Home / Database / Oracle Database Online Documentation 11g Release 2 (11.2) / Database Administration

Database Security Guide

9 Verifying Security Access with Auditing

[https://docs.oracle.com/cd/E11882\_01/network.112/e36292/auditing.htm#DBSEG006](https://docs.oracle.com/cd/E11882_01/network.112/e36292/auditing.htm" \l "DBSEG006)

》什么是审计

Auditing is the monitoring and recording of selected user database actions

Oracle recommends that you enable and configure auditing.

Auditing is an effective method of enforcing strong internal controls so that your site can meet its regulatory compliance requirements, as defined in the Sarbanes-Oxley Act

》为什么使用审计

保护受信任的职位。如：银行收纳

阻止用户的不当行为。防止用户在自己责任范围内做不当的操作，如：恶意篡改数据

调查可疑的活动。如：如果一个用户删除了某条数据，可以从审计记录中确认其行为

监视和收集数据库活动数据。如依据审计记录统计某个表的并发访问，数据库登录等行为

符合监管需要。如一些法律和制度要求

》保护数据库的审计

在审核可疑数据库活动时, 应保护审计跟踪记录的完整性, 以保证审计记录的准确性和完整性。

（When auditing for suspicious database activity, you should protect the integrity of the audit trail records to guarantee the accuracy and completeness of the auditing information.）

数据库的审计记录一般存储在 SYS.AUD$ and SYS.FGA\_LOG$ tables

1 O7\_DICTIONARY\_ACCESSIBILITY = FALSE (the default).

只允许sysdba权限的用户对SYS.AUD$ and SYS.FGA\_LOG$ tables DML操作

》审计记录的生成

non-SYS用户总是生成审计记录存储在SYS.AUD$ and SYS.FGA\_LOG$ tables（存放在数据库外部，由参数AUDIT\_FILE\_DEST定义）

SYS用户默认不生成审计记录，**除非额外配置**

》审计的类型

**1 强制审计（ mandatory auditing）**

**为什么$ORACLE\_HOME所在磁盘满了，sys用户无法连接数据库？？**

Oracle总是审计以SYSDBA or SYSOPER权限登陆数据库的动作，记录在操作系统审计文件中

默认位置$ORACLE\_BASE/admin/$ORACLE\_SID/adump

可通过参数AUDIT\_FILE\_DEST更改

强制审计审计的操作

Database startup

SYSDBA and SYSOPER logins

Database shutdown

os 路径audit\_trail\_dest,不可用则使用默认路径$ORACLE\_HOME/rdbms/audit  !!

必要的时候，这两个路径需要清理。！

script-delete trace file

======================================

**2 审计SYS管理员账户**

标准数据库审计和细粒度审计均不包括SYS管理账户审计

对SYS用户的审计，需要配置参数

ALTER SYSTEM SET AUDIT\_SYS\_OPERATIONS=TRUE SCOPE=SPFILE;

重启数据库

存储路径位于操作系统上，由参数AUDIT\_FILE\_DEST指定

第一默认路径： $ORACLE\_BASE/admin/$ORACLE\_SID/adump

默认路径不可用使用 $ORACLE\_HOME/rdbms/audit

eg:

select spid from v$process where pid in (select userenv('pid') from dual);

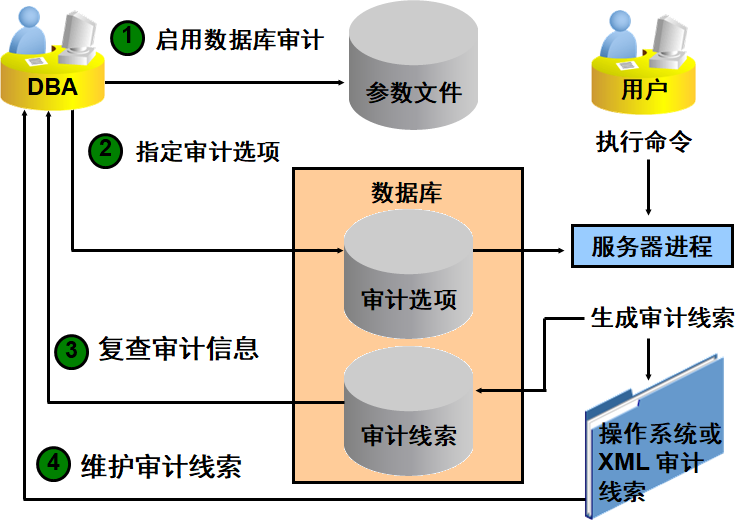
alter database backup controlfile to trace;

============================

**3 标准数据库审计（Standard Auditing）**

可以审计SQL statements, privileges, schema objects, and network activity.

