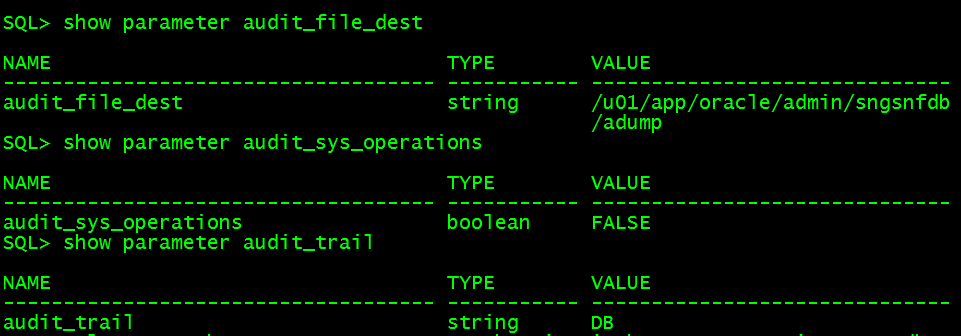
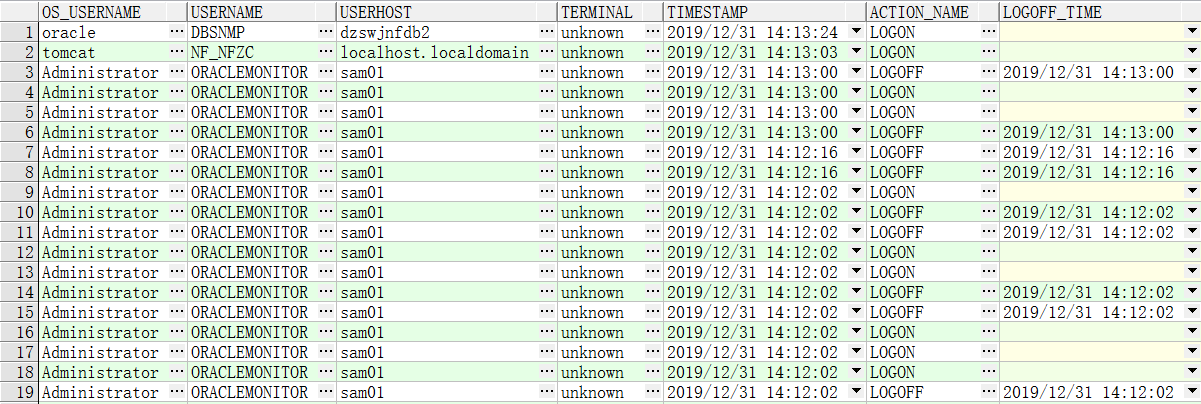
**电子事务局数据库审计报告**

1. **数据库采用DB审计方式，将audit trail 审计记录在数据库的相关表中**

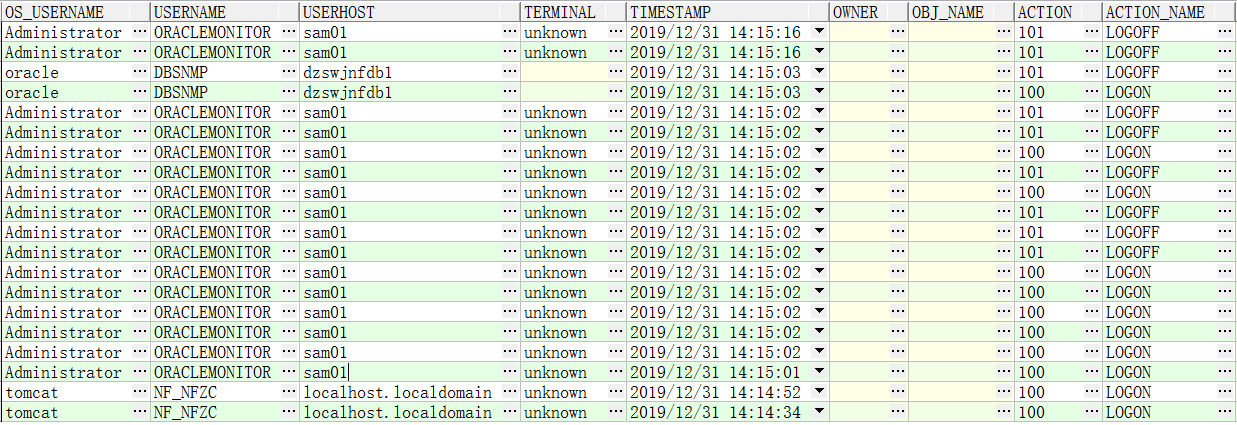
**2、数据库中的会话审计跟踪**

从表中的信息，我们用来追溯是否有异常的用户登录数据库，用来审核指定的用户访问数据库，若有异常，及时处理及上报。

SELECT \* FROM dba\_audit\_session t order by t.timestamp desc;



SELECT \* FROM dba\_audit\_trail t where to\_char(t.timestamp,'yyyymmdd') ='20200727' order by t.timestamp desc;



**3、数据库中的用户权限审计跟踪**

在生产环境中，NF\_NFZC用户用来配置在weblogic及tomcat的连接oracle数据库的用户，采用了细粒度的权限划分，从而保证只能是正确的权限，才可以对数据库的表进行操作，保证审计的合规性。

而其它的HX用户，均同步于核心征管，从而保证权限的一致性。

SELECT \* FROM dba\_role\_privs t WHERE t.grantee = upper('&role\_name') or t.granted\_role=upper('&role\_name');

