Securing the Oracle Database

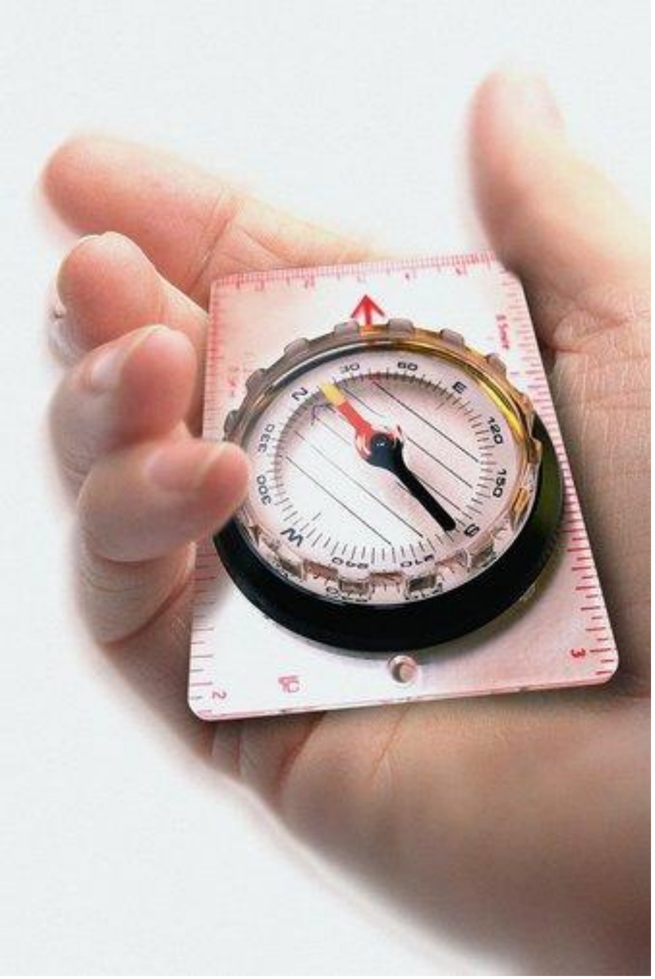
The International Institute of
SUPINFO
Information Technology

www.supinfo.com

Supinfo Official
SOC
Curriculum

Course objectives

By completing this course, you will:



- Apply the principle of least privilege
- Manage default user accounts
- Implement standard password security features
- Register for security updates

Securing the Oracle Database

Course topics

Course's plan:

- Security Parameters and Privileges
- Password Profiles
- Security Updates

Security Parameters and Privileges

Preview

- Database Security
- Security Parameters
- Privileges

Adjusting Default Security Settings

- DBCA can create more than a dozen default user accounts
- By default, there is no access to most of them

```
SELECT username, account_status
FROM dba_users;
```

- With exception of four users, all the users created by DBCA have their accounts marked as **`EXPIRED & LOCKED`**.
    - **`EXPIRED`** refers to the password
    - **`LOCKED`** means that it is impossible to connect with that account anyway

Security Parameters and Privileges

Adjusting Default Security Settings

- The passwords for the usable default accounts (**`SYS`**, **`SYSTEM`**, **`DBSNMP`**, and **`SYSMAN`**) are set at database creation time
- The other accounts have well-known passwords: they are the same as username
- When you unlock these accounts, you also have to change the password

```
SQL> ALTER USER wk_test ACCOUNT UNLOCK;

SQL> CONN wk_test/wk_test
ORA-28001: the password has expired

Changing password for wk_test
New password:
Retype new password:
Password changed
```

Adjusting Default Security Settings

The `DBSNMP` and `SYSMAN` accounts are for the use of Enterprise Manager. To change their passwords, you must use the `emctl` utility.