标准数据库审计是全局的，要么启用，要么关闭。



**启用标准数据库审计**

设置参数

AUDIT\_TRAIL=DB

禁用标准数据库审计

AUDIT\_TRAIL=NONE

注：静态参数，需要重启生效

**指定审计项-AUDIT语句选项**

标准数据库审计使用AUDIT语句生成审计项，可以实现重点审计和非重点审计

使用NOAUDIT删除审计项

审计所有用户或指定的用户

--标准数据库审计语句（audit）可以使用Successful, Unsuccessful, or Both

WHENEVER SUCCESSFUL clause: This clause audits only successful executions of the audited statement.

WHENEVER NOT SUCCESSFUL clause: This clause audits only unsuccessful executions of the audited statement.

both：默认

--标准数据库审计语句（audit）可以使用BY ACCESS and BY SESSION

BY ACCESS：每次审计事件发生都会产生一条审计记录    --默认，11.2.0.2及以上

BY SESSION：相同审计事件发生时，会话中只产生一条审计记录

--标准数据库审计语句（audit）可以使用by user

**指定审计项-审计SQL语句**

审计特定对象上的相关SQL语句或特定类型的SQL，而不是SQL本身

对象上的SQL包括

DDL statements. For example, AUDIT TABLE audits all CREATE and DROP TABLE statements

DML statements. For example, AUDIT SELECT TABLE audits all SELECT ... FROM TABLE/VIEW statements, regardless of the table or view

默认可以AUDIT自己用户下对象上的SQL，如果AUDIT其他用户下对象需要AUDIT SYSTEM系统权限

EG:

AUDIT DELETE TABLE BY HR BY ACCESS;

AUDIT DELETE TABLE BY SCOTT;     --？by session默认？

ALL STATEMENTS子句审计所有sql

AUDIT ALL STATEMENTS BY HR, SCOTT BY ACCESS WHENEVER SUCCESSFUL;

NOAUDIT DELETE TABLE BY HR BY ACCESS;  --删除单个语句审计项

NOAUDIT ALL STATEMENTS;     --删除所有语句审计项

select \* from DBA\_STMT\_AUDIT\_OPTS WHERE USER\_NAME='HR';

Auditing login and logoff connections and disconnections.

AUDIT SESSION BY hr,scott BY ACCESS;

**指定审计项-审计权限**

审计使用 **系统权限** 的SQL

审计所有用户或指定的用户

权限审计比语句审计更具针对性，审计的范围更小

注意：

如果为语句和权限审计设置了类似的审核选项, 则只生成单个审核记录

对于系统权限，如果已有权限足够，不需要系统权限，则不生成审计记录（如：对于select any table系统权限，scott查询自己用户下的dmp表不生成审计记录，查询hr.employees则会生成审计记录）

eg：

AUDIT DELETE ANY TABLE by hr BY ACCESS;

NOAUDIT DELETE ANY TABLE by hr;

NOAUDIT ALL PRIVILEGES;  --删除所有权限审计项

select \* from DBA\_PRIV\_AUDIT\_OPTS WHERE USER\_NAME='HR';;

**指定审计项-审计模式对象**

审计模式对象的操作（包括表，视图，索引，存储过程，函数等）

审计所有用户，不能指定用户

eg：

AUDIT DELETE ON hr.employees BY ACCESS;

AUDIT INSERT, UPDATE ON hr.employees BY ACCESS WHENEVER SUCCESSFUL;

AUDIT all ON hr.employees BY ACCESS WHENEVER SUCCESSFUL;

NOAUDIT SELECT, INSERT, DELETE ON hr.employees;

