

# Oracle Database Security Update

ISACA – Nashville Chapter

Susan Wolford – Manager, Advisory Services  
Ahmad Sabbarini – Manager, Advisory Services

November 2009

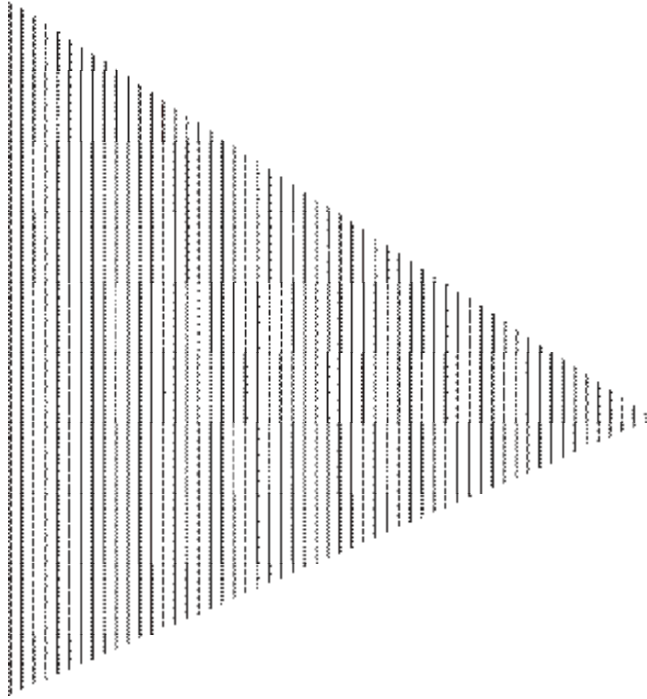


---

# Objectives

---

- ▶ Synergize the risk of the Database to the Operating System or Applications
- ▶ Understand the basic architecture of the Oracle Database Management System
- ▶ Understand the unique risks and security controls for Oracle Database and underlying operating systems



# Oracle Database IT General Controls Workshop

## Module 1: Oracle Database Essentials



---

# Data is a Target ... the roles of O/S to DB to Data is Changing

---

- ▶ With databases becoming more distributed, security is less dependent on the operating system (OS)
- ▶ Numerous regulations require extensive controls at the database layer
- ▶ Users can access the data through the application or network (no need for operating system accounts)
- ▶ Still see applications that rely on the database for authentication (both in-house and purchased applications)
- ▶ With the advent of application and service oriented architecture, remote access is becoming the norm
- ▶ Perimeter (firewalls) and O/S defenses are no longer sufficient

---

# Synergizing the risks between DB and O/S

---

- ▶ Most of the attacks are internal
- ▶ The inherent risks are data loss, modification and theft
- ▶ Management's focus should be more internal:
  - ▶ Apply data security at the source (this principle should apply in both O/S file level and DB table level)
  - ▶ Examine the integrity of database execution path and internal functions (e.g. stored procedures, views)
  - ▶ Access level for legitimate users from the database users through application, operating systems, or the database are carefully designed and documented
  - ▶ Monitor and review the database users, processes, and jobs periodically

---

# Synergizing the risks between DB and O/S (Cont'd)

---

- ▶ Then, focus externally
  - ▶ Database network services
  - ▶ Internal and third party utilities
  - ▶ Hooks and interactions with applications (e.g., ERP, translation engines, adaptors)
  - ▶ Network connectivity (exposure of the Internet)
  - ▶ Patch management
  
- ▶ Multiple Levels of Security is the norm
  - ▶ Regularly perform audits and penetration tests on your database
  - ▶ Encryption of data-in-motion / data-at-rest / data-in-use
  - ▶ Monitor database activity log files
  - ▶ Implement database intrusion detection and auditing

