Oracle Database Security Risk Assessment - Highly Confidential

Assessment Date & Time

```
Date of Data Collection  Date of Report           Re
------------------------ ------------------------ --
Wed Feb 01 2017 22:18:00 Wed Feb 01 2017 22:22:18 1.
```

Database Identity

```
Name Platform         Database Role Log Mode   Creat
Database Container ID Container Name
---- ---------------- ------------- ---------- -----
```

Basic Information

Item	ID	Status	Result

Database Version

```
Oracle Database 12c Enterprise Edition Release 12.1.
Security options used: (none)
```

Security Features

```
Feature                                    Currently Usec
------------------------------------------ --------------
AUTHORIZATION CONTROL
Database Vault                                       No
Privilege Analysis                                   No

DATA ENCRYPTION
Column Encryption                                    No
Tablespace Encryption                                No
Network Encryption                                   No

FINE-GRAINED ACCESS CONTROL
Data Redaction                                       No
Virtual Private Database                            Yes
Real Application Security                            No
Label Security                                       No
Transparent Sensitive Data Protection                No

AUDITING
Traditional Audit                                   Yes
Fine Grained Audit                                   No
Unified Audit                                       Yes

USER AUTHENTICATION
External Authentication                              No
Global Authentication                                No
```

Patch Check	INFO.PATCH	Severe Risk	Latest Oracle Database PSU not found.

User Accounts

Item	ID	Status	Result
User Accounts	User Name Status Profile Tablespace Predefined Type --------- ------ ------- ---------- ---------- ----- DBSNMP OPEN DEFAULT SYSAUX Yes PASSW SYS OPEN DEFAULT SYSTEM Yes PASSW SYSTEM OPEN DEFAULT SYSTEM Yes PASSW		
User Accounts in SYSTEM or SYSAUX Tablespace	USER.TBLSPACE	Pass	No user uses SYSTEM or SYSAUX tablespace.
Sample Schemas	USER.SAMPLE	Pass	No sample schemas found.
Inactive Users	USER.INACTIVE	Some Risk	Found 2 unlocked users inactive for more than 30 days.

Case-Sensitive Passwords	USER.CASE	Pass	Case-sensitive passwords are used.
Users with Expired Passwords	USER.EXPIRED	Pass	No unlocked users with password expired for more than 30 days found.
Users with Default Passwords	USER.DEFPWD	Severe Risk	Found 1 unlocked user account with default password.
Minimum Client Authentication Version	USER.AUTHVERS	Some Risk	Minimum client version is not configured correctly.

Password Verifiers	USER.VERIFIER	Pass	All user accounts support the latest password version. No user accounts have HTTP verifiers.

User Profiles	Profile Name	Resource	Value
	DEFAULT	(Number of Users)	3
	DEFAULT	CONNECT_TIME	UNLIMITED
	DEFAULT	FAILED_LOGIN_ATTEMPTS	10
	DEFAULT	IDLE_TIME	UNLIMITED
	DEFAULT	PASSWORD_GRACE_TIME	7
	DEFAULT	PASSWORD_LIFE_TIME	180
	DEFAULT	PASSWORD_LOCK_TIME	1
	DEFAULT	PASSWORD_REUSE_MAX	UNLIMITED
	DEFAULT	PASSWORD_REUSE_TIME	UNLIMITED
	DEFAULT	PASSWORD_VERIFY_FUNCTION	NULL
	ORA_STIG_PROFILE	(Number of Users)	0
	ORA_STIG_PROFILE	CONNECT_TIME	UNLIMITED
	ORA_STIG_PROFILE	FAILED_LOGIN_ATTEMPTS	3
	ORA_STIG_PROFILE	IDLE_TIME	15
	ORA_STIG_PROFILE	PASSWORD_GRACE_TIME	5
	ORA_STIG_PROFILE	PASSWORD_LIFE_TIME	60
	ORA_STIG_PROFILE	PASSWORD_LOCK_TIME	UNLIMITED
	ORA_STIG_PROFILE	PASSWORD_REUSE_MAX	10
	ORA_STIG_PROFILE	PASSWORD_REUSE_TIME	365
	ORA_STIG_PROFILE	PASSWORD_VERIFY_FUNCTION	ORA12C_STF

Users with Unlimited Password Lifetime	USER.NOEXPIRE	Pass	Password expiration is configured for all users.

