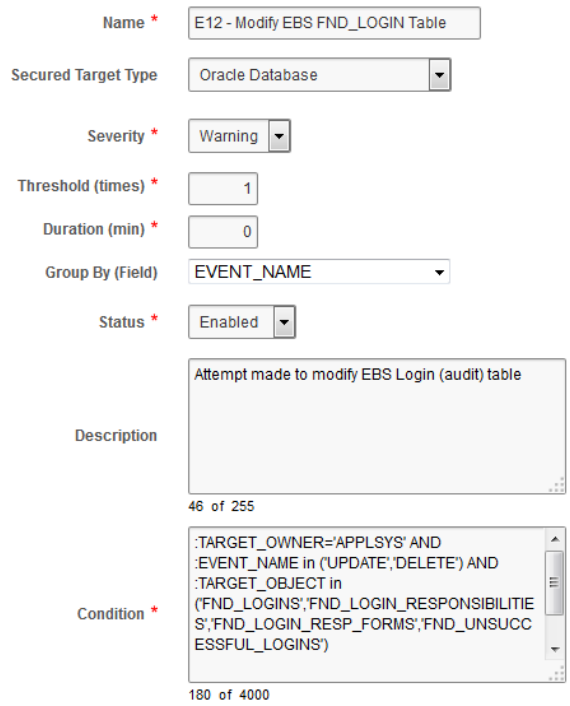
To enable standard auditing

```
AUDIT UPDATE, DELETE ON APPLSYS.FND_LOGINS BY ACCESS;
AUDIT UPDATE, DELETE ON APPLSYS.FND_LOGIN_RESPONSIBILITIES BY ACCESS;
AUDIT UPDATE, DELETE ON APPLSYS.FND_LOGIN_RESP_FORMS BY ACCESS;
AUDIT UPDATE, DELETE ON APPLSYS.FND_UNSUCCESSFUL_LOGINS BY ACCESS;
```

To create an alert in Audit Vault:
Audit Vault -> Auditor -> Policy -> Alerts -> Create Alert

```
Name: E12 - Modify audit and logging
Condition:
 :TARGET_OWNER='APPLSYS' AND :EVENT_NAME in ('UPDATE','DELETE') AND :TARGET_OBJECT in
('FND_LOGINS','FND_LOGIN_RESPONSIBILITIES','FND_LOGIN_RESP_FORMS','FND_UNSUCCESSFUL_LO
GINS')
```

Figure 3 Create Alert



E1 – Database Login by Seeded Account

All logins from the seeded Oracle E-Business Suite database users, other than that for APPS and APPLSPUB should be reported and investigated. This is based on Framework event E1.

Steps

1. Confirm the list of seeded users
2. Enable Standard Auditing
3. Create Audit Vault alert
4. Forward to Alert to Syslog

Confirm the list of seeded users:

```
SELECT f.oracle_username
FROM APPLSYS.FND_ORACLE_USERID f
WHERE exists (select 1 from dba_users u where u.username = f.oracle_username)
AND f.oracle_username not in ('APPS','APPLSYSPUB','SYS','SYSTEM')
ORDER BY 1 ASC;
```

Define the audit policy

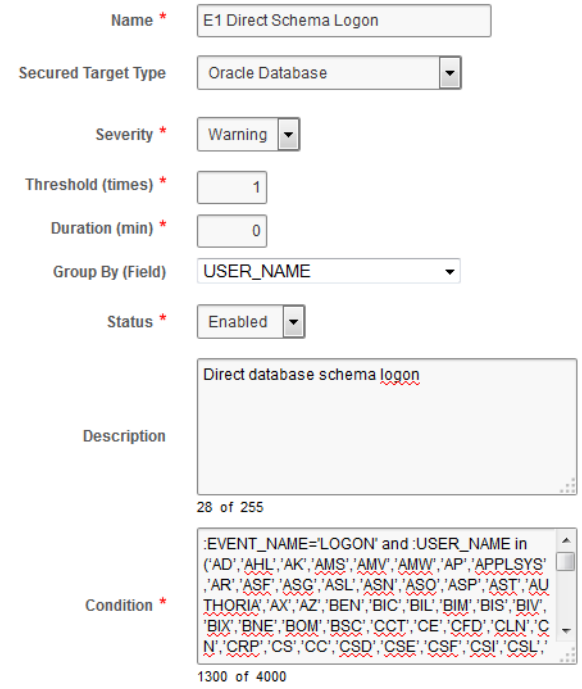
```
AUDIT SESSION; -- Audit all create session attempts, successful or unsuccessful
```