---

## Synergizing the risks between DB and O/S (Cont'd)

---

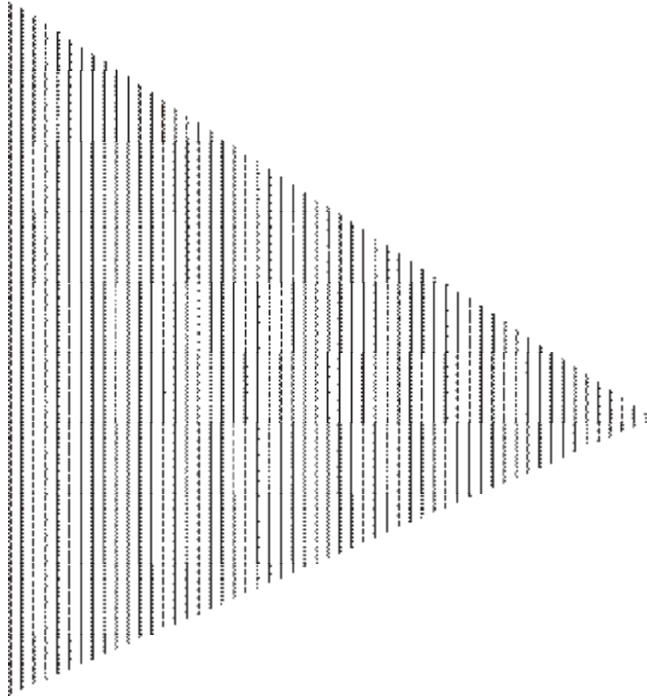
- ▶ The bottom line, a compromised database represents a higher financial reporting and compliance risk than a compromised O/S, as data can be modified and remain undetected for a period of time

---

# Oracle Database Basics

---

- ▶ Oracle Database is a relational database management system and a collection of data within a table definition
- ▶ Oracle Instance vs Database, and Oracle Processes (unique for each instance)
- ▶ A collection of physical data files are logically grouped into a tablespace. There are several types of tablespaces: system tablespace, temp tablespace user tablespace etc.
- ▶ The database is generally comprised of tables, views, indexes, clusters, sequences, functions, stored procedures etc.
- ▶ Typical structure at our clients:
  - ▶ Application Layer – Oracle E-Business Suite, SAP etc.
  - ▶ Database Layer – Oracle Database 9/10g/11g
  - ▶ Operating System – UNIX, Windows etc.



# Oracle Database IT General Controls Workshop

## Module 2: Users and Roles



---

# User Account Management

---

Oracle Database user account types:

- ▶ DBA – can access anything, do anything, except start, stop, or tune database
- ▶ Privileged User – can access anything specifically granted to it
- ▶ Unprivileged user – can access only privileges granted to PUBLIC
- ▶ All users must have CONNECT role (specifically the CREATE SESSION privilege) in order to connect to Oracle

Note: Users do not need an operating system account to connect to Oracle. They can access Oracle from the network.

---

# Required Passwords (User ID and Password Authentication Option)

---

- ▶ Each account has a password
- ▶ Other than the fact that passwords are used to authenticate users, all Oracle versions prior to Oracle 8 have no other password management features
- ▶ By default, Oracle User IDs and passwords range from 1 – 30 characters long (not null)
- ▶ To review whether an account has a password or not
  - ▶ Review the password field for all DBA users table
  - ▶ Passwords are stored in DES standard (easily obtainable or cracked)

---

# Default Accounts and Passwords

---

- ▶ Oracle Database comes with numerous (> 50) vendor provided accounts with widely known passwords. Examples are:
  - ▶ SYS:CHANGE\_ON\_INSTALL
  - ▶ SYSTEM:MANAGER
  - ▶ DBSNMP:DBSNMP
- ▶ Some non-administrative accounts (e.g., DEMO, OUTLN) should be disabled!

---

# Database Roles

---

- ▶ Roles are organized groups of related privileges that are granted to users or other roles
  
- ▶ Pre-defined roles are defined as part of Oracle database, they are
  - ▶ CONNECT – allows users to logon
  - ▶ RESOURCE – allows users to create, manage, or drop database resources (such as tables) within their schema
  - ▶ DBA – allows users to create other user ids, change user passwords, set auditing, access any data in the database, etc
  - ▶ IMP\_FULL\_DATABASE – allows users to import database
  
- ▶ Database roles are used to group users who have common privilege requirements

---

# Database Privileges

---

- ▶ A database privilege is a right to execute specific SQL statement or to access a database object
- ▶ Privileges can either be granted to or revoked from a user explicitly or be assigned through a role
- ▶ All database users have access to any resources granted to the Public user/role (PUBLIC privilege). Therefore, review of the privileges granted to PUBLIC is necessary
- ▶ Two categories of privileges:
  - ▶ System: Allows a user to log on and create/manipulate objects (e.g. users, triggers). Examples: ALTER DATABASE, GRANT ANY PRIVILEGE, CREATE PROFILE, CREATE ROLE, CREATE USER, ALTER SYSTEM, ALTER USER, etc.
  - ▶ Object: Allows access to the data within an object (e.g. table). Examples: INSERT, UPDATE, EXECUTE, ALTER, etc.