Users with Unlimited Failed Login Attempts	USER.NOLOCK	Pass	No users have unlimited failed login attempts.
Password Verification Functions	USER.PASSWD	Significant Risk	Found 3 users not using password verification function.

Privileges and Roles

Item	ID	Status	Result
All System Privileges	PRIV.SYSTEM	Evaluate	234 grants of system privileges
All Roles	PRIV.ROLES	Evaluate	30 grants of roles

Account Management Privileges	PRIV.ACCT	Evaluate	16 grants of account management privileges
Privilege Management Privileges	PRIV.MGMT	Evaluate	32 grants of privilege management privileges
Audit Management Privileges	PRIV.AUDIT	Evaluate	10 grants of audit privilege
Data Access Privileges	PRIV.DATA	Evaluate	52 grants of data access privileges
Access Control Exemption Privileges	PRIV.EXEMPT	Evaluate	3 grants of access control exemption privileges
Access to Password Verifier Tables	PRIV.PASSWD	Evaluate	8 grants of object privileges on restricted objects

Access to Restricted Objects	PRIV.OBJ	Evaluate	66 grants of object privileges on restricted objects
User Impersonation	PRIV.USER	Pass	No grants of EXECUTE on restricted packages
Data Exfiltration	PRIV.EXFIL	Pass	No grants of EXECUTE on restricted packages
System Privileges Granted to PUBLIC	PRIV.SYSPUB	Pass	No grants of system privileges to PUBLIC
Roles Granted to PUBLIC	PRIV.ROLEPUB	Pass	No grants of roles to PUBLIC
Column Privileges Granted to PUBLIC	PRIV.COLPUB	Pass	No grants of column privileges to PUBLIC
DBA Role	PRIV.DBA	Evaluate	1 grant of DBA role
Other Powerful Roles	PRIV.BIGROLES	Evaluate	9 grants of powerful roles (1 with admin option)

Java Permissions	PRIV.JAVA	Evaluate	Found 4 users or roles with Java permission.
Users with Administrative Privileges	PRIV.ADMIN	Some Risk	Found 1 user granted administrative privileges. Found 3 administrative privileges not granted to any user.

Authorization Control

Item	ID	Status	Result
Database Vault	AUTH.DV	Opportunity	Database Vault is not enabled.
Privilege Analysis	AUTH.PRIV	Opportunity	No privilege analysis policies found.

Data Encryption

Item	ID	Status	Result

Transparent Data Encryption	CRYPT.TDE	Opportunity	No encrypted tablespaces found. No encrypted columns found.
Encryption Key Wallet	CRYPT.WALLET	Evaluate	Found 1 wallet. No wallets are stored in the data file directory.

Fine-Grained Access Control

Item	ID	Status	Result
Data Redaction	ACCESS.REDACT	Opportunity	No data redaction policies found.

Virtual Private Database	ACCESS.VPD	Evaluate	Found 1 VPD policy protecting 51 objects.
Real Application Security	ACCESS.RAS	Opportunity	No RAS policies found.
Label Security	ACCESS.OLS	Opportunity	Label Security is not enabled.
Transparent Sensitive Data Protection	ACCESS.TSDP	Opportunity	No sensitive types and columns found. Found 0 TSDP policies.

Auditing

Item	ID	Status	Result
Audit Records	AUDIT.RECORDS	Evaluate	Examined 3 audit trails. Found records in 1 audit trail. No errors found in audit initialization parameters.
Statement Audit	AUDIT.STMT	Evaluate	Auditing enabled for 17 statements.
Object Audit	AUDIT.OBJ	Evaluate	Auditing enabled for 223 objects.
Privilege Audit	AUDIT.PRIV	Evaluate	Auditing enabled for 29 privileges.
Administrative User Audit	AUDIT.ADMIN	Pass	Actions of the SYS user are audited.
Privilege Management Audit	AUDIT.PRIVMGMT	Pass	Actions related to privilege management are sufficiently audited.
Account Management Audit	AUDIT.ACCTMGMT	Pass	Actions related to account management are sufficiently audited.

