Oracle Database Security Checklist

An Oracle White Paper
June 2008

ORACLE

Oracle Database Security Checklist

PROTECTING THE DATABASE ENVIRONMENT

Since Oracle9i, Oracle has been working with customers to better understand their desired default configurations and harden the Oracle environment. For several major releases of the database, the Oracle documentation has provided guidance on securely configuring the Oracle Database. New with Oracle Database 11g is the Oracle Database 2 Day + Security Guide, an excellent introductory reference for Oracle Database Security.

Significant changes have been made since Oracle9i to make it easier for customers to securely configure the Oracle Database. Oracle9i provided post installation locking and expiration of most default accounts. Oracle Database 10g provided optional install of demonstration accounts, new secure configuration scanning functionality with Enterprise Manager, and changes to the default database role CONNECT. Oracle Database 11g introduced a standards based password hashing algorithm (SHA-1), optional default audit settings and optional default user profile settings, enabling password expiration to be automatically enforced.

This paper recaps the security checklist that can be found in newer versions of the Oracle Database Security Guide. The recommendations contained in this document are intended to be general in nature. This document provides guidance on configuring the Oracle Database based on security best practices for operational database deployments. Details on specific database-related tasks and actions can be found throughout the Oracle documentation set.

INSTALL ONLY WHAT IS REQUIRED

The Oracle Database software installation has two modes - typical and custom. For production systems, the custom installation mode can be used to install the minimum set of features and options required. If in the future, you wish to install additional features or options, simply re-run the Oracle installer.

During installation you have the option to install a set of sample schemas. For production environments, Oracle recommends you do not install the sample schemas. If you have the sample schemas in your production system, Oracle recommends either locking or removing them.

LOCK AND EXPIRE DEFAULT USER ACCOUNTS

The Oracle database installs with a number of default (preset) user accounts. Each account has a default (preset) database password. After successful installation of the database the database configuration assistant (DBCA) automatically locks and expires most default database user accounts. In addition, the password for accounts such as SYSTEM are changed to the value specified during database installation.

If a database is created manually then no default database user accounts are locked because the Database Configuration Assistant is not being used to create the database. After performing a manual database creation you should lock and expire the database user accounts listed in the appendixes of this document that correspond to your version of Oracle. Some Oracle products and features require default accounts to remain unlocked. Descriptions of default accounts can be found in the Oracle Database 2 Day - Security Guide. The guide lists all Oracle Database 11g default accounts created during installation along with a brief description of the account. In addition, you can find a list of all default accounts and their status at the end of this document

The following SQL can be used to lock and expire database accounts.

sqlplus> connect mydba

sqlplus> alter user jsmith account lock and expire

CHANGING DEFAULT USER PASSWORDS

Choosing secure passwords and implementing good password policies are by far the most important defense for protecting against password based security threats. Oracle recommends customers use passwords at least 10 values in length. In addition, the complexity of the password is critical. Passwords that are based on dictionary words are vulnerable to "Dictionary based attacks". A complex password should contain:

- At least 10 values in length
- A mixture of letters and numbers
- Contain mixed case (Supported in Oracle Database 11g)
- Include symbols (Supported in Oracle Database 11g)
- Little or no relation to an actual word

Please note that Pre-Oracle Database 11g allows "_", "$" and "#" symbols.

Although there is no substitute for a strong, complex password, the following techniques can be used to generate longer passwords from a shorter, easier to remember password.

- Create passwords from the 1st letters of the words of an easy-to-remember sentence

- Combine 2 weaker passwords like "welcome1" and "tiger" into "WeltigerCome1"
- Repeat a character at the beginning or end of the password
- Add or append a string of some sort
- Append part of the same password
- Double some or all of the letters: "Welcome13" becomes "wweelcome1313"

Note that Oracle database passwords may not begin with a symbol or number and may not exceed 30 characters in length. Using a technique from the above list increases the work that an attacker must do before they can crack a password.

CHANGE PASSWORDS FOR ADMINISTRATIVE ACCOUNTS

While you can use the same password for administrative accounts such as SYSTEM, SYSMAN and DBSNMP, Oracle recommends using different passwords for each. In any Oracle environment, be it production or test, assign strong and distinct passwords to these administrative accounts.

