Oracle Database 12c: Unified Auditing

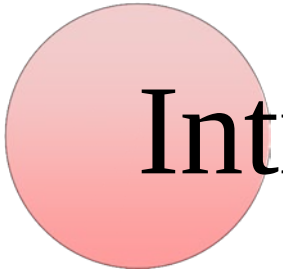
Maja Veselica, Security Consultant, Parallel
Zoran Pavlović, Security Team Lead, Parallel

Agenda

- *Introduction*
- *Architecture*
- *Mixed auditing mode*
- *How to enable the unified auditing mode*
- *New audit roles*
- *Using Auditing in Multitenant environment*
- *Create audit policies to audit privileges, actions and roles under specified conditions*

Agenda

- *Audit RMAN operations*
- *Audit Oracle Data Pump operations*
- *Use data dictionary views to display the audit policies and the audited data*
- *How to disable and drop audit policies*
- *How to clean up audit data*
- *Conclusion*

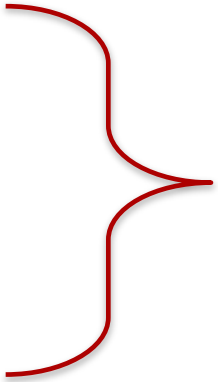


Introduction

Traditional vs Unified Audit Trail

Traditional Audit Trails

- SYS.AUD$
- SYS.FGA_LOG$
- V$XML_AUDIT_TRAIL
- DBA_COMMON_AUDIT_TRAIL
- DVSYS.AUDIT_TRAIL$
- OS files

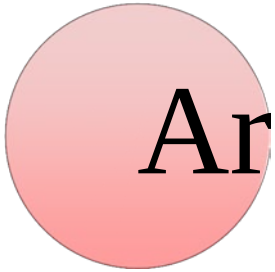


Unified Audit Trail

SYS.UNIFIED_AUDIT_TRAIL

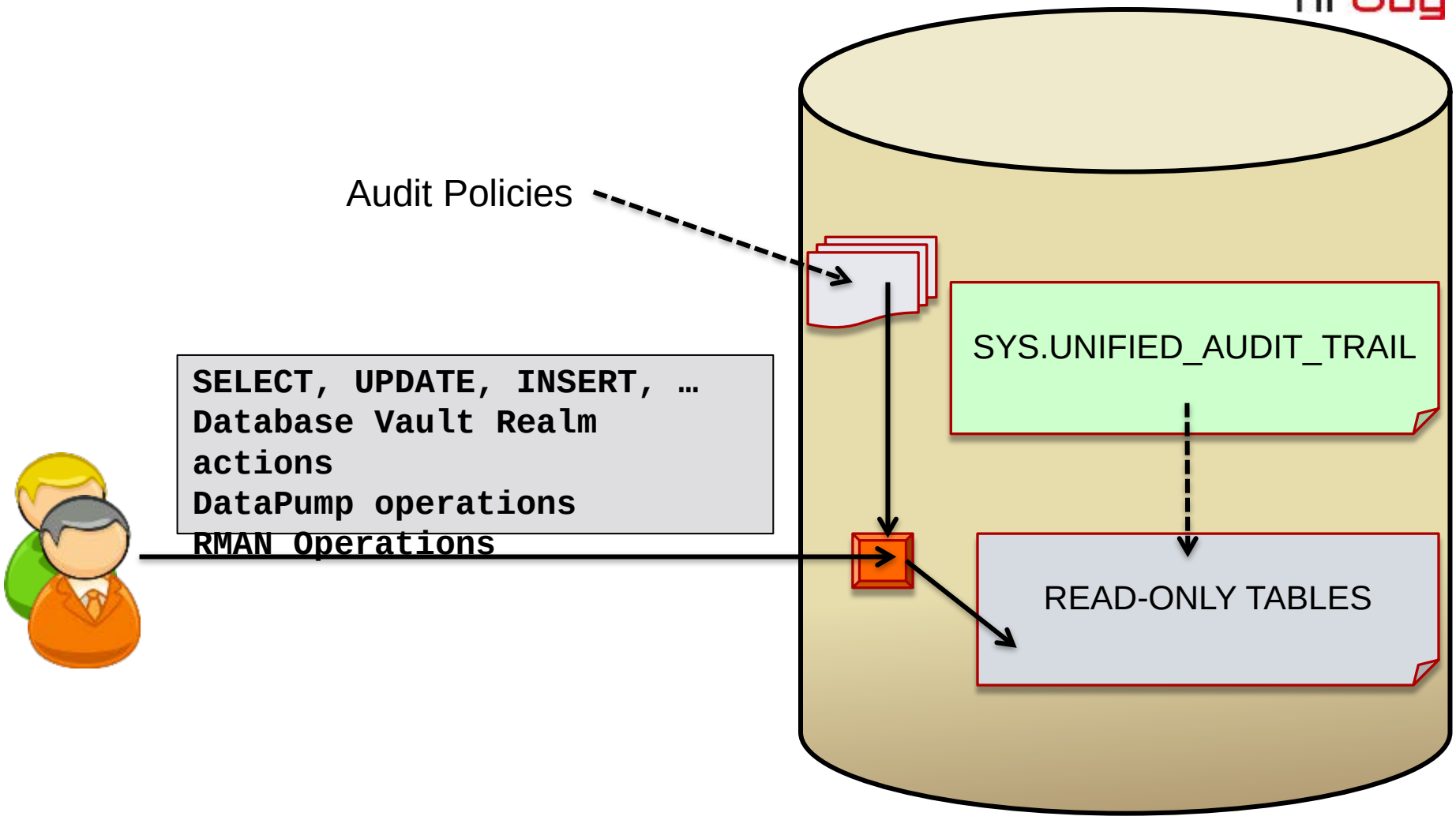
Unified Auditing Characteristics

- *Single audit trail*
- *Based on read-only table*
- *Extensible Audit Framework for additional columns*
- *Separation of audit administration with new roles*
