WELCOME

Oracle Database 12 New Security Features

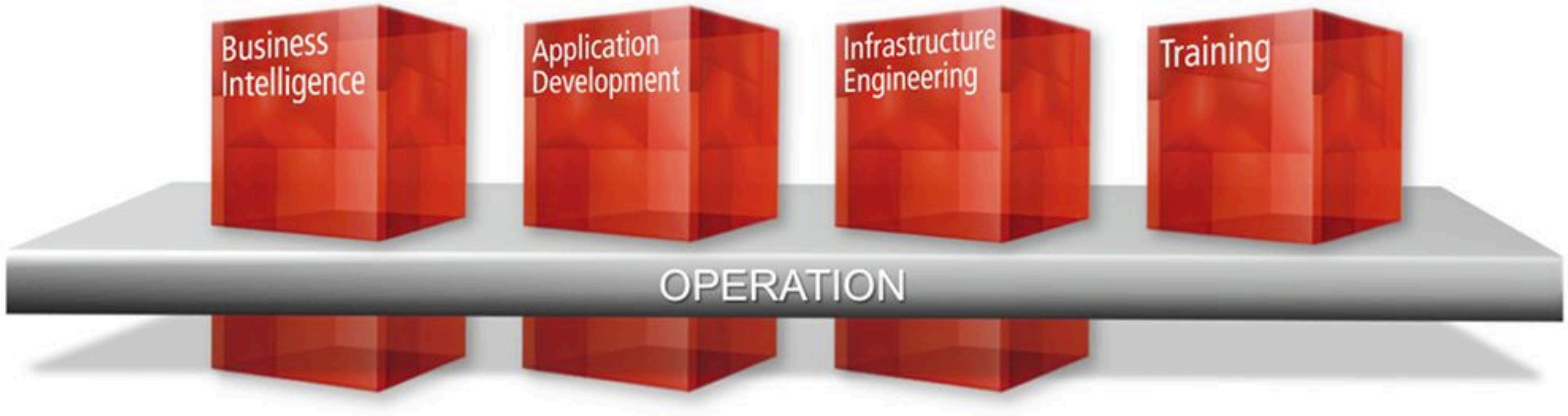
Stefan Oehrli
Senior Consultant
Discipline Manager
Trivadis AG

BASEL BERN LAUSANNE ZÜRICH DÜSSELDORF FRANKFURT A.M. FREIBURG I.BR. HAMBURG MÜNCHEN STUTTGART WIEN

trivadis
makes IT easier.

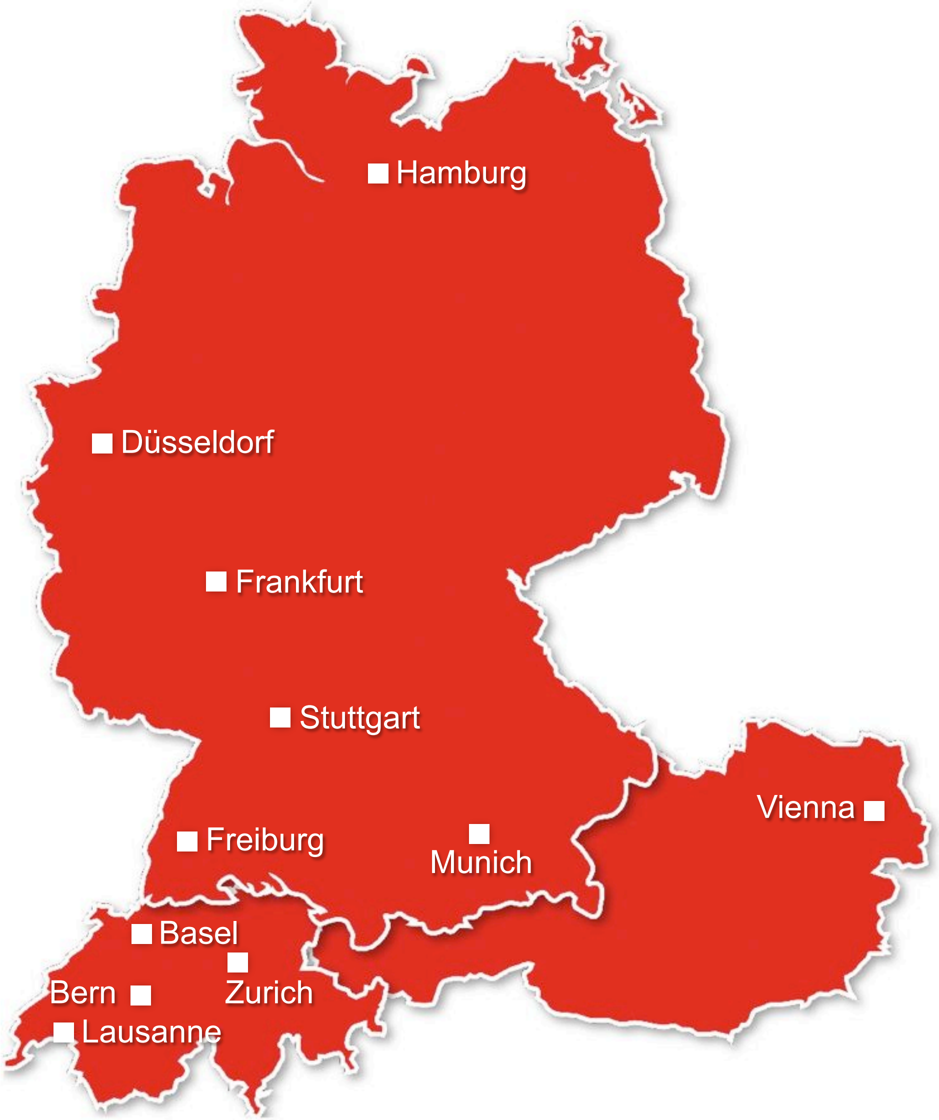
Our company

Trivadis is a market leader in IT consulting, system integration and the provision of IT services focusing on ORACLE and Microsoft technologies in Switzerland, Germany and Austria.



Trivadis Services takes over the interacting operation of your IT systems.