NOAUDIT ALL ON hr.employees;  --删除所有对象上的审计项

select \* from  DBA\_OBJ\_AUDIT\_OPTS;

**指定审计项-审计网络活动**

审计网络协议中的意外错误或网络层中的内部错误。

eg：

AUDIT NETWORK BY ACCESS;

NOAUDIT NETWORK;

**默认审计项**

默认审计审计了数据库安全相关的**SQL语句和权限**

Database Configuration Assistant (DBCA)创建的数据库，有默认审计

手动建库，运行脚本secconf.sql生成默认审计

Privileges That Oracle Database Audits by Default

Oracle Database audits the following privileges by default:

ALTER ANY PROCEDURE

CREATE ANY LIBRARY

**DROP ANY TABLE**

**ALTER ANY TABLE**

CREATE ANY PROCEDURE

DROP PROFILE

ALTER DATABASE

**CREATE ANY TABLE**

**DROP USER**

ALTER PROFILE

CREATE EXTERNAL JOB

EXEMPT ACCESS POLICY

ALTER SYSTEM

CREATE PUBLIC DATABASE LINK

GRANT ANY OBJECT PRIVILEGE

**ALTER USER**

CREATE SESSION

GRANT ANY PRIVILEGE

AUDIT SYSTEM

**CREATE USER**

GRANT ANY ROLE

CREATE ANY JOB

DROP ANY PROCEDURE

Oracle Database audits the following SQL shortcuts by default:

DATABASE LINK

PUBLIC SYNONYM

SYSTEM AUDIT

PROFILE

ROLE

SYSTEM GRANT

**禁用默认审计项**

**$ORACLE\_HOME/rdbms/admin/undoaud.sql**

**重新生成默认审计项**

**$ORACLE\_HOME/rdbms/admin/secconf.sql**

**这两个脚本也可以自定义**

注意：默认审计会审计LOGON/LOGFF

eg：

SELECT

    os\_username,

    username,

    userhost,

    timestamp,

    action\_name,

    comment\_text

FROM

    dba\_audit\_trail

WHERE

    username = 'MOBILESERVER'

    AND action\_name = 'LOGON'

    AND timestamp > TO\_DATE('2018-07-30','YYYY-MM-DD');

    MOBILESERVER    localhost.localdomain    01-AUG-18    LOGON    Authenticated by: DATABASE; Client address: (ADDRESS=(PROTOCOL=tcp)(HOST=10.243.3.42)(PORT=56517))

    MOBILESERVER    localhost.localdomain    01-AUG-18    LOGON    Authenticated by: DATABASE; Client address: (ADDRESS=(PROTOCOL=tcp)(HOST=10.243.3.42)(PORT=60597))

    MOBILESERVER    localhost.localdomain    01-AUG-18    LOGON    Authenticated by: DATABASE; Client address: (ADDRESS=(PROTOCOL=tcp)(HOST=10.243.3.42)(PORT=56513))

    MOBILESERVER    localhost.localdomain    01-AUG-18    LOGON    Authenticated by: DATABASE; Client address: (ADDRESS=(PROTOCOL=tcp)(HOST=10.243.3.42)(PORT=60593))

    MOBILESERVER    localhost.localdomain    01-AUG-18    LOGON    Authenticated by: DATABASE; Client address: (ADDRESS=(PROTOCOL=tcp)(HOST=10.243.3.42)(PORT=60584))

    MOBILESERVER    localhost.localdomain    01-AUG-18    LOGON    Authenticated by: DATABASE; Client address: (ADDRESS=(PROTOCOL=tcp)(HOST=10.243.3.42)(PORT=60582))

--标准数据库审计实验

查看默认审计记录

create user aud identified by aud;

grant dba to aud;

conn aud/aud

create table hr.test\_audit (name varchar2(22));    --必须是没有resource权限，使用create any table系统权限才会生成审计记录，不能在自己用户下创建

insert into hr.test\_audit values ('iii');

audit update,delete on hr.test\_audit;

delete from hr.test\_audit;

select \* from  DBA\_OBJ\_AUDIT\_OPTS WHERE object\_name='TEST\_AUDIT';

select \* from DBA\_COMMON\_AUDIT\_TRAIL where object\_name='TEST\_AUDIT';

delete from aud$;

select userhost,username,owner,obj\_name,action\_name,timestamp from dba\_audit\_trail where username='HR';

noaudit delete on hr.test\_audit;

