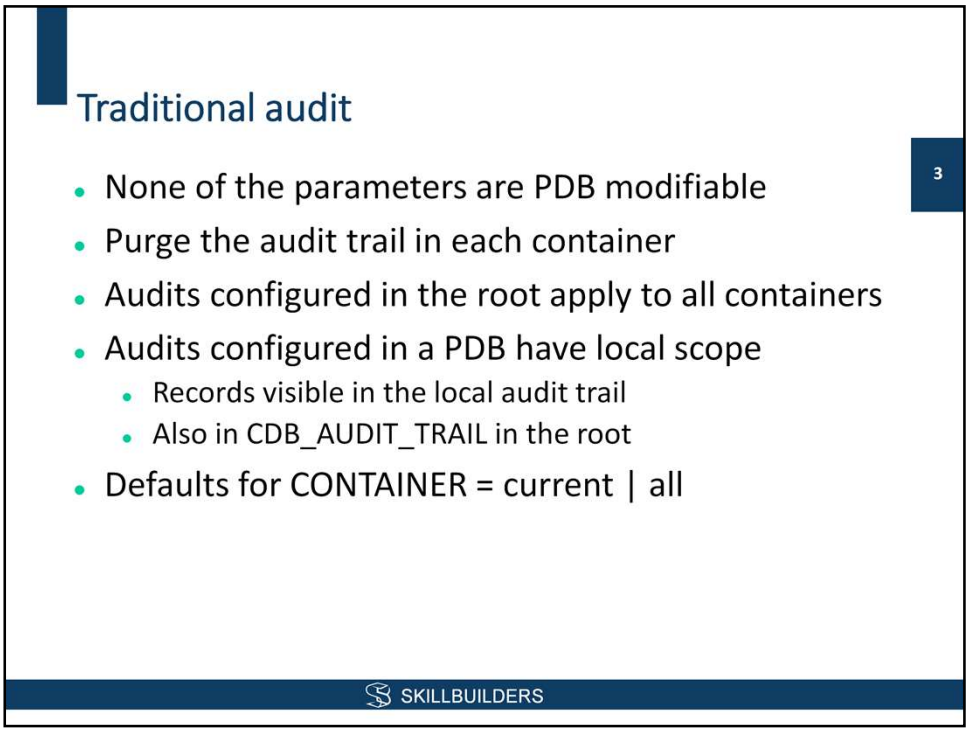
Lesson 7
Security Considerations

SKILLBUILDERS

Objectives

- Audit
- Encryption
- Data Vault
- Some fine-control capabilities

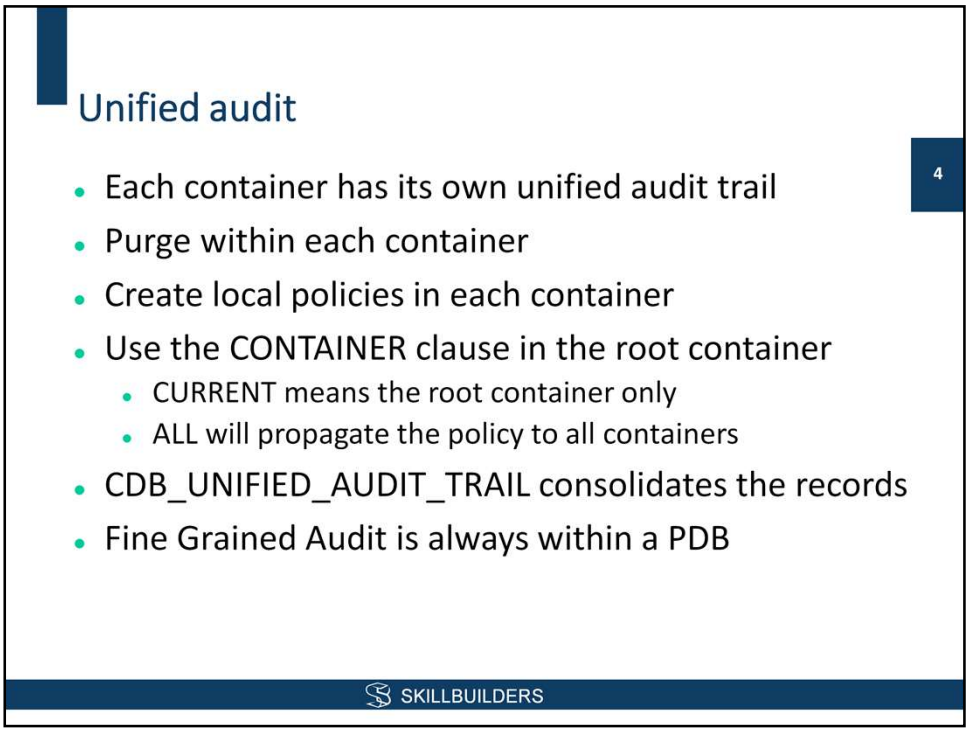


Traditional audit:

In a PDB, AUDIT DROP ANY TABLE BY SYSTEM BY ACCESS CONTAINER = CURRENT;

In the root, AUDIT DROP ANY TABLE BY SYSTEM BY ACCESS CONTAINER = ALL;

For audits that specify objects or users, if executed in the root they must be common objects or users.



