

Checklist Application Report for Oracle Database Administration

Table of Contents

1. [Lock and expire default user accounts](#)
2. [Document database incident response and escalation procedure](#)
3. [Review log files periodically](#)
4. [Apply latest CPU patches provided by Oracle](#)
5. [Manage Oracle Software License Agreement](#)
6. [Implement strong password verify function](#)
7. [Manage shared or generic database user accounts](#)
8. [Enable idle time parameter for user profiles](#)
9. [Manage terminated or transferred employee's database user account](#)
10. [Eliminate the practice of storing plaintext passwords](#)
11. [Revoke privileges and roles from the database server user group PUBLIC](#)
12. [Restrict permissions on run-time facilities](#)
13. [Manage database links](#)
14. [Restrict administrative privileges/roles granted to users](#)
15. [Protect copy of sensitive production data in non-production environments](#)
16. [Restrict access to system audit logs](#)
17. [Control operating system access for Oracle directories and files](#)
18. [Limit OS level access to Oracle software account](#)
19. [Configure LogMiner to analyze and identify transactions](#)
20. [Harden sqlnet.ora configuration](#)
21. [Harden init.ora configuration](#)
22. [Harden listener.ora configuration](#)
23. [Set default tablespace to non-SYSTEM tablespace for user accounts](#)
24. [Encrypt critical data](#)
25. [Audit privileged users activities in the database](#)
26. [Implement change control management](#)
27. [Control access to Oracle data dictionary objects](#)
28. [Backup Database](#)
29. [Test backup and restore procedures regularly](#)
30. [Secure backup media](#)
31. [Restrict developer access to production databases](#)
32. [Maintain disaster recovery and standby database](#)
33. [Implement data retention and archiving policy](#)
34. [New User Creation Policy and Procedure](#)

1. Lock and expire default user accounts

Oracle database installs with a number of default database user accounts. Upon successful installation of the database, the Database Configuration Assistant automatically locks and expires most default database user accounts.

If you perform a manual (without using Database Configuration Assistant) installation of Oracle Database, then no default database users are locked upon successful installation of the database server. Or, if you have upgraded from a previous release of Oracle Database, you might have default accounts from earlier releases. Left open in their default states, these user accounts can be exploited, to gain unauthorized access to data or disrupt database operations.

You should lock and expire all default database user accounts. Oracle Database provides SQL statements to perform these operations.

REFERENCE

ALTER USER ANONYMOUS PASSWORD EXPIRE ACCOUNT LOCK;

http://download.oracle.com/docs/cd/B28359_01/server.111/b28337/tdpsg_user_accounts.htm

<http://www.cirt.net/passwords?vendor=Oracle%3f>

MAINOPTIONS

Compliance: S-OX, PCI-DSS

Product Verion: 8i, 9i, 10g, r11

Frequency: On-Demand

Type: Authentication, Access Control, Configuration

Risk Level: High

Operating System: Linux, Unix

2. Document database incident response and escalation procedure

Are you prepared to make the best decisions and responses to database security incidents in your business?

Prevention is always best, in other words: cheapest. Prevention is generally more economical, less stressful, and incurs less downtime however it requires a very full understanding of the security landscape. But eventually, the inevitable happens and the cost of recovery is directly related to the amount of fore-planning applied. Following are the suggested approaches to handle database incidents:

Assessing the situation
Identifying the people to handle the incident
Forming a plan for resolution
Return to Operation
Preventing Reoccurrence
Review the Causes
Review Resolution
Create a Final Report
The key is to

prevent re-occurrence.

REFERENCE

There are several well known sources for incident response management:

NIST SP800-61 Computer Security Incident Handling Guide Tim Grance, Karen Kent, Brian Kim
<http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>

NIST SP800-83 Guide to Malware Incident Prevention and Handling
Peter Mell, Karen Kent, Joseph Nusbaum
<http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf>

NIST SP800-86 Guide to Network and Computer Data analysis: Applying Forensic Techniques to Incident Response
Tim Grance, Suzanne Chevalier, Karen Kent, Hung Dang
<http://csrc.nist.gov/publications/drafts/Draft-SP800-86.pdf>

Best Practices for Security Incident Response, Kerry Thompson
http://www.crypt.gen.nz/papers/incident_response.html

Incident Response
Kenneth R. van Wyk, Richard Forno
O.Reilly & Associates. ISBN 0-596-00130-4
<http://www.oreilly.com/catalog/incidentres/index.html>

MAINOPTIONS

Product Verion: 8i, 9i, 10g, r11
Frequency: Monthly
Risk Level: Medium
Operating System: Linux, Unix, Windows

3. Review log files periodically

Oracle generates several log files and many of them can provide useful information to assist in auditing and securing the database. Automated or manual review of these log files on a daily/weekly basis should be one of the key responsibilities of a database administrator.

alert. log - Chronologically records messages and errors arising from the daily database operation. Also, there are pointers to trace files and dump files. Monitor alert log periodically for ORA- type errors. This log file is stored under background_dump_dest specified in init.ora or spfile.

listener. log -The logfile shows a timestamp, command issued, and result code. If an Oracle error is returned, it will include the error message. The default directory is \$ORACLE_HOME/network/admin

REFERENCE

<http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf>

http://www.sawmill.net/formats/Oracle_Listener.html

MAINOPTIONS

Product Verion: 8i, 9i, 10g, r11
Frequency: Daily, Weekly
Type: User Audit
Risk Level: Medium
Operating System: Linux, Unix, Windows

VENDOR DETAILS

- Oracle - www.oracle.com
- MySQL - www.mysql.com

4. Apply latest CPU patches provided by Oracle

Oracle issues a Cumulative Patch Update (CPU) every quarter that fixes number of security vulnerabilities. It is imperative to keep the Oracle database instance at the latest patch level. While creating a new Oracle database instance make sure you install the latest security patch. Oracle database security patches are cumulative, so you need to install only the latest patch update. Notes: Oracle CPU may have dependencies on other patches or features/components. Analyze the documentation before applying the patch. Steps:

1. Check the security patch level of your database instance
SQL > select version from v\$instance; The only way to find the latest CPU on the database is to use opatch oracle command on the Oracle code tree. First three digits show the Oracle version and fourth-fifth digits show the latest patch.
2. Check on Oracle Metalink the latest security patch release by Oracle.

