

<https://dbasobrinho.com.br/oracle-unified-auditing-habilitar-auditoria-de-logins-malsucedidos-e-ddl-passo-a-passo/>

1. Verificar o status do Unified Auditing

```
SQL> SELECT VALUE FROM V$OPTION WHERE PARAMETER = 'Unified Auditing';  
-----  
VALUE  
-----  
FALSE  
SQL>
```

Status do AUDIT_TRAIL:

```
SQL> SHOW PARAMETER AUDIT_TRAIL;  
-----  
NAME          TYPE    VALUE  
-----  
audit_trail   string  DB, EXTENDED  
SQL>
```

Entendendo os modos de auditoria

Modo de Auditoria	Unified Auditing	Parâmetro AUDIT_TRAIL	Recompilação Necessária?	Comandos AUDIT/NOAUDIT
Tradicional	FALSE	DB, EXTENDED ou XML	Não	Sim
Modo Misto	FALSE	DB, EXTENDED ou XML	Não	Sim
Modo Exclusivo	TRUE	NONE	Sim (uniaud_on)	Não

Se Unified Auditing = TRUE e AUDIT_TRAIL = NONE, o banco está no **modo exclusivo** e apenas a auditoria unificada está ativa.

Se Unified Auditing = FALSE e AUDIT_TRAIL = DB, EXTENDED ou XML, o banco está no **modo misto**, permitindo auditoria tradicional e unificada.

Se Unified Auditing = FALSE e AUDIT_TRAIL = NONE, a auditoria está completamente desativada.

Caso precise ativar o **modo exclusivo**, é necessário recompilar o Oracle com uniaud_on, conforme descrito na documentação:

[How To Enable The New Unified Auditing In 12c and 19c? \(Doc ID 1567006.1\)](#)

Eu costumo usar o **modo misto** para ambientes em operação, pois **não há necessidade de recompilação**. No entanto, se for um ambiente novo, você já pode iniciar diretamente no **modo puro (exclusivo)**.

Este post **não entrará nesse aspecto técnico**. No nosso teste, vamos usar o **modo misto**.

2. Configurar a tablespace da auditoria

Por padrão, os registros da auditoria unificada são armazenados na tablespace SYSAUX. É recomendado que os dados de auditoria fiquem em uma tablespace isolada.

2.1 Verificar a tablespace usada pela auditoria

```
SQL> SET LINES      188
SQL> SET PAGES     300
SQL> COLUMN PARAMETER_NAME FORMAT A30
SQL> COLUMN PARAMETER_VALUE FORMAT A30
SQL> COLUMN AUDIT_TRAIL FORMAT A30
SQL>
SQL> SELECT PARAMETER_NAME, PARAMETER_VALUE, AUDIT_TRAIL
  2  FROM DBA_AUDIT_MGMT_CONFIG_PARAMS
  3 WHERE PARAMETER_NAME = 'DB_AUDIT_TABLESPACE';
PARAMETER_NAME          PARAMETER_VALUE          AUDIT_TRAIL
-----  -----  -----
DB AUDIT TABLESPACE      SYSAUX        STANDARD AUDIT TRAIL
DB AUDIT TABLESPACE      SYSAUX        FGA AUDIT TRAIL
DB AUDIT TABLESPACE      SYSAUX        UNIFIED AUDIT TRAIL
SQL>
```

2.2 Alterar a tablespace da auditoria unificada

Se necessário criar uma nova tablespace dedicada (TBS_AUDIT):

```
SQL>

CREATE TABLESPACE TBS_AUDIT
DATAFILE '/u01/app/oracle/oradata/ORCL/tbs_audit01.dbf'
SIZE 1G AUTOEXTEND ON NEXT 512M MAXSIZE 10G;

Tablespace created.

SQL>
```

Mover a auditoria para essa nova tablespace:

```
SQL>

BEGIN
  DBMS_AUDIT_MGMT.SET_AUDIT_TRAIL_LOCATION(
    AUDIT_TRAIL_TYPE => DBMS_AUDIT_MGMT.AUDIT_TRAIL_UNIFIED,
    AUDIT_TRAIL_LOCATION_VALUE => 'TBS_AUDIT'
  );
END;
/
PL/SQL procedure successfully completed.

SQL>
```

Verificar se a alteração foi aplicada:

```
SQL>

SET LINES      188
SET PAGES     300
COLUMN PARAMETER_NAME FORMAT A30
COLUMN PARAMETER_VALUE FORMAT A30
COLUMN AUDIT_TRAIL FORMAT A30

SELECT PARAMETER_NAME, PARAMETER_VALUE, AUDIT_TRAIL
FROM DBA_AUDIT_MGMT_CONFIG_PARAMS
WHERE PARAMETER_NAME = 'DB AUDIT TABLESPACE';

PARAMETER_NAME          PARAMETER_VALUE          AUDIT_TRAIL
-----                  -----                  -----
DB AUDIT TABLESPACE    SYSAUX                STANDARD AUDIT TRAIL
DB AUDIT TABLESPACE    SYSAUX                FGA AUDIT TRAIL
DB AUDIT TABLESPACE    TBS_AUDIT             UNIFIED AUDIT TRAIL
```