- *Mixed and Unified Auditing Mode*
- *SYSLOG is not supported*



Architecture

Unified Audit - Architecture



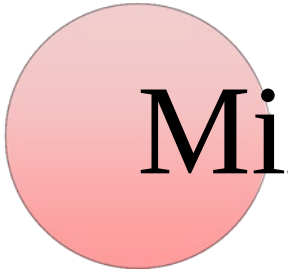
Write modes

- *Immediate-Write mode*
  - *Audit records are immediately written to disk*
  - *Performance impact exists*
- *Queued-Write mode*
  - *Audit records are written to SGA queues*
  - *Automatic / manual flush of the content of queues to disk*
  - *Audit records can be lost*

Setting Write mode

- *DBMS_AUDIT_MGMT.SET_AUDIT_TRAIL_PROPERTY*

```
SQL> EXEC DBMS_AUDIT_MGMT.SET_AUDIT_TRAIL_PROPERTY(
2 DBMS_AUDIT_MGMT.AUDIT_TRAIL_UNIFIED,
3 DBMS_AUDIT_MGMT.AUDIT_TRAIL_WRITE_MODE,
4 DBMS_AUDIT_MGMT.AUDIT_TRAIL_IMMEDIATE_WRITE);
```



Mixed auditing mode

Mixed auditing mode

- *Mixed auditing mode provides a way for both traditional and new engine to work at the same time.*

- *If existing database is upgraded to 12c to use mixed mode,*
  - *Create new audit policies or*
  - *You can use predefined policies:*
    - *ORA_SECURECONFIG, ORA_ACCOUNT_MGMT, ORA_DATABASE_PARAMETER*

Mixed auditing mode

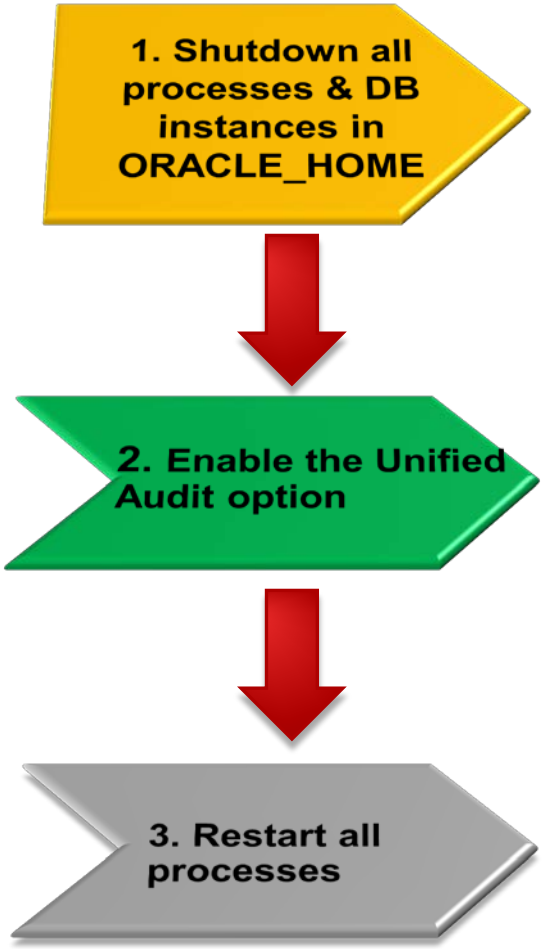
- *Audit data is written to old audit destinations and new unified audit trail*