<http://www.oracle.com/technology/deploy/security/alerts.htm>

Any critical vulnerability that exposes the installed module needs to be patched immediately.

REFERENCE

Subscribe to the following RSS feeds:

http://www.red-database-security.com/advisory/published_alerts.xml

MAINOPTIONS

Applicable Compliance: S-OX, PCI-DSS, HIPAA, EU Privacy Law
Product Verion: 9i, 10g, r11
Data Classification: Financial, Confidential
Frequency: Continuous
Type: Patch Management
Risk Level: High

5. Manage Oracle Software License Agreement

It is a key business imperative to have robust and flexible procedures in place to monitor and control software assets. Failure to do so may lead to financial inaccuracies impacting corporate governance. But, effective license agreement helps companies reduce cost.

TASK LIST

- 1. Understand your license agreement
- 2. Understand your software usage
- 3. Implement a Software tracking process

REFERENCE

<http://www.miroconsulting.com/>

MAINOPTIONS

Product Verion: 8i, 9i, 10g, r11
Frequency: On-Demand
Risk Level: Low
Operating System: Linux, Unix, Windows

6. Implement strong password verify function

Establishing and enforcing limitations on password complexity, expiration, lockout, and reuse will reduce the risk that threat Agents may gain access by exploiting a weakness in these settings. Create a strong password verify function and attach the function to default or custom profile which will be assigned to all user accounts created in the database. Following values are recommended for the password profile options:

- failed_login_attempts=10
- password_life_time=90
- password_reuse_max=20
- password_reuse_time=365
- password_lock_time=1
- password_grace_time=3

REFERENCE

http://www.red-database-security.com/whitepaper/oracle_passwords.html
<http://www.cqure.net/wp/test/>

MAINOPTIONS

Product Verion: 8i, 9i, 10g, r11
Frequency: Daily, Weekly, Monthly
Type: Authentication, Access Control, Configuration

Risk Level: High

Operating System: Linux, Unix, Windows

7. Manage shared or generic database user accounts

Shared database accounts with high-level access rights can pose significant risks to organizations. Also, the use of a generic account represents a security risk in terms of both access control and auditing. From an access control perspective, anyone who knows the generic accounts password can execute privileged commands on databases. From an auditing perspective, it is impossible to directly associate a specific SQL statement with a specific user. So, care should be given when managing shared database accounts.

TASK LIST

- 1. Actively manage list of individual users who have access to shared or generic accounts. In some cases, the shared accounts are accessed using sudo or other operating system privileges.
- 2. Change password for shared accounts every 30 days.
- 3. Restrict the servers or hostname from where users can connect to the database using the shared account.
- 4. Assign role-based privileges to generic database accounts.
- 5. Log all activities carried out by the generic users.
- 6. Assign active account custodian for each generic account.

MAINOPTIONS

Applicable Compliance: S-OX, PCI-DSS, HIPAA, EU Privacy Law

Product Version: 8i, 9i, 10g, r11

Data Classification: Financial, Confidential

Frequency: Continuous

Type: Authentication, Access Control, User Audit

Risk Level: High

Operating System: Linux, Unix, Windows

8. Enable `idle_time` parameter for user profiles

Typically, malicious users target the inactive sessions to gain access into the database. By reducing the period of time an inactive session stays connected, the probability of that session being a victim of abuse is reduced. Also, setting up `idle_time` helps to reduce problems of having too many INACTIVE sessions. Oracle has several ways to disconnect idle connections, both from within SQL*Plus via resources profiles (`connect_time`, `idle_time`), and with the SQL*net expire time parameter. However, it's much easier to manage connection timeout using `idle_time` attached with user profiles.

MAINOPTIONS

Applicable Compliance: S-OX, PCI-DSS, HIPAA
Product Verion: 8i, 9i, 10g, r11
Data Classification: Financial
Frequency: Daily
Type: Access Control, User Audit
Risk Level: Medium
Operating System: Linux, Unix, Windows

9. Manage terminated or transferred employee's database user account

To mitigate the risk of unauthorized access of information, establish control in place for managing terminated or transferred employees' Oracle user accounts and rules for access. When a user is transferred or terminated, the user's access to database must be terminated to minimize risk. Following best practices are recommended for managing the access:

1) Direct supervisor or manager to contact the database administrator immediately when the user is transferred or terminated. 2) Establish daily monitoring report to match Microsoft Active Directory, LDAP or other enterprise identify management database user directory with Oracle Database User Access to generate daily report on the differences.

MAINOPTIONS

Applicable Compliance: S-OX, PCI-DSS, HIPAA, EU Privacy Law, GLBA
Product Verion: 8i, 9i, 10g, r11
Data Classification: Financial, Confidential
Frequency: Continuous
Type: Authentication, Access Control
Risk Level: High
Operating System: Linux, Unix, Windows

10. Eliminate the practice of storing plaintext passwords

Compromise of a database user password is one of the most difficult intrusions to detect. The best strategy is to eliminate storing of plaintext passwords in the first place. This can be done in several ways: 1) Do not store database user passwords in a plaintext file or in the database 2) Salt and hash every password that's stored 3) Scan operating system files and cron jobs to check if the database user passwords are stored in plaintext format 4) Change database user passwords regularly

MAINOPTIONS

Product Verion: 8i, 9i, 10g, r11
Frequency: Weekly
Type: Authentication, Access Control
Risk Level: Medium
Operating System: Linux, Unix, Windows

11. Revoke privileges and roles from the database server user group PUBLIC

PUBLIC acts the default Oracle user/group, granted to everyone in the database. (Any authenticated user can use the privileges granted to PUBLIC.) These privileges include EXECUTE on certain PL/SQL packages, potentially allowing a minimally privileged threat Agent to access/execute functions otherwise unavailable by

direct access. If unnecessary privileges and roles are not revoked from PUBLIC, this default role, granted to every user in an Oracle database, enables unrestricted use of its privileges, such as EXECUTE on various PL/SQL packages. Revoke PUBLIC privileges for the following:

TASK LIST

- 1. UTL_SMTP: UTL_SMTP enables the use of mail services by unauthorized users.
- 2. UTL_TCP: UTL_TCP enables network connections from one database to another database and unauthorized sending of data to other servers
- 3. UTL_HTTP: UTL_HTTP enables the processing of http requests and sending of data to malicious web sites
- 4. UTL_FILE: UTL_FILE enables access and writing of files in the operating system and can be used to replace critical files
- 5. DBMS_RANDOM: DBMS_RANDOM can be used for unauthorized encryption of stored data.
- 6. DBMS_LOB: DBMS_LOB can be used for defining and manipulating large objects.
- 7. DBMS_OBFUSCATION_TOOLKIT: Revoke execute privileges assigned PUBLIC
- 8. Review all PUBLIC synonyms created.