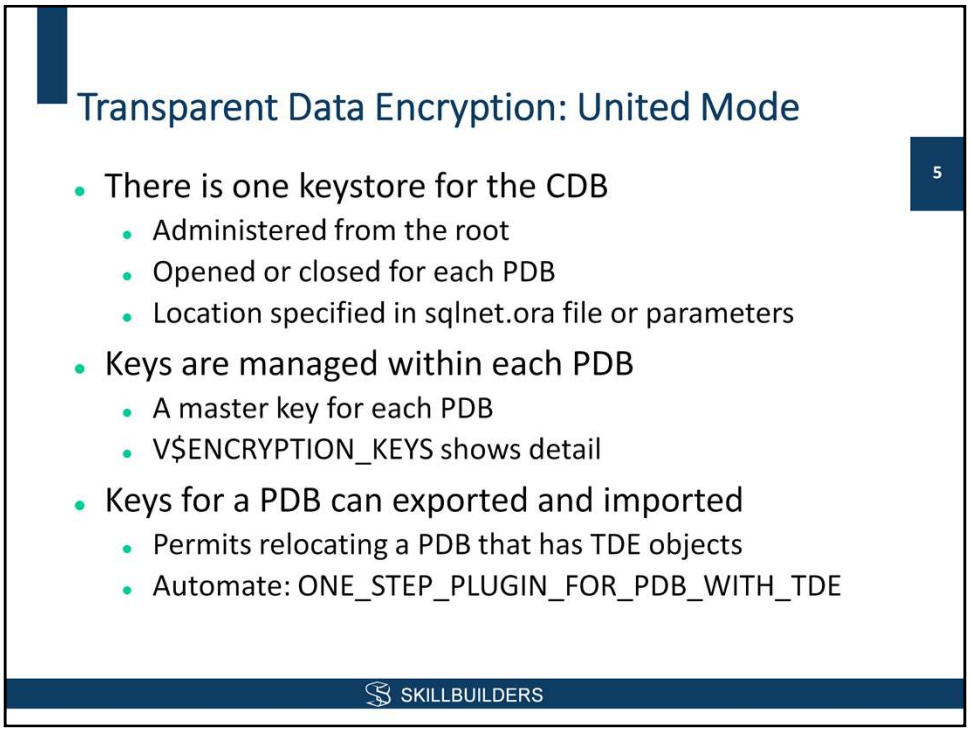
A common unified audit policy:

CREATE AUDIT POLICY any_trigger PRIVILEGES CREATE ANY TRIGGER

CONTAINER=ALL;

Enabling a common policy (which does not take a CONTAINER clause) enables it in all PDBs. Within each container, the UNIFIED_AUDIT_TRAIL view shows audited events in that container. In the root, the CDB view shows everything.

Fine Grained Audit can be configured only in containers, not as common policies. This applies whether Unified Audit has been enabled or not.

