Evaluated Configuration for Oracle 7™ Database Server
Release 7.2.2.4.13

May 1998

ORACLE CORPORATION
ATTN: Security Evaluations
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Evaluated Configuration for Oracle7™ Database Server
Release 7.2.2.4.13

May 1998

Author: Rajiv Sinha

Contributors: Rae Burns, Jeff DeMello, Duncan Harris, Stephen Pannifer, Howard Smith

Contents

CHAPTER

1 Introduction

1.1 Scope

The Target of Evaluation (TOE) is the Oracle7 Release 7.2.2.4.13 Relational Database Management System (RDBMS).

The TOE is hosted on the Microsoft Windows NT Version 3.51 with Service Pack 4 operating system.

This *Evaluated Configuration for Oracle7 Relational Database Management System* document explains the manner in which the TOE must be configured along with the host operating system and network services so as to provide the security functionality and assurance as required under the Common Criteria for Information Technology Security Evaluation [CC].

The Evaluation Assurance Level for the TOE is EAL4. The Protection Profile used for the evaluation of the TOE is the [C.DBMS PP].

1.2 Intended Audience

The intended audience for this document includes evaluators of the TOE, system integrators who will be working with the TOE, and accreditors of the systems into which the TOE is being integrated.

1.3 Organization

This document is composed of five (5) sections.

Section 1 contains the introduction to the document.

Section 2 describes the physical environment of the TOE and the network services required to support the TOE.

Section 3 describes the host operating system, network services, and client application configurations required to support the TOE.

Section 4 describes the configuration of the TOE, and all TOE-related network services and applications.

Section 5 lists the references that are used in this document.

CHAPTER

2 Physical Configuration

2.1 Assumptions

[A-1] The processing resources of the TOE shall be located within controlled access facilities which will prevent unauthorized physical access.

[A-2] The processing resources of the underlying operating system required to support the TOE shall be located within controlled access facilities which will prevent unauthorized physical access.

[A-3] The processing resources of the network services required to support the TOE shall be located within controlled access facilities which will prevent unauthorized physical access.

[A-4] The media on which authentication data for the underlying operating system data resides shall not be physically removable from the underlying operating system by unauthorized users.

[A-5] The media on which the TOE audit data resides shall not be physically removable from the underlying operating system by unauthorized users.

[A-6] Any on-line and/or off-line storage media on which security relevant data resides shall be located within controlled access facilities which will prevent unauthorized physical access.

CHAPTER

3 Host Configuration

The TOE was evaluated and tested on two (2) Compaq Proliant 4500 x86 (Family 5 Model 2 Stepping 5) server machines and one (1) Compaq Deskpro 4200 client machine. All the three machines were connected by a Local Area Network (LAN).

The TOE was evaluated and tested on Compaq NT 3.51 Server (build 1057) operating systems running on both server machines, and on one Compaq NT 3.51 Workstation operating system running on the client machine.

3.1 Operating System

[OS-1] The underlying operating system shall be the Microsoft Windows NT 3.51 Server (with Service Pack 4) operating system.

Guidance - The underlying operating system identified in [OS-1] satisfies the requirements of the [ITSEC] Functionality Class F-C2 or greater, the requirements of the [TCSEC] Class C2 or greater, or the requirements of the [CC] Evaluation Assurance Level EAL3 or greater.

[OS-2] The underlying operating system identified in [OS-1] shall be installed and operated in a manner as described in the [ITSEC] or [CC] Certification Report or in the [TCSEC] Final Evaluation Report, and in accordance with its evaluated configuration and operational documentation.

[OS-3] The Windows NT File System (NTFS) shall be used on all host machines supporting the TOE.

3.1.1 Identification and Authentication

[OS.IA-1] The operating system shall provide and implement authentication for database users attempting to connect to an RDBMS.

[OS.IA-2] The operating system shall protect its authentication mechanism against modification.

[OS.IA-3] The operating system shall support the creation and maintenance of uniquely identified operating system users accounts.