SQL>

3. Criar e ativar auditorias

3.1 Auditoria de logins malsucedidos



```
SQL>

CREATE AUDIT POLICY AUDIT_LOGON_FAIL ACTIONS LOGON;
Audit policy created.

SQL>
```

Ativar a auditoria somente para logins malsucedidos:

```
SQL>

AUDIT POLICY AUDIT_LOGON_FAIL WHENEVER NOT SUCCESSFUL;
Audit succeeded.

SQL>
```

3.1 Auditoria de alterações em objetos

```
SQL>

CREATE AUDIT POLICY AUDIT_DDL_CHANGES
ACTIONS
  CREATE TABLE, ALTER TABLE, DROP TABLE,
  CREATE INDEX, ALTER INDEX, DROP INDEX,
  CREATE VIEW, ALTER VIEW, DROP VIEW,
  CREATE SEQUENCE, ALTER SEQUENCE, DROP SEQUENCE,
  CREATE PROCEDURE, ALTER PROCEDURE, DROP PROCEDURE,
  CREATE FUNCTION, ALTER FUNCTION, DROP FUNCTION,
  CREATE PACKAGE, ALTER PACKAGE, DROP PACKAGE,
  CREATE TRIGGER, ALTER TRIGGER, DROP TRIGGER,
  CREATE SYNONYM, DROP SYNONYM,
  CREATE TYPE, ALTER TYPE, DROP TYPE,
  CREATE USER, ALTER USER, DROP USER;
```

```
Audit policy created.
```

```
SQL>
```

Ativar a auditoria:

```
SQL>

AUDIT POLICY AUDIT_DDL_CHANGES;

Audit succeeded.

SQL>
```

3.3 Verificar quais políticas de auditoria estão ativas

```
SQL>

SELECT POLICY_NAME FROM AUDIT_UNIFIED_ENABLED_POLICIES;

POLICY_NAME
-----
AUDIT_LOGON_FAIL
AUDIT_DDL_CHANGES

SQL>
```

4. Testar e consultar as auditorias

4.1 Testar auditoria de login malsucedido

```
lnxorany01:/home/oracle$ sqlplus USER_FAKE/senha@DWPRD
SQL*Plus: Release 19.0.0.0.0 - Production on Wed Feb 26 15:00:12 2025
Version 19.16.0.0.0
Copyright (c) 1982, 2022, Oracle. All rights reserved.

ERROR:
ORA-01017: invalid username/password; logon denied

Enter user-name:
lnxorany01:/home/oracle$
```

4.2 Testar auditoria DDL

Executar os seguintes comandos para verificar se a auditoria de DDL (criação, alteração e exclusão de objetos) está funcionando:

```
SQL>
CREATE TABLE TEST_AUDIT (ID NUMBER);
Table created.
SQL>
ALTER TABLE TEST_AUDIT ADD (NAME VARCHAR2(100));
Table altered.
SQL>
DROP TABLE TEST_AUDIT;
Table dropped.
```

4.3 Consultar auditorias registradas

Executar os seguintes comandos para verificar se as auditorias estão funcionando:

```
SQL>

SET LINESIZE 200
SET PAGESIZE 100
SET TRIMOUT ON
SET TRIMSPOOL ON
SET LONG 2000
COLUMN EVENT_TIMESTAMP FORMAT A30
COLUMN DBUSERNAME FORMAT A20
COLUMN ACTION_NAME FORMAT A30
COLUMN OBJECT_NAME FORMAT A30
COLUMN RETURN_CODE FORMAT 99999
COLUMN UNIFIED_AUDIT_POLICIES FORMAT A30

SELECT EVENT_TIMESTAMP,
       DBUSERNAME,
       ACTION_NAME,
       OBJECT_NAME,
       RETURN_CODE,
       UNIFIED_AUDIT_POLICIES
FROM UNIFIED_AUDIT_TRAIL
ORDER BY EVENT_TIMESTAMP DESC;

EVENT_TIMESTAMP          DBUSERNAME    ACTION_NAME   OBJECT_NAME  RETURN_CODE UNIFIED_AUDIT_POLICIES
-----  -----  -----  -----  -----
25-FEB-24 13:40:00      SYSTEM        DROP TABLE   TEST_AUDIT    0        AUDIT_DDL_CHANGES
25-FEB-24 13:39:45      SYSTEM        ALTER TABLE  TEST_AUDIT    0        AUDIT_DDL_CHANGES
25-FEB-24 13:39:30      SYSTEM        CREATE TABLE TEST_AUDIT    0        AUDIT_DDL_CHANGES
25-FEB-24 13:30:15      FAKE_USER    LOGON        -           1017     AUDIT_LOGON_FAIL

SQL>
```

Todos os eventos de logins malsucedidos e alterações em objetos foram registrados.