REFERENCE

To revoke a privilege, connect as SYS and do the following:

```
REVOKE EXECUTE ON UTL_SMTP FROM PUBLIC; REVOKE EXECUTE ON UTL_TCP FROM PUBLIC;  
REVOKE EXECUTE ON UTL_HTTP FROM PUBLIC; REVOKE EXECUTE ON UTL_FILE FROM PUBLIC;  
REVOKE EXECUTE ON DBMS_RANDOM FROM PUBLIC;
```

MAINOPTIONS

Product Verion: 8i, 9i, 10g, r11
Frequency: Weekly
Type: Access Control, Configuration
Risk Level: High
Operating System: Linux, Unix, Windows

12. Restrict permissions on run-time facilities

Do not assign all permissions to any database server run-time facility, such as the Oracle Java Virtual Machine (OJVM). Instead, grant specific permissions to the explicit document root file paths for such facilities

that may execute files and packages outside the database server.

REFERENCE

Here is an example of a vulnerable run-time call, which individual files are specified:

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

Here is an example of a better (more secure) run-time call, which specifies a directory path instead:

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

MAINOPTIONS

Applicable Compliance: S-OX, PCI-DSS, HIPAA

Product Verion: 9i, 10g, r11

Data Classification: Financial

Frequency: Daily

Type: Access Control

Risk Level: Medium

Operating System: Linux, Unix, Windows

13. Manage database links

Protecting production data is vital to any company. Database (DB) links, which allows users to connect from one database to another, pose a risk to production data that needed to be addressed.

Following factors need to be considered when managing database links:1) A database link owned by PUBLIC can be used by any user in the database. Unless it's really required stay away from creating public database links.

2) Oracle keeps clear-text passwords for created database links in the SYS.LINK\$ table in earlier Oracle versions. Apply Oracle patch or recreate link\$ to hide password column

3) Prevent unauthorized database links from being created between production schemas and non-production schemas

REFERENCE

<http://blogs.ittoolbox.com/oracle/guide/archives/database-links-a-definition-in-plain-english-7023>

MAINOPTIONS

Applicable Compliance: S-OX, PCI-DSS, HIPAA, EU Privacy Law

Product Verion: 8i, 9i, 10g, r11

Data Classification: Financial

Frequency: Continuous

Type: Access Control, Configuration

Risk Level: High

□ 14. Restrict administrative privileges/roles granted to users

Do not provide database users more privileges than necessary. Enable only those privileges actually required to perform necessary jobs efficiently:1) Restrict the number of system and object privileges granted to database users.2) Restrict the number of SYS-privileged connections to the database as much as possible. For example, there is generally no need to grant CREATE ANY TABLE to any non-DBA-privileged user.3) Check for any user or role that has the ANY keyword and revoke this role where possible.4) Prevent granting of privileges that have "WITH ADMIN".5) Prevent granting of privileges that have "WITH GRANT"

REFERENCE

LIST OF RESTRICTED_PRIVILEGES IN ORACLE

ADMINISTER DATABASE TRIGGER
ADMINISTER RESOURCE MANAGER
ADMINISTER SECURITY
ADVISOR
ALTER ANY CLUSTER
ALTER ANY DIMENSION
ALTER ANY INDEX
ALTER ANY INDEXTYPE
ALTER ANY LIBRARY
ALTER ANY MATERIALIZED VIEW
ALTER ANY OPERATOR
ALTER ANY PROCEDURE
ALTER ANY ROLE
ALTER ANY RULE
ALTER ANY RULE SET
ALTER ANY SECURITY PROFILE
ALTER ANY SEQUENCE
ALTER ANY SNAPSHOT
ALTER ANY TABLE
ALTER ANY TRIGGER
ALTER ANY TYPE
ALTER DATABASE
ALTER PROFILE
ALTER RESOURCE COST
ALTER SYSTEM
ALTER TABLESPACE
ALTER USER
AUDIT ANY
AUDIT SYSTEM
BACKUP ANY TABLE
BECOME USER

CREATE PUBLIC DATABASE LINK

CREATE ANY DIRECTORY

CREATE JOB
DELETE ANY TABLE

DROP ANY CLUSTER
DROP ANY CONTEXT
DROP ANY DIMENSION
DROP ANY DIRECTORY
DROP ANY EVALUATION CONTEXT
DROP ANY INDEX
DROP ANY INDEXTYPE
DROP ANY LIBRARY
DROP ANY MATERIALIZED VIEW
DROP ANY OPERATOR
DROP ANY PROCEDURE
DROP ANY ROLE
DROP ANY RULE
DROP ANY RULE SET
DROP ANY SECURITY PROFILE
DROP ANY SEQUENCE
DROP ANY SNAPSHOT
DROP ANY SYNONYM
DROP ANY TABLE
DROP ANY TRIGGER
DROP ANY TYPE
DROP ANY VIEW
DROP PUBLIC DATABASE LINK
DROP PUBLIC SYNONYM
DROP ROLLBACK SEGMENT
DROP TABLESPACE
DROP USER
EXECUTE ANY PROCEDURE
EXECUTE ANY PROGRAM
EXECUTE ANY TYPE

EXEMPT ACCESS POLICY

EXPORT FULL DATABASE
FLASHBACK ANY TABLE
GRANT ANY OBJECT PRIVILEGE
GRANT ANY PRIVILEGE
GRANT ANY ROLE
IMPORT FULL DATABASE
INSERT ANY TABLE
LOCK ANY TABLE
MANAGE TABLESPACE
RESTRICTED SESSION
SYSDBA
SYSOPER
UPDATE ANY TABLE
WRITEDOWN
WRITEUP