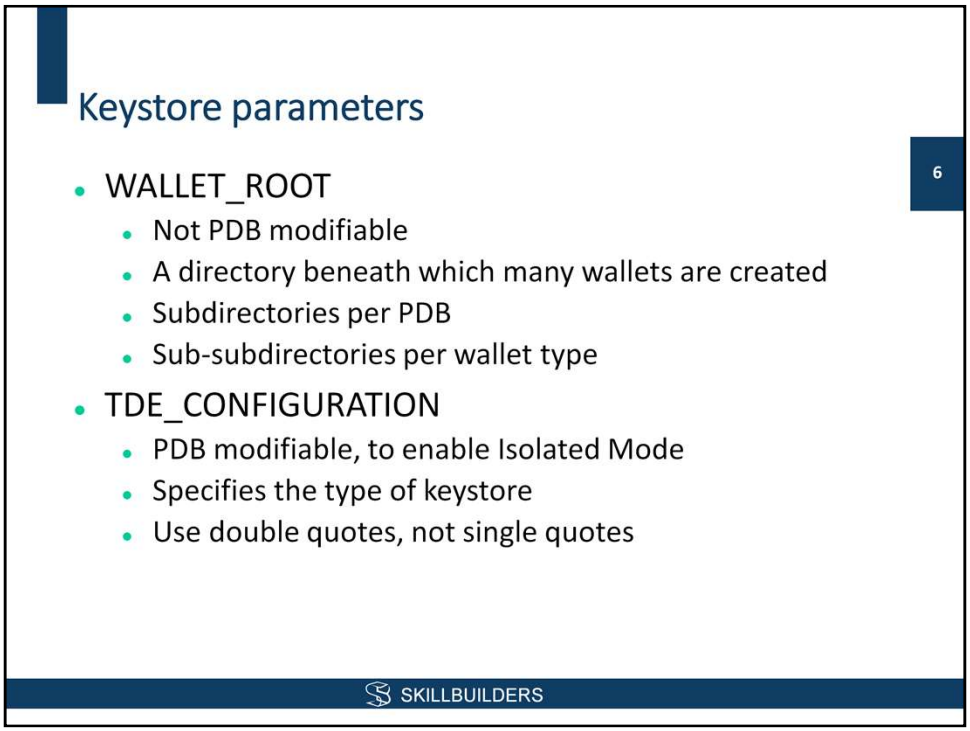


"United Mode" is the term introduced in release 18 to describe PDBs using TDE in the release 12 fashion.

There is one keystore per database. Within a CDB, the keystore has a set of keys per container. The keystore is created from the root, then within each PDB the keystore can be opened and closed.

The location and type of the keystore is specified either with the sqlnet.ora parameter SQLNET.ENCRYPTION_WALLET_LOCATION as in earlier releases, or with the WALLET_ROOT and TDE_CONFIGURATION instance parameters.

To move a PDB with TDE enabled from one CDB to another, it is necessary to export the keys from the source CDB's keystore and import them into the destination CDB's keystore. When doing this, it is necessary to provide the keystore password. Setting ONE_STEP_PLUGIN_FOR_PDB_WITH_TDE=true permits automating this process when doing a remote network clone.



The wallet_root determines the location of the wallet(s) and is set in the root container. For example,

wallet_root=/app/oracle/admin/orcl/wallet

Then set tde_configuration to the type of wallet. For example.

tde_configuration="keystore_configuration=file"

The examples above would be equivalent to this entry in sqlnet.ora:

encryption_wallet_location=

(source=(method=file)(method_data=(directory=/app/oracle/admin/orcl/wallet)))