---

# Database Profile

---

- ▶ Profile is used to restrict resource and password limits for a group of users
- ▶ Each user is assigned to one profile only
- ▶ If a specific assignment is not available, the system DEFAULT profile is assigned
- ▶ Profiles are available to the following data dictionary/views:
  - ▶ DBA\_USERS (views of all users and their assigned profiles)
  - ▶ DBA\_PROFILES (views of all profiles and their configurations)

---

# Privileges, Roles and Profiles Tables/Views

---

- ▶ DBA\_USERS
- ▶ DBA\_ROLE\_PRIVS
- ▶ DBA\_SYS\_PRIVS
- ▶ DBA\_TAB\_PRIVS
- ▶ DBA\_PROFILES

---

# Restrict Role Functionality

---

- ▶ Roles with Insert, update, or delete object privileges can be created with passwords
- ▶ All non-DBA user IDs/roles must be granted specific access to the data tables (or subset “views”)
- ▶ Tables privileges can be given on a table-by-table basis, or many tables can be grouped together in “roles” and granted collectively
- ▶ Table, view, or role access can only be granted by the table or role “owner” (or user id that has been granted access with “grant authority”)

---

# Temporary & Contractor Type Accounts

---

- ▶ Contractor and temporary database accounts should expire or be removed after a specified period of time
- ▶ In addition to periodic reviews, consider other controls such as:
  - ▶ User naming conventions for temporary & contractor accounts
  - ▶ Assigning specific roles to temporary & contractor accounts with formal documentation
  - ▶ More stringent requirements of resource limitation (such as dedicated profiles)

---

# Roles/System Privileges with Admin Option

---

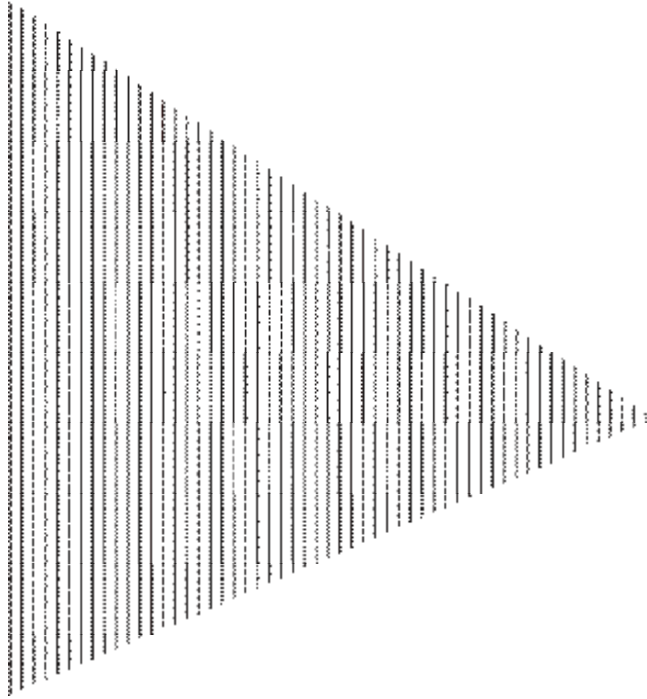
- ▶ Roles/System Privileges should not be granted with the “WITH ADMIN OPTION” unless required for authorized security or application administration purposes
- ▶ Only users granted a system privilege “WITH ADMIN OPTION” or a user with “GRANT ANY PRIVILEGE” system privilege can grant or revoke a system privilege to or from other users or roles of the database
- ▶ Any user granted a role with the WITH ADMIN OPTION can grant or revoke the role to or from other users or roles of the database

---

# Object Privileges with Grant Option

---

- ▶ Object privileges should not be granted with the “With GRANT OPTION” unless required for authorized security administration purposes
- ▶ Different from GRANT ANY ROLE, where GRANT is system privilege operator that grants and revokes any role to or from other users or roles of the database in cascade
- ▶ WITH GRANT OPTION is ad-hoc, and the grantee need not be a username or a set of usernames. It is permitted to specify PUBLIC, which means that the privileges are granted to everyone (e.g., GRANT SELECT ON <userlist> TO PUBLIC)