===================================

**4 细粒度审计（Fine-Grained Auditing）**

细粒度审计允许创建一个策略，自定义触发条件。如使用布尔条件，范围比较，审计列，这些细粒度审计满足深层次需求

细粒度审计使用不需要初始化参数，不需要特许配置，使用PLSQL程序包DBMS\_FGA,需要有这个包的权限。

**细粒度审计的记录存储在SYS.FGA\_LOG$表，对于SYS.FGA\_LOG$表的DML操作总是生成审计记录存储在sys.aud$表**

eg：配置细粒度审计

生成审计策略

BEGIN

  DBMS\_FGA.ADD\_POLICY(object\_schema     => 'HR',

                      object\_name       => 'EMPLOYEES',

                      policy\_name       => 'chk\_hr\_employees',

                      audit\_condition   => 'DEPARTMENT\_ID = 50',

                      audit\_column      => 'SALARY,COMMISSION\_PCT',

                      audit\_column\_opts => DBMS\_FGA.ANY\_COLUMNS,

                      enable            => TRUE,

                      statement\_types   => 'INSERT, UPDATE, SELECT, DELETE',

                      handler\_schema    => '',

                      handler\_module    => '',

                      audit\_trail       => DBMS\_FGA.DB + DBMS\_FGA.EXTENDED);

END;

/

You cannot modify a fine-grained audit policy after you have created it. If you need to modify the policy, drop it and then recreate it.

audit\_trail       => DBMS\_FGA.DB + DBMS\_FGA.EXTENDED

禁用

begin

  DBMS\_FGA.DISABLE\_POLICY(object\_schema => 'HR',

                       object\_name   => 'EMPLOYEES',

                       policy\_name   => 'chk\_hr\_employees');

end;

/

启用

begin

  DBMS\_FGA.ENABLE\_POLICY(object\_schema => 'HR',

                         object\_name   => 'EMPLOYEES',

                         policy\_name   => 'chk\_hr\_employees',

                         enable        => TRUE);

end;

/

删除

begin

  DBMS\_FGA.DROP\_POLICY(object\_schema => 'HR',

                       object\_name   => 'EMPLOYEES',

                       policy\_name   => 'chk\_hr\_employees');

end;

/

查询细粒度审计策略

select \* from DBA\_AUDIT\_POLICIES;

产生审计记录

conn aud/aud

select employee\_id,salary from hr.employees where department\_id=50;

查询细粒度审计记录

select \* from DBA\_COMMON\_AUDIT\_TRAIL where object\_name='EMPLOYEES';

将审计记录放置到新表空间

BEGIN

  DBMS\_AUDIT\_MGMT.SET\_AUDIT\_TRAIL\_LOCATION(AUDIT\_TRAIL\_TYPE           => DBMS\_AUDIT\_MGMT.AUDIT\_TRAIL\_FGA\_STD,

                                           AUDIT\_TRAIL\_LOCATION\_VALUE => 'USERS');

END;

/

======================================

**》管理审计线索**

审计线索由参数 AUDIT\_TRAIL定义

AUDIT\_TRAIL=DB  --将审计记录存储在数据库中（sys.aud$）

DB,EXTENDED  --如同DB，但额外抓取sql语句，绑定变量和clob文本

OS  --将审计记录存储在操作系统上

XML  --以XML格式将审计记录存储在操作系统上

XML, EXTENDED  --类似DB,EXTENDED

if you have set the AUDIT\_TRAIL initialization parameter to DB, EXTENDED or XML, EXTENDED, then the SQL\_BIND and SQL\_TEXT columns show any SQL bind variables used for a SQL statement and SQL text that triggered the audit,