Adjusting Default Security Settings

- It should only be necessary to unlock a default account in exceptional circumstances.
- These accounts are used to store data and code required by certain options within the database, not for users to connect to.
- Example:

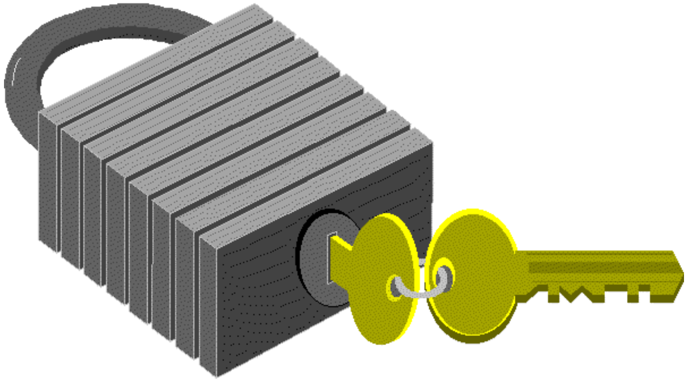
  “*The MDSYS schema stores the objects required by the Oracle Spatial option, which extends the capabilities of the database to manage geographical information. Users can make use of the spatial option without needing to connect to the schema.*”

Adjusting Default Security Settings

Even the demonstration schemas (HR, OE, and so on) are locked after you create them.

Adjusting Default Security Settings

- If your database was created from the SQL*Plus command line, security may be much weaker than using DBCA.
- For example, the **`SYS`** and **`SYSTEM`** passwords may be on the very weel-known defaults of **`CHANGE_ON_INSTALL`** and **`MANAGER`** respectively.
- On a frightening number of production systems, these defaults are never changed.



Database Security

- A secure system ensures the confidentiality of the data it contains. There are several aspects of security:
  - Restricting access to data and services
  - Authenticating users
  - Monitoring for suspicious activity

Database Security

Apply the Principle of Least Privilege

- Protect the data dictionary
- Revoke unnecessary privileges from `PUBLIC`
- Restrict the directories accessible by users
- Limit users with administrative privileges
- Restrict remote database authentication

Security Parameters

Protect the Data Dictionary

- Protect the data dictionary by ensuring the following **static** initialization parameter is set to **FALSE**:

```
O7_DICTIONARY_ACCESSIBILITY = FALSE
```

- This configuration prevents users with **ANY TABLE** system privileges from accessing data dictionary base tables.
- A **FALSE** setting also prevents user **SYS** from logging in as anything other than **SYSDBA**
- The default value of this parameter is **FALSE**. If you find it set to **TRUE**, ensure there is a good business reason.

Security Parameters

Protect the Data Dictionary

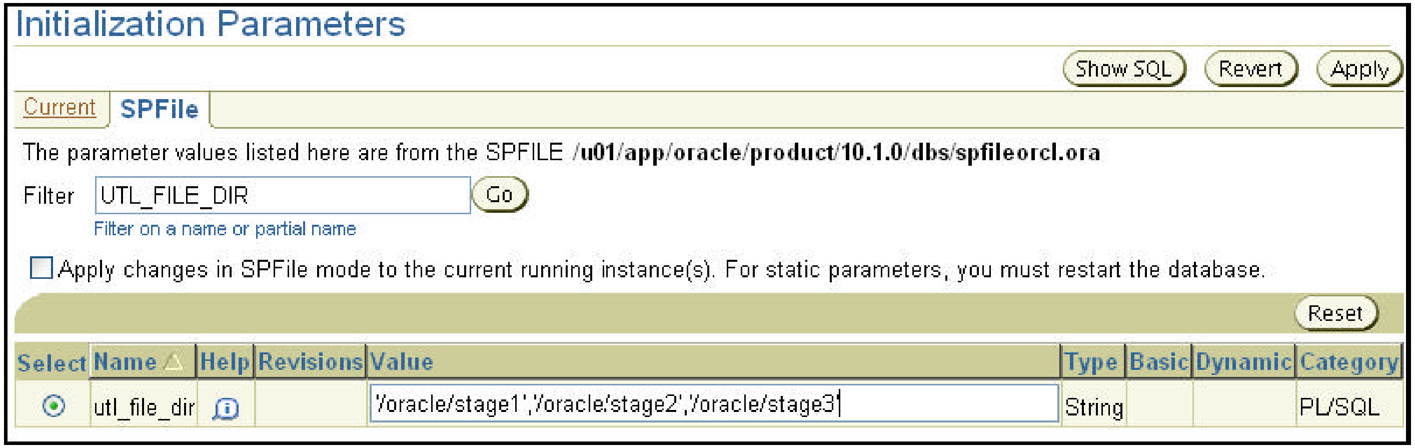
- Data dictionary accessibility is sometimes a problem for application installation routines. You may have to set **`O7_DICTIONARY_ACCESSIBILITY`** to true while installing a product, and then be able to put it back on default when the installation is finished.