[OS.IA-4] The operating system shall prevent unauthorized modification of operating system us-

ers accounts.

Guidance - This should be accomplished by ensuring that only the operating system administrator belong to the ADMINISTRATORS operating system group. The operating system administrator may also belong to the DOMAIN ADMINS group to create and administer user accounts on other machines within a domain.

[OS.IA-5] No other user (existing or newly created) shall belong to either the ADMINISTRATORS or DOMAIN ADMINS groups on either the host machine on which the TOE is installed, or on their local (client) machines from which they will connect to the TOE.

[OS.IA-6] All normal users should belong to the USERS operating system group on their local and (if applicable) remote host machines.

[OS.IA-7] There shall be a single domain of user identification for the TOE and the operating system.

[OS.IA-8] In a networked environment, this single domain of identification should be configured in the operating system and the TOE for each node on the underlying network.

[OS.IA-9] The operating system shall allow only users in the ADMINISTRATORS group to access the operating system registry. No other user should be permitted to access the operating system registry.

[OS.IA-10] The operating system administrator shall ensure that the DBA_AUTHORIZATION parameter for the RDBMS is not present in the NT registry.

[OS.IA-11] The operating system administrator shall ensure that the DBA password in the operating system registry is set to null.

3.1.2 Protection of Resources

[OS.PR-1] The operating system shall protect all of the installed TOE-related files and directories by means of its Discretionary Access Control mechanisms to ensure that they are accessible to authorized users only.

Guidance - The TOE directories and files include the ORACLE_HOME directory, the parameter and control files' directory, and the directory containing the TOE executables (which is normally ORACLE_HOME\BIN). The permissions set on these directories should be set to FULL CONTROL for users in the local RDBMS administrator operating system group and READ ACCESS for all other users.

[OS.PR-2] The operating system shall protect system clocks against unauthorized modification so as to maintain the integrity of audit timestamps.

Guidance - This is accomplished by permitting only operating system administrators to access the operating system clock configuration. Access permissions for all other users should be set to NO ACCESS for the operating system clock.

3.1.3 Accounting and Auditing

[OS.AA-1] The operating system shall protect operating system audit trails or any other audit trails used by the RDBMS against unauthorized modification and deletion by means of its Discretionary Access Control mechanisms.

Guidance - The directory containing audit trail files should be set to FULL CONTROL permissions for users in the local RDBMS administrator operating group, and NO ACCESS for all other users.

[OS.AA-2] The operating system shall include procedures that support the archiving of operating

system audit trails prior to audit trail exhaustion.

Guidance - The operating system should support the audit of RDBMS generated audit records of all RDBMS privileged connections, and RDBMS startup and shutdown operations in the its audit trail irrespective of whether or not auditing is turned on in the RDBMS.

3.2 Network Services

[OS.NS-1] The underlying network services shall satisfy the requirements of the [ITSEC] Functionality Class F-C2 or greater, the requirements of the [TCSEC] Class C2 or greater, or the requirements of the [CC] Evaluation Assurance Level EAL3 or greater.

[OS.NS-2] The underlying network services shall be installed, and operated in a manner as described in the [ITSEC] or [CC] Certification Report, or the [TCSEC] Final Evaluation Report, and in accordance with their evaluated configuration and operational documentation.

[OS.NS-3] In a distributed environment, the underlying network services shall be based on the available Windows NT secure communication protocols which ensure the authenticity of the operating system users.

[OS.NS-4] Only users in the `ADMINISTRATORS` group shall be able to modify the network services configuration parameters.

Guidance - No other user should be permitted to modify any network services configuration parameter. This should be accomplished by including all other users in the `USERS` operating system group.

3.3 Client Applications

[OS.CA-1] No applications shall be permitted to run on any client or server machines which access the network, unless they have been shown not to compromise the TOE's security objectives stated in the [C.DBMS PP].