**===================================**

**》管理审计记录**

DBA\_AUDIT\_TRAIL for the SYS.AUD$ contents

DBA\_FGA\_AUDIT\_TRAIL for the SYS.FGA\_LOG$ contents

DBA\_COMMON\_AUDIT\_TRAIL for both SYS.AUD$ and SYS.FGA\_LOG$ contents

reference：

审计项

DBA\_AUDIT\_POLICIES

Lists all the fine-grained auditing policies on the system

DBA\_OBJ\_AUDIT\_OPTS

Displays the objects on which auditing options have been enabled

DBA\_PRIV\_AUDIT\_OPTS

Describes current system privileges being audited across the system and by user

DBA\_STMT\_AUDIT\_OPTS

Describes current statement auditing options across the system and by user

审计记录

DBA\_AUDIT\_TRAIL

Lists all standard audit trail entries in the AUD$ table

DBA\_FGA\_AUDIT\_TRAIL

Lists audit trail records for fine-grained auditing.

DBA\_COMMON\_AUDIT\_TRAIL

Combines standard and fine-grained audit log records, and includes SYS and mandatory audit records written in XML format

当审计记录所在的空间用尽时，Oracle会报错，对那些新产生审计记录的用户

控制审计记录大小

--禁用数据库审计

--有选择的启用审计项，不要使用AUDIT ANY这种语句

--数据库审计跟踪表 (AUD $ 和 FGA\_LOG $) 的最大大小由系统表空间的默认存储参数确定, 默认情况下它存储在其中。

如果您担心太大的数据库审核跟踪会影响系统表性能, 请考虑将数据库审核跟踪表移动到不同的空间。

**移动审计记录到其他表空间**

注意：将数据库审计跟踪表移动到不同表空间可能会花费很长时间, 这取决于审计表格中的审计数据量,需要在数据库不繁忙时执行

1 sys登陆数据库

2 检查可用的表空间

3 运行DBMS\_AUDIT\_MGMT.SET\_AUDIT\_TRAIL\_LOCATION plsql程序

BEGIN

  DBMS\_AUDIT\_MGMT.SET\_AUDIT\_TRAIL\_LOCATION(AUDIT\_TRAIL\_TYPE           => DBMS\_AUDIT\_MGMT.AUDIT\_TRAIL\_AUD\_STD,

                                           AUDIT\_TRAIL\_LOCATION\_VALUE => 'USERS');

END;

/

DELETE, INSERT, UPDATE, and MERGE operations on the SYS.AUD$ and SYS.FGA\_LOG$ tables are always audited. These audit records are not allowed to be deleted.

SQL> select owner,table\_name,tablespace\_name from dba\_tables where table\_name in ('AUD$','FGA\_LOG$');

OWNER                   TABLE\_NAME              TABLESPACE\_NAME

------------------------------ ------------------------------ ------------------------------

SYS                   FGA\_LOG$               USERS

SYS                   AUD$                  SYSTEM

OWNER                   TABLE\_NAME              TABLESPACE\_NAME

------------------------------ ------------------------------ ------------------------------

SYS                   FGA\_LOG$               USERS

SYS                   AUD$                  USERS

======================================

**管理操作系统审计记录**

为了防止os audit trail文件占用全部磁盘空间，可设置空间使用限制。使用plsql程序包DBMS\_AUDIT\_MGMT

BEGIN

  DBMS\_AUDIT\_MGMT.SET\_AUDIT\_TRAIL\_PROPERTY(AUDIT\_TRAIL\_TYPE           => DBMS\_AUDIT\_MGMT.AUDIT\_TRAIL\_OS,

                                           AUDIT\_TRAIL\_PROPERTY       => DBMS\_AUDIT\_MGMT.OS\_FILE\_MAX\_SIZE,

                                           AUDIT\_TRAIL\_PROPERTY\_VALUE => 102400);

END;

/

DBMS\_AUDIT\_MGMT.AUDIT\_TRAIL\_OS：表示操作系统上 .aud 后缀的文件

限定了单个文件最大大小 100m，默认10m

取消限制更改，使用默认值

BEGIN

  DBMS\_AUDIT\_MGMT.CLEAR\_AUDIT\_TRAIL\_PROPERTY(AUDIT\_TRAIL\_TYPE     => DBMS\_AUDIT\_MGMT.AUDIT\_TRAIL\_OS,

                                             AUDIT\_TRAIL\_PROPERTY => DBMS\_AUDIT\_MGMT.OS\_FILE\_MAX\_SIZE,

                                             USE\_DEFAULT\_VALUES   => TRUE);