# Oracle Database IT General Controls Workshop

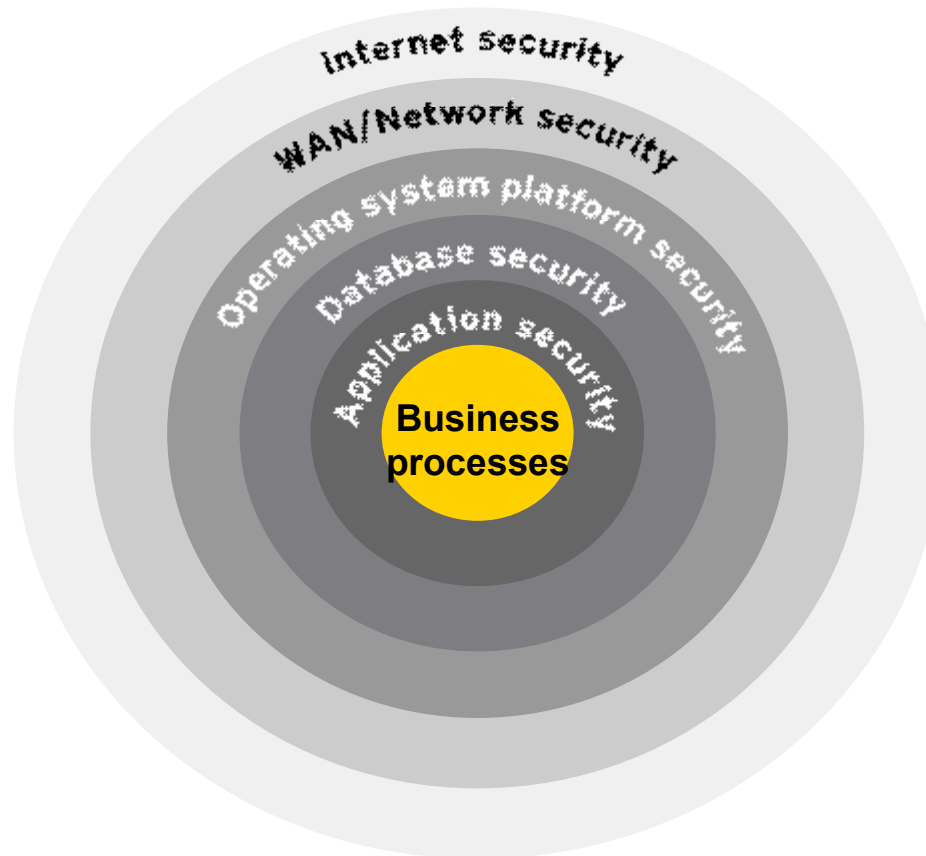
## Module 3: Operating System Security and Change Control



---

# The Logical Access Path

---



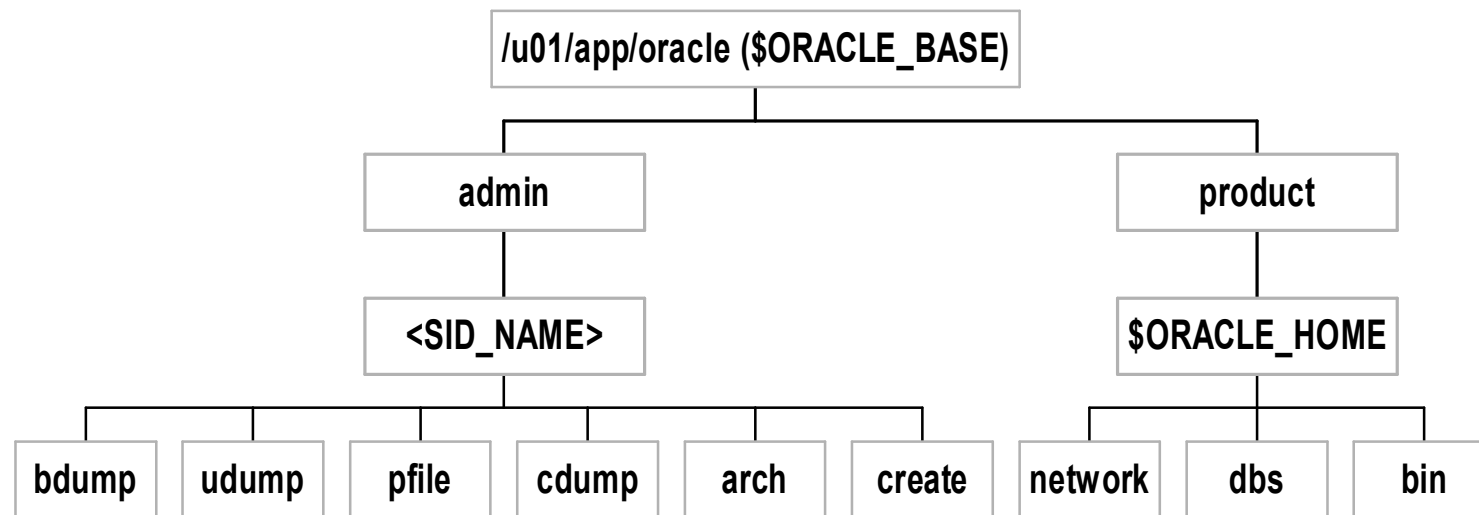
---

# Access to Underlying OS

---

- ▶ The ability to perform administrative procedures over the underlying operating system is crucial to the security of the database as it impacts:
  - ▶ Access to Oracle configuration, physical data files and logs
  - ▶ Access to start, shut down and tune the database
  - ▶ Access to database utilities and services
  - ▶ Access to database services