RETURN_CODE = 1017 indica falha de login.

A política aplicada aparece na coluna UNIFIED_AUDIT_POLICIES.

DBA SOBRINHO

5. Purge dos registros de auditoria

A auditoria pode gerar um grande volume de dados com o tempo, e esses registros não são removidos automaticamente.

5.1 Remover registros com mais de 30 dias

```
SQL>

SELECT COUNT(*) FROM UNIFIED_AUDIT_TRAIL;

COUNT(*)
-----
12573

SQL>

BEGIN
  DBMS_AUDIT_MGMT.SET_LAST_ARCHIVE_TIMESTAMP(
    AUDIT_TRAIL_TYPE => DBMS_AUDIT_MGMT.AUDIT_TRAIL_UNIFIED,
    LAST_ARCHIVE_TIME => SYSTIMESTAMP - INTERVAL '30' DAY );
  DBMS_AUDIT_MGMT.CLEAN_AUDIT_TRAIL(
    AUDIT_TRAIL_TYPE => DBMS_AUDIT_MGMT.AUDIT_TRAIL_UNIFIED,
    USE_LAST_ARCH_TIMESTAMP => TRUE );
END;
/

PL/SQL procedure successfully completed.

SELECT COUNT(*) FROM UNIFIED_AUDIT_TRAIL;

COUNT(*)
-----
8592

SQL>
```

Define que apenas registros com mais de 30 dias serão removidos.

DBA SOBRINHO

5.2 Remover todos os registros da auditoria

```
SELECT COUNT(*) FROM UNIFIED_AUDIT_TRAIL;
COUNT(*)
-----
8592
SQL>
SQL>
BEGIN
  DBMS_AUDIT_MGMT.CLEAN_AUDIT_TRAIL(
    AUDIT_TRAIL_TYPE => DBMS_AUDIT_MGMT.AUDIT_TRAIL_UNIFIED,
    USE_LAST_ARCH_TIMESTAMP => FALSE
  );
END;
/
PL/SQL procedure successfully completed.

SELECT COUNT(*) FROM UNIFIED_AUDIT_TRAIL;
COUNT(*)
-----
0
SQL>
```

Todos os registros foram removidos e a trilha de auditoria.

Importante! A execução do comando CLEAN_AUDIT_TRAIL não é automática. Ele apenas executa a limpeza uma única vez no momento da execução.

Se quiser que a remoção dos registros aconteça regularmente, configurar um **job no Oracle Scheduler**

6. Desativar e excluir uma política de auditoria

Antes de desativar ou excluir, verificar quais políticas estão ativas no banco:

```
SQL>
SELECT POLICY_NAME FROM AUDIT_UNIFIED_ENABLED_POLICIES;
POLICY_NAME
-----
AUDIT_LOGON_FAIL
AUDIT_DDL_CHANGES
SQL>
```

6.1 Desativar uma política de auditoria (sem excluir)

A política continua existindo, mas **os eventos não serão mais auditados**.

```
SQL>  
  
NOAUDIT POLICY AUDIT_LOGON_FAIL;  
  
Noaudit succeeded.  
  
NOAUDIT POLICY AUDIT_DDL_CHANGES;  
  
Noaudit succeeded.  
  
SQL>
```

6.2 Desativar uma política de auditoria (sem excluir)

Se a política **não for mais necessária** e quiser removê-la definitivamente do banco, usar o comando DROP AUDIT POLICY:

```
SQL>  
  
DROP AUDIT POLICY AUDIT_LOGON_FAIL;  
  
Audit policy dropped.  
  
DROP AUDIT POLICY AUDIT_DDL_CHANGES;  
  
Audit policy dropped.  
  
SQL>
```

Conclusão

- ✓ **O modo misto** permite usar auditoria tradicional e unificada sem recompilar nada.
- ✓ Recomenda-se mover os registros de auditoria para uma tablespace separada, evitando impacto na SYSAUX.
- ✓ A limpeza de registros não é automática, sendo necessário executar manualmente ou configurar um job para automação.
- ✓ Políticas podem ser desativadas temporariamente ou excluídas permanentemente, dependendo da necessidade.
- ✓ Aqui estão as configurações básicas para uma auditoria muito requisitada pelos DBAs, no entanto, isso não representa nem 1% do que é possível fazer com auditoria no Oracle.

Para mais detalhes e aprofundamento.

- 🔗 [Unified Auditing – Oracle Docs](#)
- 🔗 [Auditing Enhancements \(Audit Policies and Unified Audit Trail\) in Oracle Database](#)

#20250303 #DBASobrinho #GuinaNãoTinhaDó #BóBó #CaceteDeAguilha #OracleACE

- 🔗 [audit_unified_login_fail_and_all_ddl.sql](#)
-