END;

/

更改age，  单个文件打开的最长时间

BEGIN

  DBMS\_AUDIT\_MGMT.SET\_AUDIT\_TRAIL\_PROPERTY(AUDIT\_TRAIL\_TYPE           => DBMS\_AUDIT\_MGMT.AUDIT\_TRAIL\_OS,

                                           AUDIT\_TRAIL\_PROPERTY       => DBMS\_AUDIT\_MGMT.OS\_FILE\_MAX\_AGE,

                                           AUDIT\_TRAIL\_PROPERTY\_VALUE => 10);

END;

/

取消age更改，使用默认值

BEGIN

  DBMS\_AUDIT\_MGMT.CLEAR\_AUDIT\_TRAIL\_PROPERTY(AUDIT\_TRAIL\_TYPE     => DBMS\_AUDIT\_MGMT.AUDIT\_TRAIL\_OS,

                                             AUDIT\_TRAIL\_PROPERTY => DBMS\_AUDIT\_MGMT.OS\_FILE\_MAX\_AGE,

                                             USE\_DEFAULT\_VALUES   => TRUE);

END;

/

select \* from DBA\_AUDIT\_MGMT\_CONFIG\_PARAMS;  --查询配置

SQL> select \* from DBA\_AUDIT\_MGMT\_CONFIG\_PARAMS;

PARAMETER\_NAME                 PARAMETER\_VALUE              AUDIT\_TRAIL

---------------------------------------- ---------------------------------------- ----------------------------

DB AUDIT TABLESPACE             SYSAUX                   STANDARD AUDIT TRAIL

DB AUDIT TABLESPACE             SYSAUX                   FGA AUDIT TRAIL

AUDIT FILE MAX SIZE             10000                      OS AUDIT TRAIL

AUDIT FILE MAX SIZE             10000                      XML AUDIT TRAIL

AUDIT FILE MAX AGE             5                      OS AUDIT TRAIL

AUDIT FILE MAX AGE             5                      XML AUDIT TRAIL

DB AUDIT CLEAN BATCH SIZE         10000                      STANDARD AUDIT TRAIL

DB AUDIT CLEAN BATCH SIZE         10000                      FGA AUDIT TRAIL

OS FILE CLEAN BATCH SIZE         1000                      OS AUDIT TRAIL

OS FILE CLEAN BATCH SIZE         1000                      XML AUDIT TRAIL

10 rows selected.

====================================

**》删除审计记录**

对于审计记录，可以手动删除也可以设置定期删除任务，配置定期任务，需要使用DBMS\_AUDIT\_MGMT PL/SQL package

删除前通常是先归档审计记录。

**删除的方法**

**以下均已FGA类型为例**

1 手动删除：在需要的时候删除所有或指定时间点的部分审计记录

2 自动删除：定期删除所有或指定时间点的部分审计记录

注意：删除审计记录需要花费时间

**删除任务**

1 删除审计记录会生成redo数据，必要时，加大在线日志组大小

2 确定删除的时间

必须先记录数据库和操作系统审核记录的时间戳, 然后才能对其进行存档。您可以通过查询 DBA\_AUDIT\_MGMT\_LAST\_ARCH\_TS 数据字典视图来检查时间戳日期。稍后, 当清除发生时, Oracle 数据库只清除在该时间戳日期之前创建的审核跟踪记录

3 初始化，指定默认删除策略（删除类型，删除间隔时间）

BEGIN

  DBMS\_AUDIT\_MGMT.INIT\_CLEANUP(AUDIT\_TRAIL\_TYPE         => DBMS\_AUDIT\_MGMT.AUDIT\_TRAIL\_AUD\_STD,

                               DEFAULT\_CLEANUP\_INTERVAL => 12);

END;

/

DBMS\_AUDIT\_MGMT.AUDIT\_TRAIL\_OS: Operating system audit trail files with the .aud extension. (This setting does not apply to Windows Event Log entries.)

DEFAULT\_CLEANUP\_INTERVAL: Specify the desired default hourly purge interval (for example, 12 for every 12 hours).