CHAPTER

4

Oracle Configuration

The TOE consists of software only. The TOE contains no hardware or firmware components and there are no hardware or firmware dependencies which affect the evaluation.

[DB-1] The TOE shall be installed, configured, and maintained in accordance with this document and with the instructions provided in the [IUG].

[DB-2] The TOE shall be installed using the Oracle Installer Release 3.1.2.1.3 and within it, the Custom Product Install option.

[DB-3] The following software components shall be selected from the list of available products presented on the product installation screen:

- Oracle Named Pipes Adapter 2.2.2.1.0
- Oracle SPX Adapter 2.2.2.1.0
- Oracle TCP/IP Adapter 2.2.2.1.0
- Oracle Distributed Option 7.2.2.4.0
- Oracle7 Server 7.2.2.4.13
- Oracle7 Utilities 7.2.2.4.6
- Required Support Files 7.2.2.4.12D
- SQL*Net Client 2.2.2.1.0
- SQL*Net Server 2.2.2.1.0
- SQL*Plus 3.2.2.0.1

In addition to these components, the following software components are automatically installed by the Oracle Installer:

- SQL*DBA Release 7.2.2.4.0
- OCILIB Release 7.2.2.4.0

4.1 Evaluated Configuration Boundaries

[DB-4] SQL*DBA Release 7.2.2.4.0 shall only be run in *Line Mode*.

Guidance - SQL*DBA Release 7.2.2.4.0 when run in *Line Mode* is part of the evaluated configuration.

OCILIB Release 7.2.2.4.0 is not part of the evaluated configuration.

SQL*Plus Release 3.2.2.0.1 is used by the evaluators for testing the TOE components. However, it is not part of the evaluated configuration.

Oracle7 Release 7.2.2.4.13 is a patch which is installed over Oracle 7.2.2.4.0. The patch replaces the Oracle7 Server, Oracle7 Utilities, and Required Support Files executables of the product. The other executables are unchanged.

The evaluated configuration of the TOE therefore comprises exactly the following software components:

- Oracle Named Pipes Adapter 2.2.2.1.0
- Oracle SPX Adapter 2.2.2.1.0
- Oracle TCP/IP Adapter 2.2.2.1.0
- Oracle Distributed Option 7.2.2.4.0
- Oracle7 Server 7.2.2.4.13
- Oracle7 Utilities 7.2.2.4.6
- Required Support Files 7.2.2.4.12D
- SQL*Net Client 2.2.2.1.0
- SQL*Net Server 2.2.2.1.0
- SQL*DBA 7.2.2.4.0 (line mode only)

4.2 RDBMS Server

4.2.1 Identification and Authentication

In the evaluated configuration, the TOE supports Identification.

[DB.IA-1] The TOE shall be configured to use RDBMS identification and operating system authentication.

[DB.IA-2] Administrators that create users within the RDBMS shall follow the SQL syntax for creating users identified externally.

Guidance - This includes any predefined accounts such as `SYS` and `SYSTEM`, and any demonstration account such as `SCOTT`, created during RDBMS installation.

[DB.IA-3] The RDBMS parameter file `INIT<SID>.ORA` is located in the `ORACLE_HOME\DATABASE` directory. The following parameters shall be set in each of the RDBMS parameter files being used for each of the RDBMS instances:

- `sql92_security = TRUE`
- `remote_os_authent = TRUE`

[DB.IA-4] User identification for all users in each of the RDBMS instances shall be set in the

INIT<*SID*>.ORA parameter file to support a single domain of identification as follows:

- os_authent_prefix = ""

[DB.IA-5] The TOE shall support both privileged and non-privileged database users. To connect to the RDBMS as a privileged database user such as a database administrator, the following parameter shall be set in the appropriate INIT<*SID*>.ORA file:

- remote_login_passwordfile = NONE

Also delete the password file ORAPWD.PWF which is located in ORACLE_HOME\DATABASE.

[DB.IA-6] Database administrators who are required to use the CONNECT / AS SYSOPER syntax to connect to an RDBMS shall belong to one or more of the following operating system local groups.