With over 600 specialists and IT experts in your region



11 Trivadis branches and more than 600 employees

200 Service Level Agreements

Over 4,000 training participants

Research and development budget: CHF 5.0 / EUR 4 million

Financially self-supporting and sustainably profitable

Experience from more than 1,900 projects per year at over 800 customers

Disclaimer

- Analysis, opinions, and representations expressed in this presentation are solely those of the author and have not been approved or endorsed by Oracle.
- This presentation does not contain any Licensing information. Review Database Licensing Information 12c Release 1 (12.1) for detailed information on the licenses required to use the features discussed in this presentation

Agenda

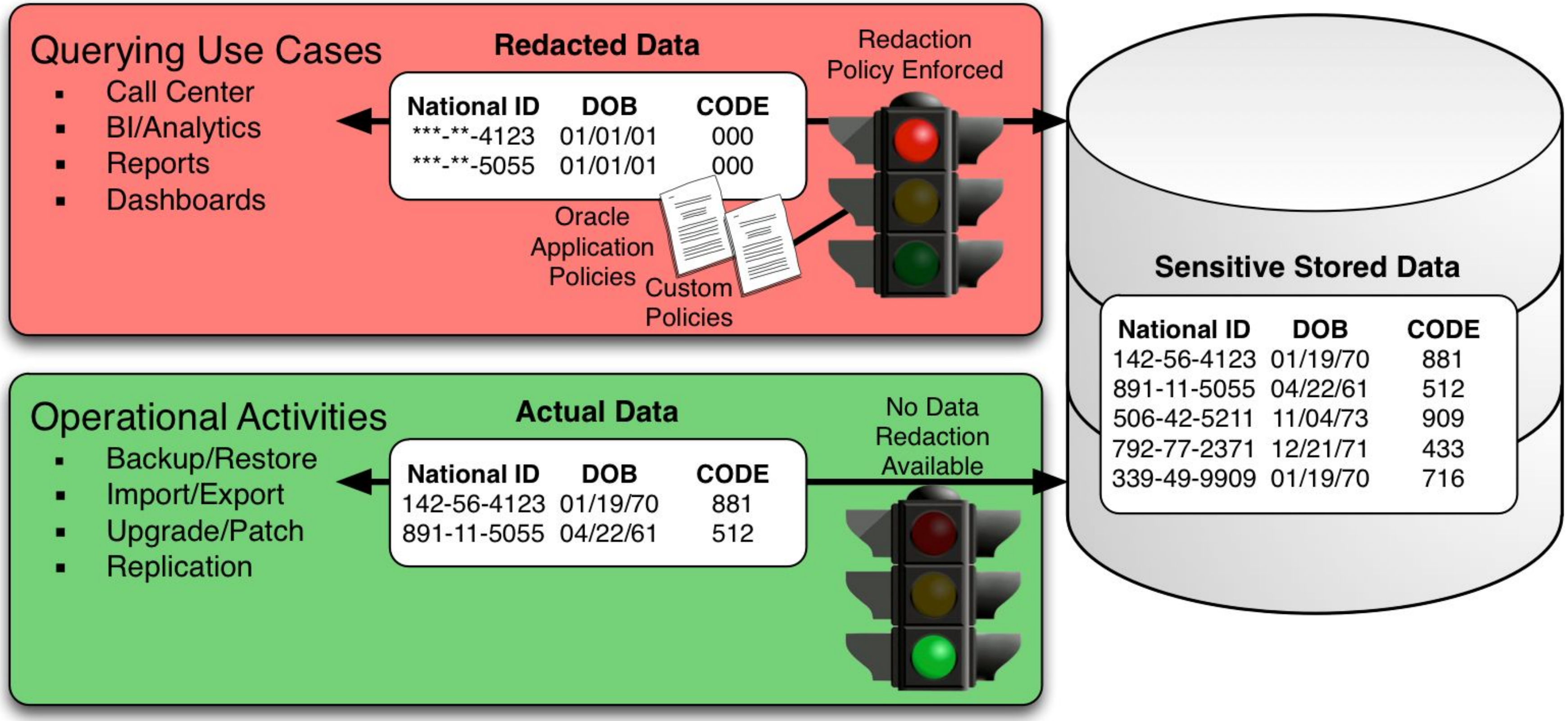
1. Data Redaction
2. Role and Privilege Analysis
3. Unified Auditing
4. Audit Roles and Policies
5. Database Vault
6. Other Enhancements

Data Redaction – The old days

- Traditional masking solutions are targeted for DEV / TEST systems
- So far Oracle does not provide any masking functionality when sensitive data is accessed / displayed
  - credit card number, addresses, social security number
- Any masking functionality must be implemented within the application
  - Partial mask credit card number
- Oracle does address this issue with data redaction (DBMS_REDACT)
- Typical use cases
  - Hide credit card Numbers
  - Partially hide social security numbers

