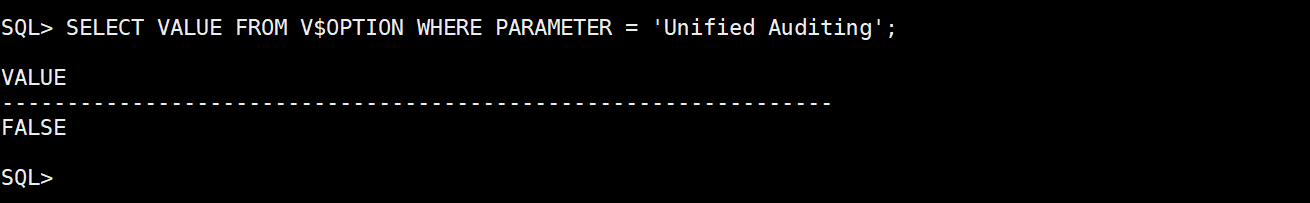
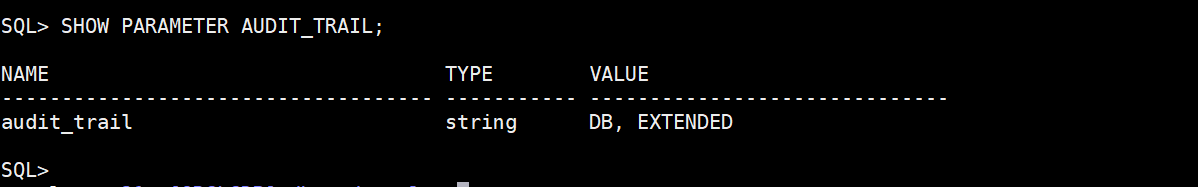
<https://dbasobrinho.com.br/oracle-unified-auditing-habilitar-auditoria-de-logins-malsucedidos-e-ddl-passo-a-passo/>

**1. Verificar o status do Unified Auditing**



Status do AUDIT\_TRAIL:



**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)](https://support.oracle.com/epmos/faces/DocumentDisplay?id=1567006.1)

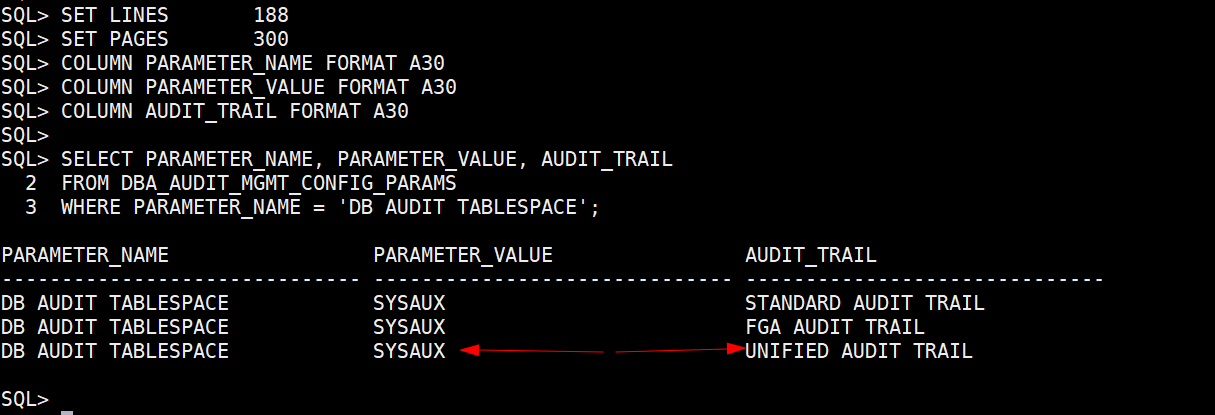
Eu costumo usar o **modo misto** para ambientes em operação, pois **não há necessidade de recompilação**. No entanto, se for um ambiente novo, você já pode iniciar diretamente no **modo puro (exclusivo)**.