Database Management Audit	AUDIT.DBMGMT	Significant Risk	Actions related to database management are not sufficiently audited.
Privilege Usage Audit	AUDIT.PRIVUSE	Significant Risk	Usages of powerful system privileges are not sufficiently audited.
Database Connection Audit	AUDIT.CONN	Pass	Database connections are sufficiently audited.
Fine Grained Audit	AUDIT.FGA	Opportunity	No fine grained audit policies found.
Unified Audit	AUDIT.UNIFIED	Evaluate	Found 8 unified audit policies. Found 47 objects or statements being audited.

Database Configuration

Item	ID	Status	Result

Initialization Parameters for Security	Name --- AUDIT_FILE_DEST AUDIT_SYSLOG_LEVEL AUDIT_SYS_OPERATIONS AUDIT_TRAIL COMPATIBLE DBFIPS_140 DISPATCHERS GLOBAL_NAMES LDAP_DIRECTORY_ACCESS LDAP_DIRECTORY_SYSAUTH O7_DICTIONARY_ACCESSIBILITY OS_AUTHENT_PREFIX OS_ROLES PDB_LOCKDOWN PDB_OS_CREDENTIAL REMOTE_LISTENER REMOTE_LOGIN_PASSWORDFILE REMOTE_OS_AUTHENT REMOTE_OS_ROLES RESOURCE_LIMIT SEC_CASE_SENSITIVE_LOGON SEC_MAX_FAILED_LOGIN_ATTEMPTS SEC_PROTOCOL_ERROR_FURTHER_ACTION SEC_PROTOCOL_ERROR_TRACE_ACTION SEC_RETURN_SERVER_RELEASE_BANNER SQL92_SECURITY UNIFIED_AUDIT_SGA_QUEUE_SIZE UTL_FILE_DIR	Value --- /u01/app/oracle/ac TRUE DB 12.1.0.2.0 FALSE (PROTOCOL=TCP) (SE FALSE NONE no FALSE ops$ FALSE EXCLUSIVE FALSE FALSE TRUE TRUE 3 (DROP,3) TRACE FALSE FALSE 1048576	
Access to Dictionary Objects	CONF.SYSOBJ	Pass	Access to dictionary objects is properly limited.
Inference of Table Data	CONF.INFER	Significant Risk	UPDATE and DELETE statements can be used to infer data values.

Network Communications	CONF.NETCOM	Pass	Examined 3 initialization parameters. No issues found.
External Authorization	CONF.EXTAUTH	Pass	Examined 2 initialization parameters. No issues found.
File System Access	CONF.FILESYS	Pass	Examined 1 initialization parameter. No issues found.
Triggers	CONF.TRIG	Pass	No logon triggers found. No disabled triggers found.
Disabled Constraints	CONF.CONST	Pass	No disabled constraints found.

External Procedures	CONF.EXTPROC	Evaluate	Found 3 external procedures. No external services found.
Directory Objects	CONF.DIR	Evaluate	Found 10 directory objects. No directory objects allow access to restricted Oracle directory paths. No directory objects allow both write and execute access.
Database Links	CONF.LINKS	Pass	No database links found.
Network Access Control	CONF.NETACL	Evaluate	Found 1 network ACL.

XML Database Access Control	CONF.XMLACL	Evaluate	Found 9 XML Database ACLs.

Network Configuration

Item	ID	Status	Result
Network Encryption	NET.CRYPT	Significant Risk	Native encryption is partially enabled. Integrity check using checksums is partially enabled.
Client Nodes	NET.CLIENTS	Significant Risk	Valid node check is not enabled. Neither TCP.INVITED_NODES nor TCP.EXCLUDED_NODES is set.
SQLNET Banners	NET.BANNER	Some Risk	Connect banners are not fully configured.

