Oracle 12c
Unified Auditing

October 23, 2014

Mike Miller
Chief Security Officer
Integrigy Corporation

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation
Agenda

1. Overview
2. Unified Auditing
3. Other 12c Auditing
4. Integrigy Log & Audit Framework
4. Q&A
About Integrigy

**Products**

- **AppSentry**
  ERP Application and Database Security Auditing Tool

- **AppDefend**
  Enterprise Application Firewall for the Oracle E-Business Suite

**Services**

- **Security Assessments**
  Oracle EBS, Apex, OBIEE, Databases, Sensitive Data, Penetration Testing

- **Compliance Assistance**
  SOX, PCI, HIPAA

- **Security Design Services**
  Auditing, Encryption, DMZ

**About Integrigy**

ERP Applications
Oracle E-Business Suite

INTEGRIGY

Databases
Oracle, SQL Server, MySQL

You
Oracle Database Security

- **Incremental improvements in Oracle 12c**
  - Unified Auditing
  - Mandatory Auditing
  - Real Application Security
  - Data Redaction
  - Multitenant (pluggable databases)
Today’s Objectives for Unified Auditing

- **Everything has changed**
  - Pure mode
- **Nothing has changed**
  - Mixed mode
- **Initial survey to make decisions**
  - Impact to logging, auditing and monitoring
Auditing and Logging

- Log so can audit, monitor, and alert
  - Related but separate disciplines

- Requirements are difficult
  - Technical, Compliance, Audit, and Security

- The Oracle database offers rich log and audit functionality
  - Most organizations do not fully take advantage
  - Oracle 12c can change this
Pre-Oracle 12c Database Auditing

1. **Listener**
   - **Type of auditing and logging:** LOGGING_name = ON

2. **DB Alert Log**
   - **Location of audit data:** TNS_ADMIN/log dir

3. **SYS Auditing**
   - **Audit and logging parameters:**
     - **AUDIT_SYS_OPERATIONS**
     - **AUDIT_SYSLOG_LEVEL**
   - **Location of audit data:** Syslog

4. **Native Auditing**
   - **Type of auditing and logging:** DBMS_FGA.add_policy
   - **Audit and logging parameters:**
     - **AUDIT_TRAIL**
   - **Location of audit data:**
     - **FGA_LOG$ table**
     - **AUDIT_FILE_DEST dir**

5. **Fine Grained Auditing**
   - **Type of auditing and logging:** DBMS_FGA.add_policy
   - **Audit and logging parameters:**
     - **AUDIT_TRAIL**
   - **Location of audit data:**
     - **FGA_LOG$ table**
     - **AUDIT_FILE_DEST dir**

- **BG_DUMP_DEST dir**
- **AUDIT_FILE_DEST dir**
Unified Auditing Has Two Modes

- **Pure**
  - Only 12c Unified Audit functionality available

- **Mixed (Default)**
  - Has both traditional and Unified Auditing
  - Provided as introduction and transition
Mixed Mode

- All traditional audit features and functionality work same as before
  - Default Oracle 12c

- Unified Audit Trail populated in parallel to traditional auditing
  - Because default policy ORA_SECURECONFIG
  - Purge or disable ORA_SECURECONFIG [Doc ID 1624051.1]
SYS.UNIFIED_AUDIT_TRAIL IS A VIEW

<table>
<thead>
<tr>
<th>Column Description*</th>
<th>Number of Columns</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard auditing including SYS audit records</td>
<td>44</td>
</tr>
<tr>
<td>Real Application Security (RAS) and RAS auditing</td>
<td>17</td>
</tr>
<tr>
<td>Oracle Label Security</td>
<td>14</td>
</tr>
<tr>
<td>Oracle Data Pump</td>
<td>2</td>
</tr>
<tr>
<td>Fine grained audit (FGA)</td>
<td>1</td>
</tr>
<tr>
<td>Data Vault (DV)</td>
<td>10</td>
</tr>
<tr>
<td>Oracle RMAN</td>
<td>5</td>
</tr>
<tr>
<td>SQL*Loader Direct Load</td>
<td>1</td>
</tr>
<tr>
<td>Total</td>
<td>94</td>
</tr>
</tbody>
</table>