Data Redaction – Overview

Overview



Querying Use Cases

- Call Center
- BI/Analytics
- Reports
- Dashboards

Redacted Data

National ID	DOB	CODE
***-**-4123	01/01/01	000
***-**-5055	01/01/01	000

Redaction Policy Enforced

Oracle Application Policies

Custom Policies

Operational Activities

- Backup/Restore
- Import/Export
- Upgrade/Patch
- Replication

Actual Data

National ID	DOB	CODE
142-56-4123	01/19/70	881
891-11-5055	04/22/61	512

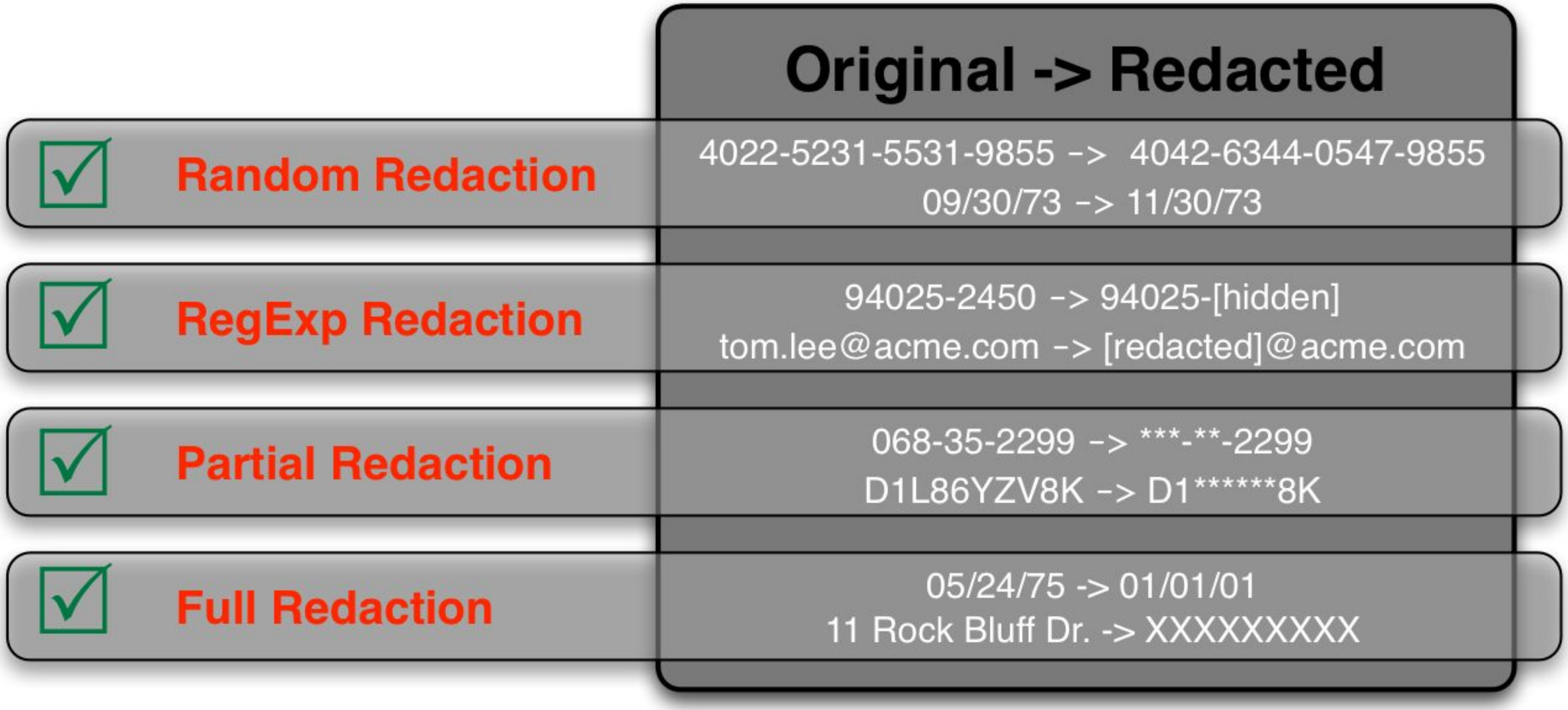
No Data Redaction Available

Sensitive Stored Data

National ID	DOB	CODE
142-56-4123	01/19/70	881
891-11-5055	04/22/61	512
506-42-5211	11/04/73	909
792-77-2371	12/21/71	433
339-49-9909	01/19/70	716

Data Redaction – Features

Feature summary



	Original -> Redacted
☑ Random Redaction	4022-5231-5531-9855 -> 4042-6344-0547-9855 09/30/73 -> 11/30/73
☑ RegExp Redaction	94025-2450 -> 94025-[hidden] tom.lee@acme.com -> [redacted]@acme.com
☑ Partial Redaction	068-35-2299 -> ***-**-2299 D1L86YZV8K -> D1******8K
☑ Full Redaction	05/24/75 -> 01/01/01 11 Rock Bluff Dr. -> XXXXXXXXX

Data Redaction – Example

- Data redact is done based on a condition
  - Using SYS_CONTEXT to get database user/role, IP address, client identifier,...
  - App user/role or other information passed in by the application
  - Supported Functions: SYS_CONTEXT(), V(), NV() or DOMINATES ()
    => *no custom PL/SQL*

```
BEGIN
  DBMS_REDACT.ADD_POLICY(
    object_schema => 'HR',
    object_name   => 'EMPLOYEES',
    column_name   => 'SALARY',
    policy_name   => 'HR_redact_salary',
    function_type => DBMS_REDACT.FULL,
    expression    => 'SYS_CONTEXT(''USERENV'',''SESSION_USER'')!=,''EUGEN''');
END;
/
```

- List of existing redaction policies in REDACTION_POLICIES

Data Redaction – Restrictions

- Create table as select on redacted table does not work

```
create table hr.emp as select first_name,last_name,salary from hr.employees
where department_id=30
                                                   *
ERROR at line 1:
ORA-28081: Insufficient privileges - the command references a redacted
object.
```

- Export of redacted data with Data Pump is limited

```
ORA-31693: Table data object "HR"."EMPLOYEES" failed to load/unload and is
being skipped due to error:
ORA-28081: Insufficient privileges - the command references a redacted
object.
```

- New system privilege are required to bypass redaction policies
  - EXEMPT REDACTION POLICY
  - EXEMPT DML REDACTION POLICY
  - EXEMPT DDL REDACTION POLICY

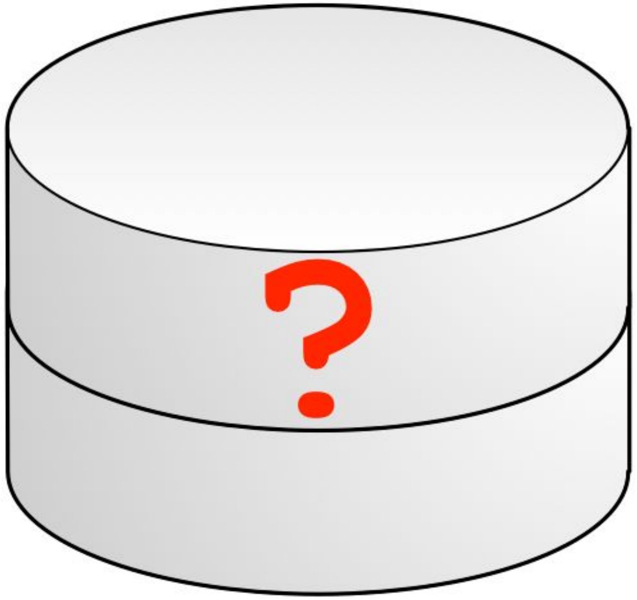
Agenda

1. Data Redaction
2. Role and Privilege Analysis
3. Unified Auditing
4. Audit Roles and Policies
5. Database Vault
6. Other Enhancements

Role and Privilege Analysis – Challenges

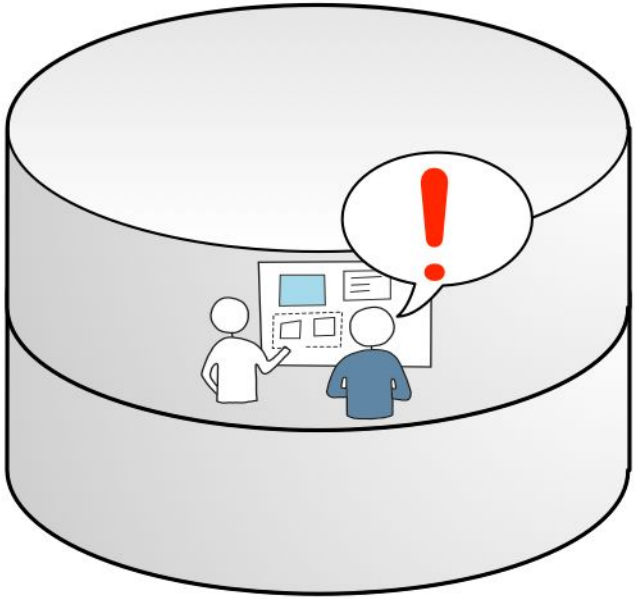
Challenges with database roles and privileges

- Most applications run with high privileges similar to DBA
- Privilege analysis was not performed during the design phase
- Focus was on finalizing the application, rather than on defining a minimum set of privileges eg. Least privileges
- Security simply wasn't a focus for many legacy applications