The possibilities for the keystore_configuration are

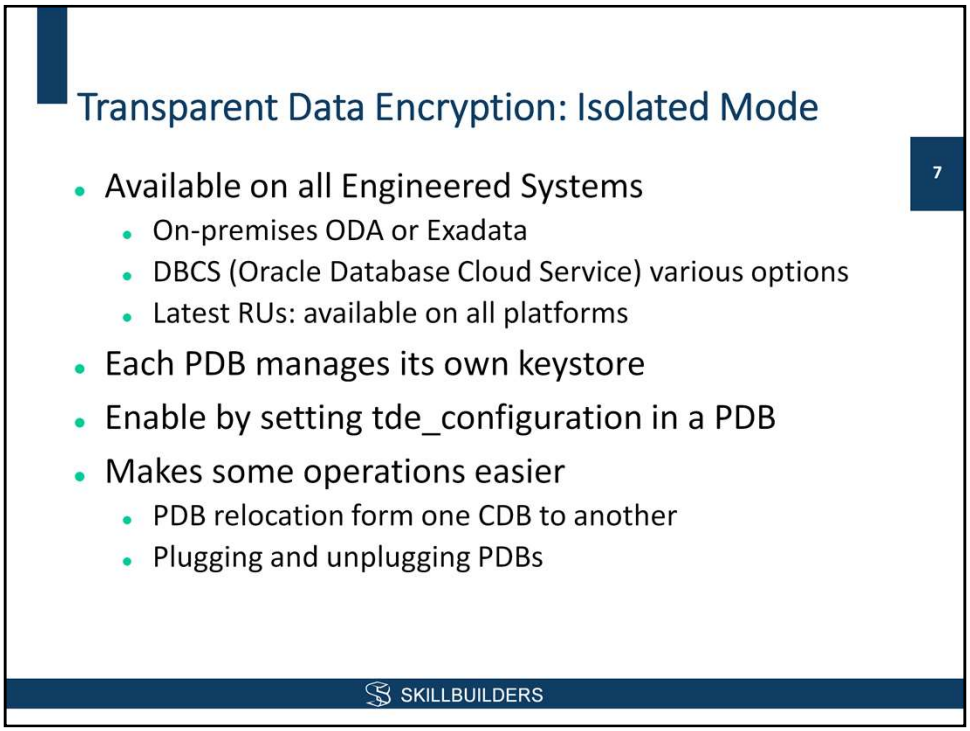
FILE: a wallet based keystore

OKV: an Oracle Key Vault keystore

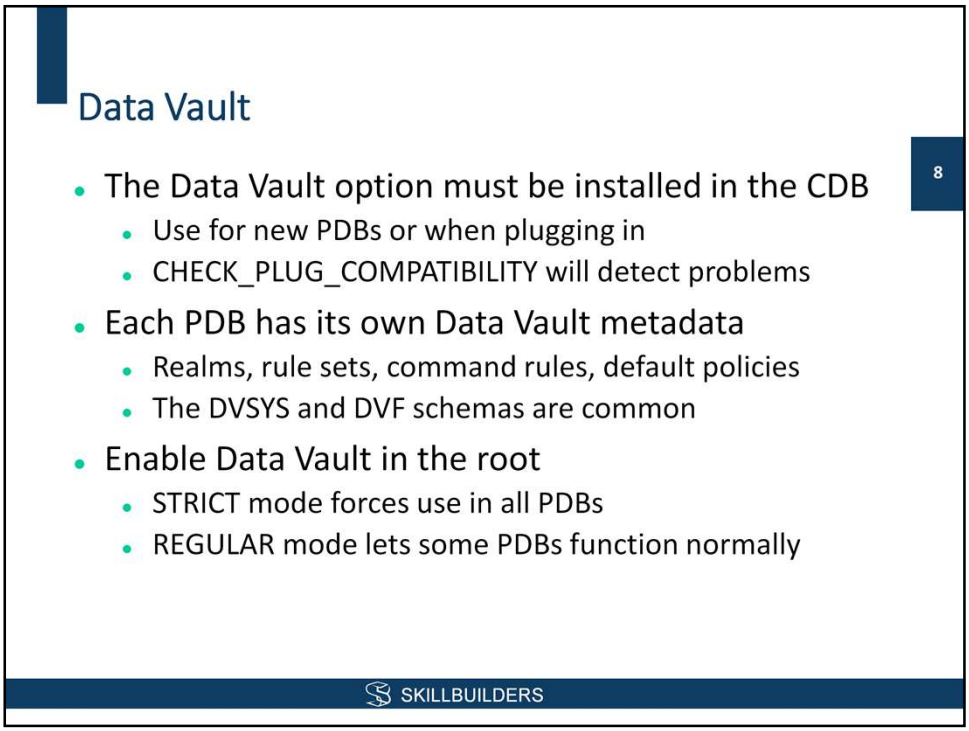
HSM: an externally provided Hardware Security Module

If tde_configuration is set only in the root container, then TDE will be running in United Mode. Setting it in a PDB converts that PDB to Isolated Mode.

v$encryption_wallet shows the mode of each container.