Create Alert in Audit Vault:

Audit Vault -> Auditor -> Policy -> Alerts -> Create Alert

```
Name: E1 Direct Schema Logon
Condition:   :EVENT_NAME='LOGON' and :USER_NAME in
('AD','AHL','AK','AMS','AMV','AMW','AP','APPLSYS','AR','ASF','ASG','ASL','ASN','ASO','
ASP','AST','AUTHORIA','AX','AZ','BEN','BIC','BIL','BIM','BIS','BIV','BIX','BNE','BOM',
'BSC','CCT','CE','CFD','CLN','CN','CRP','CS','CC','CSD','CSE','CSF','CSI','CSL','CSM',
'CSP','CSR','CTXSYS','CUA','CUF','CUG','CUI','CUP','CUS','CZ','DDD','DDR','DGRAY','DMS
','DNA','DOM','DPP','EAM','EC','ECX','EDR','EGO','ENG','ENI','FA','FEM','FII','FLM','F
PA','FRM','FTE','FTP','FUN','FV','GCS','GL','GMA','GMD','GME','GMF','GMI','GML','GMO',
'GMP','GMS','GR','HCC','HR','HRI','HXC','HXT','IA','IBC','IBE','IBP','IBU','IBW','BY',
'ICX','IEB','IEC','IEM','IEO','IES','IEU','IEX','IGC','IGF','IGI','IGS','IGW','ILEARN4
1','ILEARN41_RPT','IMC','INL','INV','IPA','IPM','ISC','ITA','ITG','IZU','JA','JG','JL'
,'JMF','JTF','JTI','JTM','JTR','JTS','LNS','MFG','MRP','MSC','MSD','MSO','MSR','MST','
MTH','MTR','MWA','ODM','OE','OKC','OKE','OKI','OKL','OKS','OKX','ONT','OPI','OSM','OTA
','OWAPUB','OZF','PA','PFT','PJI','PJM','PMI','PN','PO','POA','POM','PON','POS','PRP',
'PSA','PSB','PSP','PV','QA','QOT','QP','QPR','QRM','RE','RESTRICTED_US','RG','RLM','RR
S','SCOTT','SERVICES','SSP','VEA','WH','WIP','WMS','WPS','WSH','WSM','XDO','XDP','XLA'
,'XLE','XNB','XNP','XTR','ZFA','ZPB','ZSA','ZXS','EUL_US')
```

Figure 4 Direct Schema Logon



E1 Direct database logins using APPS

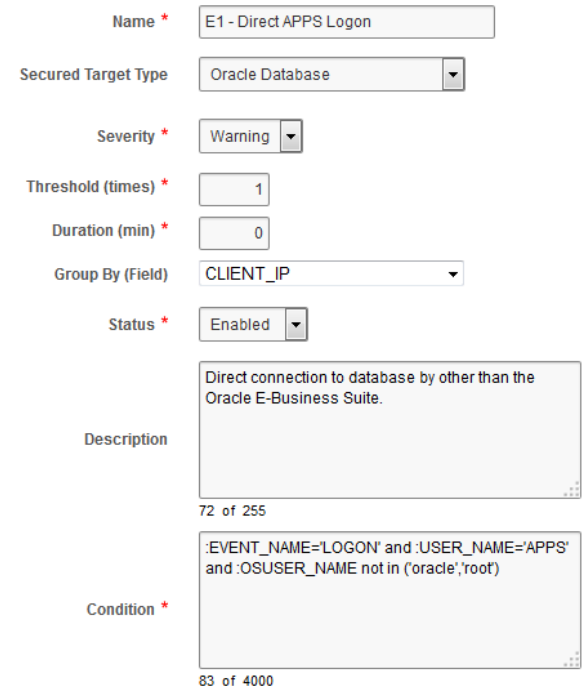
(E1) direct database logins using the APPS account not from the Application. For example, by developers or support personnel.