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

**2. Configurar a tablespace da auditoria**

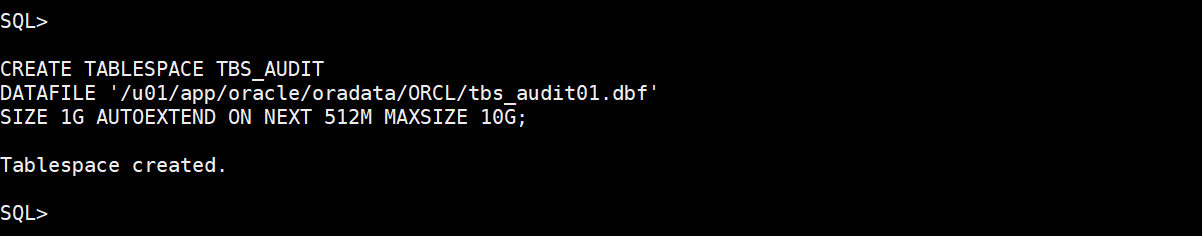
Por padrão, os registros da auditoria unificada são armazenados na tablespace SYSAUX. É recomendado que os dados de auditoria fiquem em uma tablespace isolada.

**2.1 Verificar a tablespace usada pela auditoria**

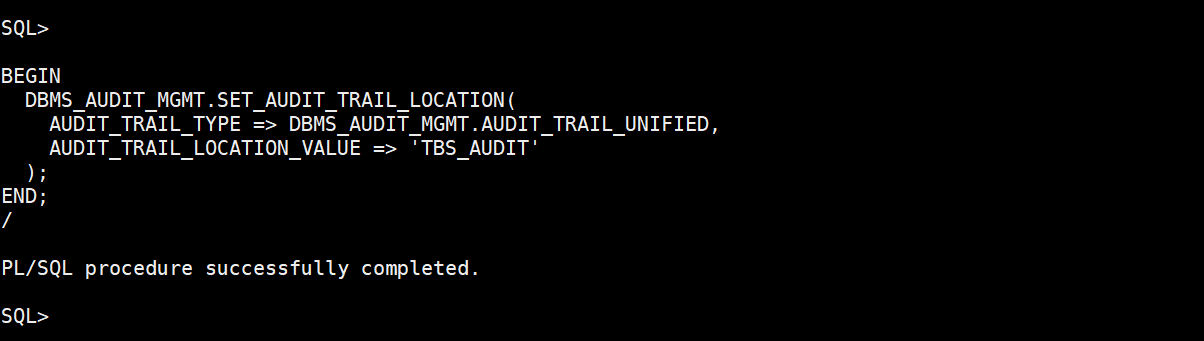


**2.2 Alterar a tablespace da auditoria unificada**

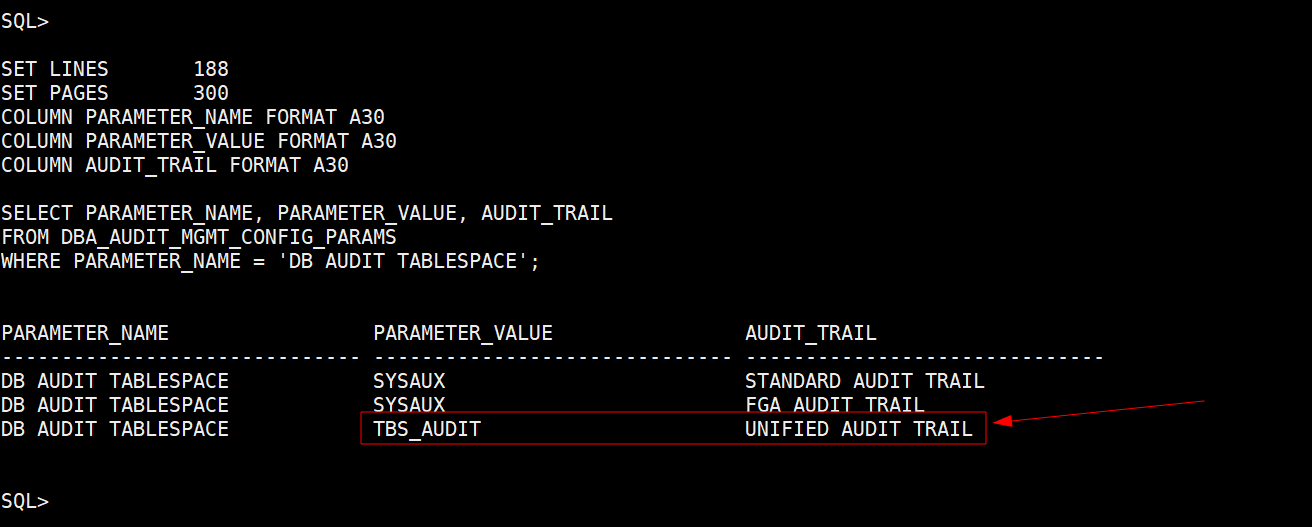
Se necessário criar uma nova tablespace dedicada (TBS\_AUDIT):