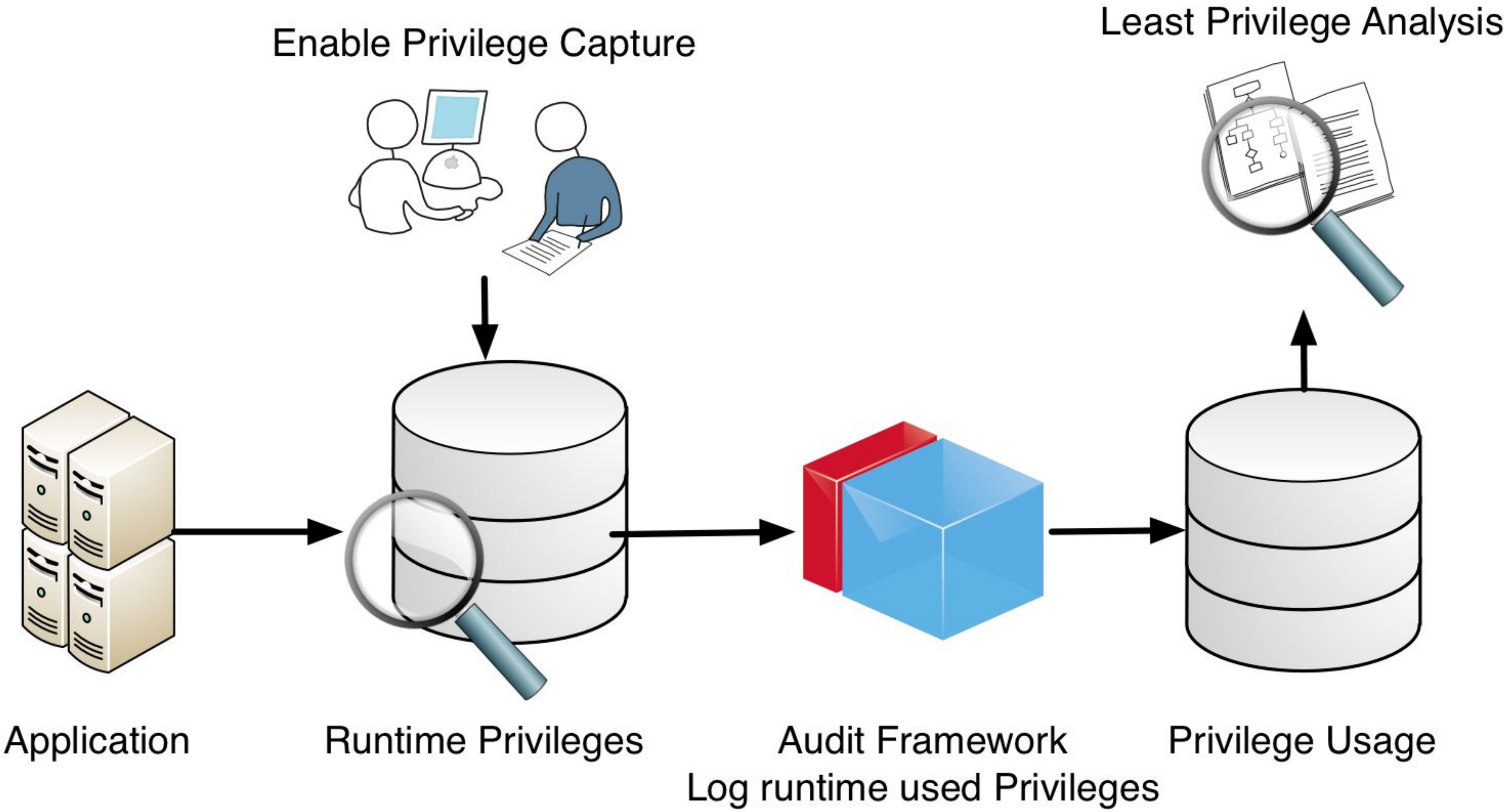


Role and Privilege Analysis – The Solution

- Capture and report on database privilege usage at runtime
  - For users, sessions, roles, PUBLIC
  - Show used system, object, and PUBLIC privileges
  - Show how the user got the privilege
- Show unused privileges:
  - System and object
- Achieve least privilege model
  - Make the database and applications more secure



Role and Privilege Analysis – Architecture



Enable Privilege Capture

Least Privilege Analysis

Application

Runtime Privileges

Audit Framework

Log runtime used Privileges

Privilege Usage

Role and Privilege Analysis - Precondition

- New Role CAPTURE_ADMIN

```
select ROLE,PRIVILEGE,TABLE_NAME from ROLE_TAB_PRIVS
where ROLE='CAPTURE_ADMIN‘;

ROLE              PRIVILEGE   TABLE_NAME
--------------- ---------- -------------------------
CAPTURE_ADMIN   SELECT      DBA_PRIV_CAPTURES
CAPTURE_ADMIN   SELECT      DBA_UNUSED_OBJPRIVS
CAPTURE_ADMIN   SELECT      DBA_UNUSED_OBJPRIVS_PATH
CAPTURE_ADMIN   SELECT      DBA_UNUSED_PRIVS
CAPTURE_ADMIN   SELECT      DBA_UNUSED_SYSPRIVS
CAPTURE_ADMIN   SELECT      DBA_UNUSED_SYSPRIVS_PATH
CAPTURE_ADMIN   SELECT      DBA_UNUSED_USERPRIVS
CAPTURE_ADMIN   SELECT      DBA_UNUSED_USERPRIVS_PATH
CAPTURE_ADMIN   SELECT      DBA_USED_OBJPRIVS
...
CAPTURE_ADMIN   SELECT      DBA_USED_USERPRIVS_PATH
CAPTURE_ADMIN   EXECUTE     DBMS_PRIVILEGE_CAPTURE
```

Role and Privilege Analysis – Initiate capture

- Create the Capture Policy

```
EXEC DBMS_PRIVILEGE_CAPTURE.CREATE_CAPTURE(
NAME      =>'scott_dba_analysis',
TYPE      =>DBMS_PRIVILEGE_CAPTURE.G_CONTEXT,
CONDITION =>'SYS_CONTEXT(''USERENV'',''SESSION_USER'')=''SCOTT''');
```

- Enable the Capture Policy

```
EXEC DBMS_PRIVILEGE_CAPTURE.ENABLE_CAPTURE('scott_dba_analysis');
```

- Run Job, Task etc which has to be analyzed

Role and Privilege Analysis – Analysis capture

- Disable the Capture Policy

```
EXEC DBMS_PRIVILEGE_CAPTURE.DISABLE_CAPTURE('scott_dba_analysis');
```

- Generate Report

```
EXEC DBMS_PRIVILEG_CAPTURE.GENERATE_RESULT('scott_dba_analysis');
```