*Key column is AUDIT_TYPE
Pure Mode

- Not default, but is the future
  - Re-link kernel to use

- Traditional sources no longer populated

- Has new parameters and syntax
  - Old init.ora parameters ignored

- Uses OracleSecure files
  - No syslog

- Can revert back to Mixed Mode
Oracle 12c Database Auditing - Mixed

1. Listener
   - LOGGING_name = ON
   - TNS_ADMIN/log dir

2. DB Alert Log
   - BG_DUMP_DEST
   - DB Alert Log

3. SYS Auditing
   - AUDIT_SYS_OPERATIONS
   - SYS.UNIFIED_AUDIT_TRAIL

4. Standard Auditing
   - AUDIT_TRAIL
   - DB
   - OS/XML
   - AUDIT_SYSLOG_LEVEL
   - AUDIT_FILE_DEST dir
   - AUD$ table

5. Fine Grained Auditing
   - DBMS_FGA.add_policy
   - FGA_LOG$ table
   - AUDIT_FILE_DEST dir
   - Unified Audit

Type of auditing and logging
Audit and logging parameters
Location of audit data
Oracle 12c Database Auditing - Pure

**Fine**
- **5** Fine Grained Auditing
  - DBMS_FGA.add_policy

**Native**
- **4** Standard Auditing
  - Unified Audit Policies
  - SYS.UNIFIED_AUDIT_TRAIL

**Privileged**
- **3** SYS Auditing
- **2** DB Alert Log
  - BG_DUMP_DEST dir

**Net**
- **1** Listener
  - LOGGING_name = ON
  - TNS_ADMIN/log dir

---

**Type of auditing and logging**
- Fine
- Native
- Privileged
- Net

**Audit and logging parameters**
- LOGGING_name = ON
- DBMS_FGA.add_policy

**Location of audit data**
- TNS_ADMIN/log dir
- BG_DUMP_DEST dir
- SYS.UNIFIED_AUDIT_TRAIL
## Mixed vs. Pure Mode Audit Configurations

<table>
<thead>
<tr>
<th>System Parameters</th>
<th>Mixed Mode</th>
<th>Pure Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUDIT_TRAIL</td>
<td>Same as 11g</td>
<td>Not used</td>
</tr>
<tr>
<td>AUDIT_FILE_DEST</td>
<td>Same as 11g</td>
<td>Not used</td>
</tr>
<tr>
<td>AUDIT_SYS_OPERATIONS</td>
<td>Same as 11g</td>
<td>Not used</td>
</tr>
<tr>
<td>AUDIT_SYSLOG_LEVEL</td>
<td>Same as 11g</td>
<td>Not used</td>
</tr>
<tr>
<td>UNIFIED_AUDIT_SGA_QUEUE_SIZE</td>
<td>Same as 11g</td>
<td>Used</td>
</tr>
</tbody>
</table>
Use create/alter audit policy statement*

```
CREATE AUDIT POLICY policy_name
    
    { {privilege_audit_clause [action_audit_clause ] [role_audit_clause ]}  
    | { action_audit_clause [role_audit_clause ] }  
    | { role_audit_clause } }  

    [WHEN audit_condition EVALUATE PER {STATEMENT | SESSION | INSTANCE}]  
    [CONTAINER = {CURRENT | ALL}]  
```

*DBMS_FGA used to configure fine-grained column and event handlers
CREATE AUDIT POLICY logon_pol
ACTIONS LOGON
WHEN 'INSTR(UPPER(SYS_CONTEXT(''USERENV'', ''CLIENT_PROGRAM_NAME'')), ''SQLPLUS'') > 0'
AND 'SYS_CONTEXT (''USERENV'', ''HOST'')
    NOT IN (''prod_db_rac1'', ''prod_db_rac2'')'
EVALUATE PER SESSION;