Mover a auditoria para essa nova tablespace:

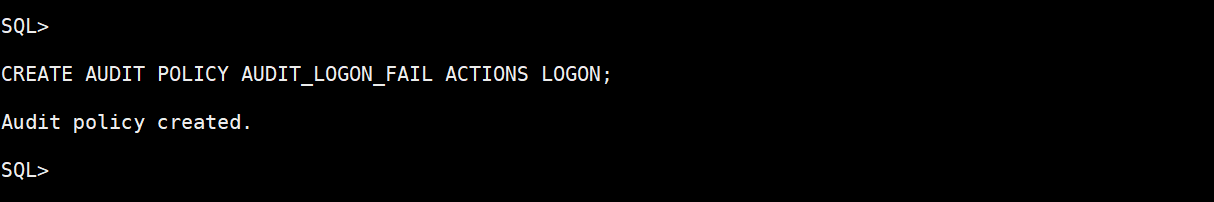


Verificar se a alteração foi aplicada:

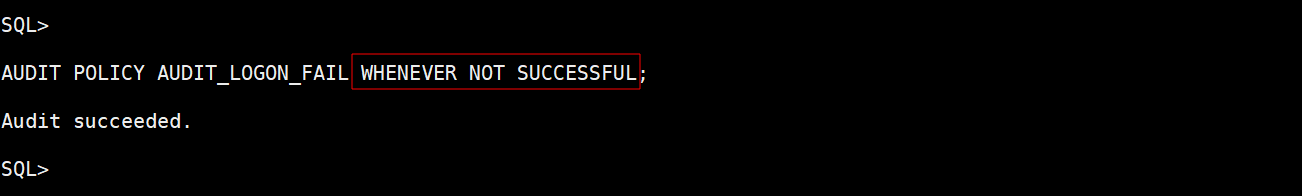


**3. Criar e ativar auditorias**

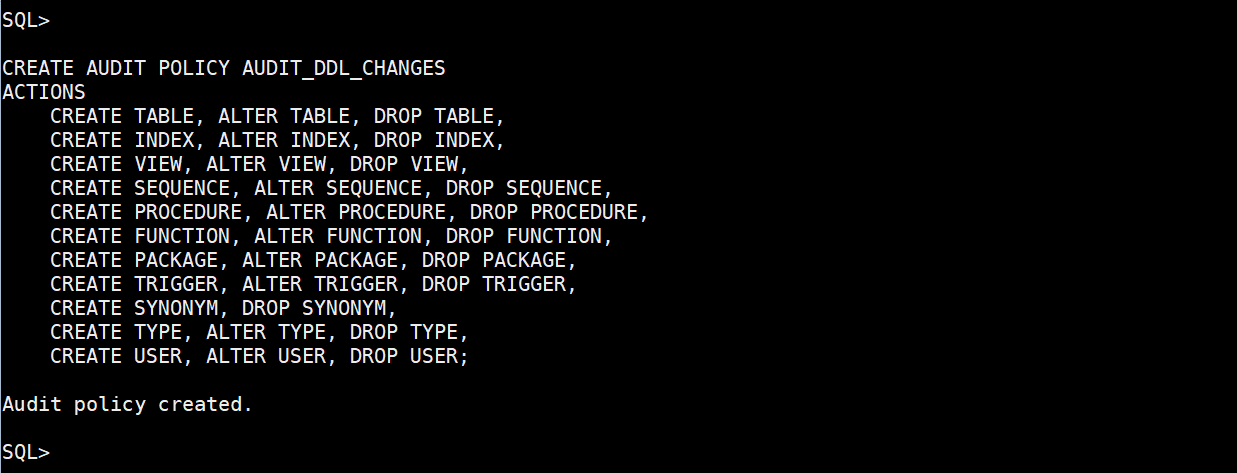
**3.1 Auditoria de logins malsucedidos**