- *When database is created (12c),*
  - *Mixed auditing mode is the default mode*
  - *Enabled predefined policy ORA_SECURECONFIG*

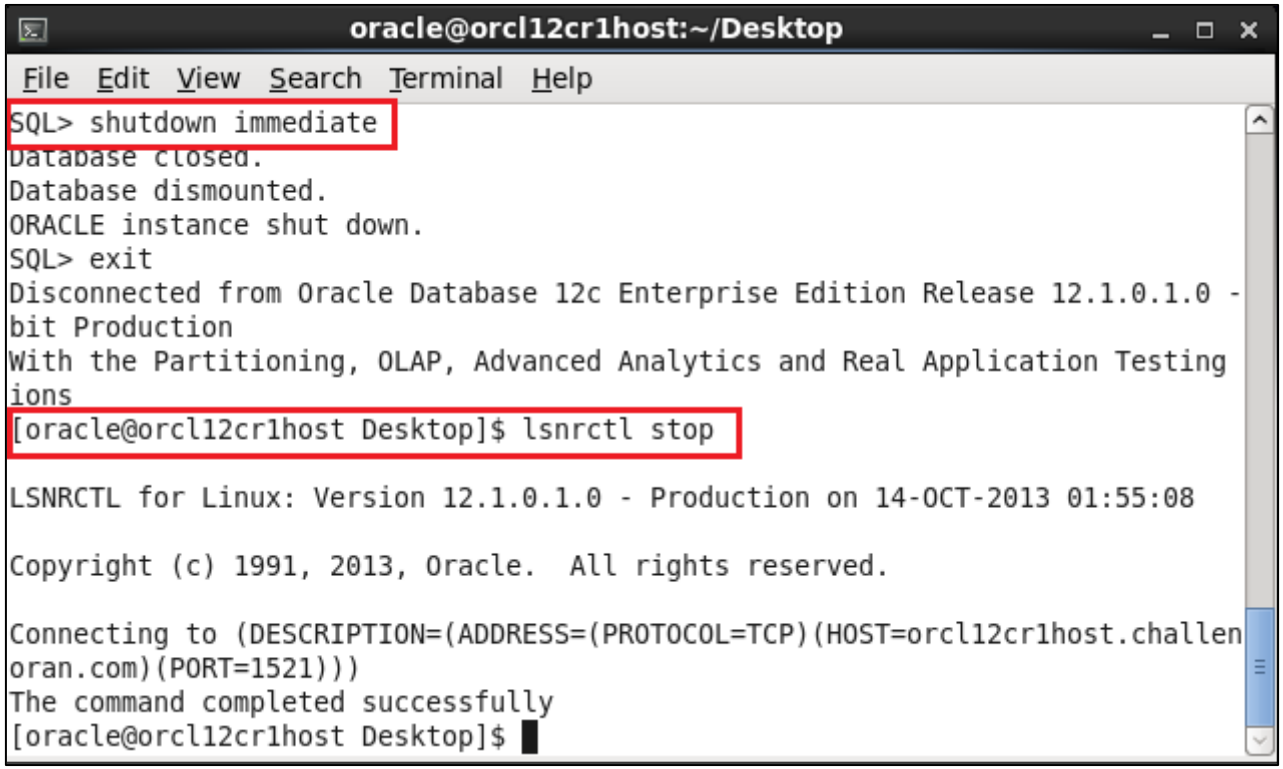
- *Unified auditing mode is not enabled*