# Oracle Operating System Files



The standard convention for file extensions or endings to file names are

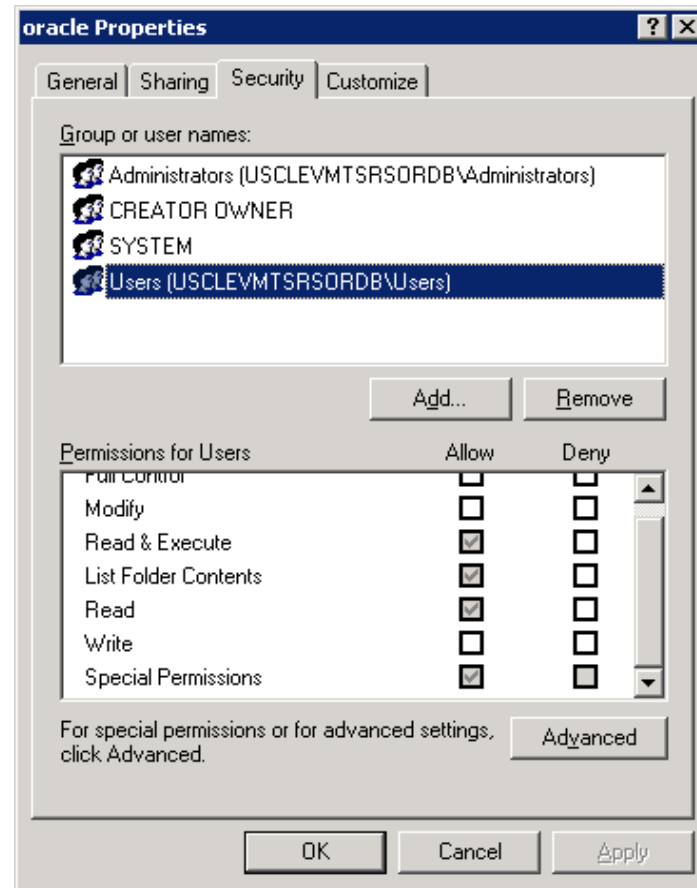
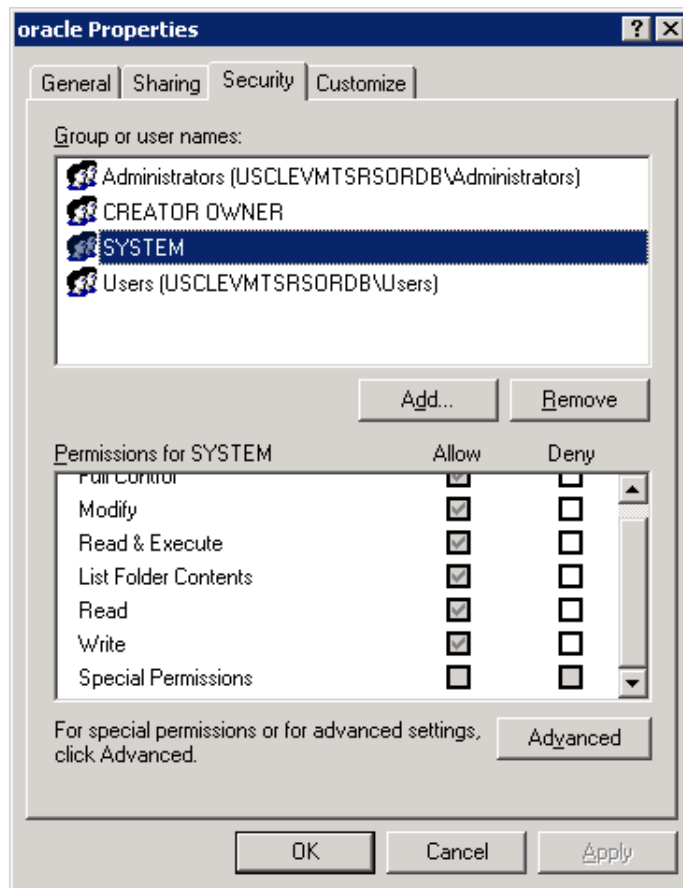
- data files .dbf
- control files .ctl
- redo log files .dbf (some use .rdo)
- parameter file .ora