- Review Views DBA_USED_% and DBA_UNUSED_%

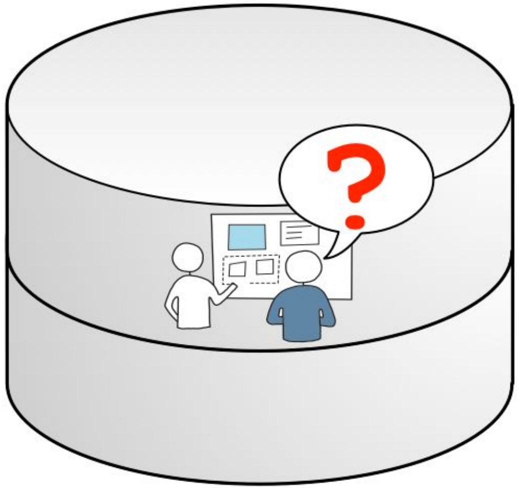
```
select CAPTURE, USERNAME,USED_ROLE,SYS_PRIV,PATH
from DBA_USED_SYSPRIVS_PATH where CAPTURE='scott_dba_analysis';

CAPTURE            USER  USED_ROLE   SYS_PRIV         PATH
------------------ ----  ---------   --------------   ----------------------
scott_dba_analysis SCOTT CONNECT     CREATE SESSION   GRANT_PATH('SCOTT‘,'CONNECT')
scott_dba_analysis SCOTT VERY_SECRET SELECT ANY TABLE GRANT_PATH('SCOTT‘,'SECRET',
                                                                      'VERY_SECRET‘)
```

Role and Privilege Analysis – Solution

Pin down the privileges

- Setup Privilege Analysis to …
  - … Identify unused privileges
  - … Identify the source of the unused privileges
  - … analyze PUBLIC privileges
  - … different use cases eg. report user vs power user
- Application owner can decide whether the unused privileges could be revoked
- Re-test your application



Agenda

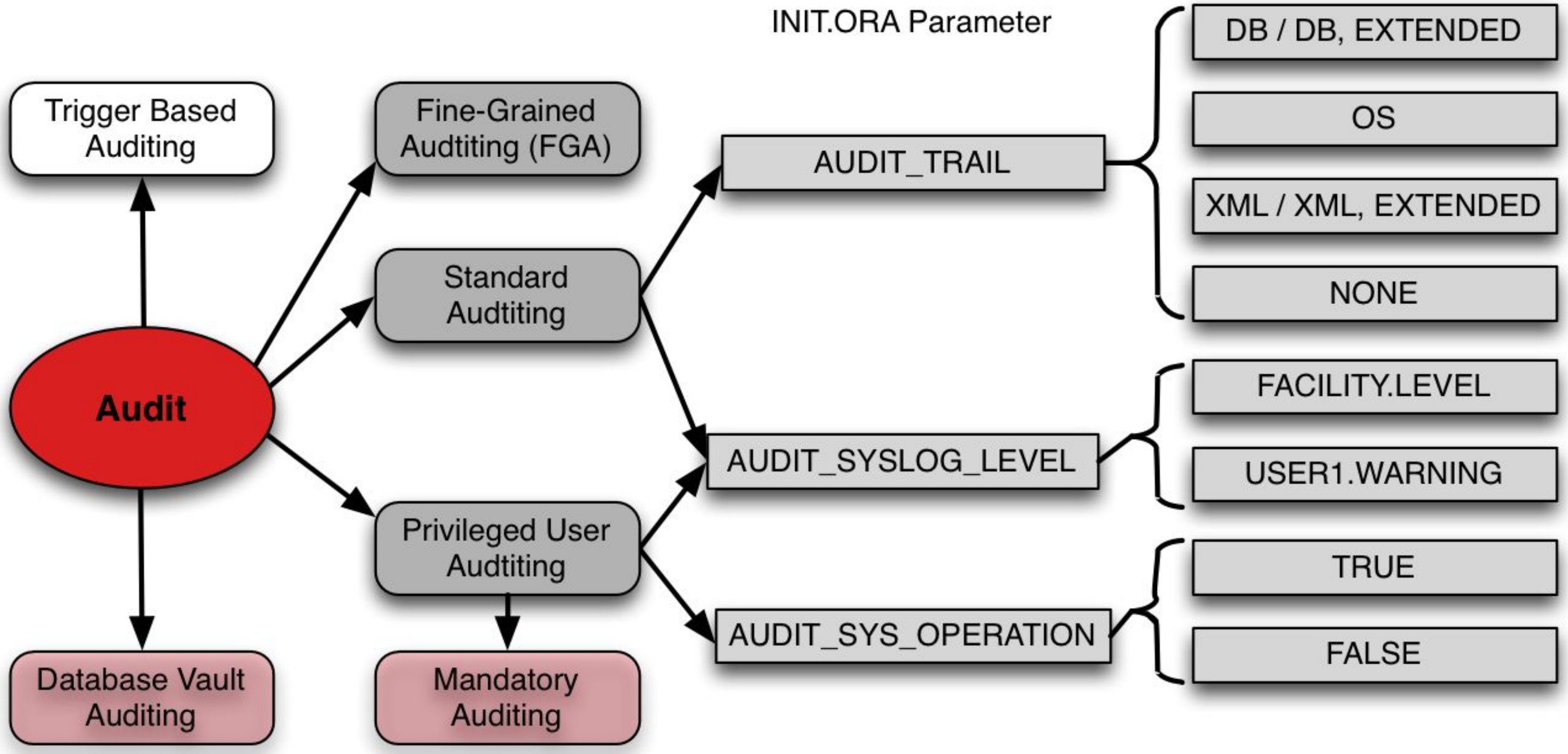
1. Data Redaction
2. Role and Privilege Analysis
3. Unified Auditing
4. Audit Roles and Policies
5. Database Vault
6. Other Enhancements

Database Auditing – The challenges

- Defining complex audit scenarios could become quite cumbersome
  - Ending with a lot of `audit xyz` statements
  - Can not easily be switched off/on
  - Having to much audit data
- Performance impact depending on what is audited
  - Audit highly used objects could lead to a lot of audit records / redo
- No strait forward solution to limit access to audit data
- Different data stores of audit information
  - Mandatory Audit
  - SYS Audit
  - Standard database audit
  - Fine grained auditing

Database Auditing – The old days

- Auditing until Oracle 11g R2 (and a little bit beyond)