How to enable the unified auditing mode

Unified Auditing mode

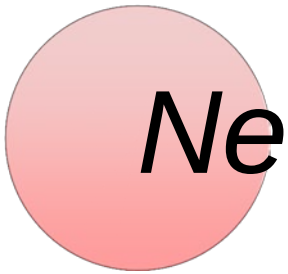


Step 1


oracle@orcl12cr1host:~/Desktop
File Edit View Search Terminal Help
SQL> shutdown immediate
Database closed.
Database dismounted.
ORACLE instance shut down.
SQL> exit
Disconnected from Oracle Database 12c Enterprise Edition Release 12.1.0.1.0 -
bit Production
With the Partitioning, OLAP, Advanced Analytics and Real Application Testing
ions
[oracle@orcl12cr1host Desktop]$ lsnrctl stop
LSNRCTL for Linux: Version 12.1.0.1.0 - Production on 14-OCT-2013 01:55:08
Copyright (c) 1991, 2013, Oracle. All rights reserved.
Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=orcl12cr1host.challen
oran.com)(PORT=1521)))
The command completed successfully
[oracle@orcl12cr1host Desktop]$

Step 2


oracle@orcl12cr1host:/u01/app/oracle/product/12.1.0/dbhome_1/rdbms
File Edit View Search Terminal Help
[oracle@orcl12cr1host Desktop]$ cd $ORACLE_HOME/rdbms/lib
[oracle@orcl12cr1host lib]$ make -f ins_rdbms.mk uniaud_on ioracle
/usr/bin/ar d /u01/app/oracle/product/12.1.0/dbhome_1/rdbms/lib/libknlopt.a k
zanang.o
/usr/bin/ar cr /u01/app/oracle/product/12.1.0/dbhome_1/rdbms/lib/libknlopt.a
/u01/app/oracle/product/12.1.0/dbhome_1/rdbms/lib/kzaiang.o
chmod 755 /u01/app/oracle/product/12.1.0/dbhome_1/bin
- Linking Oracle
rm -f /u01/app/oracle/product/12.1.0/dbhome_1/rdbms/lib/oracle
/u01/app/oracle/product/12.1.0/dbhome_1/bin/orald -o /u01/app/oracle/product
/12.1.0/dbhome_1/rdbms/lib/oracle -m64 -z noexecstack -Wl,--disable-new-dtags
-L/u01/app/oracle/product/12.1.0/dbhome_1/rdbms/lib/ -L/u01/app/oracle/produ
ct/12.1.0/dbhome_1/lib/ -L/u01/app/oracle/product/12.1.0/dbhome_1/lib/stubs/
-Wl,-E /u01/app/oracle/product/12.1.0/dbhome_1/rdbms/lib/opimai.o /u01/app/
oracle/product/12.1.0/dbhome_1/rdbms/lib/ssoraed.o /u01/app/oracle/product/12
.1.0/dbhome_1/rdbms/lib/ttcsoi.o -Wl,--whole-archive -lperfsrv12 -Wl,--no-who
le-archive /u01/app/oracle/product/12.1.0/dbhome_1/lib/nautab.o /u01/app/orac
le/product/12.1.0/dbhome_1/lib/naeet.o /u01/app/oracle/product/12.1.0/dbhome_



New audit roles

New Roles for Auditing

AUDIT_ADMIN

Manages audit configuration & audit trail

AUDIT_VIEWER

Analysis audit data

Using Auditing in Multitenant environment

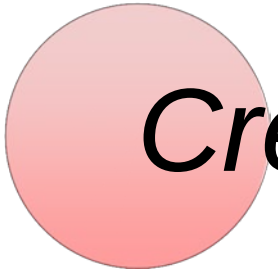
Auditing in the Multitenant environment

- *Local audit policy*
  - *Exists in: root or PDB*

- *Common audit policy*
  - *Exists in: all PDB*
  - *Create: only in root*
  - *Enable*(d): only common users*

  * *must have AUDIT_ADMIN role*

- *Default: Audit policies are local to current PDB*



Create audit policies

Audit Policies

```
SQL> CREATE AUDIT POLICY MY_POLICY
  2 PRIVILEGES SELECT ANY TABLE
  3 ACTIONS    CREATE TABLE, DROP TABLE;
```

```
SQL> AUDIT POLICY MY_POLICY BY HR;
```

- *Execute some auditable statements and view results*

```
SQL> CREATE TABLE T (a NUMBER(4));
SQL> DROP TABLE T;
SQL> EXEC SYS.DBMS_AUDIT_MGMT.FLUSH_UNIFIED_AUDIT_TRAIL;
```