# Oracle Operating System Files (Cont'd)

**Figure 7.2—Recommended Oracle Database UNIX Directory**

<b>Files and Directories</b>	<b>Production Permissions</b>
All database, redo log and control files (extensions for these files are typically .dbf, .log and .ctl)	640 rw-r----
\$ORACLE_HOME/bin	751 rwxr-x—x
The Oracle executables and the following network executables: \$ORACLE_HOME/bin/oracle and \$ORACLE_HOME/bin/dbsnmp	6750 rws-r-s—x
All other executables under the \$ORACLE_HOME/bin/ directory	755 rwxr-xr-x
\$ORACLE_HOME/lib/	755 rwxr-xr-x
All files under the \$ORACLE_HOME/lib/	644 rw-r—r__
\$ORACLE_HOME/rdbms/log/	751 rwxr-x—x
Product subdirectories such as \$ORACLE_HOME/sqlplus or \$ORACLE_HOME/rdbms	751 rwxr-x—x
Files in \$ORACLE_HOME/sqlplus or \$ORACLE_HOME/rdbms	644 rw-r—r__
\$ORACLE_HOME/network/trace	730 rwx-wx---
All files under the product admin directories, such as \$ORACLE_HOME/rdbms/admin/ and \$ORACLE_HOME/sqlplus/admin/	644 -rw-r—r__
All audit files under the \$ORACLE_HOME/rdbms/audit directory files ending in .aud	640 rw-r-----

# Oracle Operating System Files (Cont'd)



---

# Permission on Oracle Data Files

---

- ▶ The Oracle Data files should be set to read/write for the Oracle software owner, for all instances where the Oracle software owner is running the Oracle processes
- ▶ Determine whether the INIT.ORA and CONFIG.ORA files should be properly secured and periodically reviewed by security personnel or database administrators for unauthorized changes. The init.ora file stores the initialization parameters of Oracle.
- ▶ Database data is stored in O/S files, which may not be well protected. Accessing data this way obviously circumvents any database-level security controls

---

# Access to Database Utilities

---

- ▶ Powerful system and database utilities are restricted to those users requiring them to perform their job function
- ▶ Besides locating the directory where the Oracle binaries and utilities are installed and generate a listing of users and groups that have execute access to the files or utilities, we should be aware of the processes running within Oracle
- ▶ Processes are stored in a special view v\$session located in the schema SYS

---

# Access to Database Utilities (Cont'd)

---

## Common database utilities:

### Oracle Native

- ▶ SQL\*Plus (SQL shell)
- ▶ SQL\*forms (application control)
- ▶ SQL\*Loader (loads data from system files)
- ▶ SQL\*Net (TCP/IP protocols)
- ▶ SQL\*DBA (admin tool)

### Non-Oracle

- ▶ Toads
- ▶ ERwin

---

# Database Restart and Shutdown

---

- ▶ Only authorized personnel should shutdown and restart database processes

## Internally

- ▶ Usually users with SYSDBA and SYSOPER privileges
- ▶ Restricting the number of users and roles with these permissions

## External

- ▶ In addition, review the O/S specific jobs (cron, at) and shutdown/startup scripts to ensure proper file permissions are set and only the authorized personnel have rights to execute these scripts

---

# Change Control

---

- ▶ Ensure that database configuration changes and changes to key objects are managed/controlled in line with the company's change control policy.
  
- ▶ Maintain and upkeep the following documentation:
  - ▶ Pre-Installation (pre-install kernel configuration, mount points, dba group)
  - ▶ Post-Installation and configuration [baselines of configuration files (init.ora, listener.ora, etc)]
  - ▶ Any operational procedures and security policy
  - ▶ Change requests for update/patches/implementation
  
- ▶ Review change logs against the inventory and baselines of configuration files (use of tools such as IPLocks, Repscan, Oracle EM Change Management Pack)