Database Auditing – The UNIFIED AUDIT

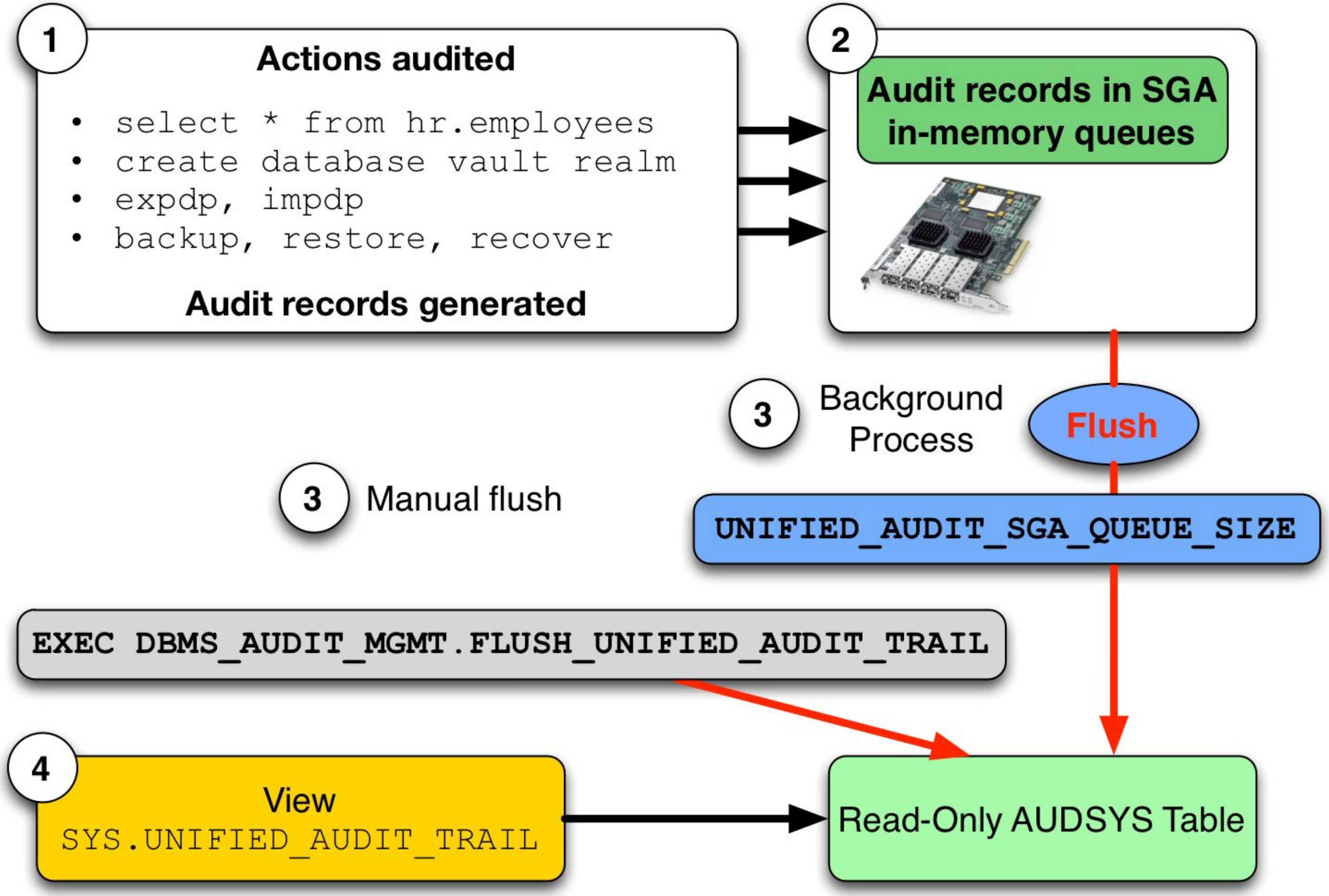
- Oracle introduces the new UNIFIED AUDIT TRAIL
  - All audit data stored in Oracle secure files
  - unified_audit_trail view replaces AUD$, FGA$
  - Security with new AUDITOR and AUDIT_ADMIN accounts
- Always ON Auditing
  - No initialization parameters required to enable auditing
  - No need to bounce the database (ehm. At least once... ☺ to link it)
- Audit the audit configuration by default
  - Records every event that modifies the audit configuration
  - Records every modification to audit trail and its settings

Database Auditing – The UNIFIED AUDIT

- Fast audit engine, easier access control to DB, increased performance
  - Low processing overhead (records are stored in proprietary format)
  - Low transactional overhead (audit records are buffered)
  - Dynamic views to query audit data stored in proprietary format
- Queued Mode
  - Default mode
  - Audit records stored in SGA and periodically flushed
  - Configured with UNIFIED_AUDIT_SGA_QUEUE_SIZE (1MB to 30MB)
- Immediate Mode
  - Audit records written immediately
- Manual flush queue to disk
  - Connect as user with AUDIT_ADMIN role

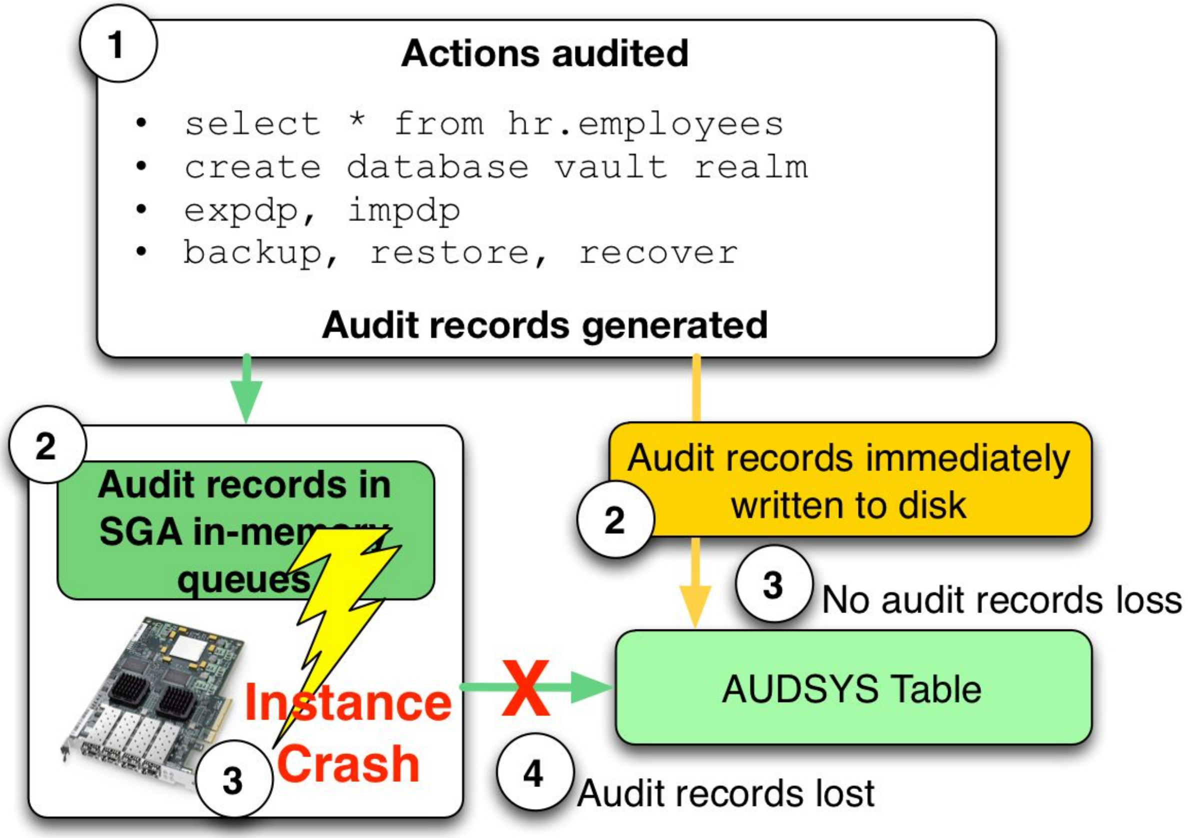
```
EXEC DBMS_AUDIT_MGMT.FLUSH_UNIFIED_AUDIT_TRAIL;
```