Steps

1. Enable Standard Auditing for all session create: `AUDIT SESSION;`
2. Create Alert using the following condition:

   `:EVENT_NAME='LOGON' and :USER_NAME='APPS' and` :OSUSER_NAME not in ('oracle','root')

Figure 5 Direct APPS Logon



REFERENCES

GENERAL

- "Building an Audit Trail in an Oracle Applications Environment," Jeff Hare and Stephen Kost, http://www.integrigy.com/files/Building_an_Audit_Trail_in_an_Oracle_Applications_Environment.pdf
- "Real World Database Auditing," Stephen Kost, Collaborate 2009, Session #602, http://www.integrigy.com/files/IOUG%202009%20-%20Real%20World%20Database%20Auditing.pdf
- "Applied Oracle Security," Knox et al., Oracle Press, 2010
- "Protecting Oracle Database 12c," Paul Wright, Apress 2014

ORACLE DOCUMENTATION

- "Oracle Database Security Guide 12c Release 1 (12.2) E48135-09," Oracle Corporation, July 2014 http://docs.oracle.com/database/121/DBSEG/E48135-09.pdf
- "Oracle Database Reference 12c Release 1 (12.1) E41527-12," Oracle Corporation, August 2014 http://docs.oracle.com/database/121/REFRN/refrn23884.htm#REFRN23884
- "Oracle Audit Vault Best Practices," Oracle Corporation, November 2007 http://www.oracle.com/technetwork/testcontent/twp-auditvault-bestpractices-200711-1-130326.pdf
- "Oracle Audit Vault Auditor's Guide Release 10.3 E16813-02," Oracle Corporation, August 2012 http://docs.oracle.com/cd/E23574_01/server.103/e16813.pdf
- "Security and Compliance with Oracle Database 12c," Oracle Corporation, April 2014, http://docs.oracle.com/cd/E23574_01/server.103/e16813.pdf
- "Oracle Database Concepts 12*c* Release 1 (12.1) E41396-10" , Oracle Corporation, August 2014 http://docs.oracle.com/database/121/CNCPT/E41396-10.pdf

ORACLE SUPPORT

- "Troubleshooting (Audit Trail)," Oracle Support Note ID 105624.1, Oracle Corporation, 10 December 2013, https://support.oracle.com/rs?type=doc&id=105624.1
- "Auditing How To, Troubleshooting, and Error Message Document," Oracle Support Note ID 1579731.1, Oracle Corporation, 3 September 2013, https://support.oracle.com/rs?type=doc&id=1579731.1
- "Master Note For Oracle Database Auditing," Oracle Support Note ID 1299033.1, Oracle Corporation, 7 January 2014, https://support.oracle.com/rs?type=doc&id=1299033.1
- "Master Note for Oracle Database Fine-Grained Auditing," Oracle Support Note ID 1533543.1, Oracle Corporation, 25 April 2013, https://support.oracle.com/rs?type=doc&id=1533543.1
- "Master Note For Oracle Audit Vault," Oracle Support Note ID 1199033.1, Oracle Corporation, 23 October 2013, https://support.oracle.com/rs?type=doc&id=1199033.1

ABOUT INTEGRIGY

Integrigy Corporation (www.integrigy.com)

Integrigy Corporation is a leader in application security for enterprise mission-critical applications. AppSentry, our application and database security assessment tool, assists companies in securing their largest and most important applications through detailed security audits and actionable recommendations. AppDefend, our enterprise web application firewall is specifically designed for the Oracle E-Business Suite. Integrigy Consulting offers comprehensive security assessment services for leading databases and ERP applications, enabling companies to leverage our in-depth knowledge of this significant threat to business operations.

Integrigy Corporation
P.O. Box 81545
Chicago, Illinois 60681 USA
888/542-4802
www.integrigy.com