Review all "%ANY%" privilege assigned to users

LIST OF RESTRICTED_PRIVILEGES IN ORACLE

DBA
EXP_FULL_DATABASE
IMP_FULL_DATABASE
OEM_ADVISOR
OEM_MONITOR

RESOURCE
SCHEDULER_ADMIN
TIMESERIES_DBA

_%_CATALOG_%

MAINOPTIONS

Applicable Compliance: S-OX, PCI-DSS, HIPAA, EU Privacy Law

Product Verion: 8i, 9i, 10g, r11

Data Classification: IP, Financial, Confidential

Frequency: Daily

Type: Access Control

Risk Level: Medium

15. [Protect copy of sensitive production data in non-production environments](#)

Data which is sensitive in nature, which is protected in the Production Environment, is less protected and is at risk of exposure when it is cloned for use in non-production environments such as Development, Test and Training instances. This practice puts businesses at unacceptable risk for loss of customer trust, damage to brand, expensive notification, remediation efforts, and in violation of various regulatory and statutory requirements with resulting fines and penalties. Based on several California legislations and other worldwide data privacy regulations (See References for a listing of legislation and regulations), business needs to mask and restrict unauthorized use of data deemed confidential or restricted in test and development systems. Data masking is a process by which production data would be disguised in the supporting instances to production. Organizations routinely share production data, for example, database administrators copy production data into testing environments for realistic and accurate testing. This requires most organizations to mask sensitive parts of its production data. One of the easiest ways to both efficiently provide test and development data while protecting employee and customer identities is to mask data elements used to establish a persons identity. Data Masking is needed solution for data protection from both internal and external security threats. Data masking is also referred to as data obfuscation, data de-identification, data depersonalization, data scrubbing, data scrambling, etc.

REFERENCE

Legislation and Data Privacy Regulations

1. California legislation SB-1386:

Any agency, person or business that conducts business in California and owns or licenses computerized 'personal information are required to disclose any breach of security (to any resident whose unencrypted data is believed to have been disclosed).

2. Gramm-Leach-Bliley:

The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLB Act, includes provisions to protect consumers' personal financial information held by financial institutions. There are three principal parts to the privacy requirements: the Financial Privacy Rule, Safeguards Rule and pretexting provisions.

3. Health Insurance Portability and Accountability Act (HIPAA):

The U.S. Department of Health and Human Services (HHS) issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Privacy Rule standards address the use and disclosure of individuals health information called protected health information by organizations subject to the Privacy Rule called covered entities, as well as standards for individuals' privacy rights to understand and control how their health information is used.

4. EU Regulation (27 Member State) - Personal Data Protection Directive:

The EU Directive on Data Protection (DDP) of 1998 is a framework that stipulates the minimum data protection legislation EU member countries must have in place. The legislation is intended to protect the rights of EU citizens regarding the processing of their personal data. Any organization doing business in one or more EU countries must comply with the national data privacy legislation of each member country in which it operates.

5. Canadian Regulation - Personal Information Protection and Electronic Documents Act:

Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) ensures the protection of personal information. The PIPEDA applies to any work undertaking or business that is under the legislative authority of Parliament. Organizations must protect personal information regardless of the format by:

Developing and implementing a security policy.

Using appropriate security safeguards, including physical measures, technological tools (passwords, encryption, firewalls and anonymizing software) and organizational controls.

Removing or masking any personal information that has no relevance when providing copies of information.

6. UK Regulation - Data Protection Act:

The Data Protection Act (DPA) of 1998 applies to UK residents and UK-based organizations. It requires that all personal information, even data not stored in computerized systems, be protected from abuse and secured from unauthorized access. The DPA requires that data controllers take appropriate technical and organization measures to prevent unauthorized or unlawful processing or disclosure of personal data. Data must be protected during storage, transport, transition and update.

7. Australia Regulation - Privacy Amendment Act of 2000

The Privacy Amendment (Private Sector) Act 2000, which amended the Privacy Act 1988, came into effect on 21 December 2001, establishing a national scheme to regulate private sector organizations' handling of personal information.

The legislation, as amended, was designed to bring Australia into line with international standards on personal information and to instill confidence in how Australian businesses handle personal information. The Government also aimed to address concerns about the development and take up of online business and eCommerce.

8. Japan Regulation - The Personal Information Protection Act

Japan enacted the Personal Information Protection Act (JPIPA) in 2003 to protect individual's rights and personal information while preserving the usefulness of information technology and personal information for legitimate purposes. The law establishes responsibilities for businesses that handle personal information for citizens of Japan and outlines potential fines and punishments for organizations that do not comply. The act requires businesses to communicate their purpose in collecting and using personal information. They must also take reasonable steps to protect personal information from disclosure, unauthorized use or destruction.

9. Hong Kong Regulation The Personal Data (Privacy) Ordinance

The Personal Data (Privacy) Ordinance ('Privacy Ordinance') sets out a number of strict obligations and restrictions for dealing with an individual's personal data.

'Personal data', which is covered by the Privacy Ordinance includes any information about a living individual, so long as that information includes some data which would allow the individual to be identified. Personal data must include data from which it is reasonably practicable to ascertain the identity of the person. It includes paper documents, microfilm, audio tapes, video tapes, and computer files.

10. Argentinean Regulation - Law for the Protection of Personal Data

The purpose of this Act is the full protection of personal information recorded in data files, registers, banks or other technical means of data-treatment, either public or private for purposes of providing reports, in order to guarantee the honor and intimacy of persons, as well as the access to the information that may be recorded about such persons

11. Industry Privacy Standard - Payment Card Industry Data Security Standard (PCI DSS):

The PCI DSS a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover, JCB, MasterCard and Visa International, to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

MAINOPTIONS

Applicable Compliance: S-OX, PCI-DSS, HIPAA, EU Privacy Law

Product Verion: 8i, 9i, 10g, r11

Data Classification: IP, Financial, Confidential

Type: Access Control, Privacy

Risk Level: Medium

Operating System: Linux, Unix, Windows



16. Restrict access to system audit logs

Given the central role of audit logs in performing auditing of interactions with the data (modification, exposure) as well as of the base data itself, it is critical that audit logs be correct and inalterable. The integrity of the audit log itself must also be guaranteed.

There are several ways to protect audit logs in an Oracle system:

1) Protect the permission for the audit directory and files from Oracle OS account
2) The alternative is to put audit trail in the operating system. Following the principle of separation of duties, DBAs should not be able to view the audit trail.