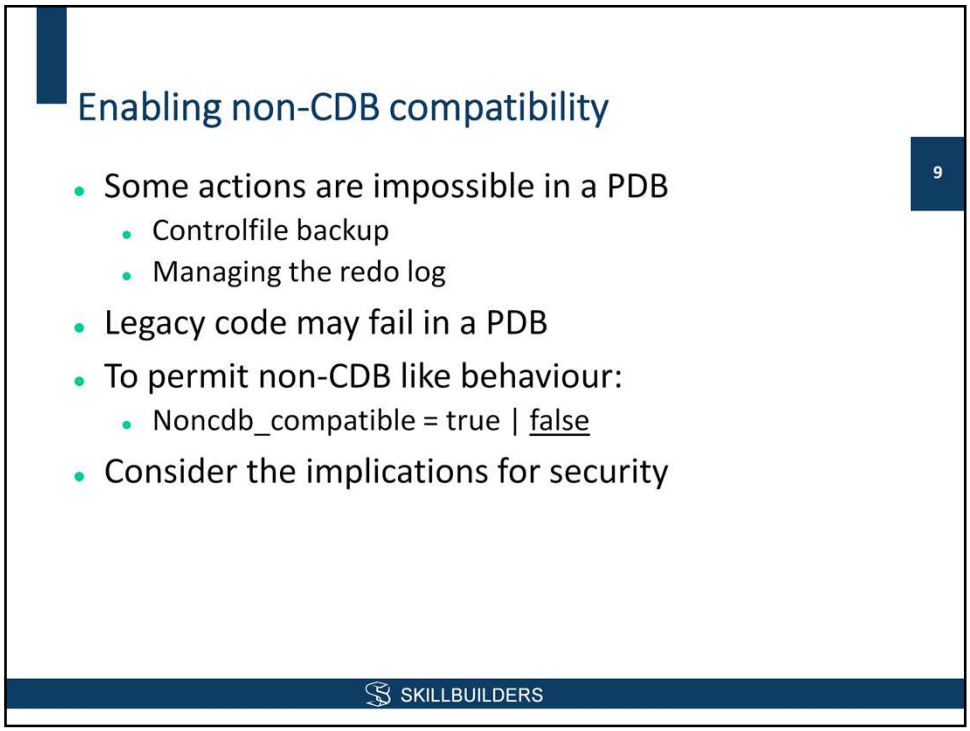


Isolated mode is aimed at easing management of large scale environments. In cases where there is a fleet of CDBs supporting hundreds or thousands of PDBs there will be frequent requirements to move PDBs around. This might be for upgrade and patching, or perhaps to balance workloads across CDBs and servers. In such cases, the process of exporting and importing keys from the United Mode wallets complicates the processes hugely and may make automation impossible.