- If you have users who really do need access to the data dictionary, consider granting them the **`SELECT ANY DICTIONARY`** privilege.
  - Let see the data dictionary and dynamic performance views
  - Will not allow to see any user data

Security Parameters

Restrict the Operating System Directories Accessible by the User

- The **`UTL_FILE_DIR`** configuration parameter:
  - Designates which directories are available for PL/SQL file I/O
  - Enables database users to read or write from the listed directories on the database server



Initialization Parameters

The parameter values listed here are from the SPFILE **/u01/app/oracle/product/10.1.0/dbs/spfileorcl.ora**

Filter: UTL_FILE_DIR

Filter on a name or partial name

□ Apply changes in SPFile mode to the current running instance(s). For static parameters, you must restart the database.

Select	Name △	Help	Revisions	Value	Type	Basic	Dynamic	Category
●	utl_file_dir	ⓘ		'/oracle/stage1','/oracle/stage2','/oracle/stage3'	String			PL/SQL

Security Parameters

UTL_FILE_DIR

- The difficulty with this parameter is that, being set at the instance level, it offers no way to allow some users access to some directories and other users to other directories.
- You can consider using:

```
SQL> CREATE DIRECTORY directory_name
  2  AS '/home/oracle/stage';

SQL> GRANT READ, WRITE
  2  ON directory_name
  3  TO user, role, PUBLIC;
```

Security Parameters

The `UTL_FILE_DIR` parameter can include wildcards. Never set it to '*', because that will allow all users access to everything that the database owner can see, including `ORACLE_HOME` and all the database files.

Security Parameters

Disable Remote Operating System Authentication

- Remote authentications should be used only when you trust all clients to appropriately authenticate users.
- Remote authentication process:
  - The database user is authenticated externally.
  - The remote system authenticates the user.
  - The user logs on to the database without further authentication.
- To disable, ensure that the following instance initialization parameter is at its default setting:

```
REMOTE_OS_AUTHENT = FALSE
```

Privileges

- There is a pseudo-user called **PUBLIC**. Any privileges granted to **PUBLIC** have, in effect, been granted to every user.
- Every account you create will have access to these privileges.
- By default, the **PUBLIC** user has a large number of privileges. In particular, he has **EXECUTE** permission on a number of PL/SQL utility packages.

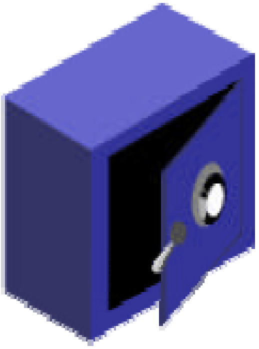
```
SELECT COUNT(*) FROM dba_tab_privs WHERE grantee='PUBLIC';

 COUNT(*)
--------
   20762

SELECT table_name FROM dba_tab_privs WHERE grantee='PUBLIC'
AND privilege='EXECUTE' AND table_name LIKE 'UTL%';
```

Privileges

- Revoke all unnecessary privileges and roles from the database server user group **PUBLIC**.
- Many built-in packages grant **EXECUTE** to **PUBLIC**.
- Execute on the following packages should usually be revoked from **PUBLIC**:
  - **UTL_SMTP**
  - **UTL_TCP**
  - **UTL_HTP**
  - **UTL_FILE**
  - **DBMS_OBFUSCATION_TOOLKIT** / **DBMS_CRYPTO**



- Example:

```
REVOKE execute ON utl_file FROM PUBLIC;
```

Privileges

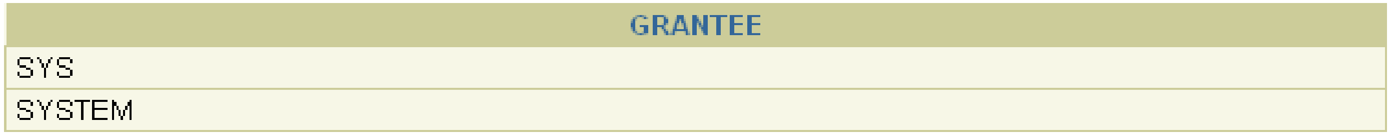
Always remember that, by default, these packages are available to absolutely anyone who has a logon to your database, and furthermore that your database may have a number of well-known accounts with well-known passwords.