MAINOPTIONS

Applicable Compliance: S-OX, PCI-DSS, HIPAA

Product Verion: 8i, 9i, 10g, r11

Data Classification: IP, Financial, Confidential

Frequency: Daily

Type: Access Control, Segregation of Duties

Risk Level: High

Operating System: Linux, Unix, Windows

17. Control operating system access for Oracle directories and files

In addition to the security Oracle maintains on tables and other database objects, the operating system controls access to Oracle files. Access to these files should be restricted on a need only basis and preferable restricted to the operating system account that owns the Oracle installation. Windows

Remove the Everyone Group from the installation drive or partition and give System and local Administrators Full Control.

Remove permissions for the Users group from the [OS drive]:\Program Files\Oracle folder. The Oracle program installation folder must allow only limited access.

Tighten the permission on tools (*.exe) in the WINNT and System32 folders, e.g., only Administrators should have permissions on these files; however, deny access to the Oracle service account. The Oracle service account is an administrator account, but also must be denied access to executables.

The everyone group must not be able review registry settings.

Give Full Control over the HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE key to the account that will run the Oracle services and

remove the local Users group if its not required. Give read permissions to those users that require it. Access to the Oracle registry key must be limited to those users that require it. Unix

All files in the \$ORACLE_HOME/bin must be owned by the Oracle software account. All files in the \$ORACLE_HOME/bin directory must have permissions set to 0755 or less.

All files in \$ORACLE_HOME directories (except for \$ORACLE_HOME/bin) must have permission set to 0750 or less. Ensure the umask value is 022 for the owner of the Oracle software before installing Oracle.

Regardless of where the umask is set, umask must be set to 022 before installing Oracle.

File permissions must be restricted to the owner of the Oracle software and the dba group. (init, spfile, database files, ifile, listner.ora, sqlnet.ora etc.) The Oracle 10g installer application could potentially create files in a temporary directory with public privileges. It would be possible for any local user to delete, overwrite or corrupt these files during the installation process. Try to ensure that no other users are connected while installing Oracle 10g. Also set the \$TMP and \$TMPDIR environment variables to a protected directory with access given only to the Oracle software owner and the ORA_INSTALL group.

MAINOPTIONS

Applicable Compliance: S-OX, PCI-DSS, HIPAA, EU Privacy Law
Product Verion: 8i, 9i, 10g, r11
Data Classification: Financial, Confidential
Frequency: Weekly
Type: Access Control, Configuration
Risk Level: Medium
Operating System: Linux, Unix, Windows

18. Limit OS level access to Oracle software account

Oracle software comes with several powerful OS utilities like export, import and trace. Restrict administrative access to OS account that owns Oracle software. In addition, review the membership of the DBA group on the host to ensure that only authorized OS accounts are included.

MAINOPTIONS

Applicable Compliance: S-OX, PCI-DSS, HIPAA, EU Privacy Law
Product Verion: 8i, 9i, 10g, r11
Data Classification: Financial, Confidential
Frequency: Weekly
Type: Authentication, Access Control, Segregation of Duties
Risk Level: Medium
Operating System: Linux, Unix

19. Configure LogMiner to analyze and identify transactions

All changes made to user data or to the database dictionary are recorded in the Oracle redo log files so that database recovery operations can be performed. Redo log files contain information about the history of activity on a database. Oracle LogMiner, which is part of Oracle Database, enables you to query online and archived redo log files through a SQL interface. LogMiner is a powerful audit tool for Oracle databases, allowing administrators to easily locate changes in the database, enabling sophisticated data analyses, and providing undo capabilities to rollback logical data corruptions, user errors or undo damage.

REFERENCE

http://download-west.oracle.com/docs/cd/A87860_01/doc/server.817/a76956/archredo.htm#12680

MAINOPTIONS

Product Verion: 8i, 9i, 10g, r11
Frequency: Continuous
Type: Configuration, User Audit
Risk Level: Low

20. Harden sqlnet.ora configuration

The sqlnet.ora contains the configuration files for the communication between the user and the server including the level of required encryption.

TASK LIST

1. log_directory_client : This value must be set to a valid directory owned by the Oracle account and permissions restricted to read/write only for the owner and dba group.

2. log_directory_server: This value must be set to a valid directory owned by the Oracle account and set with owner and group read/write permissions only.

3. trace_directory_client: This parameter settings must be set to a valid directory owned by the Oracle account and permissions restricted to read/write only for the owner and dba group.

4. trace_directory_server: This value must be set to a valid directory owned by the Oracle account and permissions restricted to read/write only for the owner and dba group.

5. tcp.validnode_checking=YES: Set this parameter in the \$ORACLE_HOME/network/admin/sqlnet.ora file.

6. tcp.invited_nodes: Set this value to valid values. Use IP addresses of authorized hosts to set this parameter in the sqlnet.ora file.

7. tcp.excluded_nodes: Set his value to valid values. Use IP addresses of unauthorized hosts to set this parameter in the sqlnet.ora file. Note: if the tcp.invited_nodes is set, the tcp.excluded_nodes values are ignored.

8. sqlnet.inbound_connect_timeout=3 Set this parameter to a low initial value and adjust upward if normal clients are unable to connect within the time allocated.

9. tcp.validnode_checking= YES Set this parameter in the \$ORACLE_HOME/network/admin/sqlnet.ora file.

10. sqlnet.expire_time= 10 If this is not set in the sqlnet.ora file, the default is never to expire.

MAINOPTIONS

Applicable Compliance: S-OX, PCI-DSS, HIPAA

Product Verion: 8i, 9i, 10g, r11

Data Classification: IP, Financial, Confidential

Frequency: Weekly

Type: Configuration

Risk Level: High

Operating System: Linux, Unix, Windows

21. Harden init.ora configuration

The init.ora file stores the initialization parameters of Oracle. The values that are currently in effect can be viewed through v\$parameter.

TASK LIST

1. SQL92_SECURITY= TRUE - Enforce the requirement that a user must have SELECT privilege on a table in order to be able to execute UPDATE and DELETE statements using WHERE clauses on a given table.

□2. REMOTE_OS_ROLES=FALSE - Setting REMOTE_OS_ROLES to TRUE allows operating system groups to control Oracle roles. The default value of FALSE causes roles to be identified and managed only by the database. If REMOTE_OS_ROLES is set to TRUE, a remote user could impersonate another operating system user over a network connection. It is a security risk to use operating system role authentication for network clients.