CHANGE DEFAULT PASSWORDS FOR ALL USERS

The default account SCOTT no longer installs with the default password TIGER. The account is now locked and expired upon install. All other accounts installed with a default password that is the same as the user account. If any of these accounts is unlocked, assign a new stronger password. Starting with Oracle Database 11g security administrators can easily check for default passwords by using the new database view DBA_USERS_WITH_DEF_PWD.

ENFORCE PASSWORD MANAGEMENT

Oracle recommends customers enforce failed login, password expiration, password complexity and reuse policies using Oracle profiles and follow best practices defined by Oracle Applications. Oracle Database 11g provides an optional installation choice that will pre-configure a default profile to enforce password expiration and reuse. Oracle recommends that basic password management rules be applied to all user passwords and that all users be required to change their passwords periodically.

SECURE BATCH JOBS

The *Secure External Password Store* feature introduced with Oracle Database 10g Release 2 is designed to help secure batch jobs that authenticate to the database using username / password credentials. The secure external password store uses an Oracle Wallet to hold one or more user name/password combinations to run batch processes and other tasks that run without user interaction. The secure external password store simplifies large-scale deployments that rely on password credentials for connecting to databases. The best way to envision the password store is as a table with three columns: - `TNSALIAS`, `USERNAME`, and `PASSWORD`. The `TNSALIAS`

is basically the primary key that maps to a single user name/password combination. Once setup, a batch job can simply specify a TNSALIAS and connect to the database. It is very important that the permissions on the Wallet containing the username and password be set accordingly as anyone with access to the Wallet could us it to authenticate to the database. Usage of the Wallet for the authentication credentials removes the requirement to hard code username and password combinations in shell scripts and other batch type jobs.

MANAGE ACCESS TO SYSDBA AND SYSOPER ROLES

Special attention should be given to managing access to the SYSDBA and SYSOPER roles. As with any database role, careful consideration should be given when granting these roles. Oracle recommends customers refrain from connecting with the SYSDBA role except when absolutely required such as called for by an existing Oracle feature or patching. Moving forward Oracle will be eliminating all dependencies on direct connections using SYSDBA. Large and small organizations should create separate administrative accounts.

Note that connections specifying the SYSDBA or SYSOPER roles require a password when connecting remotely and when an Oracle password file has been created. Oracle recommends monitoring the Oracle audit log for unsuccessful SYSDBA and SYSOPER connections.

ENABLE ORACLE DATA DICTIONARY PROTECTION

Oracle recommends that customers implement data dictionary protection to prevent users who have the "ANY" system privileges from using such privileges to modify or harm the Oracle data dictionary.

To enable data dictionary protection, set the O7_DICTIONARY_ACCESSIBILITY parameter to FALSE. This can be accomplished by using Oracle Enterprise Manager Database Control.

Some applications and tools may require access to the data dictionary. In those cases, the individual user can be granted the SELECT ANY DICTIONARY system privilege individually. Note that the SELECT ANY DICTIONARY privilege is not included in the GRANT ALL PRIVILEGES statement.

Note that in Oracle8i the O7_DICTIONARY_ACCESSIBILITY parameter was set to TRUE. Since Oracle9i the default setting for this parameter has been FALSE.

FOLLOW THE PRINCIPLE OF LEAST PRIVILEGE

Oracle recommends you avoid granting powerful privileges to new database users, even privileged users. The Oracle DBA role should be granted with caution and only to those privileged user who need full DBA privileges. Special attention should be given when assigning privileges to application schemas. Access to the SYSDBA role should be granted with extreme care and only to those who are in

the most trusted position. Auditing should be used to monitor all activities of users connecting with the SYSDBA role or other administrative roles such as the DBA role, CREATE ANY TABLE privilege and so forth. For optimal auditing performance set your audit destination to point to the operating system.

PUBLIC PRIVILEGES

The topic of PUBLIC privileges is part of Oracle's overall secure-by-default initiative that started with Oracle Database 9i. New in the Oracle Database 11g release are granular authorizations for numerous PL/SQL network utility packages granted to PUBLIC. If you have upgraded from a previous release of Oracle Database, and your applications depend on PL/SQL network utility packages such as UTL_TCP, UTL_SMTP, UTL_MAIL, UTL_HTTP AND UTL_INADDR the following error may occur when you try to run the application:

ORA-24247: network access denied by access control list (ACL)

Additional information on the enhancements can be found in the Oracle Database PL/SQL Types and References manual and the Managing Fine-grained Access to External Network Services in the Oracle Database Security Guide. The Oracle Database 11g enhancements to the packages increases their security and removes the need to consider revoking access to them from the PUBLIC user group.