Privileges

Limit Users with Administrative Privileges

- Restrict the following types of privileges:
  - Grants of system and object privileges
  - SYS-privileged connections: **SYSDBA** and **SYSOPER**
  - DBA-type privileges, such as **DROP ANY TABLE**
  - Run-time permissions
- Example: List all users with the **DBA** role:

```
SELECT grantee
FROM dba_role_privs
WHERE  granted_role = 'DBA';
```



GRANTEE
SYS
SYSTEM

Part 1 Summary

Privileges

Database Security

Security Parameters

Part 1 Stop-and-think

Do you have any questions ?

Password Profiles

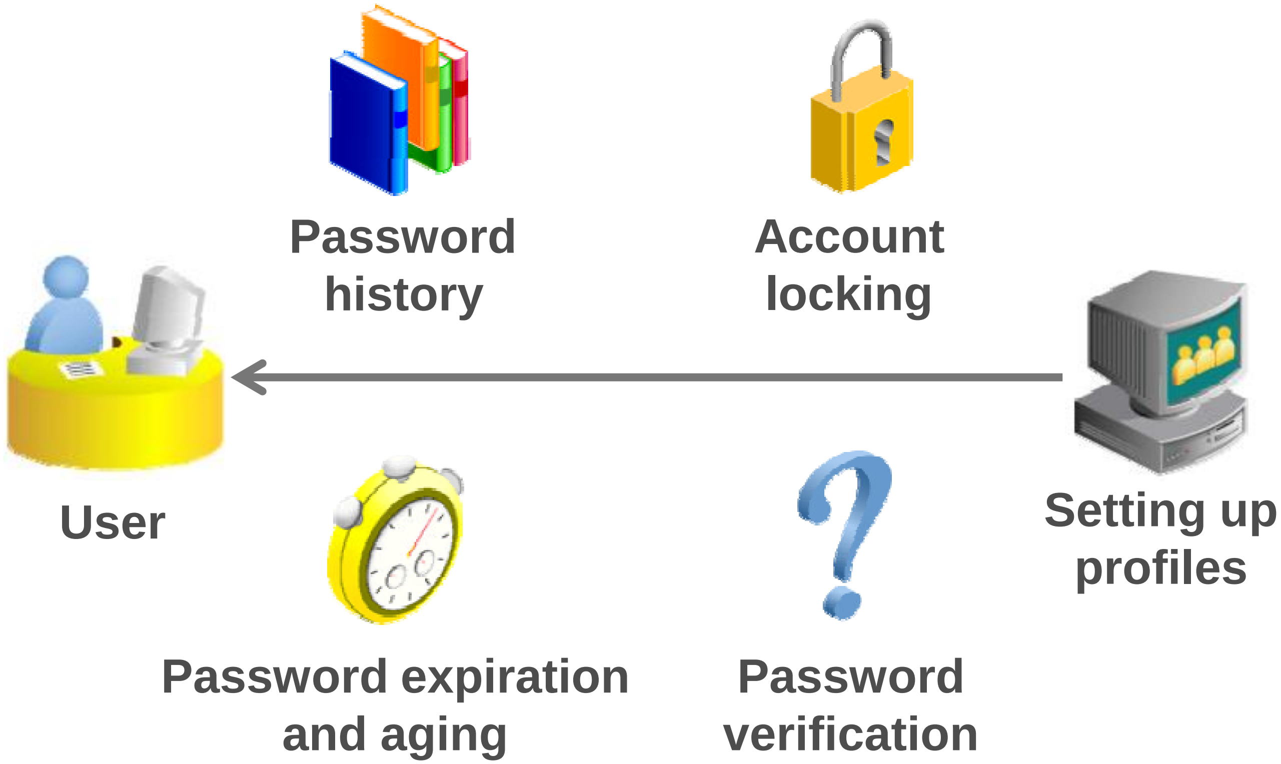
Preview

- Features
- Managing Password Profiles

Password Profiles

Features

Password Account Locking



Password history

Account locking

User

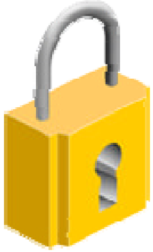
Setting up profiles

Password expiration and aging

Password verification

Features

Password Account Locking



Parameter	Description
`FAILED_LOGIN_ATTEMPS`	Number of failed login attempts before lockout of the account
`PASSWORD_LOCK_TIME`	Number of days the account is locked after the specified number of failed login attempts