- ORA_OPER
- ORA_<*SID*>_OPER

[DB.IA-7] Database administrators who are required to use the CONNECT / AS SYSDBA syntax to connect to an RDBMS shall belong to one or more of the following operating system local groups:

- ORA_DBA
- ORA_<*SID*>_DBA

[DB.IA-8] Database administrators who are required to use the CONNECT INTERNAL syntax to connect to an RDBMS shall belong to one or more of the following operating system local groups:

- ORA_DBA
- ORA_<*SID*>_DBA

Guidance - An RDBMS privileged user who belongs to an operating system local group (on that host machine itself) having a particular RDBMS <*SID*> as defined above, can connect as a privileged user only to that database. When the <*SID*> is not specified for a particular operating system local group, then a user belonging to such a local group can connect as a privileged user to all instances of the RDBMS.

4.2.2 Accounting and Auditing

The TOE supports and implements Accounting and Auditing.

[DB.AA-1] The TOE can record all auditing or accounting information for all database users and operations except for a few privileged operations by database administrators.

Guidance - Privileged operations such as RDBMS startup and shutdown, and privileged connections such as INTERNAL, AS SYSDBA, and AS SYSOPER are always audited and recorded directly in the operating system audit trail.

[DB.AA-2] In the evaluated configuration for a specific RDBMS, the audit_trail parameter in the appropriate INIT<*SID*>.ORA parameter file for that RDBMS shall be assigned in one of the following two ways:

- audit_trail = OS
- audit_trail = DB

Guidance - The `audit_trail` parameter should be set to `OS` to ensure that the TOE audit records are recorded only in the operating system audit trail, or the `audit_trail` parameter should be set to `DB` to ensure that the TOE audit records are written to the database audit trail.

Guidance - The database audit trail is a `SYS`-owned table, `SYS.AUD$`. Only users connected as `SYS`, `INTERNAL`, and `AS SYSDBA` can directly read and write all rows in `SYS.AUD$`.

[DB.AA-3] Database administrators shall create database audit trail views for all other appropriately privileged RDBMS users to be able to read and analyse database audit trail data.

Guidance - Some database audit trail views are automatically created during the installation and creation of the database.

[DB.AA-4] Database administrators shall perform regular archiving of database and operating system audit trails before audit trail exhaustion to ensure sufficient free space for continued auditing operations.

Guidance - Therefore, access permissions on directories and files containing audit trail information should be set to `FULL CONTROL` for database administrators.

4.2.3 Availability and Reliability

In the evaluated configuration, the TOE supports and implements Availability and Reliability.

[AR.DB-1] Only privileged RDBMS users such as database administrators shall be permitted to perform privileged RDBMS operations such as backup and recovery, and enforce tablespace quotas and resource profiles.

Guidance - This should be accomplished by ensuring that only privileged RDBMS users have the necessary administrative system privileges to perform these types of operations.

[DB.AR-2] Administrative system privileges shall not be granted to normal RDBMS users directly or through the use of database roles. See section 4.1.5.

Guidance - For example, a normal RDBMS user should not be granted the `ALTER PROFILE` system privilege either directly or through a database role, as it would enable that user to modify his resource limits.

4.2.4 Access Controls

In the evaluated configuration, the TOE supports and implements Access Controls. The RDBMS implements Discretionary Access Controls to implement access controls.

[DB.AC-1] Normal RDBMS users shall have access to only those database objects which they own (ownership of an object being defined as storage of that object within a user's schema).

[DB.AC-2] Normal RDBMS users shall only have access to database objects they do not own if they possess appropriate privileges to access database objects in other RDBMS user schemas.

[DB.AC-3] Privileged users such as database administrators, or with `CONNECT INTERNAL` and `AS SYSDBA` privileges shall have access to all database objects in any user schema.

4.2.5 Security Administration and Management

In the evaluated configuration, the TOE supports and implements Security Administration and Management by the use of over eighty distinct and separately managed object and system privileges.