Network Listener Configuration	NET.COST	Significant Risk	Examined 1 listener. Found 1 listener not configured properly.
Listener Logging Control	NET.LISTENLOG	Pass	Examined 1 listener. Found 0 listeners not configured properly.

Operating System

Item	ID	Status	Result
OS Authentication	OS.AUTH	Evaluate	1 OS user can connect to the database via OS authentication.
Process Monitor Process	OS.PMON	Pass	Found 1 PMON process. The owner of the PMON process matches the ORACLE_HOME owner.
Agent Processes	OS.AGENT	Some Risk	Some Agent process owners overlap with Listener or PMON process owners.
Listener Processes	OS.LISTEN	Some Risk	Found 1 Listener process. Some Listener process owners overlap with Agent or PMON process owners.

This report is focused on detecting areas of potential security vulnerabilities or misconfigurations and pr
those potential vulnerabilities.

The report provides a view on the current status. These recommendations are provided for informationa
substitute for a thorough analysis or interpreted to contain any legal or regulatory advice or guidance.

You are solely responsible for your system, and the data and information gathered during the productio
for the execution of software to produce this report, and for the effect and results of the execution of ar

Oracle provides this analysis on an "as is" basis without warranty of any kind and Oracle hereby disclaim
express, implied or statutory.

eporter Version

.0.2 (October 2016) - 7409

ted Container

Remarks

.0.2.0 - 64bit Production

d
-

It is vital to keep the database software up-to-date with security fixes as they are released. Oracle issues Patch Set Updates (PSU) on a regular quarterly schedule. These updates should be applied as soon as they are available. For releases prior to Oracle Database 12c, quarterly updates may be delivered by patches not marked as PSUs.

Remarks

WORD
WORD
WORD

The SYSTEM and SYSAUX tablespaces are reserved for Oracle-supplied user accounts. To avoid a possible denial of service caused by exhausting these resources, regular user accounts should not use these tablespaces. Prior to Oracle Database 12.2, the SYSTEM tablespace cannot be encrypted, and this is another reason to avoid user schemas in this tablespace.

Sample schemas are well-known accounts provided by Oracle to serve as simple examples for developers. They generally serve no purpose in a production database and should be removed because they unnecessarily increase the attack surface of the database.

If a user account is no longer in use, it increases the attack surface of the system unnecessarily while providing no corresponding benefit. Furthermore, unauthorized use is less likely to be noticed when no one is regularly using the account. Accounts that have been unused for more than 30 days should be investigated to determine whether they should remain active.

Case-sensitive passwords are recommended because including both upper and lower-case letters greatly increases the set of possible passwords that must be searched by an attacker who is attempting to guess a password by exhaustive search. Setting SEC_CASE_SENSITIVE_LOGON to TRUE ensures that the database distinguishes between upper and lower-case letters in passwords.

Password expiration is used to ensure that users change their passwords on a regular basis. If a user's password has been expired for more than 30 days, it indicates that the user has not logged in for at least that long. Accounts that have been unused for an extended period of time should be investigated to determine whether they should remain active.

Default account passwords for predefined Oracle accounts are well known. Open accounts with default passwords provide a trivial means of entry for attackers, but well-known passwords should be changed for locked accounts as well.

Over time, Oracle releases have added support for increasingly secure versions of the algorithm used for password authentication of user accounts. In order to remain compatible with older client software, the database continues to support previous password versions as well. The sqlnet.ora parameter ALLOWED_LOGON_VERSION_SERVER determines the minimum password version that the database will accept. For maximum security, this parameter should be set to the highest value supported by the database once all client systems have been upgraded.

For each user account, the database may store multiple verifiers, which are hashes of the user password. Each verifier supports a different version of the password authentication algorithm. Every user account should include a verifier for the latest password version supported by the database so that the user can be authenticated using the latest algorithm supported by the client. When all clients have been updated, the security of user accounts can be improved by removing the obsolete verifiers. HTTP password verifiers are used for XML Database authentication. Use the ALTER USER command to remove these verifiers from user accounts that do not require this access.