Directories accessible to the UTL _FILE package should be created using the CREATE DIRECTORY command. Early releases of the UTL_FILE package relied on the initialization parameter UTL_FILE_DIR to specify the accessible directories. Usage of the CREATE DIRECTORY command enables finer granularity and stronger security. For example the following commands create two directories and authorize DBA group and the user APPUSER to access to access each.

```
SQL> CREATE DIRECTORY log_dir AS '/appl/gl/log';

SQL> GRANT READ ON DIRECTORY log_dir TO DBA;

SQL> GRANT WRITE ON DIRECTORY log_dir TO DBA;

SQL> CREATE DIRECTORY out_dir AS '/appl/gl/appuser'';

SQL> GRANT READ ON DIRECTORY user_dir TO appuser;

SQL> GRANT WRITE ON DIRECTORY user_dir TO appuser;
```

Depending on the application model, it may be possible to remove grants from the PUBLIC user group by first making grants directly to the application schema or end user (depending on the application model) and then revoking the privilege from the PUBLIC user group. For example, assume an application uses the database schema APPCT. During install EXECUTE on the APPCT. ADDACCT

function is granted to the PUBLIC user group. If the EXECUTE privilege on ADDACCT was granted to the PUBLIC user group to allow another application APPHR to access the APPCT.ADDACCT function, then EXECUTE on the function could be granted directly to the APPHR schema and then revoked from the PUBLIC user group.

RESTRICT PERMISSIONS ON RUN-TIME FACILITIES

When granting permissions on run-time facilities such as the Oracle Java Virtual Machine (OJVM), grant permissions to the explicit or actual document root file path. This code can be changed to use the explicit file path.

```
dbms_java.grant_permission
('SCOTT','SYS:java.io.FilePermission','<<ALL FILES>>','read');

dbms_java.grant_permission
('SCOTT','SYS:java.io.FilePermission','<<actual directory
path>>','read');
```

AUTHENTICATE CLIENTS

Oracle recommends verifying that the database initialization parameter REMOTE_OS_AUTHENT is set to FALSE. Setting the value to FALSE creates a more secure configuration by enforcing server-based authentication of clients connecting to an Oracle database. The default setting for this parameter is FALSE and it should not be changed.

RESTRICT OPERATING SYSTEM ACCESS

Limit the number of users with operating system access on the Oracle Database host. Oracle recommends restricting the ability to modify the default file and directory permissions for the Oracle Database home (installation) directory or its contents. Even privileged operating system users and the Oracle owner should not modify these permissions, unless instructed otherwise by Oracle.

Restrict usage of symbolic links on the operating system. When providing a path or file to the Oracle database, neither the file nor any part of the path should be modifiable by an un-trusted user. The file and all components of the path should be owned by the DBA or another trusted operating system account.

SECURE THE ORACLE LISTENER

The Oracle Listener should be properly configured for optimal security. Oracle Database 10g Release 1 and higher uses local OS authentication as the default authentication mode. This mode requires the Oracle Net administrator to be a member of the local DBA group. Setting a password for the TNS listener in Oracle Database 10g Release 1 and higher simplifies local administration. However, setting a password requires good password management to prevent unauthorized users from guessing the password and potentially gaining access to

privileged listener operations. Customers may wish to consider not setting a password for the TNS listener starting with Oracle Database 10g Release 1. Passwords should be used for databases prior to Oracle Database 10g Release 1 or for remote administration of listeners on Oracle Database 10g Release 1 and higher databases.

You should also consider using a firewall. Proper use of a firewall will reduce exposure to security related information including port openings and other configuration information located behind the firewall. Oracle Net supports a variety of firewalls.

SECURE EXTERNAL PROCEDURES

The default configuration for external procedures no longer requires a network listener to work with Oracle Database and EXTPROC agent. The EXTPROC agent is spawned directly by Oracle Database and eliminates the risks that extproc might be spawned by Oracle Listener, unexpectedly. This default configuration is recommended for maximum security.

You can change the default configuration for external procedures and have your EXTPROC agent spawned by Oracle Listener. To do this, however, you must perform additional network configuration steps.