AUDIT POLICY logon_pol BY APPS;
<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Default Enabled</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORA_SECURECONFIG</td>
<td>Yes</td>
<td>Secure configuration audit. Same as default 11g auditing.</td>
</tr>
<tr>
<td>ORA_RAS_POLICY_MGMT</td>
<td>No</td>
<td>Oracle Real Application Security admin actions for RAS users, roles, and policies</td>
</tr>
<tr>
<td>ORA_RAS_SESSION_MGMT</td>
<td>No</td>
<td>Run-time RAS session and namespace actions</td>
</tr>
<tr>
<td>ORA_ACCOUNT_MGMT</td>
<td>No</td>
<td>Commonly used user account and privilege settings for create user, role and privilege grants</td>
</tr>
<tr>
<td>ORA_DATABASE_PARAMETER</td>
<td>No</td>
<td>Audits commonly used Oracle Database parameter settings</td>
</tr>
</tbody>
</table>
Unified Auditing Separation of Duties

- Two new roles with Oracle 12c
  - **AUDIT_ADMIN** – define and maintain audit policies
  - **AUDIT_VIEWER** – view and analyze audit data
New Schema for Unified Audit Data

- **AUDSYS** – New schema used solely for storage Unified Audit trail data in SYSAUX
  - Pure Mode uses Oracle SecureFiles

- **AUD$** and **FGA_LOG$** system tables and objects remain in the SYS schema
Improved Performance

- Auditing now implemented in SGA
  - Negligible overhead

- Two queuing modes
  - Immediate-write: immediately written
  - Queued-Write (default): periodically dequeued
Agenda

1. Overview
2. Unified Auditing
3. Other 12c Auditing
4. Integrigy Log & Audit Framework
4. Q&A
Pluggable Databases and Common Audit

- **Oracle 12c Multitenant option (Pluggable databases)**
  - Separate license NOT enabled by default

- **For Oracle 12c pluggable databases audit policies can be:**
  - **Common** – Available to all pluggable databases (PDB)s. Enable common audit policies only for common users for common objects.

  - **Local** - These policies apply only to a single pluggable database. By default, audit policies are local to the current PDB.
Oracle 12c Mandatory Auditing

- **New Oracle 12c always-on-auditing for SYSDBA**
  - SYS, SYSDBA, SYSOPER, SYSASM, SYSBACKUP, SYSDG, SYSKM

- **Mandatory Auditing Events (SYS.UNIFIED_AUDIT_TRIAL)**
  - CREATE AUDIT POLICY
  - ALTER AUDIT POLICY
  - DROP AUDIT POLICY
  - AUDIT
  - NOAUDIT
  - Database Vault configurations
  - DBMS_FGA PL/SQL package
  - DBMS_AUDIT_MGMT PL/SQL package
  - ALTER TABLE attempts on the AUDSYS audit trail
Real Application Security

- **New with Oracle 12c**
  - Next generation VPD

- **Define users separately from DBA_USERS**
  - DBA_XS_USERS
  - Can directly connect to the database

- **Log RAS users using Unified Audit Trail**
  - XS$NULL vs. xs_user_name

- **RAS role and event auditing is separate**
<table>
<thead>
<tr>
<th>Application</th>
<th>Example of how used</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-Business Suite</td>
<td>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)]</td>
</tr>
<tr>
<td>PeopleSoft</td>
<td>Starting with PeopleTools 8.50, the PSOPRID is now additionally set in the Oracle database CLIENT_IDENTIFIER attribute.</td>
</tr>
<tr>
<td>SAP</td>
<td>With SAP version 7.10 above, the SAP user name is stored in the CLIENT_IDENTIFIER.</td>
</tr>
<tr>
<td>Oracle Business Intelligence Enterprise Edition (OBIEE)</td>
<td>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. Edit the RPD 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)')</td>
</tr>
</tbody>
</table>
CREATE AUDIT POLICY sales_clerk_mm_pol
ACTIONS DELETE ON OE.ORDERS
WHEN 'SYS_CONTEXT(''USERENV'', 'CLIENT_IDENTIFIER''))
    = '``mmiller'''
EVALUATE PER STATEMENT;

AUDIT POLICY sales_clerk_mm_pol by APPS;
11g Auditing Features to Note

- **Alert log access in a view**
  - SYS.X$DBGALERTEXT

- **V$DIAG_ALERT_EXT view shows both the Alert and Listener Logs:**
  - For alert log use: Where trim(COMPONENT_ID)='rdbms';
  - For listener log use: WHERE trim(COMPONENT_ID)='tnslsnr';
Integrigy Framework for Auditing and Logging

Foundation security events and actions
(logins, logoffs, account creation, privileges, etc.)