(DEFAULT)

RONG_VERIFY_FUNCTION

Password expiration is used to ensure that users change their passwords on a regular basis. Passwords that never expire may remain unchanged for an extended period of time. When passwords do not have to be changed regularly, users are also more likely to use the same passwords for multiple accounts.

Attackers sometimes attempt to guess a user's password by simply trying all possibilities from a set of common passwords. To defend against this attack, it is advisable to lock a user account when there are multiple failed login attempts without a successful login.

Password verification functions are used to ensure that user passwords meet minimum requirements for complexity, which may include factors such as length, use of numbers or punctuation characters, difference from previous passwords, etc. Oracle supplies several predefined functions, or a custom PL/SQL function can be used. Every user profile should include a password verification function.

Remarks

System privileges provide the ability to access data or perform administrative operations for the entire database. Consistent with the principle of least privilege, these privileges should be granted sparingly. The Privilege Analysis feature of Database Vault may be helpful to determine the minimum set of privileges required by a user or role. In some cases, it may be possible to substitute a more limited object privilege grant in place of a system privilege grant that applies to all objects. System privileges should be granted with admin option only when the recipient needs the ability to grant the privilege to others.

Roles are a convenient way to manage groups of related privileges, especially when the privileges are required for a particular task or job function. Beware of broadly defined roles, which may confer more privileges than an individual recipient requires. Roles should be granted with admin option only when the recipient needs the ability to modify the role or grant it to others.

User management privileges (ALTER USER, CREATE USER, DROP USER) can be used to create and modify other user accounts, including changing passwords. This power can be abused to gain access to another user's account, which may have greater privileges.
Users with privilege management privileges (ALTER ANY ROLE, CREATE ROLE, DROP ANY ROLE, GRANT ANY OBJECT PRIVILEGE, GRANT ANY PRIVILEGE, GRANT ANY ROLE) can change the set of privileges granted to themselves and other users. This ability should be granted sparingly, since it can be used to circumvent many security controls in the database.
Audit management privileges (AUDIT ANY, AUDIT SYSTEM) can be used to change the audit policies for the database. This ability should be granted sparingly, since it may be used to hide malicious activity.
Users with data access privileges (ALTER ANY TABLE, ALTER ANY TRIGGER, CREATE ANY INDEX, CREATE ANY PROCEDURE, CREATE ANY TRIGGER, DELETE ANY TABLE, INSERT ANY TABLE, READ ANY TABLE, SELECT ANY DICTIONARY, SELECT ANY TABLE, UPDATE ANY TABLE) can override various access controls on data. Most administrative tasks do not require access to the data itself, so these privileges should be granted rarely even to administrators. In addition to minimizing grants of these privileges, consider the use of Database Vault realms to limit the use of these privileges to access sensitive data.
Users with exemption privileges (EXEMPT ACCESS POLICY, EXEMPT REDACTION POLICY) can bypass the access control policies created using Virtual Private Database and Data Redaction. Most administrative tasks do not require access to the data itself, so these privileges should be granted rarely even to administrators.
Users with these privileges can access objects that contain user password verifiers. The verifiers can be used in offline attacks to discover user passwords.

Users with these privileges can directly modify objects in the SYS, DVSYS, or LBACSYS schemas. Manipulating these system objects may allow security protections to be circumvented or otherwise interfere with normal operation of the database.
These PL/SQL packages (DBMS_SCHEDULER, DBMS_SYS_SQL) allow for execution of SQL code or external jobs using the identity of a different user. Access should be strictly limited and granted only to users with a legitimate need for this functionality.
These PL/SQL packages (DBMS_BACKUP_RESTORE) can send data from the database using the network or file system. Access should be granted only to users with a legitimate need for this functionality.