The DBMS\_AUDIT\_MGMT procedures use this value to determine how to purge audit records

确认AUDIT TRAIL删除区间DEFAULT\_CLEANUP\_INTERVAL

select \* from DBA\_AUDIT\_MGMT\_CONFIG\_PARAMS;

修改AUDIT TRAIL删除区间DEFAULT\_CLEANUP\_INTERVAL

BEGIN

DBMS\_AUDIT\_MGMT.SET\_AUDIT\_TRAIL\_PROPERTY(

  AUDIT\_TRAIL\_TYPE            => DBMS\_AUDIT\_MGMT.AUDIT\_TRAIL\_FGA\_STD,

  AUDIT\_TRAIL\_PROPERTY        => DBMS\_AUDIT\_MGMT.CLEAN\_UP\_INTERVAL,

  AUDIT\_TRAIL\_PROPERTY\_VALUE  =>10 );

END;

/

查询是否初始化

SET SERVEROUTPUT ON

BEGIN

IF

   DBMS\_AUDIT\_MGMT.IS\_CLEANUP\_INITIALIZED(DBMS\_AUDIT\_MGMT.AUDIT\_TRAIL\_FGA\_STD)

THEN

   DBMS\_OUTPUT.PUT\_LINE('FGA\_lOG$ is initialized for cleanup');

ELSE

   DBMS\_OUTPUT.PUT\_LINE('FGA\_LOG$ is not initialized for cleanup.');

END IF;

END;

/

4 产生归档时间

If you want to delete all of the audit trail, you can bypass this step.

begin

   dbms\_audit\_mgmt.set\_last\_archive\_timestamp(

     audit\_trail\_type  => dbms\_audit\_mgmt.audit\_trail\_fga\_std,

     last\_archive\_time =>

        to\_timestamp('2018-07-20 1:00:00','YYYY-MM-DD HH24:MI:SS'),

     rac\_instance\_number  => null

   );

end;

/

清理归档时间设置

BEGIN

  DBMS\_AUDIT\_MGMT.CLEAR\_LAST\_ARCHIVE\_TIMESTAMP(

   AUDIT\_TRAIL\_TYPE     =>  dbms\_audit\_mgmt.audit\_trail\_fga\_std,

   RAC\_INSTANCE\_NUMBER  =>  null );

END;

/

这个归档时间一直不变？？？？？？？？？？？？？？？？？？

手动清理

begin

  dbms\_audit\_mgmt.clean\_audit\_trail(

   audit\_trail\_type        =>  dbms\_audit\_mgmt.audit\_trail\_fga\_std,

   use\_last\_arch\_timestamp => TRUE

  );

end;

/

以上可以手动调用dbms\_audit\_mgmt手动清理trail,主要目的还是用于自动清理job，自动清理

5 创建计划任务

BEGIN

  DBMS\_AUDIT\_MGMT.CREATE\_PURGE\_JOB(AUDIT\_TRAIL\_TYPE           => DBMS\_AUDIT\_MGMT.AUDIT\_TRAIL\_FGA\_STD,

                                   AUDIT\_TRAIL\_PURGE\_INTERVAL => 12,

                                   AUDIT\_TRAIL\_PURGE\_NAME     => 'standard\_p',

                                   USE\_LAST\_ARCH\_TIMESTAMP    => true);

END;

/

如果使用归档时间  USE\_LAST\_ARCH\_TIMESTAMP    => TRUE，

当不适用归档时间    USE\_LAST\_ARCH\_TIMESTAMP    => false   --即全部清理

BEGIN

DBMS\_AUDIT\_MGMT.SET\_PURGE\_JOB\_INTERVAL(

  AUDIT\_TRAIL\_PURGE\_NAME       => 'standard\_p',

  AUDIT\_TRAIL\_INTERVAL\_VALUE   => 24 );

END;

/

查看看AUDIT TRAIL job

SELECT \* FROM DBA\_AUDIT\_MGMT\_CLEANUP\_JOBS;