System privileges which are administrative in nature such as those which allow database-wide object, role, user, privilege, and profile manipulation should generally not be granted to normal RDBMS users either directly or through database roles.

Guidance - System privileges are very powerful and can be used to manipulate the RDBMS in a variety of ways. Only highly trusted RDBMS users and RDBMS administrators should be allowed to posses system privileges which are administrative in nature. An example of such a privilege is the `ALTER PROFILE` system privilege which can be used to alter any user profile in the RDBMS.

Guidance - Object privileges and other system privileges (which are non-administrative in nature) are required by normal RDBMS users to perform their tasks under the *Principle of Least Privilege.* These privileges are generally grouped together into database roles and granted to normal RDBMS users. An example of these types of privileges is the `CREATE TABLE` privilege which by default allows RDBMS users to create and modify tables within their own schema, but not in any other user schema.

4.2.6 Secure Data Exchange

In the evaluated configuration, the TOE supports and implements Secure Data Exchange.

[DB.SDE-1] Database administrators shall ensure that any system privilege (directly or through the use of roles) required to implement database import and export be only granted to RDBMS users who are trusted to perform these operations, and who normally do not have the appropriate privileges for read and write access to such data.

4.2.7 Secure Distributed Processing and Databases

In the evaluated configuration, the TOE supports and implements Secure Distributed Processing and Distributed Databases.

Guidance - The TOE can be operated in standalone, client/server and server/server configurations. Database links may be used to connect between different RDBMS servers over a network. The TOE provides site autonomy which implies that each server participating in a distributed environment is administered independently from other servers in the distributed system.

[DB.SDD-1] Database administrators shall therefore implement site security policy as described above.

4.3 Oracle Network Services

[DB.NS-1] The network services that shall be installed using the Oracle Installer Release 3.1.2.1.3 and by using the Selective Product Install option are:

- SQL*Net Client 2.2.2.1.0
- SQL*Net Server 2.2.2.1.0

[DB.NS-2] The installed network services shall be configured in the manner described in the [NP-IUG].

[DB.NS-3] Only users in the operating system ADMINISTRATORS group or the RDBMS administrator shall be able to modify the installed network services configuration parameters.

Guidance - No other user should be permitted to modify any network services configuration parameter in the Oracle network configuration files such as TNSNAMES.ORA, LISTENER.ORA and SQLNET.ORA. These files are generally located in ORACLE_HOME\NETWORK\ADMIN. Permissions on these directories should be set to FULL CONTROL for users in the operating system ADMINISTRATORS group, and READ ACCESS to all other users included in the USERS operating system group.

[DB.NS-4] The network configuration files mentioned in [DB.NS-3] shall use a consistent RDBMS naming convention.

4.4 Oracle Client Applications

[DB.CA-1] The only client application that shall be installed using the Oracle Installer Release 3.1.2.1.3 and by using the Selective Product Install option is:

- SQL*Plus 3.2.2.0.1

[DB.CA-2] No applications except SQL*Plus Release 3.2.2.0.1 shall be permitted to run on any client or server host machines which access the network, unless they have been shown not to compromise the TOE's security objectives as stated in the [C.DBMS PP].

CHAPTER

5 References

[CC] *Common Criteria for Information Technology Security Evaluation*, Version 2.0 Draft CCIB-97/081R

[C.DBMS PP] *Commercial Database Management System Protection Profile*, Version 2.0

[IUG] *Oracle7 Server for Windows NT Installation and User's Guide*, Oracle Corporation

[ITSEC] *Information Technology Security Evaluation Criteria*, Version 1.2, June 1991, UK IT Security Evaluation and Certification Scheme

[TCSEC] *Trusted Computer System Security Evaluation Criteria*, 5200 28-STD, December 1985, US Department of Defense

[NP-IUG] *Oracle Network Products for Windows NT Installation and User's Guide*, A36290, Oracle Corporation