Privileges granted to PUBLIC are available to all users. This generally should include few, if any, system privileges since these will not be needed by ordinary users who are not administrators.
Roles granted to PUBLIC are available to all users. Most roles contain privileges that are not appropriate for all users.
Privileges granted to PUBLIC are available to all users. This should include column privileges only for data that is intended to be accessible to everyone.
The DBA role is very powerful and can be used to bypass many security protections. It should be granted to only a small number of trusted administrators. Furthermore, each trusted user should have an individual account for accountability reasons. As with any powerful role, avoid granting the DBA role with admin option unless absolutely necessary.
Like the DBA role, these roles (AQ_ADMINISTRATOR_ROLE, EM_EXPRESS_ALL, EXP_FULL_DATABASE, IMP_FULL_DATABASE, OEM_MONITOR) contain powerful privileges that can be used to bypass security protections. They should be granted only to a small number of trusted administrators.

Java permission grants control the ability of database users to execute Java classes within the database server. A database user executing Java code must have both Java security permissions and database privileges to access resources within the database. These resources include database resources, such as tables and PL/SQL packages, operating system resources, such as files and sockets, Oracle JVM classes, and user-loaded classes. Make sure that these permissions are limited to the minimum required by each user.

Administrative privileges allow a user to perform maintenance operations, including some that may occur while the database is not open. The SYSDBA privilege allows the user to run as SYS and perform virtually all privileged operations. Starting with Oracle Database 12.1, less powerful administrative privileges were introduced to allow users to perform common administrative tasks with less than full SYSDBA privileges. To achieve the benefit of this separation of duty, each of these administrative privileges should be granted to at least one user account.

Remarks

Database Vault provides for configurable policies to control the actions of privileged administrative users, in order to protect against insider threats, stolen credentials, and human error. Data realms prevent unauthorized access to sensitive data objects, even by users with system privileges. Command rules limit the SQL commands and options that administrators can execute.

Privilege Analysis records the privileges used during a real or simulated workload. After collecting data about the privileges that are actually used, this information can be used to revoke privilege grants that are no longer needed.

Remarks

Encryption of some sensitive data is a requirement in certain regulated environments. Transparent Data Encryption automatically encrypts data as it is stored and decrypts it upon retrieval. This protects sensitive data from attacks that bypass the database to read data files directly. Encryption keys may be stored in wallets on the database server itself, or stored remotely in Oracle Key Vault for improved security.

Wallets are encrypted files used to store encryption keys, passwords, and other sensitive data. Wallet files should not be stored in the same directory with database data files, to avoid accidentally creating backups that include both encrypted data files and the wallet containing the master key protecting those files. For maximum separation of keys and data, consider storing encryption keys in Oracle Key Vault instead of wallet files.

Remarks

Data Redaction automatically masks sensitive data found in the results of a database query. The data is masked immediately before it is returned as part of the result set, so it does not interfere with any conditions specified as part of the query. Access by users with the EXEMPT REDACTION POLICY privilege will not be affected by the redaction policy. Users who can execute the DBMS_REDACT package are able to create and modify redaction policies. Also consider the use of Oracle Data Masking and Subsetting to permanently mask sensitive data when making copies for test or development use.

Virtual Private Database (VPD) allows for fine-grained control over which rows and columns of a table are visible to a SQL statement. Access control using VPD limits each database session to only the specific data it should be able to access. Access by users with the EXEMPT ACCESS POLICY privilege will not be affected by VPD policies. Users who can execute the DBMS_RLS package are able to create and modify these policies.
Like Virtual Private Database, Real Application Security (RAS) provides fine-grained control over the rows and columns of a table that are visible to a SQL statement. Specification of RAS data access policies uses a declarative syntax based on access control lists. Access by users with the EXEMPT ACCESS POLICY privilege will not be affected by RAS access policies. Users with ADMIN_SEC_POLICY and APPLY_SEC_POLICY privileges are able to create and modify these policies.
Oracle Label Security provides the ability to tag data with a data label or a data classification. Access to sensitive data is controlled by comparing the data label with the requesting user's label or security clearance. A user label or security clearance can be thought of as an extension to standard database privileges and roles. Access by users with the EXEMPT ACCESS POLICY privilege will not be affected by the Label Security policies. Each policy has a corresponding role; users who have this role are able to administer the policy.
Transparent Sensitive Data Protection (TSDP), introduced in Oracle Database 12.1, allows a data type to be associated with each column that contains sensitive data. TSDP can then apply various data security features to all instances of a particular type so that protection is uniform and consistent. Data from columns marked as sensitive is also automatically redacted in the database audit trail and trace logs. Users who can execute the DBMS_TSDP_MANAGE and DBMS_TSDP_PROTECT packages are able to manage sensitive data types and the protection actions that are applied to them.