□3. OS_AUTHENT_PREFIX= - Usually, OS_AUTHENT_PREFIX is set to the default value of OPS\$, it removes the Oracle security restriction that requires users to be IDENTIFIED EXTERNALLY in order to logon via OS authentication. This removes an important control and presents some security risk. If the OS_AUTHENT_PREFIX = OPS\$ is set in init.ora, then any username that begins with the string OPS\$ can logon via the OS. If OS_AUTHENT_PREFIX is set to any other value, only users that are IDENTIFIED EXTERNALLY (Password column in DBA_USERS/SYS.USER\$ will read EXTERNAL) and whose username begins with the OS_AUTHENT_PREFIX can login via the OS.

□4. FAILED_LOGIN_ATTEMPTS=5 - Setting up failed_login_attempts in init.ora configuration file helps to limit the number of failed attempts to log in to the user account before the account is locked. It's recommended to set the failed_login_attempts to 5. Frequently monitoring the failed login attempts values from LCOUNT column in user\$ helps to figure out if there's any attempts being made to break-in to the user account using false credentials.

□5. DBLINK_ENCRYPT_LOGIN = TRUE dblink_encrypt_login specifies whether attempts to connect to remote Oracle databases through database links should use encrypted passwords. Ensure that DBLINK_ENCRYPT_LOGIN = TRUE in the init.ora configuration file.

□6. _TRACE_FILES_PUBLIC= FALSE - By default only the Oracle user can read trace files. This parameter allows other users to read the trace files by modifying the file permissions. This particularly applies to UNIX operating systems.

The default value is FALSE.

□7. REMOTE_OS_AUTHENT=FALSE - The REMOTE_OS_AUTHENT parameter in the init parameter file of the database specifies whether remote clients will be authenticated with the value of the OS_AUTHENT_PREFIX parameter or not. The type of the REMOTE_OS_AUTHENT parameter is Boolean, the default value is false, and the parameter class is static.

It is strongly recommended that when configuring the Oracle database, the initialization parameter file used for the database instance

REMOTE_OS_AUTHENT=FALSE is set.

Setting REMOTE_OS_AUTHENT to TRUE may create a security hole because it allows someone using a non-secure protocol (for example, TCP) to perform an operating system-authorized login.

If REMOTE_OS_AUTHENT is set to FALSE, and the server cannot support any of the authentication services requested by the client, the authentication service negotiation will fail, and the connection will be

terminated.

If REMOTE_OS_AUTHENT is set to TRUE for a particular database, and the client has the following parameter set in its SQLNET.ORA file:

```
SQLNET.AUTHENTICATION_SERVICES=(NONE)
```

and the server has, for example,

```
SQLNET.AUTHENTICATION_SERVICES=(BEQ,KERBEROS5)
```

set in its SQLNET.ORA file, the connection will fail.

If the following parameter is set in the SQLNET.ORA file on either the client or server side:

```
SQLNET.AUTHENTICATION_SERVICES=(NONE)
```

the database will attempt to use the provided username and password to log the user in.

8. O7_DICTIONARY_ACCESSIBILITY = FALSE - Oracle recommends that customers implement data dictionary protection to prevent users having the ANY system privileges from using such privileges on the data dictionary. By doing so, only those authorized users making DBA-privileged (e.g. CONNECT / AS SYSDBA) connections can use the ANY system privilege on the data dictionary. If this parameter is not set to the value recommended above, any user with a DROP ANY TABLE (for example) system privilege will be able to maliciously drop parts of the data dictionary.

9. OS_ROLES is an init.ora file parameter that, if set to true, enables the operating system to manage authorization of an external role for a database user. By default, OS_ROLES is set to false. O/S roles are subject to control outside the database. This separates the duties and responsibilities of DBAs and system administrators.

REFERENCE

http://www.oracle.com/technology/deploy/security/oracle9i/pdf/9i_checklist.pdf

MAINOPTIONS

Product Verion: 8i, 9i, 10g, r11
Frequency: Monthly
Type: Configuration
Risk Level: High
Operating System: Linux, Unix, Windows

22. Harden listener.ora configuration

Listener configuration, stored in the listener.ora file, consists of the following elements:1) Name of the listener2) Protocol addresses that the listener is accepting connection requests on Database services 3) Dynamic service registration4) Control parameters

TASK LIST

- 1. Set an encrypted password for the listener. By default, the listener password is not set.
- 2. Standard ports(1521 etc.,) are well known and can be used by attackers to verify applications running on a server.
- 3. File permissions must be restricted to the owner of the Oracle software and the dba group. If backup copies of the listener.ora file are created these backup files must be removed or they must have their permissions restricted to the owner of the Oracle software and the dba group.
- 4. The log_file_listener file must be set to a valid directory owned by the Oracle account and permissions restricted to read/write only for the owner and dba group.By default this is not set. Be aware, this is usually set to \$ORACLE_HOME/network/log/listener.log.
- 5. The trace_directory_listener_name must be set to a valid directory owned by the Oracle account and permissions restricted to read/write only for the owner and dba group.By default this is not set. Be aware, this is usually set to \$ORACLE_HOME/network/trace.
- 6. The trace_file_listener_name file set in the listener.ora should be owned by the Oracle account and permissions restricted to read/write only for the owner and dba group.By default this is not set. Be aware, this is usually set to \$ORACLE_HOME/network/trace
- 7. Set admin_restrictions_listener_name=on
- 8. Set logging_listener=ON. It is recommended to set this parameter on
- 9. Set inbound_connect_timeout_listener=2. Suggestion is to set to a low initial value and adjust upward if normal clients are unable to connect within the time allocated.
- 10. ExtProc functionality allows external C and Java functions to be called from within PL/SQL. If extproc functionality is not required, remove this entry. If extproc functionality is required, refer to Oracle Metalink Security Alert 57 (244523.1) for instructions on securing extproc. In short, create a new listener specifically for extproc. This listener must run as an unprivileged OS user.
- 11. The listener must not be called by the default name. A distinct name must be selected.
- 12. IP addresses instead of host names in the listener.ora file must be used.

MAINOPTIONS

Applicable Compliance: S-OX, PCI-DSS, HIPAA
Product Verion: 8i, 9i, 10g, r11

Data Classification: Financial, Confidential
Frequency: Weekly
Type: Configuration
Risk Level: High
Operating System: Linux, Unix, Windows

23. [Set default_tablespace to non-SYSTEM tablespace for user accounts](#)

System tablespace contains the data dictionary information that needs to maintain the Oracle database. Any user should not have SYSTEM tablespace as his/her default tablespace. Change the value of default tablespace by following the steps below.