Having your EXTPROC agent spawned by Oracle Listener is necessary if you use:

- Multi-threaded Agent
- Oracle Database in MTS mode on Windows
- AGENT clause of the LIBRARY specification or AGENT IN clause of the PROCECDURE specification such that you can redirect external procedures to a different EXTPROC agent.

Please refer to the Oracle Net Services Guide for instructions on properly configuring Oracle Net Services for external procedures.

PREVENT RUNTIME CHANGES TO LISTENER

When the ADMIN_RESTRICTIONS_LISTENER is set to ON (Default) runtime changes to the listener parameters is disabled. To make changes, the LISTENER.ORA file must be modified and manually reloaded.

CHECKING NETWORK IP ADDRESSES

Use the Oracle Net valid note checking security feature to allow or deny access to Oracle server processes from network clients with specified IP address. To use this feature, set the following protocol.ora (Oracle Net configuration file) parameters:

```
tcp.validnote_checking = YES

tcp.excluded_nodes = {list of IP addresses}
```

```
tcp.invited_nodes = {list of IP addresses}
```

The first parameter turns on the feature whereas the latter parameters respectively deny or allow specific client IP address from making connections to the Oracle listener.

HARDEN THE OPERATING SYSTEM

Both UNIX and Windows platforms provide a variety of operating system services, most of which are not necessary for most deployments. Such services include FTP, TFTP, TELNET and so forth. Be sure to close both the UDP and TCP ports for each service that is being disabled. Disabling one type of port and not the other does not make the operating system more secure.

ENCRYPT NETWORK TRAFFIC

Consider encrypting network traffic between clients, databases and application servers. Oracle supports both SSL using X.509v3 certificates as well as native network encryption without certificates.

APPLY ALL SECURITY PATCHES

Always apply relevant security patches for both the operating system and Oracle. Periodically check the Oracle Technology Network (OTN) security site for details on security alerts released by Oracle. Also check Oracle Worldwide Supports services site, Metalink, for detailed on available and upcoming security related patches and application specific secure configuration information.

REPORT SECURITY ISSUES TO ORACLE

If you believe that you have found a security vulnerability in the Oracle Database, submit an service request to Oracle Worldwide Support Services using Metalink, or email a complete description of the problem including product version and platform, together with any scripts and examples to the following address:

`secalert_us@oracle.com`

APPENDIX A - ORACLE DATABASE 11G RELEASE 1 ENTERPRISE EDITION DEFAULT ACCOUNTS AND THEIR STATUS

Username	Account Status
ANONYMOUS	EXPIRED & LOCKED
APEX_PUBLIC_USER	EXPIRED & LOCKED
CTXSYS	EXPIRED & LOCKED
DBSNMP	EXPIRED & LOCKED
DIP	OPEN
DMSYS	EXPIRED & LOCKED
EXFSYS	EXPIRED & LOCKED
FLOWS_3000	EXPIRED & LOCKED
FLOWS_FILES	EXPIRED & LOCKED
HR	EXPIRED & LOCKED
LBACSYS	EXPIRED & LOCKED
MDDATA	EXPIRED & LOCKED
MDSYS	EXPIRED & LOCKED
MGMT_VIEW	OPEN
ODM	EXPIRED & LOCKED
ODM_MTR	EXPIRED & LOCKED
OE	EXPIRED & LOCKED
OLAPSYS	EXPIRED & LOCKED
ORACLE_OCM	EXPIRED & LOCKED
ORDPLUGINS	EXPIRED & LOCKED
ORDSYS	EXPIRED & LOCKED
OUTLN	EXPIRED & LOCKED
OWBSYS	EXPIRED & LOCKED
PM	EXPIRED & LOCKED
PUBLIC	EXPIRED & LOCKED
QS	EXPIRED & LOCKED