Remarks

Auditing is an essential component for securing any system. The audit trail allows for monitoring the activities of highly privileged users. For any attack that exploits gaps in other security policies, auditing cannot prevent the attack but it forms the critical last line of defense by detecting the malicious activity. Sending audit data to a remote system is recommended in order to prevent any possible tampering with the audit records. The AUDIT_SYSLOG_LEVEL parameter can be set to send an abbreviated version of some audit records to a remote syslog collector. A better solution is to use Oracle Audit Vault and Database Firewall to centrally collect full audit records from multiple databases.

This finding shows the SQL statements that are audited by enabled audit policies.

This finding shows the object accesses that are audited by enabled audit policies.

This finding shows the privileges that are audited by enabled audit policies.

It is important to audit administrative actions performed by the SYS user. Traditional audit policies do not apply to SYS, so the AUDIT_SYS_OPERATIONS parameter must be set to record SYS actions to a separate audit trail. Beginning with Oracle 12c, the same Unified Audit policies can be applied to SYS that are used to monitor other users.

Granting additional privileges to users or roles potentially affects most security protections and should be audited. Each action or privilege listed here should be included in at least one enabled audit policy.

Creation of new user accounts or modification of existing accounts can be used to gain access to the privileges of those accounts and should be audited. Each action or privilege listed here should be included in at least one enabled audit policy.

Actions that affect the management of database features should always be audited. Each action or privilege listed here should be included in at least one enabled audit policy.

Usage of powerful system privileges should always be audited. Each privilege listed here should be included in at least one enabled audit policy.

Successful user connections to the database should be audited to assist with future forensic analysis. Unsuccessful connection attempts can provide early warning of an attacker's attempt to gain access to the database.

Fine Grained Audit policies can record highly specific activity, such as access to particular table columns or access that occurs under specified conditions. This is a useful way to monitor unexpected data access while avoiding unnecessary audit records that correspond to normal activity.

Unified Audit, available in Oracle Database 12.1 and later releases, combines multiple audit trails into a single unified view. It also introduces new syntax for specifying effective audit policies.

Remarks

```
---------------
dmin/orcl/adump
```

```
ERVICE=orclXDB)
```

When O7_DICTIONARY_ACCESSIBILITY is set to FALSE, tables owned by SYS are not affected by the ANY TABLE system privileges. This parameter should always be set to FALSE because tables owned by SYS control the overall state of the database and should not be subject to manipulation by users with ANY TABLE privileges.
When SQL92_SECURITY is set to TRUE, UPDATE and DELETE statements that refer to a column in their WHERE clauses will succeed only when the user has the privilege to SELECT from the same column. This parameter should be set to TRUE so that this requirement is enforced in order to prevent users from inferring the value of a column which they do not have the privilege to view.

The SEC_PROTOCOL_ERROR parameters control the database server's response when it receives malformed network packets from a client. Because these malformed packets may indicate an attempted attack by a malicious client, the parameters should be set to log the incident and terminate the connection. SEC_RETURN_SERVER_RELEASE_BANNER should be set to FALSE to limit the information that is returned to an unauthenticated client, which could be used to help determine the server's vulnerability to a remote attack.

The OS_ROLES and REMOTE_OS_ROLES parameters determine whether roles granted to users are controlled by GRANT statements in the database or by the operating system environment. Both parameters should be set to FALSE so that the authorizations of database users are managed by the database itself.

The UTL_FILE_DIR parameter controls which part of the server's file system can be accessed by PL/SQL code. Note that as the directories specified in the UTL_FILE_DIR parameter may be accessed by any database user, it should be set to specify one or more safe directories that do not contain restricted files such as the configuration or data files for the database. For maximum security, use directory objects which allow finer grained control of access, rather than relying on this parameter.