(a) Invoke SQL*Plus

(b) Run the query:

```
-"alter user "USER_NAME" default tablespace;"
```

MAINOPTIONS

Product Verion: 8i, 9i, 10g, r11
Frequency: Continuous
Type: Configuration
Risk Level: Low
Operating System: Linux, Unix, Windows

24. [Encrypt critical data](#)

Critical data must be encrypted to prevent the DBAs and other users who have access to production system from accessing it. Alternately, You can audit key tables. This does not prevent the DBA from viewing the data, but would create a record of the activity. Management of the encryption key must be done carefully as exposure of the key will render the encryption moot.

MAINOPTIONS

Applicable Compliance: PCI-DSS, HIPAA, EU Privacy Law
Product Verion: 8i, 9i, 10g, r11
Data Classification: Confidential
Frequency: Continuous
Type: Access Control
Risk Level: Medium
Operating System: Linux, Unix, Windows

25. [Audit privileged users activities in the database](#)

Full access credentials accorded to DBAs and system administrators creates a significant vulnerability for an enterprises data simply because these privileged users have access to all or a significant fraction of data. Auditing of the users authenticated as the SYSDBA or the SYSOPER provides an oversight of the most privileged of users. Ensure this by setting the AUDIT_SYS_OPERATIONS to TRUE. Note: It is important that the database user should not have access to the system directories where the audits will be recorded.

REFERENCE

MAINOPTIONS

Product Verion: 8i, 9i, 10g, r11
Frequency: Continuous
Type: Access Control, User Audit
Risk Level: High

26. Implement change control management

The objective of Change management is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes to controlled database infrastructure, in order to minimize the number and impact of any related incidents upon service. Changes in the database infrastructure may arise reactively in response to problems or externally imposed requirements, e.g. legislative changes, or proactively from seeking imposed efficiency and effectiveness or to enable or reflect business initiatives, or from programs, projects or service improvement initiatives. Change Management can ensure standardized methods, processes and procedures are used for all changes, facilitate efficient and prompt handling of all changes, and maintain the proper balance between the need for change and the potential detrimental impact of changes. Some of the common functions included in change control management include:> Code Review for common vulnerabilities

MAINOPTIONS

Applicable Compliance: S-OX, PCI-DSS, HIPAA
Product Verion: 8i, 9i, 10g, r11
Data Classification: Financial
Frequency: Continuous
Type: Program Change Control
Risk Level: Medium
Operating System: Linux, Unix, Windows

27. Control access to Oracle data dictionary objects

Check for any user accounts that have access to the following objects and revoke where possible:

REFERENCE

All_% views
ALL_USERS view
DBA_%
Link\$
PERFSTAT.STATS\$SQL_SUMMARY
PERFSTAT.STATS\$SQLTEXT
ROLE_ROLE_PRIVS
SYS.AUD\$
SYS.EXU7LNK;
SYS.EXU7LNKU;
SYS.EXU7ROL;
SYS.EXU7USR;

SYS.EXU7USRU;
SYS.EXU8LNK;
SYS.EXU8LNKU;
SYS.EXU8PHS;
SYS.EXU8PHS;
SYS.EXU8ROL;
SYS.EXU8USR;
SYS.EXU8USRU;
SYS.EXU9LNK;
SYS.EXU9LNK;
SYS.EXU9LNKU;
SYS.EXU9LNKU;
SYS.KU\$_ROLE_VIEW;
SYS.KU\$_USER_VIEW;
SYS.SOURCE\$
SYS.USER_DB_LINKS;
SYS.USER_HISTORY\$
User\$
USER_ROLE_PRIVS
USER_TAB_PRIVS
V_\$%
X\$%

MAINOPTIONS

Applicable Compliance: S-OX, PCI-DSS, HIPAA
Product Verion: 8i, 9i, 10g, r11
Data Classification: Financial, Confidential
Frequency: Daily
Type: Access Control, Configuration
Risk Level: High
Operating System: Linux, Unix, Windows

28. Backup Database

Backup and recovery is one of the most important aspects of database administration. If a database crashed and there was no way to recover it, the devastating results to a business could include lost data, lost revenue and customer dissatisfaction. Whether companies operate a single database or multiple databases storing hundreds of gigabytes or even terabytes of data, they share one common factor - the need to back up important data and protect themselves from disaster by developing a backup and recovery plan. Backup and recovery of your Oracle database is important to protecting data from corruptions, hardware failures, and data failures. While Oracle provides many features to protect your data, nothing can replace a backup. Either back up the database files with Recovery Manager (RMAN), or use operating system utilities. RMAN is an Oracle utility that manages backup and recovery operations, creates backups of database files (datafiles, control files, and archived redo log files), and restores or recovers a database from backups.

REFERENCE

http://www.oracle.com/technology/deploy/availability/htdocs/BR_Overview.htm

http://sahaa.net/wp/Database_Backup_Sample_Policy.pdf

MAINOPTIONS

Applicable Compliance: S-OX, PCI-DSS, HIPAA

Product Verion: 8i, 9i, 10g, r11

Data Classification: Financial

Frequency: Continuous, Daily

Type: Business Continuity

Risk Level: High

Operating System: Linux, Unix, Windows

29. Test backup and restore procedures regularly

Backups should be verified by performing recoveries to ensure backups function properly. Failure to ensure this could cause inability to recover data, leading to data loss.

REFERENCE

Following eight-step process validates whether an Oracle database could be properly recovered from the backup copy:

SQL #1:

```
select count(*) from v$recover_file;
```

The v\$recover_file view displays the status of files needing media recovery. The SQL should return one row of value 0. If the result is anything other than 0, it means that the database backup was not consistent. The database backup has to be taken again.

SQL #2:

```
select count(*) from v$recovery_log;
```

The v\$recovery_log view lists information about archived logs that are needed to complete media recovery. The SQL should return one row of value 0. If the result is anything other than 0, it means that the database backup was not consistent. The database backup has to be taken again.

SQL #3:

```
select count(*) from v$recovery_status;
```

The v\$recovery_status view contains statistics of the current recovery process. The SQL should return one row of value 0. If the result is anything other than 0, it means that the database backup was not consistent. The database backup has to be taken again.