Audit Policies

```
SQL> SELECT DBUSERNAME, ACTION_NAME, SYSTEM_PRIVILEGE_USED
  2  from unified_audit_trail
  3  where DBUSERNAME = 'HR';
```

```
DBUSERNAME           ACTION_NAME   SYSTEM_PRIVILEGE_USE
-------------------- ---------------- ---------------
HR                   CREATE TABLE CREATE TABLE
HR                   DROP TABLE
HR                   LOGON        CREATE SESSION
HR                   LOGON
HR                   LOGON        CREATE SESSION
HR                   LOGON        CREATE SESSION
HR                   LOGON        CREATE SESSION
HR                   LOGON        CREATE SESSION
HR                   LOGOFF
HR                   LOGOFF
HR                   LOGOFF
```

Audit Policies

```
SQL> CREATE AUDIT POLICY MY_POLICY2
  2  ROLES GLDB_MGR
  3  WHEN
    SYS_CONTEXT(''USERENV'',’’SESSION_USER'')=’’JOHN'''
  4  EVALUATE PER SESSION;
```

```
SQL> AUDIT POLICY MY_POLICY2 WHENEVER SUCCESSFUL;
```

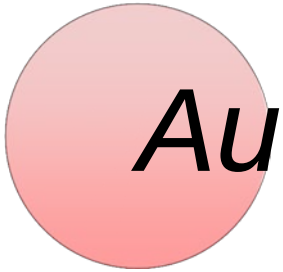
Audit Policies

```
SQL> CREATE AUDIT POLICY MY_POLICY3
  2  ACTIONS SELECT, UPDATE ON GLDB.CUSTOMERS;
```

- *Possible pitfall in the policy my_policy3*

```
SQL> AUDIT POLICY MY_POLICY3 EXCEPT ZORAN, MAJA;
```

- *You can't use both BY and EXCEPT lists*



Audit RMAN operations

Audit RMAN operations

- *RMAN events are automatically audited (you don't create audit policy)*

Audit RMAN operations

```
SQL> SELECT DBUSERNAME, RMAN_OPERATION
2 FROM UNIFIED_AUDIT_TRAIL
3 WHERE RMAN_OPERATION IS NOT NULL;
```

DBUSERNAME	RMAN_OPERATION
SYSBACKUP	Backup

Audit Oracle Data Pump operations

Unified Audit – DataPump Audit


```
SQL> CREATE AUDIT POLICY DP_POLICY ACTIONS
  2  COMPONENT=datapump export;
```

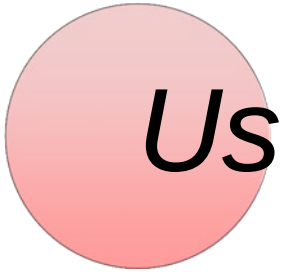

```
SQL> AUDIT POLICY DP_POLICY;
```


```
$ expdp system/passwd dumpfile=gldb_tables
    tables=gldb.customers
    directory=DATA_PUMP_DIR
```

Unified Audit – DataPump Audit

```
SQL> SELECT DBUSERNAME, DP_TEXT_PARAMETERS1, DP_BOOLEAN_PARAMETERS1
  2  FROM  UNIFIED_AUDIT_TRAIL;

DBUSERNAME
------------------------------
DP_TEXT_PARAMETERS1
--------------------------------------------------------------------
DP_BOOLEAN_PARAMETERS1
--------------------------------------------------------------------
SYSTEM
MASTER TABLE: "SYSTEM"."SYS_EXPORT_TABLE_01" , JOB_TYPE: EXPORT,
METADATA_JOB_M
ODE: TABLE_EXPORT, JOB VERSION: 12.0.0.0.0, ACCESS METHOD:
AUTOMATIC, DATA OPTIONS: 0, DUMPER DIRECTORY: NULL REMOTE LINK:
NULL, TABLE EXISTS: NULL, PARTITION
OPTIONS: NONE
MASTER_ONLY: FALSE, DATA_ONLY: FALSE, METADATA_ONLY: FALSE,
DUMPFILE_PRESENT: TRUE, JOB_RESTARTED: FALSE
```



Use data dictionary views

Data Dictionary Views

Data Dictionary Views: (not complete list)