Database Auditing – Fast audit engine



1
Actions audited
• select * from hr.employees
• create database vault realm
• expdp, impdp
• backup, restore, recover
Audit records generated
2
Audit records in SGA in-memory queues
3
Background Process
Flush
UNIFIED_AUDIT_SGA_QUEUE_SIZE
3
Manual flush
EXEC DBMS_AUDIT_MGMT.FLUSH_UNIFIED_AUDIT_TRAIL
4
View
SYS.UNIFIED_AUDIT_TRAIL
Read-Only AUDSYS Table

Database Auditing – Ups…



1 **Actions audited**

- `select * from hr.employees`
- `create database vault realm`
- `expdp, impdp`
- `backup, restore, recover`

Audit records generated

2 **Audit records in SGA in-memory queues**

3 **Instance Crash**

X

4 Audit records lost

2 Audit records immediately written to disk

3 No audit records loss

AUDSYS Table

```
DBMS_AUDIT_MGMT.SET_AUDIT_TRAIL_PROPERTY

AUDIT_TRAIL_IMMEDIATE_WRITE
AUDIT_TRAIL_QUEUED_WRITE
```

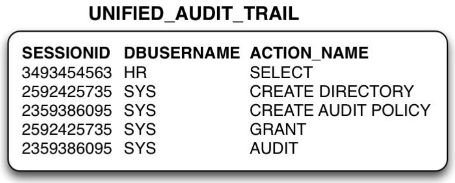
Agenda

1. Data Redaction
2. Role and Privilege Analysis
3. Unified Auditing
4. Audit Roles and Policies
5. Database Vault
6. Other Enhancements

Database Auditing – Audit Roles

- DBA
  - Create tablespace to store the audit table
- AUDIT_ADMIN role to …
  - Manages audit policies eg. define auditing
  - Maintain audit data retention and initiate housekeeping
- AUDIT_VIEWER role to …
  - View and report on audit data
- Best Practice
  - Create dedicated users and grant appropriate roles

```
create audit policy ...;
exec DBMS_FGA ...
exec DBMS_AUDIT_MGMT.MOVE_DBAUDIT_TABLES
exec DBMS_AUDIT_MGMT.INIT_CLEANUP
```



UNIFIED_AUDIT_TRAIL

SESSIONID	DBUSERNAME	ACTION_NAME
3493454563	HR	SELECT
2592425735	SYS	CREATE DIRECTORY
2359386095	SYS	CREATE AUDIT POLICY
2592425735	SYS	GRANT
2359386095	SYS	AUDIT

```
grant audit_admin to AUDITOR_OEHRLI;
grant audit_viewer to AUDITOR_MEIER;
```

Database Auditing – Audit policies

- Audit policies
  - Named containers for audit settings
- Audit policies …
  - … is used to audit ACTIONS, PRIVILEGES, OBJECTS
  - … based on system wide or object-specific audit options
  - … can contain a role
  - … can contain conditions / exceptions
  - … are enabled / disabled with audit and noaudit statement
- Condition limited to Oracle Functions ➔ no custom PL/SQL functions

Database Auditing – Audit policies

- Create audit policy with conditions and exceptions

```
CREATE AUDIT POLICY dba_pol ROLE DBA;

CREATE AUDIT POLICY hr_employees_pol
    PRIVILEGES CREATE TABLE
    ACTIONS UPDATE ON HR.EMPLOYEES
    WHEN 'SYS_CONTEXT(''USERENV'', ''IDENTIFICATION_TYPE'') =
''EXTERNAL''' EVALUATE PER STATEMENT;

AUDIT POLICY hr_employees_pol EXCEPT HR;
```

- Enabled audit policies

```
select * from audit_unified_enabled_policies;

USER_NAME   POLICY_NAME       ENABLED_ SUC FAI
----------- ----------------- -------- --- ---
SCOTT_DBA   ORA_ACCOUNT_MGMT  BY       YES YES
ALL USERS   ORA_SECURECONFIG  BY       YES YES
```

Database Auditing – Default policies

- ORA_SECURECONFIG
  - Audit configuration and trail
  - enabled by default
- ORA_ACCOUNT_MGMT
  - Create user, role and privilege grants
- ORA_DATABASE_PARAMETER
  - Database initialization file (spfile) changes

Database Auditing – More on “unified”

- Unified Auditing does / can as well audit…
  - Fine Grained Audit (FGA)
  - Data Pump
  - Oracle RMAN
  - Oracle Label Security (OLS)
  - Oracle Database Vault (DV)
  - Real Application Security (RAS)
- Component auditing do use dedicated columns
  - RMAN_OPERATION, RMAN_OBJECT_TYPE, RMAN_DEVICE_TYPE
  - DP_TEXT_PARAMETERS1, DP_BOOLEAN_PARAMETERS1
- Can be specified as well in an audit policy

```
CREATE AUDIT POLICY audit_dp
ACTIONS COMPONENT=DATAPUMP ALL;
```

Database Auditing – More on “unified”

- Auditing for Oracle Database Vault (DV)
  - Is defined by the DV Framework
  - DV Configuration changes are tracked by default
  - DV Violations are tracked as defined in DV realms etc.
- RMAN is audited by default and it audit…
  - … successful rman backup’s
  - … successful rman restores
  - … some list and report statements
  - but not everthing…

```
SELECT event_timestamp, dbusername,
  rman_operation, rman_object_type,rman_device_type
  FROM unified_audit_trail WHERE action_name='RMAN ACTION'
  ORDER BY event_timestamp;
```