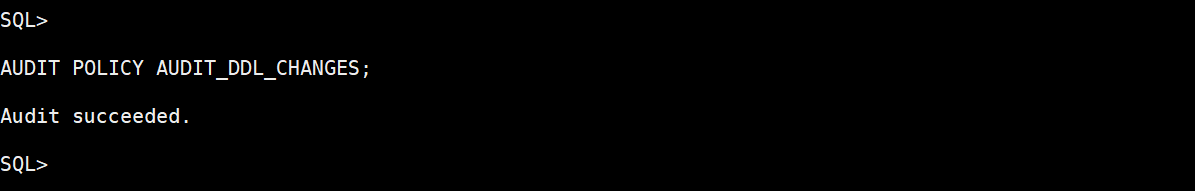
Ativar a auditoria somente para logins malsucedidos:



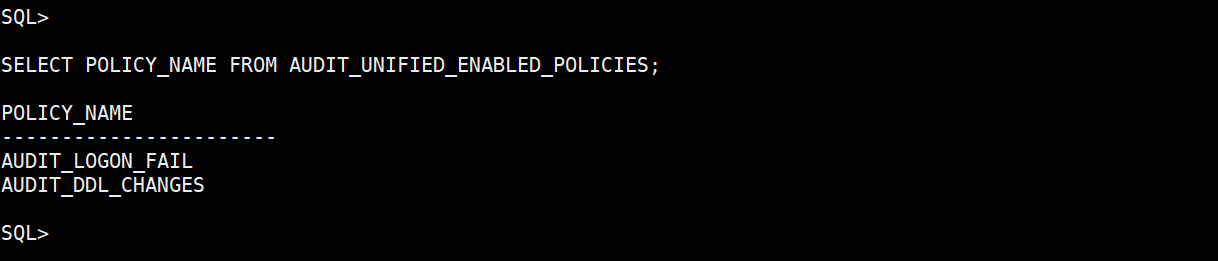
**3.1 Auditoria de alterações em objetos**



Ativar a auditoria:

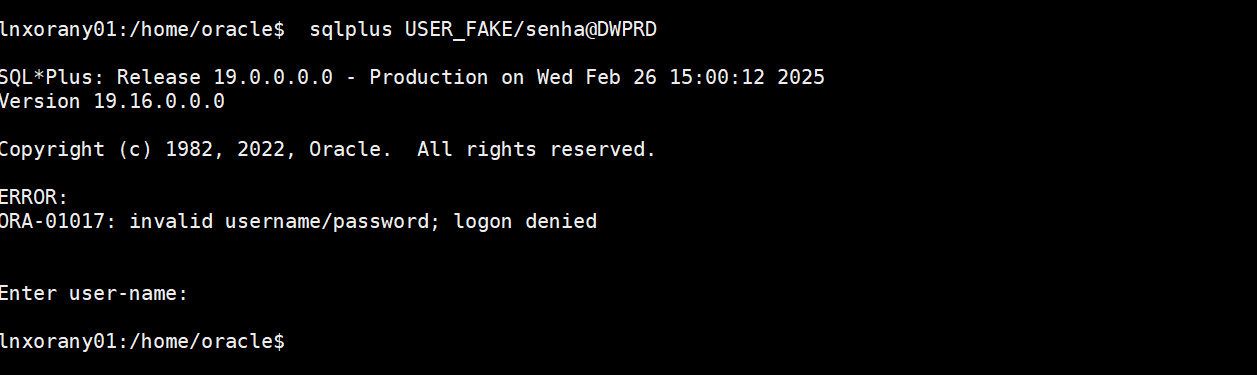


**3.3 Verificar quais políticas de auditoria estão ativas**



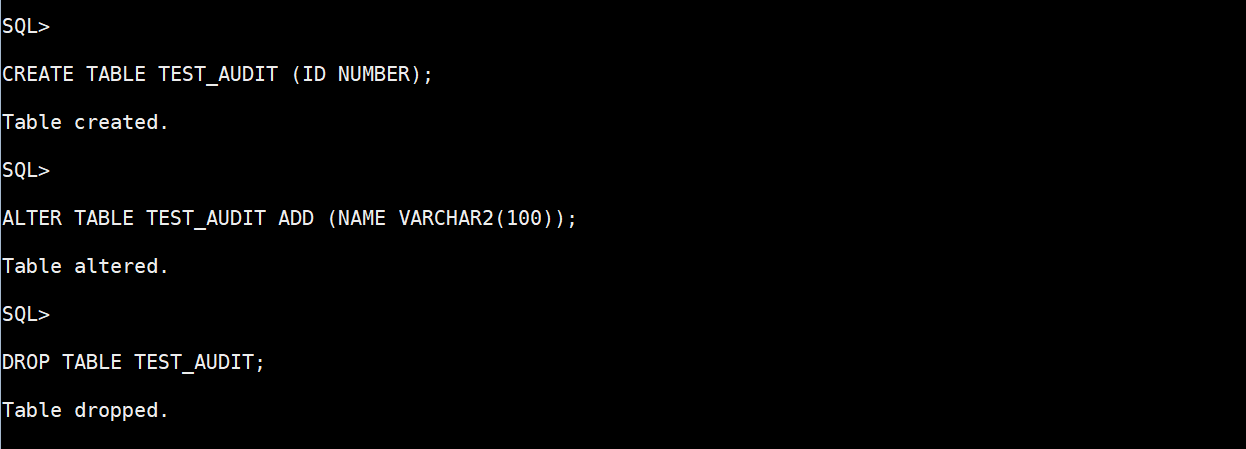
**4. Testar e consultar as auditorias**

**4.1 Testar auditoria de login malsucedido**



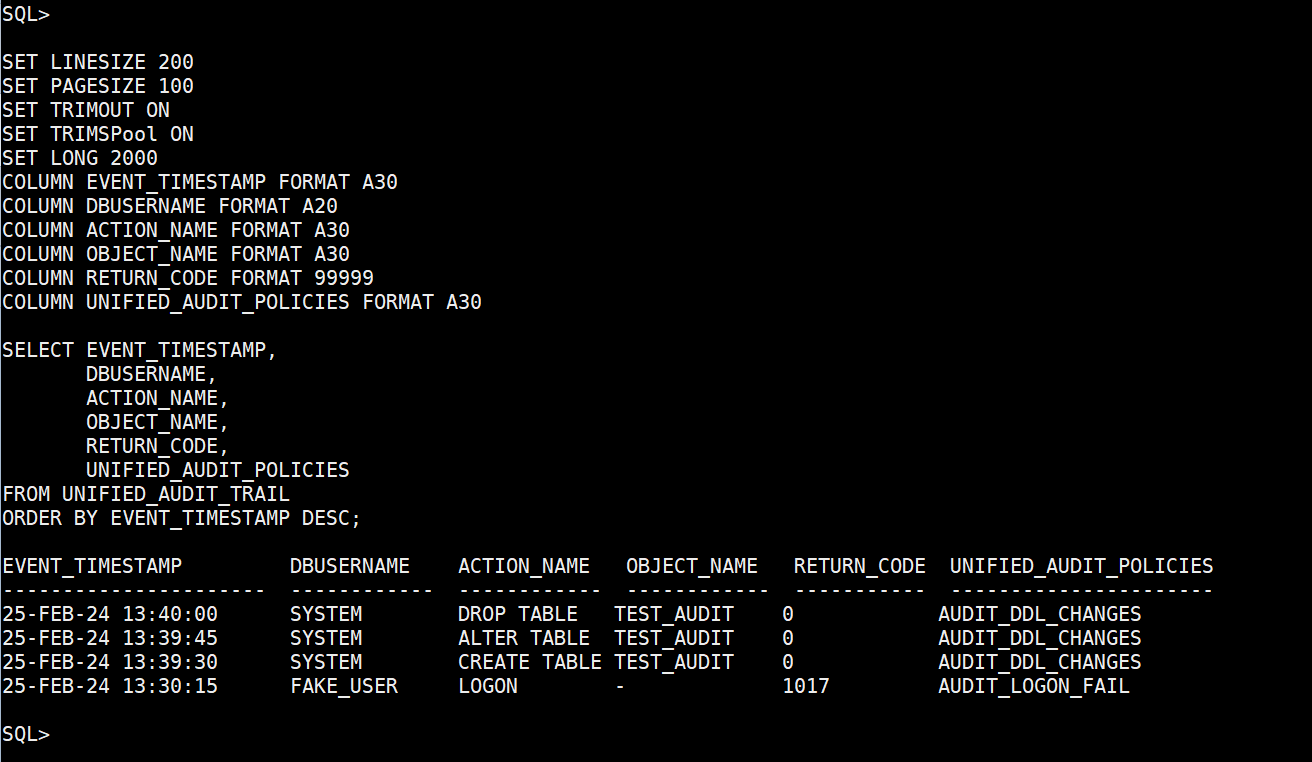