Features

Password Expiration and Aging

Parameter	Description
`PASSWORD_LIFE_TIME`	Lifetime of the password in days after which the password expires
`PASSWORD_GRACE_TIME`	Grace period in days for changing the password after the first successful login after the password has expired

Password Profiles

Features

Password History

Parameter	Description
PASSWORD_REUSE_TIME	Number of days before a password can be reused
PASSWORD_REUSE_MAX	Number of password changes required before the current password can be reused, irrespective of the PASSWORD_REUSE_TIME setting.

Features

Password Verification

Parameter	Description
`PASSWORD_VERIFY_FUNCTION`	A PL/SQL function that makes a password complexity check before a password is assigned

- Password verification functions must:
  - Be owned by the **`SYS`** user
  - Return a Boolean value (true or false)

Password Profiles

Features

Supplied Password Verification Function: `VERIFY_FUNCTION`

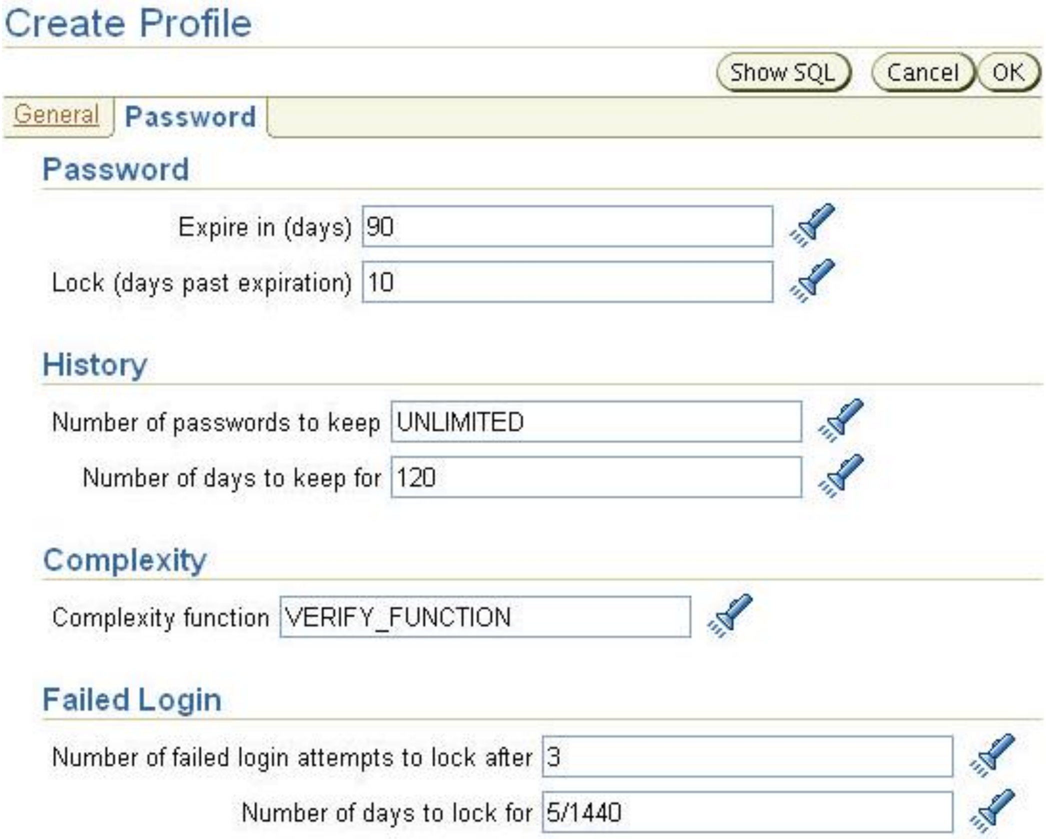
The supplied password verification function enforces password restrictions where the:

- Minimum length is four characters
- Password cannot be equal to username
- Password must have at least one alphabetic, one numeric, and one special character
- Password must differ from the previous password by at least three letters

```
@ $ORACLE_HOME/rdbms/admin/utlpwdmg.sql
```

Managing Password Profiles

Creating a Password Profile



Password

Expire in (days) 90

Lock (days past expiration) 10

History

Number of passwords to keep UNLIMITED

Number of days to keep for 120

Complexity

Complexity function VERIFY_FUNCTION

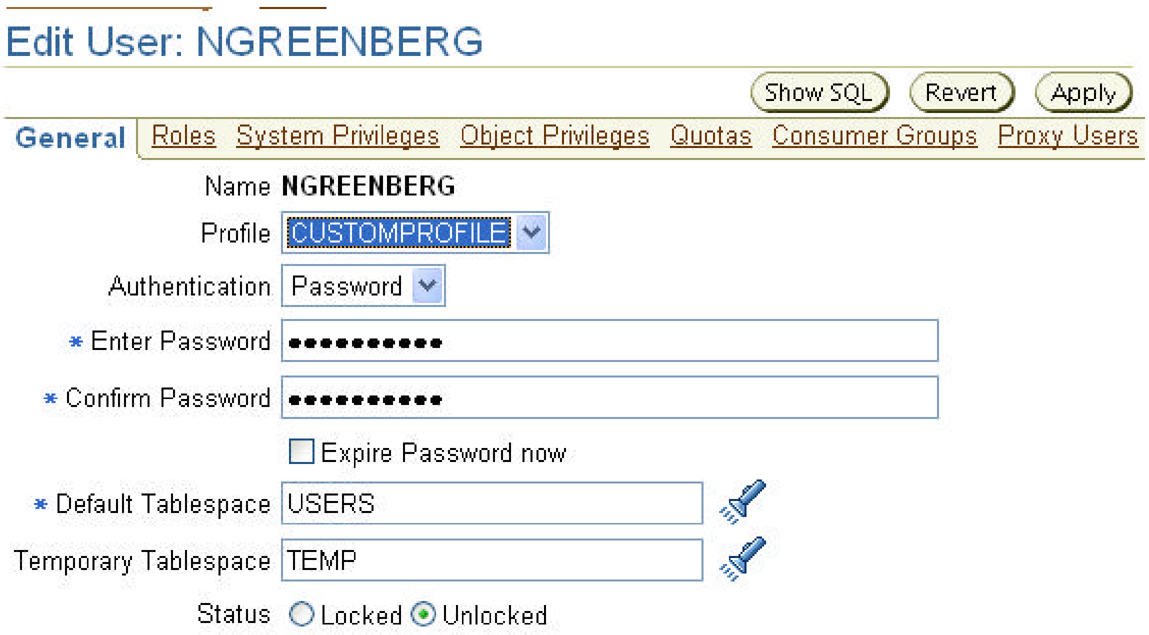
Failed Login

Number of failed login attempts to lock after 3

Number of days to lock for 5/1440

Managing Password Profiles

Assigning a Password Profile to Users



Edit User: NGREENBERG

Name NGREENBERG

Profile CUSTOMPROFILE

Authentication Password

* Enter Password ●●●●●●●●●●●

* Confirm Password ●●●●●●●●●●●

□ Expire Password now

* Default Tablespace USERS

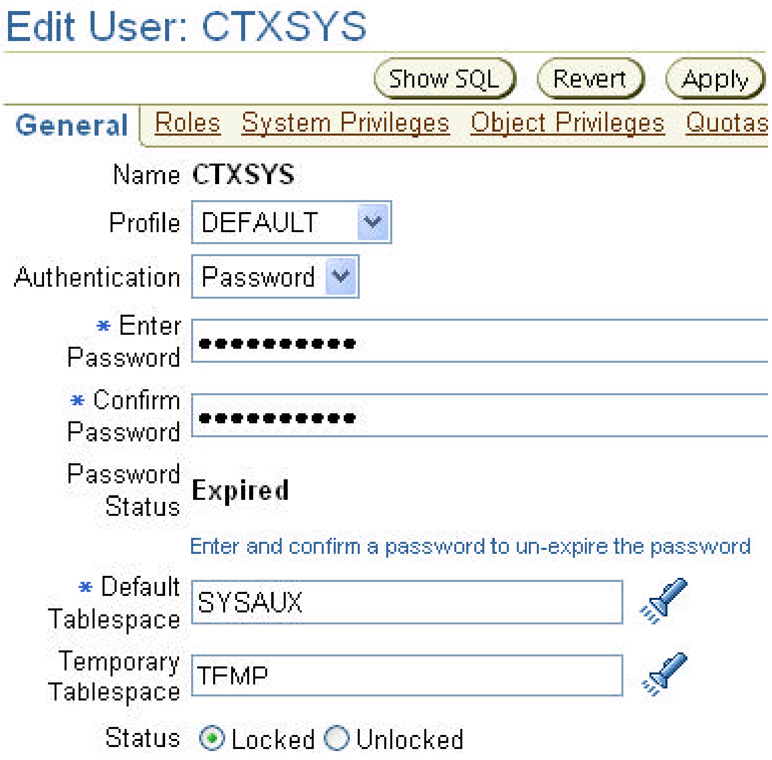
Temporary Tablespace TEMP

Status ○ Locked ● Unlocked

Managing Password Profiles

Manage Default User Accounts

- DBCA expires and locks all accounts, except:
  - **`SYS`**
  - **`SYSTEM`**
  - **`SYSMAN`**
  - **`DBSNMP`**
- For a manually created database, lock and expire any unused accounts.



Edit User: CTXSYS

Name	CTXSYS
Profile	DEFAULT
Authentication	Password
* Enter Password	●●●●●●●●●●●
* Confirm Password	●●●●●●●●●●●
Password Status	Expired
	Enter and confirm a password to un-expire the password
* Default Tablespace	SYSAUX