SQL #4:

```
select count(*) from v$recovery_file_status;
```

The v\$recovery_file_status view contains one row for each data file for each RECOVER statement. The SQL should return one row of value 0. If the result is anything other than 0, it means that the database backup was not consistent. The database backup has to be taken again.

SQL #5:

```
select name,status from v$datafile where (name like '%MISS%' or status not in ('ONLINE', 'SYSTEM'));
```

The v\$datafile view contains datafile information from the control file. The SQL should return two rows of values SYSTEM and ONLINE. If the query returns any other result it means that the database backup was not consistent. The database backup has to be taken again.

SQL #6:

```
Select distinct checkpoint_change# from v$datafile ;
```

The \$datafile view contains datafile information from the control file. The checkpoint_change# is written to the each of the datafile at the time of closing the database. The SQL should return only one row. If more than one row is returned it means that the database backup was not consistent. The database backup has to be taken again.

SQL #7:

```
select distinct to_char(CHECKPOINT_TIME,'DD-MON-YYYY HH24:MI:SS') from v$datafile_header;
```

The \$datafile view contains datafile information from the control file. The checkpoint_time is written to the each of the datafile at the time of closing the database. The SQL should return only one row. If more than one row is returned it means that the database backup was not consistent. The database backup has to be taken again.

SQL #8:

```
select distinct fhsta from x$kcvf;
```

x\$ tables are the sql interface to viewing oracle's memory. The SQL query should return one distinct number. Otherwise, the database backup is inconsistent and has to be taken again.

MAINOPTIONS

Applicable Compliance: S-OX, PCI-DSS, HIPAA

Product Verion: 8i, 9i, 10g, r11

Data Classification: Financial, Confidential

Frequency: Monthly

Type: Business Continuity

Risk Level: Medium

Operating System: Linux, Unix, Windows

30. Secure backup media

Backup data on secondary systems is at a much greater risk than primary data, which is protected by stringent data center policies and procedures. Carefully design a system that addresses as many of the business continuity needs as possible with the least cost and impact on operations.

TASK LIST

1. Encrypt Backup Tape

Its recommended that companies encrypt backup tapes containing sensitive information. At least, selectively encrypt only sensitive data

For example, consider an on-line shopping site having a very large product catalog database, all of which is already public data, as well as application and operating system code that may not be sensitive. Customer data, including names, addresses, authentication credentials and possibly credit cards or bank account numbers or other financial data would also be present. The time and processing cost needed to encrypt just the sensitive customer data would probably represent a fraction of the time and processing needed to encrypt all data in the system. This simple example illustrates the benefit of selective encryption, but to apply this approach to enterprise backup procedures requires that a current and accurate data classification scheme be in place.

2. Store backup media off site

REFERENCE

<http://www.zmanda.com/backup-security.html>

<http://www.oracle.com/technology/products/secure-backup/index.html>

MAINOPTIONS

Applicable Compliance: S-OX, PCI-DSS, HIPAA, EU Privacy Law

Product Verion: 8i, 9i, 10g, r11

Data Classification: IP, Financial, Confidential

Frequency: Continuous

Type: Business Continuity, Physical Security

Risk Level: Medium

Operating System: Linux, Unix, Windows

31. Restrict developer access to production databases

Developers and testers must not have direct access to production databases.

MAINOPTIONS

Applicable Compliance: S-OX, PCI-DSS, HIPAA
Product Verion: 8i, 9i, 10g, r11
Data Classification: Financial, Confidential
Frequency: Continuous
Type: Access Control, Segregation of Duties
Risk Level: High
Operating System: Linux, Unix, Windows

32. Maintain disaster recovery and standby database

The business-continuity program (BCP) and the disaster-recovery program (DRP) are on everyone's list of top 10 priorities. BCP and DRP are required to maximize systems availability and meet the most aggressive Service Level Agreements (SLAs) for system availability, quality of service, and data protection. The steps are ... Identify the critical business functions, and the databases that deliver them. Define your recovery point and recovery time objectives (RTO, RPO). Determine the activities or incidents that can disrupt those services. Architect an appropriate solution for protecting the databases, eliminating single points of failure. Some of the potential solutions for maintaining disaster recovery and/or standby databases are: Oracle Data Guard: It enables you to use either a physical standby database (Redo Apply) or a logical standby database (SQL Apply), or both, depending on the business requirements. A physical standby database provides a physically identical copy of the primary database, with on-disk database structures that are identical to the primary database on a block-for-block basis. The database schema, including indexes, is the same. A physical standby database is kept synchronized with the primary database by applying the redo data received from the primary database through media recovery.

REFERENCE

<http://www.oracle.com/technology/deploy/availability/htdocs/maa.htm>

MAINOPTIONS

Applicable Compliance: S-OX, PCI-DSS
Product Verion: 8i, 9i, 10g, r11
Frequency: Continuous
Type: Business Continuity
Risk Level: High
Operating System: Linux, Unix, Windows

33. Implement data retention and archiving policy

Data retention practice is truly protecting corporate data for long periods of time in order to meet regulatory requirements. For example, HIPAA requires that medical records be retained up to two years after a person's death. Sarbanes-Oxley requires audit data be kept for seven years after the conclusion of the audit and CFR (Life Sciences) requires that pharmaceutical companies retain clinical trial data for 35 years. Requirements are extremely stringent for companies that must retain data for legal purposes, and most are not prepared to hold data for such long time frames, let alone guarantee it hasn't been altered in any way. Also, good data retention practices help companies achieve maximum performance of applications through a reduced amount of data to process. In addition, day-to-day operations such as backups, recoveries and reorganizations will execute more efficiently. In most cases, the data is not deleted regularly even though the new transactions continue to occur within the application.

MAINOPTIONS

Applicable Compliance: S-OX, HIPAA
Product Verion: 8i, 9i, 10g, r11
Data Classification: IP
Frequency: On-Demand
Type: Purging and Archiving
Risk Level: Medium
Operating System: Linux, Unix, Windows

34. New User Creation Policy and Procedure

New user account creation policy and procedure should require new accounts to be created with a unique password and require the password to be changed upon first login.

MAINOPTIONS

Product Verion: 8i, 9i, 10g, r11
Frequency: Continuous
Type: Access Control
Risk Level: Medium
Operating System: Linux, Unix, Windows