---

# Summary

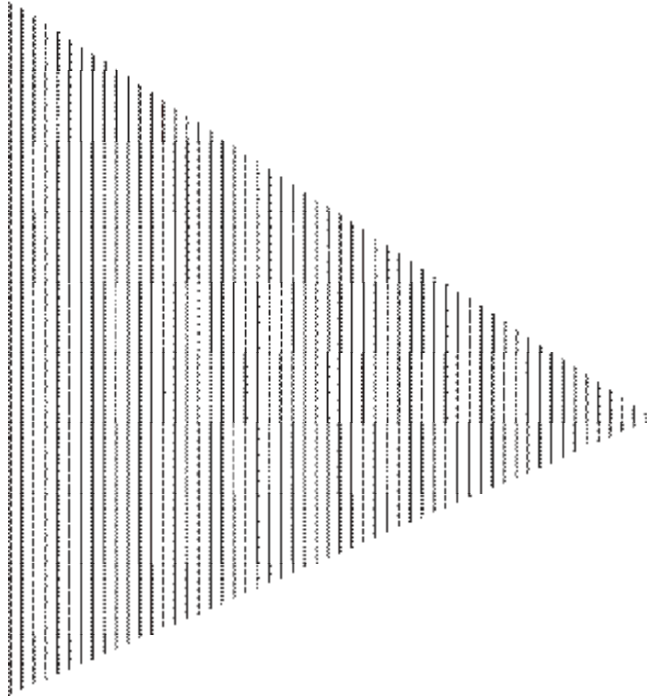
---

## UNIX

- ▶ Choose different account names (i.e., oracle) than standard suggested
- ▶ Restrict use of the Oracle Software account, secure all Oracle working directories
- ▶ Pay notice to the some Oracle files that has SUID bits set
- ▶ Restrict local group membership (e.g. dba group)
- ▶ Only enable required services

## Windows

- ▶ Secure admin accounts and local group membership (e.g. oradba group)
- ▶ Restrict use of the Oracle Software account, secure all Oracle working directories
- ▶ Restrict registry access
- ▶ Strengthen account/domain policies
- ▶ Only enable required services



# Oracle Database IT General Controls Workshop

## Module 4: Authentication Controls



---

# Host and Remote Based Authentication

---

- ▶ Users can be authenticated to the database directly or via the host operating system. If users are authenticated via host based authentication, PASSWORD field in the user table will be 'EXTERNAL' or 'GLOBAL'
- ▶ Usually set to require OPS\$ prefix to user ID in database (default established by OS\_AUTHENT\_PREFIX in INIT.ORA). **The value for this parameter should not equal " " (unless needed), as this means that all user accounts can authenticate via the operating system.** Once authenticated to OS, user can use "/" at user id prompt, password prompt is left blank
- ▶ Similar to host-based authentication but extends the ability to authenticate to remote servers. This is usually a security risk, as such, only in rare circumstances should remote authentication be used

---

# Trust Relationships

---

- ▶ Implemented using database links (DBLINK). Database links are essentially direct communication channels between databases.
- ▶ There are three types of links: public, private, and global.
- ▶ Database links can be created with an account/password or without an account/password.
- ▶ Should always protect the table where these links are defined (SYS.LINK\$)

---

# Listener and Network Security

---

- ▶ The Transparent Network Substrate (TNS) Listener is the service responsible for authenticating remote clients to the server:
  - ▶ Listens to port 1521 by default (but could be changed)
  - ▶ No password by default
  - ▶ Allows an attacker to write arbitrary files on OS
  - ▶ Could compromise the security of the database
  
- ▶ To secure Oracle TNS listener (mostly in 10g),
  - ▶ Change default port (has to be above 1024)
  - ▶ Passwords within listener.ora (PASSWORDS\_LISTENER). Password is in plain text so limit ability to read the file and change it periodically
  - ▶ Enable the ADMIN\_RESTRICTIONS\_LISTENER\_NAME that prohibits remote changes to the Listener services
  - ▶ Apply patches and log activity of the Listener

---

# Listener and Network Security (Cont'd)

---

- ▶ Oracle Connection Manager (CMAN)
  - ▶ This comes bundled with the Oracle Enterprise Edition
  - ▶ It manages the connection by acting as a proxy between the database and clients. CMAN maintains one connection with the database regardless of the number of client connections.
  
- ▶ Valid Node Checking
  - ▶ Used to allow or deny access to the Oracle server based on the client's IP addresses
  - ▶ To use this feature, change the following parameters in the sqlnet.ora:  
TCP.VALIDNODE\_CHECKING=YES, TCP.INVITED\_NODES = {list of IP addresses}, TCP.EXCLUDED\_NODES = {list of IP addresses}

---

# Password and Other Controls

---

- ▶ Passwords are controlled by profiles
- ▶ Two types of limits/parameters: PASSWORD and RESOURCE
- ▶ If the RESOURCE\_LIMIT parameter is set to FALSE, then resource limits (e.g. idle session timeout, session per user) is not enabled