SELECT t.grantee, t.owner, t.table\_name, t.privilege, t.grantable

FROM dba\_tab\_privs t

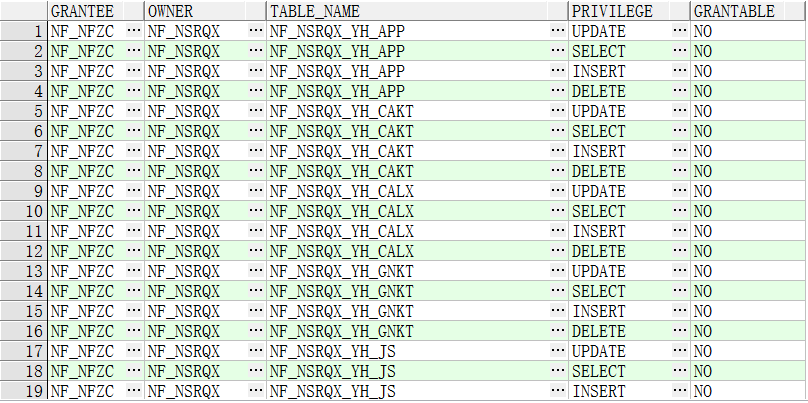
WHERE t.grantee =upper('&role\_name')

union all

SELECT b.grantee, to\_char(null), to\_char(null), b.privilege, b.admin\_option

FROM dba\_sys\_privs b

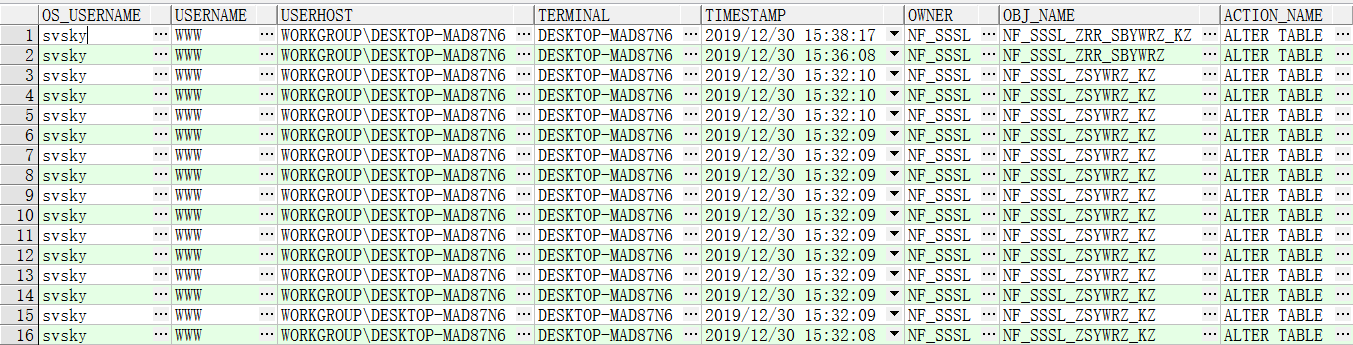
WHERE b.grantee =upper('&role\_name');



**4、数据库中的对象审计跟踪**

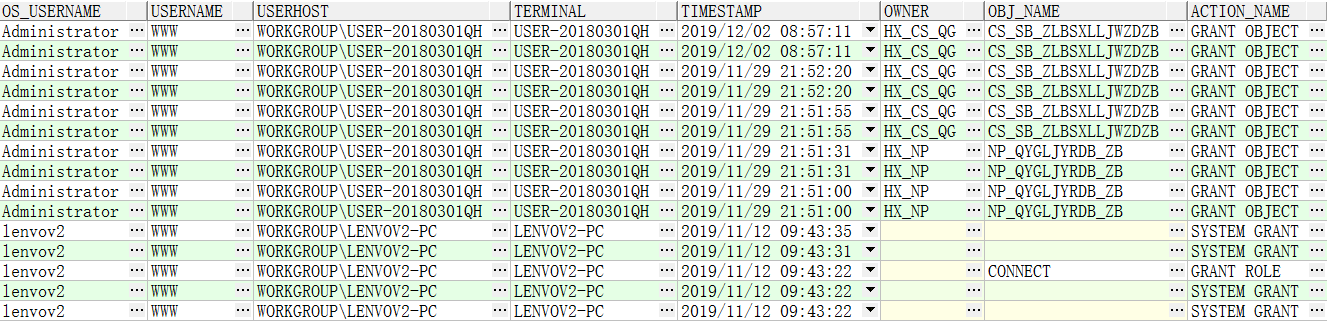
通过对象跟踪，我们可以追溯到具体的用户对数据库的对象做了哪些操作，以便我们进行追踪溯源。

SELECT \* FROM DBA\_AUDIT\_OBJECT t order by t.TIMESTAMP desc;



**5、与GRANT、REVOKE、AUDIT、NOAUDIT和ALTER SYSTEM命令相关的审计跟踪**

SELECT \* FROM DBA\_AUDIT\_STATEMENT t order by t.TIMESTAMP desc;



**总结：**

通过数据库的审计将所有审计记录指向数据库审计跟踪 (SYS.AUD$) 表中，再通过语句审计、权限审计、对象审计等关联表，各维度记录数据库的用户操作，从而保证数据库在合规的方式下正常运行，当出现重大问题时，也可追踪溯源。