Temporary Tablespace	TEMP
Status	● Locked ○ Unlocked

Part 2 Summary

Features

Managing Password Profiles

Security Updates

Security Updates

Preview

- Introduction

Introduction

- Oracle Corporation issues regular security updates. Generally each term.
- These are usually in the form of patches that you must apply to your Oracle software.
- Wherever possible, patches should be installed as patch sets. A patch set is a collection of patches that you install with the Oracle Universal Installer.
- Thanks to Oracle Metalink Credentials, you can identify and download patches directly into Database Control.
- http://www.oracle.com/technology/deploy/security/alerts.htm

Part 3 Summary

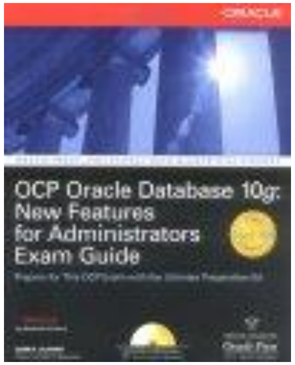
Introduction

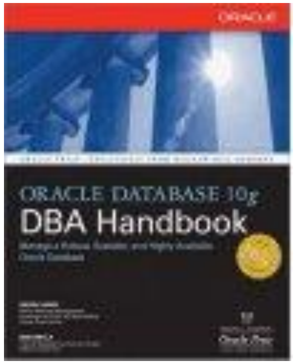
Metalink

For more

If you want to go into these subjects more deeply, …

Publications


ORACLE
OCP Oracle Database 10g New Features for Administrators Exam Guide
Oracle Press



http://www.oracle.../bookstore/

Courses

Cursus: Merise & SQL

Cursus: PL/SQL

Cursus: DBA1 & DBA2

Cursus: DWH, OAS & BIS

Web sites

http://www.labo-oracle.com

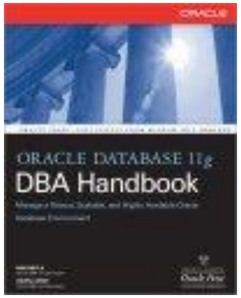
http://www.oracle.com

http://otn.oracle.com

Certifications

1Z0-042

1Z0-043



THE INTERNATIONAL INSTITUTE OF

SUPINFO

INFORMATION TECHNOLOGY

Congratulations

You have successfully completed
the SUPINFO course n°13

Oracle Technologies
Securing the Oracle Database

The end

The International Institute of
SUPINFO
Information Technology