<b>PROFILE</b>	<b>PARAMETER</b>	<b>VALUE</b>
Profile Name	COMPOSITE_LIMIT	UNLIMITED
Profile Name	FAILED_LOGIN_ATTEMPTS	10
Profile Name	SESSIONS_PER_USER	UNLIMITED
Profile Name	PASSWORD_LIFE_TIME	45
Profile Name	CPU_PER_SESSION	UNLIMITED
Profile Name	PASSWORD_REUSE_TIME	UNLIMITED
Profile Name	PASSWORD_REUSE_MAX	10
Profile Name	LOGICAL_READS_PER_SESSION	UNLIMITED
Profile Name	PASSWORD_VERIFY_FUNCTION	Pass_func
Profile Name	LOGICAL_READS_PER_CALL	UNLIMITED
Profile Name	PASSWORD_LOCK_TIME	UNLIMITED
Profile Name	IDLE_TIME	UNLIMITED
Profile Name	PASSWORD_GRACE_TIME	5
Profile Name	CONNECT_TIME	UNLIMITED

---

# Password Composition

---

- ▶ Oracle should be configured to require complex passwords (alpha and numeric characters, uppercase and special characters) to reduce the likelihood of the passwords being compromised. This is done using the PASSWORD\_VERIFY\_FUNCTION
  
- ▶ The default PASSWORD\_VERIFY\_FUNCTION is inherent weak (very likely not compliant with corporate policy)
  
- ▶ Third-party default passwords
  - ▶ [http://www.petefinnigan.com/default/default\\_password\\_list.htm](http://www.petefinnigan.com/default/default_password_list.htm) (List of 600 default usernames/passwords)
  
- ▶ Password dictionaries
  - ▶ <http://www.openwall.com/passwords/wordlists/> (The wordlists are intended primarily for use with password crackers)

---

# Password Verified Function Example

---

```
CREATE OR REPLACE FUNCTION SYS. Pass_func
(username varchar2,
password varchar2,
.....
BEGIN
digitarray:= '0123456789';
chararray:=
    'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ';
-- Check if the password is same as the username
IF NLS_LOWER(password) = NLS_LOWER(username) THEN
raise_application_error(-20001, 'Password should not be the same as the
    username');
END IF.....
```

---

# Account Lockout

---

- ▶ Controlled by the FAILED\_LOGIN\_ATTEMPTS and PASSWORD\_LOCK\_TIME parameters
- ▶ The SYSTEM account can be locked but the SYS account cannot
- ▶ With the use of Password Profiles, you can customize this settings based on the type of user account (system account, application account, end user account etc.)
- ▶ Oracle10g enabled Password Lockout for default profile

---

# Idle Session Timeout

---

- ▶ Usually controlled by the IDLE\_TIME parameter (expressed in minutes)
  
- ▶ In Oracle10g, additional idle time settings are added that can be applied to the various consumer groups (a resource consumer group is a collection of users with similar requirements for resource consumption):
  - ▶ MAX\_IDLE\_TIME (default: NULL (unlimited)) which indicates the maximum session idle time
  - ▶ MAX\_IDLE\_BLOCKER\_TIME (default: NULL (unlimited)) which indicates the maximum blocking session idle time. The block is the state waiting for a transaction to commit
  
- ▶ If not possible to enable, consider host and/or network session timeout controls

---

# Password History

---

- ▶ Can be controlled by the PASSWORD\_REUSE\_TIME (defined in days) and PASSWORD\_REUSE\_MAX parameters
- ▶ These two parameters are mutually exclusive. If one is used, the other must be set to unlimited
- ▶ If both parameters are set to UNLIMITED then Oracle will ignore both settings

---

# Oracle Enterprise Security Manager

---

- ▶ With a large number of users and servers, user management becomes more complex and requires substantial resources. This produces security challenges and in most cases security problems
- ▶ Enterprise User Security addresses these security challenges by utilizing a directory service, such as Active Directory, for user authentication and authorization
- ▶ Key concepts: Enterprise User, Enterprise Role and Global Role
  - ▶ Enterprise users are created and managed centrally in the directory server to allow access to multiple databases.
  - ▶ An enterprise user is assigned an enterprise role to grant them access. An enterprise role is a single role created in the directory server with Oracle Enterprise Security Manager. Through Oracle Enterprise Security Manager, global roles located on multiple databases are assigned to an enterprise role.
  - ▶ Each global role is defined in a specific database where it is assigned privileges, but then it is managed in the directory by using enterprise roles.

---

---

## Questions and Answers ??

**Susan Wolford:**  
**E-mail: [susan.wolford@ey.com](mailto:susan.wolford@ey.com)**  
**Phone: 615-252-2123**

**Ahmad Sabbarini:**  
**E-mail: [ahmad.sabbarini@ey.com](mailto:ahmad.sabbarini@ey.com)**  
**Phone: 615-545-6479**