Oracle Database
- Native Auditing
- Syslog
- DB log files

Applications
- Signon
- AuditTrails
- Navigation

Centralized Logging Solution
- Protected Audit Data
- Alerting & Monitoring
- Reporting
- Correlation
## Foundation Security Events and Actions

The foundation of the framework is a set of key security events and actions derived from and mapped to compliance and security requirements that are critical for all organizations.

<table>
<thead>
<tr>
<th>Event (E)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E1 - Login</td>
<td></td>
</tr>
<tr>
<td>E2 - Logoff</td>
<td></td>
</tr>
<tr>
<td>E3 - Unsuccessful login</td>
<td></td>
</tr>
<tr>
<td>E4 - Modify auth mechanisms</td>
<td></td>
</tr>
<tr>
<td>E5 - Create user account</td>
<td></td>
</tr>
<tr>
<td>E6 - Modify user account</td>
<td></td>
</tr>
<tr>
<td>E7 - Create role</td>
<td></td>
</tr>
<tr>
<td>E8 - Modify role</td>
<td></td>
</tr>
<tr>
<td>E9 - Grant/revoke user privileges</td>
<td></td>
</tr>
<tr>
<td>E10 - Grant/revoke role privileges</td>
<td></td>
</tr>
<tr>
<td>E11 - Privileged commands</td>
<td></td>
</tr>
<tr>
<td>E12 - Modify audit and logging</td>
<td></td>
</tr>
<tr>
<td>E13 - Create, Modify or Delete object</td>
<td></td>
</tr>
<tr>
<td>E14 - Modify configuration settings</td>
<td></td>
</tr>
<tr>
<td>Security Events and Actions</td>
<td>PCI DSS 10.2</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>E1 - Login</td>
<td>10.2.5</td>
</tr>
<tr>
<td>E2 - Logoff</td>
<td>10.2.5</td>
</tr>
<tr>
<td>E3 - Unsuccessful login</td>
<td>10.2.4</td>
</tr>
<tr>
<td>E4 - Modify authentication mechanisms</td>
<td>10.2.5</td>
</tr>
<tr>
<td>E5 - Create user account</td>
<td>10.2.5</td>
</tr>
<tr>
<td>E6 - Modify user account</td>
<td>10.2.5</td>
</tr>
<tr>
<td>E7 - Create role</td>
<td>10.2.5</td>
</tr>
<tr>
<td>E8 - Modify role</td>
<td>10.2.5</td>
</tr>
<tr>
<td>E9 - Grant/revoke user privileges</td>
<td>10.2.5</td>
</tr>
<tr>
<td>E10 - Grant/revoke role privileges</td>
<td>10.2.5</td>
</tr>
<tr>
<td>E11 - Privileged commands</td>
<td>10.2.2</td>
</tr>
<tr>
<td>E12 - Modify audit and logging</td>
<td>10.2.6</td>
</tr>
<tr>
<td>E13 - Objects Create/Modify/Delete</td>
<td>10.2.7</td>
</tr>
<tr>
<td>E14 - Modify configuration settings</td>
<td>10.2.2</td>
</tr>
<tr>
<td>Level 1</td>
<td>Enable <strong>baseline auditing and logging</strong> for application/database and implement security monitoring and auditing alerts</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Level 2</td>
<td>Send audit and log data to a <strong>centralized logging</strong> solution outside the Oracle Database and Application(s)</td>
</tr>
<tr>
<td>Level 3</td>
<td>Extend logging to include <strong>functional logging</strong> and more complex alerting and monitoring</td>
</tr>
</tbody>
</table>
Logging Maturity Model

0 - Not Performed
1 - Vendor Defaults
2 - Minimal Logging
   Partial Integration
3 - Centralized Logging
4 - Metrics Driven
5 - Continuous Improvement

Level 1
Level 2
Level 3
Level 3+

Common Maturity Model (CMM)  Integrigy Framework
This presentation is based on our Auditing and Logging whitepapers available for download at –

http://www.integrigy.com/security-resources
Contact Information

Michael Miller
Chief Security Officer
Integrigy Corporation

web: www.integrigy.com
e-mail: info@integrigy.com
blog: integrigy.com/oracle-security-blog
youtube: youtube.com/integrigy