A trigger is code that executes whenever a specific event occurs, such as inserting data in a table or connecting to the database. Disabled triggers are a potential cause for concern because whatever protection or monitoring they may be expected to provide is not active.

Constraints are used to enforce and guarantee specific relationships between data items stored in the database. Disabled constraints are a potential cause for concern because the conditions they ensure are not enforced.

External procedures allow code written in other languages to be executed from PL/SQL. Note that modifications to external code cannot be controlled by the database. Be careful to ensure that only trusted code libraries are available to be executed. Although the database can spawn its own process to execute the external procedure, it is advisable to configure a listener service for this purpose so that the external code can run as a less-privileged OS user. The listener configuration should set EXTPROC_DLLS to identify the specific shared library code that can be executed rather than using the default value ANY.

Directory objects allow access to the server's file system from PL/SQL code within the database. Access to files that are used by the database kernel itself should not be permitted, as this may alter the operation of the database and bypass its access controls.

Database links allow users to execute SQL statements that access tables in other databases. This allows for both querying and storing data on the remote database.

Network ACLs control the external servers that database users can access using network packages such as UTL_TCP and UTL_HTTP. Specifically, a database user needs the connect privilege to an external network host computer if he or she is connecting using the UTL_TCP, UTL_HTTP, UTL_SMTP, and UTL_MAIL utility packages. To convert between a host name and its IP address using the UTL_INADDR package, the resolve privilege is required. Make sure that these permissions are limited to the minimum required by each user.

XML ACLs control access to database resources using the XML DB feature. Every resource in the Oracle XML DB Repository hierarchy has an associated ACL. The ACL mechanism specifies a privilege-based access control for resources to principals, which are database users or roles. Whenever a resource is accessed, a security check is performed, and the ACL determines if the requesting user has sufficient privileges to access the resource. Make sure that these privileges are limited to the minimum required by each user.

Remarks

Network encryption protects the confidentiality and integrity of communication between the database server and its clients. Either Native Encryption or TLS should be enabled. For Native Encryption, both ENCRYPTION_SERVER and CRYPTO_CHECKSUM_SERVER should be set to REQUIRED. If TLS is used, TCPS should be specified for all network ports and SSL_CERT_REVOCATION should be set to REQUIRED.

TCP.VALIDNODE_CHECKING should be enabled to control which client nodes can connect to the database server. Either a whitelist of client nodes allowed to connect (TCP.INVITED_NODES) or a blacklist of nodes that are not allowed (TCP.EXCLUDED_NODES) may be specified. Configuring both lists is an error; only the invited node list will be used in this case.

These banner messages are used to warn connecting users that unauthorized access is not permitted and that their activities may be audited.

These parameters are used to limit changes to the network listener configuration. One of the following restrictions should be implemented: (a) prevent changes by disabling DYNAMIC_REGISTRATION, (b) limit the nodes that can make changes by enabling VALID_NODE_CHECKING_REGISTRATION, or (c) limit the network sources for changes using the COST parameters SECURE_PROTOCOL, SECURE_CONTROL, and SECURE_REGISTER.

This parameter enables logging of listener activity. Log information can be useful for troubleshooting and to provide early warning of attempted attacks.

Remarks

OS authentication allows operating system users within the specified user group to connect to the database with administrative privileges. This shows the OS group names and users that can exercise each administrative privilege.

The PMON process monitors user processes and frees resources when they terminate. This process should run with the user ID of the ORACLE_HOME owner.

Agent processes are used by Oracle Enterprise Manager to monitor and manage the database. These processes should run with a user ID separate from the database and listener processes.

Listener processes accept incoming network connections and connect them to the appropriate database server process. These processes should run with a user ID separate from the database and agent processes.

oviding recommendations on how to mitigate

al purposes only and should not be used as a

n of this report. You are also solely responsible
ny mitigating actions identified herein.

s all warranties and conditions whether