Database Auditing – What else…

It does get harder to tamper audit

- UNIFIED AUDIT is part of the oracle kernel
  - switch off require relink / restart
  - Using different binaries at runtime eg. for sqlplus lead to errors / ORA-00600
  - Auditing is partially available even if relinked with **uniaud_off**
- Memory could be manipulated before it has been flushed
  - Use immediate mode to minimize the risk
- ORADEBUG itself is audited by default

Database Auditing – What else…

Backward compatibility and Migration

- Traditional and UNIFIED mode (mixed mode)
  - Traditional auditing (Pre 12c) still works in 12c
  - All traditional auditing settings configured in 11g R2 continue to work
- Pure UNIFIED mode
  - Customers should migrate over time to new UNIFIED mode
  - Traditional auditing feature will be disabled in future release
  - Running in pure unified mode ➔ Relink Oracle binary unified flag **uniaud_on**

Agenda

1. Data Redaction
2. Role and Privilege Analysis
3. Unified Auditing
4. Audit Roles and Policies
5. Database Vault
6. Other Enhancements

Database Vault – Improvements in 12c

- Manageability
  - Streamline controls enforcement via Enterprise Manager 12c (☺☹)
  - One command enablement, no special installation required
- New Mandatory Realms Feature
  - Block all privileges from accessing data – even owner
  - Patching, maintenance, highly sensitive information
- Performance
  - Pushing overhead to near zero
- Installation
  - Installed by default but not configured ➔ Removes reliance on OS for linking
  - Protection is always on no matter where you restore DB backup
- Database Vault is using the UNIFIED AUDIT TRAIL

Database Vault – Configuration

- Create a security admin user as DBA

```
CREATE USER SEC_ADMIN;
GRANT CREATE SESSION TO SEC_ADMIN;
```

- Create an accounts admin

```
CREATE USER ACCTS_ADMIN;
GRANT CREATE SESSION TO ACCTS_ADMIN;
```

- One command to configure as SYS

```
EXEC DVSYS.CONFIGURE_DV(dvowner_uname => 'SEC_ADMIN', dvacctmgr_uname =>
'ACCTS_ADMIN');
```

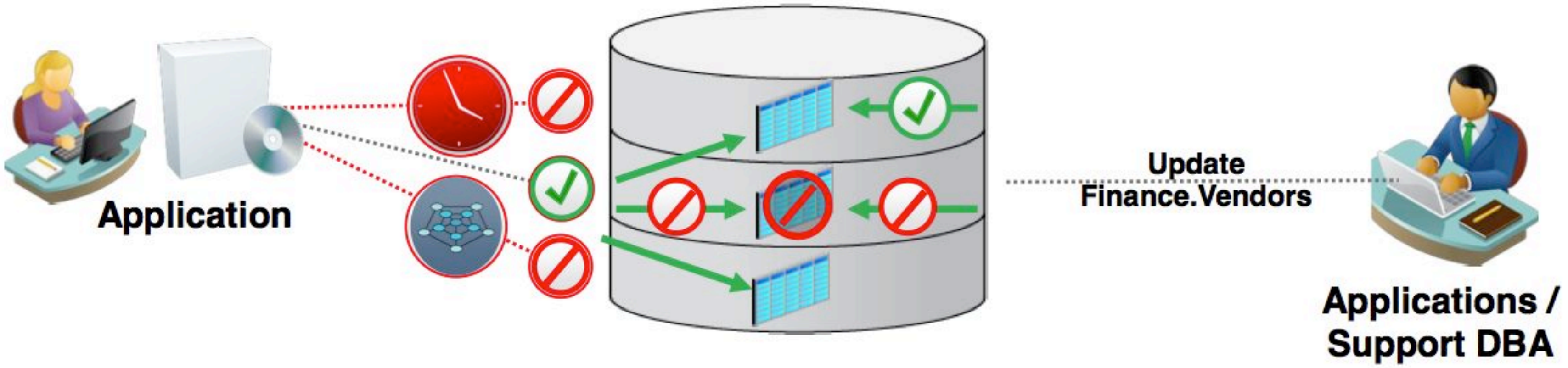
- Then enable as security admin SEC_ADMIN

```
EXEC DVSYS.DBMS_MACADM.ENABLE_DV;
```

- Restart the database as SYSDBA

Database Vault – Realm and Other Enhancements

- Protect highly sensitive information from all users, even table owner
- Enable application DBA to patch application but prevent access to highly sensitive tables
- Block access to sensitive information by support analysts who need temporary access to application schema



Agenda

1. Data Redaction
2. Role and Privilege Analysis
3. Unified Auditing
4. Audit Roles and Policies
5. Database Vault
6. Other Enhancements

Other Enhancements

- Separation of Duty, reduce dependency on SYSDBA
  - SYSBACKUP → used by RMAN
  - SYSDG → used by DataGuard
  - SYSKM → used for Key Mgmt
- Full Support for SHA-2
  - Stored password verifiers – Oracle Advanced Security – DBMS_CRYPTO
  - Oracle Database 12c Password Authentication
  - By default will only accept SHA-2 verifiers
  - Connections from earlier releases - Set compatibility parameter to earlier release
- Hardware acceleration support extended beyond TDE
  - Now supported for Network Encryption and DBMS_CRYPTO

Other Enhancements

- Sensitive Database Tables
  - The SELECT ANY DICTIONARY privilege no longer permits access to security sensitive data dictionary tables DEFAULT_PWD$, ENC$, LINK$, USER$, USER_HISTORY$, and XS$VERIFIERS.
- UNLIMITED TABLESPACE
  - removed from Resource Role
  - Upgrading to 12c ➔ No change for existing users during upgrade
  - New 12c installations ➔ Grants of resource role in 12c will not give “unlimited”
- Multiple authentication support
  - Database will fall back to password authentication
- Last login time
  - Displayed on SQL*Plus login & recorded in dictionary

Other Enhancements

- Access control mechanism based on application code
  - Restricts exercise of privileges within specific code units
  - Minimizes privileges granted to runtime user
- Runtime privilege elevation in PL/SQL program units – Allows owner’s roles to be granted to his program units
  - Functions, procedures and packages
  - Invoker rights and definer rights
  - Granted roles enabled during execution of the code
- New Kerberos stack
  - Replaced old Kerberos implementation

Conclusion:

So many security improvements as long gone

Interesting improvements to make existing feature more reliable, faster, easier

Oracle Security is on track

Privilege Analysis a a simple but useful features ☺

There will be more…

Technology on its own won't help you.
You need to know how to use it properly.
Trivadis makes IT easier.

THANK YOU.

Trivadis AG

Stefan Oehrli

Europa-Strasse 5
CH-8152 Glattbrugg

www.trivadis.com
www.oradba.ch

BASEL BERN LAUSANNE ZÜRICH DÜSSELDORF FRANKFURT A.M. FREIBURG I.BR. HAMBURG MÜNCHEN STUTTGART WIEN

trivadis
makes IT easier.