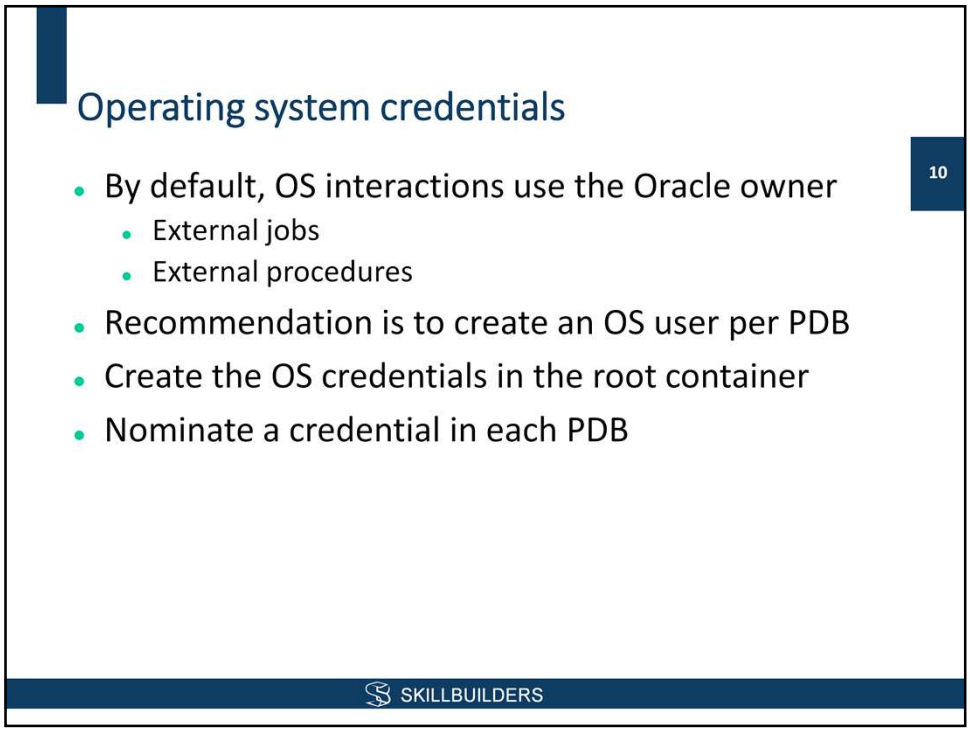


Data Vault can control privileged user access within PDBs for both local and common users. Individual local policies can be created for each PDB. When Data Vault protects an object, Data Vault subjects common privileges for common objects to the same enforcement rules as local system privileges.

In the strict mode, settings propagate from the root to all containers. In this mode, and PDBs where Data Vault is disabled will operate in restricted mode only. In regular mode, PDBs where Data Vault is not enabled function as normal.



Many ALTER SYSTEM and ALTER DATABASE commands will fail if executed in a PDB. In some cases, the failure is silent and in others an error will be returned. These statements can be permitted to succeed by setting noncdb_compatible=true. The security implications of this may be considerable, in that the DBA of one container can now perform tasks that will impact on the entire CDB.



Unless configured otherwise, any access to the server's operating system is accomplished in the security context of the Oracle owner. Oracle's advice is:

For better security, Oracle recommends that you set a unique operating system user for each PDB in a multitenant environment. Doing so helps to ensure that operating system interactions are performed as a less powerful user than the oracle operating system user, and helps to protect data that belongs to one PDB from being accessed by users who are connected to other PDBs.

To set up this environment:

Create an OS user for each PDB, with appropriate OS permissions

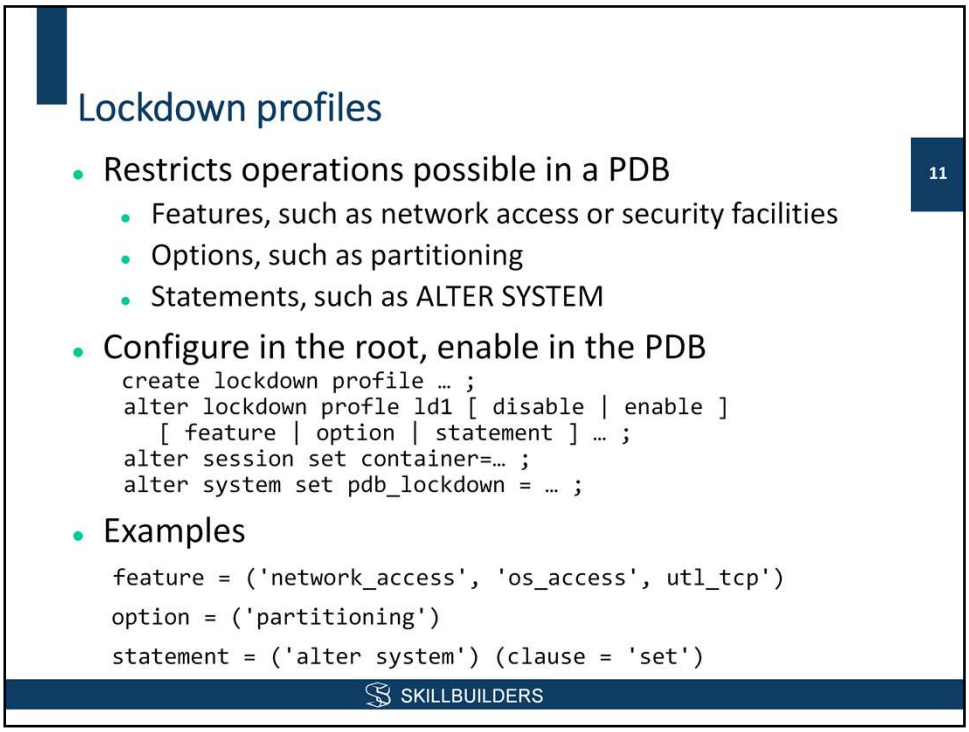
In the root container,

Exec dbms_credential.create_credential ('pdba_cred','<username>','<password>')

In the pluggable container,

Alter system set pdb_os_credential=pdba_cred scope=spfile;

Note that running jobs as the Oracle owner is bad practice in any database, and that OS credentials should always be supplied irrespective of whether the database is CDB or non-CDB.



The lockdown profile capability is clearly aimed at cloud service providers. It gives the ability to control what the users of a any one container can do. So even though, for example, partitioning might be licensed it will be usable in only some containers.

Security: summary

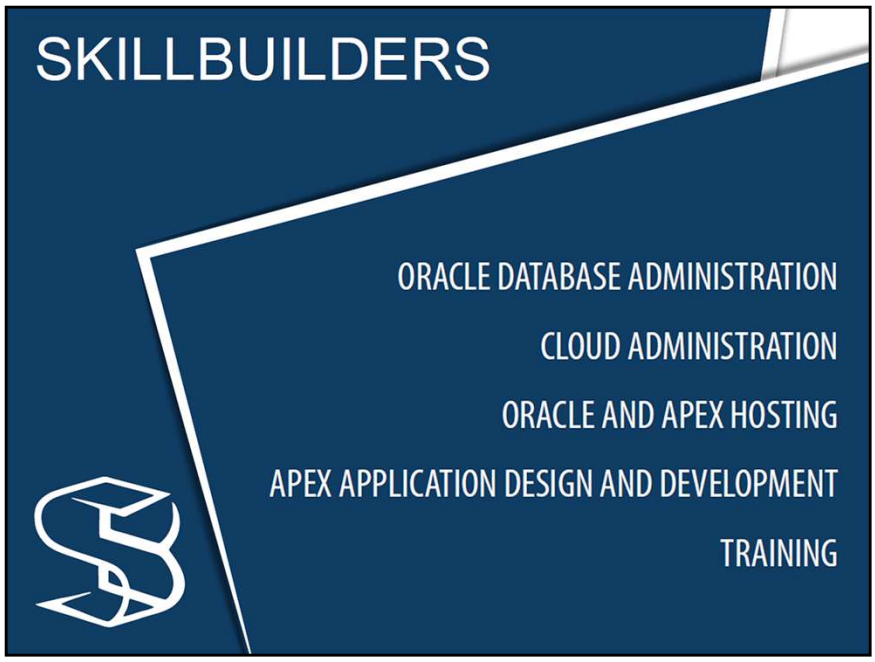
- Audit can be configured at CDB and PDB levels
  - Traditional audit is always configured in the PDBs
  - Unified Audit permits central control form the root
- Transparent Data Encryption
  - Unified Mode: one wallet per CDB
  - Isolated Mode: one wallet per PDB
- Data Vault is also Multitenant aware

Exercise

- Use Unified Audit
- Configure TDE in United Mode

13

SKILLBUILDERS


SKILLBUILDERS
ORACLE DATABASE ADMINISTRATION
CLOUD ADMINISTRATION
ORACLE AND APEX HOSTING
APEX APPLICATION DESIGN AND DEVELOPMENT
TRAINING