- *AUDIT_UNIFIED_POLICIES*
- *AUDIT_UNIFIED_ENABLED_POLICIES*
- *UNIFIED_AUDIT_TRAIL*

How to disable and drop audit policies

Disable Audit Policy

- *Verify my_policy is enabled*

```
ops$maja@ORCL12CR1> select POLICY_NAME, ENABLED_OPT, USER_NAME,
SUCCESS, FAILURE
  2  from AUDIT_UNIFIED_ENABLED_POLICIES;

POLICY_NAME          ENABLED_ USER_NAME  SUC FAI
-------------------- -------- ---------- --- ---
MY_POLICY            BY       HR         YES YES
ORA_SECURECONFIG     BY       ALL USERS  YES YES
```

- *Disable my_policy*

```
SQL> noaudit policy my_policy; // intentionally didn't write BY HR to
show that, in this case, it will still audit HR as defined in my_policy
```

Disable Audit Policy

```
ops$maja@ORCL12CR1> grant select any table to hr;

hr@ORCL12CR1> select count(*) from oe.orders;

  COUNT(*)
----------
       105

ops$maja@ORCL12CR1> SELECT DBUSERNAME, ACTION_NAME, SYSTEM_PRIVILEGE_USED
  2  from unified_audit_trail
  3  where DBUSERNAME = 'HR' and ACTION_NAME NOT IN ('LOGON','LOGOFF');

DBUSERNAME                     ACTION_NAME      SYSTEM_PRIVILEGE_USE
------------------------------ ---------------- --------------------
HR                             CREATE TABLE     CREATE TABLE
HR                             SELECT           SELECT ANY TABLE
HR                             DROP TABLE
```

- ✓ *Disable my_policy*

```
SQL> noaudit policy my_policy BY HR;
```

Drop Audit Policy

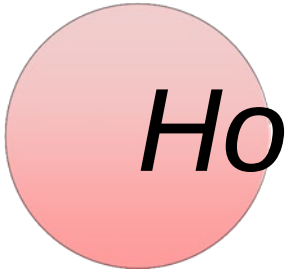
- *Verify my_policy is disabled*

```
SQL> select * from AUDIT_UNIFIED_ENABLED_POLICIES;
```

  - ✓ *Policy can be dropped only after it was disabled*

- *Drop my_policy*

```
SQL> drop audit policy my_policy;
```



How to clean up audit data

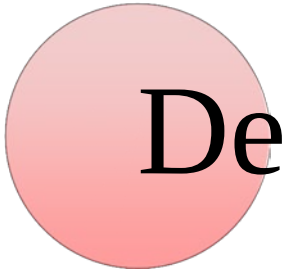
Clean up audit data

- *Manual*

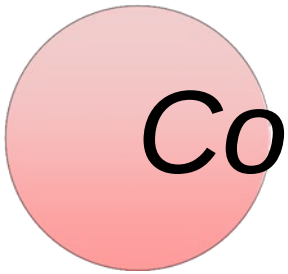
```
SQL> exec DBMS_AUDIT_MGMT.CLEAN_AUDIT_TRAIL(
AUDIT_TRAIL_TYPE => DBMS_AUDIT_MGMT.AUDIT_TRAIL_UNIFIED)
```

- *Schedule clean up job*

```
SQL> exec DBMS_AUDIT_MGMT.CREATE_PURGE_JOB
(AUDIT_TRAIL_TYPE => DBMS_AUDIT_MGMT.AUDIT_TRAIL_UNIFIED,
AUDIT_TRAIL_PURGE_INTERVAL => 24,
AUDIT_TRAIL_PURGE_NAME => 'My_Job',
USE_LAST_ARCH_TIMESTAMP => TRUE)
```



Demonstration



Conclusion

Conclusion

- *Unified Auditing is a new security feature*
- *Depending on which write mode is set, it may impact performance or security*
- *Check twice whether audit policy is written in a way that it accurately represents intended audit logic*

Contact

Maja Veselica, *Security Consultant*
maja.veselica@parallel.rs

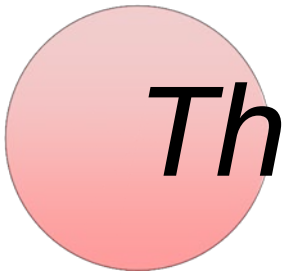
Twitter: orapassion

Zoran Pavlović, *Security Team Lead*
zoran.pavlovic@parallel.rs

Twitter: ChallengeZoran

Our Websites

www.optimasec.com – blog
www.challengezoran.com - forum
www.parallel.rs - Company



Thank you!