Username	Account Status
QS_ADM	EXPIRED & LOCKED
QS_CB	EXPIRED & LOCKED
QS_CBADM	EXPIRED & LOCKED
QS_CS	EXPIRED & LOCKED
QS_ES	EXPIRED & LOCKED
QS_OS	EXPIRED & LOCKED
QS_WS	EXPIRED & LOCKED
RMAN	EXPIRED & LOCKED
SCOTT	EXPIRED & LOCKED
SH	EXPIRED & LOCKED
SI_INFORMTN_SCHEMA	EXPIRED & LOCKED
SPATIAL_CSW_ADMIN_USR	EXPIRED & LOCKED
SPATIAL_WFS_ADMIN_USR	EXPIRED & LOCKED
SYS	OPEN
SYSMAN	OPEN
SYSTEM	OPEN
TSMSYS	EXPIRED & LOCKED
WK_TEST	EXPIRED & LOCKED
WKPROXY	EXPIRED & LOCKED
WKSYS	EXPIRED & LOCKED
WMSYS	EXPIRED & LOCKED
XDB	EXPIRED & LOCKED

APPENDIX B - ORACLE DATABASE 10G RELEASE 1 AND RELEASE 2 ENTERPRISE EDITION DEFAULT ACCOUNTS AND THEIR STATUS

Username	Account Status
ANONYMOUS	EXPIRED & LOCKED
CTXSYS	EXPIRED & LOCKED

Username	Account Status
DBSNMP	EXPIRED & LOCKED
DIP	EXPIRED & LOCKED
DMSYS	EXPIRED & LOCKED
EXFSYS	EXPIRED & LOCKED
HR	EXPIRED & LOCKED
LBACSYS	EXPIRED & LOCKED
MDDATA	EXPIRED & LOCKED
MDSYS	EXPIRED & LOCKED
MGMT_VIEW	EXPIRED & LOCKED
ODM	EXPIRED & LOCKED
ODM_MTR	EXPIRED & LOCKED
OE	EXPIRED & LOCKED
OLAPSYS	EXPIRED & LOCKED
ORDPLUGINS	EXPIRED & LOCKED
ORDSYS	EXPIRED & LOCKED
OUTLN	EXPIRED & LOCKED
PM	EXPIRED & LOCKED
QS	EXPIRED & LOCKED
QS_ADM	EXPIRED & LOCKED
QS_CB	EXPIRED & LOCKED
QS_CBADM	EXPIRED & LOCKED
QS_CS	EXPIRED & LOCKED
QS_ES	EXPIRED & LOCKED
QS_OS	EXPIRED & LOCKED
QS_WS	EXPIRED & LOCKED
RMAN	EXPIRED & LOCKED
SCOTT	EXPIRED & LOCKED
SH	EXPIRED & LOCKED
SI_INFORMTN_SCHEMA	EXPIRED & LOCKED

Username	Account Status
SYS	OPEN
SYSMAN	EXPIRED & LOCKED
SYSTEM	OPEN
TSMSYS New in 10g Release 2	EXPIRED & LOCKED
WK_TEST	EXPIRED & LOCKED
WKPROXY	EXPIRED & LOCKED
WKSYS	EXPIRED & LOCKED
WMSYS	EXPIRED & LOCKED
XDB	EXPIRED & LOCKED

APPENDIX C - ORACLE DATABASE 9I RELEASE 2 ENTERPRISE EDITION DEFAULT ACCOUNTS AND THEIR STATUS

Username	Account Status
ADAMS	EXPIRED & LOCKED
CTXSYS	EXPIRED & LOCKED
DBSNMP	OPEN
HR	EXPIRED & LOCKED
LBACSYS	EXPIRED & LOCKED
MDSYS	EXPIRED & LOCKED
ODM	EXPIRED & LOCKED
ODM_MTR	EXPIRED & LOCKED
ORDPLUGINS	EXPIRED & LOCKED
ORDSYS	EXPIRED & LOCKED
OUTLN	EXPIRED & LOCKED
PM	EXPIRED & LOCKED
QS	EXPIRED & LOCKED
QS_ADM	EXPIRED & LOCKED
QS_CB	EXPIRED & LOCKED

Username	Account Status
QS_CBADM	EXPIRED & LOCKED
QS_CS	EXPIRED & LOCKED
QS_ES	EXPIRED & LOCKED
QS_OS	EXPIRED & LOCKED
QS_WS	EXPIRED & LOCKED
SCOTT	OPEN
SH	EXPIRED & LOCKED
SYS	OPEN
SYSTEM	OPEN
WKPROXY	EXPIRED & LOCKED
WKSYS	EXPIRED & LOCKED
WMSYS	EXPIRED & LOCKED
XDB	EXPIRED & LOCKED

Oracle Database Security Checklist
June 2008

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com