**4.2 Testar auditoria DDL**

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



**4.3 Consultar auditorias registradas**

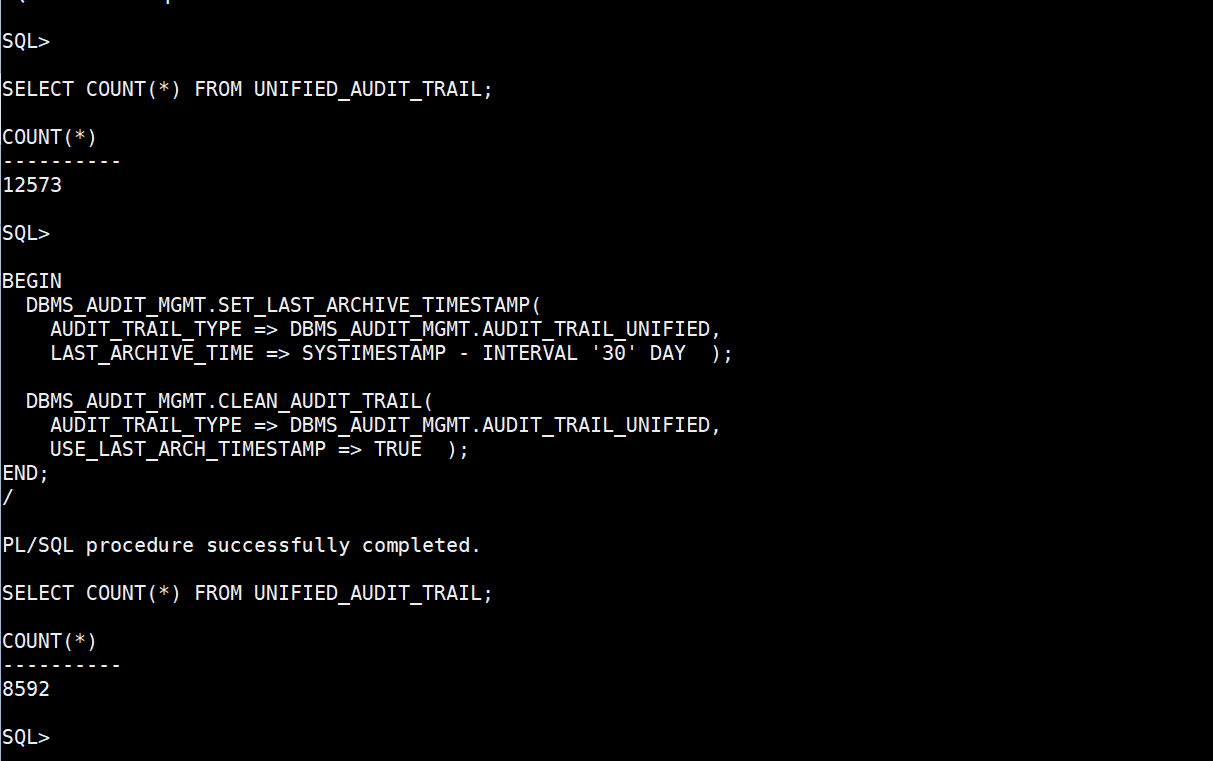
Executar os seguintes comandos para verificar se as auditorias estão funcionando:



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.

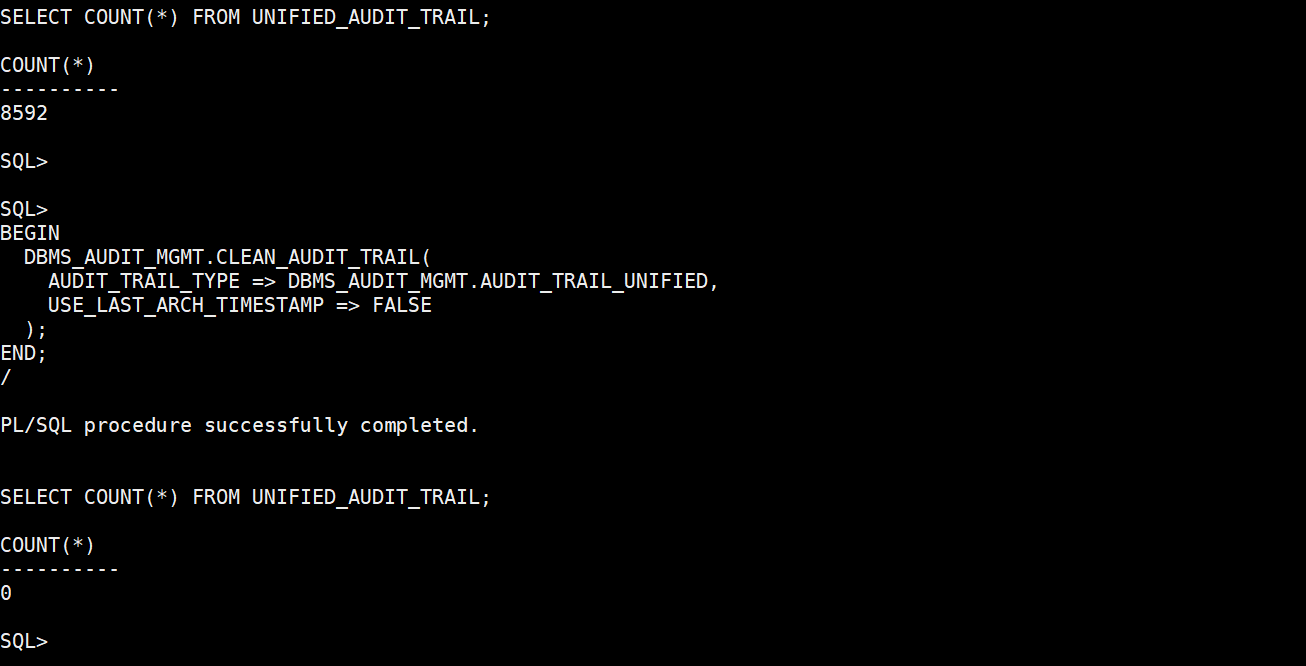
**5. Purge dos registros de auditoria**

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**

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

**5.2 Remover todos os registros da auditoria**

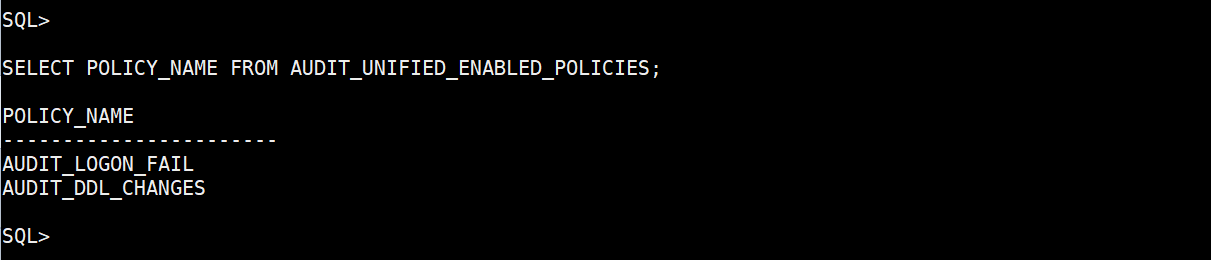
Todos os registros foram removidos e a trilha de auditoria.

**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**

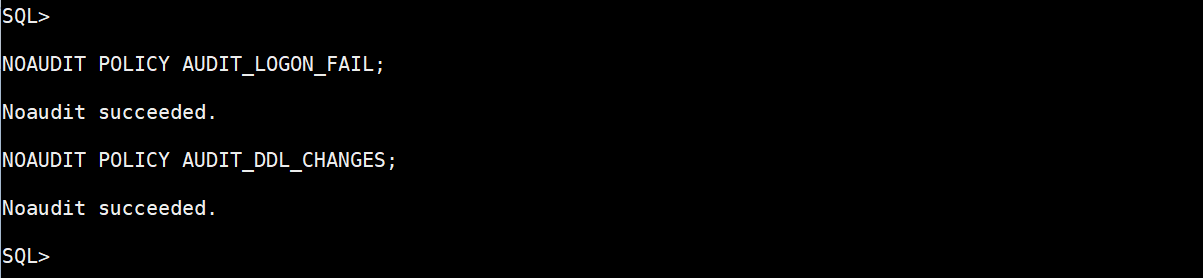
**6. Desativar e excluir uma política de auditoria**

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



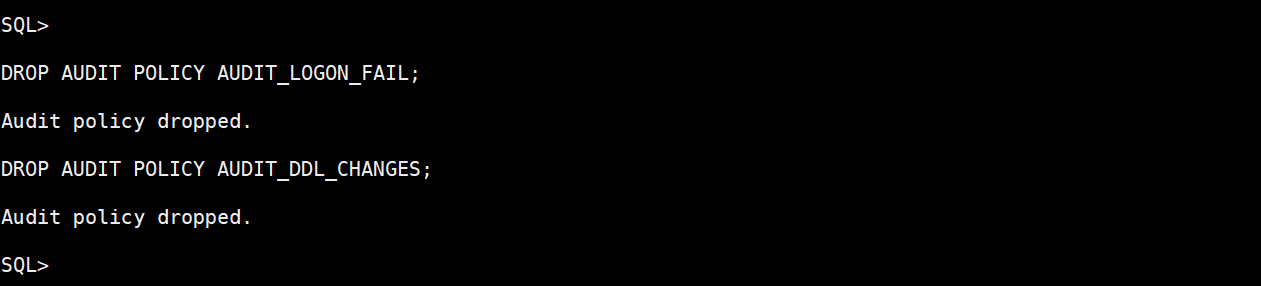
**6.1 Desativar uma política de auditoria (sem excluir)**

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



**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:



**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](https://docs.oracle.com/en/database/oracle/oracle-database/19/sqlrf/AUDIT-Unified-Auditing.html" \t "_blank)  
🔗 [Auditing Enhancements (Audit Policies and Unified Audit Trail) in Oracle Database](https://oracle-base.com/articles/12c/auditing-enhancements-12cr1" \t "_blank)

**#20250303 #DBASobrinho** **#GuinaNãoTinhaDó** **#BóBó** **#CaceteDeAgulha** **#OracleACE**

🔗 [audit\_unified\_login\_fail\_and\_all\_ddl.sql](https://oracle-base.com/articles/12c/auditing-enhancements-12cr1" \t "_blank)