DBA\_AUDIT\_MGMT\_CLEANUP\_JOBS引用了dba\_scheduler\_jobs

查看job详细信息

SELECT

    owner,

    job\_name,

    job\_creator,

    job\_action,

    TO\_CHAR(start\_date,'yyyy-mm-dd hh24:mi:ss') AS stard,

    repeat\_interval,

    TO\_CHAR(next\_run\_date,'yyyy-mm-dd hh24:mi:ss') AS nextd

FROM

    dba\_scheduler\_jobs

WHERE

    job\_name = 'STANDARD\_P';

启用或禁用AUDIT TRAIL job

BEGIN

DBMS\_AUDIT\_MGMT.SET\_PURGE\_JOB\_STATUS(

  AUDIT\_TRAIL\_PURGE\_NAME      => 'standard\_p',

  AUDIT\_TRAIL\_STATUS\_VALUE    => DBMS\_AUDIT\_MGMT.PURGE\_JOB\_ENABLE);

END;

/

DBMS\_AUDIT\_MGMT.PURGE\_JOB\_DISABLE

删除AUDIT TRAIL job

BEGIN

DBMS\_AUDIT\_MGMT.DROP\_PURGE\_JOB(

  AUDIT\_TRAIL\_PURGE\_NAME  => 'STANDARD\_AUDIT\_TRAIL\_PURGE');

END;

/

手动运行job

BEGIN

    DBMS\_SCHEDULER.RUN\_JOB(job\_name => '"SYS"."STANDARD\_P"', USE\_CURRENT\_SESSION => FALSE);

END;

/

6 可选，使用batch

到此数据库审计自动清理就可以实现了，但是从数据库的性能考虑，如果您的数据库很大，几个T或者几十T，您的审计数据也很庞大，一天的数据量上G，我们就得考虑数据的审计清理的性能，因为以上的审计清理时delete操作，不是truncate操作，oracle11g也提供了一个很好的解决方法，设置清理批处理时commit行数。如下：

默认每次删除数据库内10000条记录，操作系统1000个文件。如果产生的undo太多，可以减小batch值

BEGIN

  DBMS\_AUDIT\_MGMT.SET\_AUDIT\_TRAIL\_PROPERTY(AUDIT\_TRAIL\_TYPE           => DBMS\_AUDIT\_MGMT.AUDIT\_TRAIL\_FGA\_STD,

                                           AUDIT\_TRAIL\_PROPERTY       => DBMS\_AUDIT\_MGMT.DB\_DELETE\_BATCH\_SIZE,

                                           AUDIT\_TRAIL\_PROPERTY\_VALUE => 1000);

END;

/

三个参数，一看就懂，audit\_trail\_type清理类型，audit\_trail\_property设置删除批处理，audit\_trail\_property\_value表示每次commit行数100000。

取消，恢复默认值

BEGIN

  DBMS\_AUDIT\_MGMT.CLEAR\_AUDIT\_TRAIL\_PROPERTY(

   AUDIT\_TRAIL\_TYPE        =>  DBMS\_AUDIT\_MGMT.AUDIT\_TRAIL\_AUD\_STD,

   AUDIT\_TRAIL\_PROPERTY    =>  DBMS\_AUDIT\_MGMT.DB\_DELETE\_BATCH\_SIZE,

   USE\_DEFAULT\_VALUES      =>  TRUE );

END;

/

=============================

手动删除

1 调用DBMS\_AUDIT\_MGMT.CLEAN\_AUDIT\_TRAIL PL/SQL procedure.

全部删除

BEGIN

  DBMS\_AUDIT\_MGMT.CLEAN\_AUDIT\_TRAIL(

   AUDIT\_TRAIL\_TYPE           =>  DBMS\_AUDIT\_MGMT.AUDIT\_TRAIL\_AUD\_STD,

   USE\_LAST\_ARCH\_TIMESTAMP    =>  FALSE );

END;

/

删除部分子记录

DELETE FROM SYS.AUD$

   WHERE NTIMESTAMP# > TO\_TIMESTAMP ('28-FEB-09 09.07.59.907000 PM') AND

   NTIMESTAMP# < TO\_TIMESTAMP ('28-MAR-09 09.07.59.907000 PM');

截断表AUD$

TRUNCATE TABLE SYS.AUD$;