Author – *A.Kishore/Sachin*
http://appsdba.info

How to Protect APPS Password?

This documents suggests some steps to consider to protect APPS password.

- **Stay current with our latest Security Best Practices.**

  Regularly review the latest version of Best Practices for Securing Oracle Ebusiness Suite.

- **Regularly change your APPS password.**

  This is an essential activity from a security perspective and needs to be part of our routine operating procedures. Same is for other schema passwords and SYSADMIN user. We should not use predicable passwords.

- **Always change passwords after cloning.**

  It is recommended to change ALL schema passwords and all e-Business user passwords in a cloned instance. Similarly, we should not have any relation in the passwords used for Source and cloned instances. In Release 12, EM plug in provides some data scrambling facilities.

- **Perform data masking on any files sent to outside parties from the Production system.**

  When we send any log files or configuration files, we need to ensure that we check for any sensitive data before packing the files to be sent. Here we are discussing about the APPS password, but this applies equally for other data as well.

- **Create unique schemas with minimal access required for database access.**

  If anyone requires direct access to the E-Business Suite database, ensure that we need to create a new unique schema with the specific permissions required for him or her.

- **Protect Oracle Apps tier file system files.**

  Now days, there is little need to give anyone UNIX-level access to the servers, but it is still important to ensure that the "applmgr" operating system user password is well protected.

- **Ensure no Scripts are running with APPS username/password in command line.**

  Normally the APPS password is not listed in "ps" command output, but there may be some scripts or other processes that run with the APPS password in clear text or encoded. We need to check these scripts and should change to hide the APPS password.

- **Protect OID Password.**

  If we have integrated the E-Business Suite with Oracle Application Server 10g,Single Sign-On, and Oracle Internet Directory, then the Apps user password is stored in the OID database. OID password should be protected in the same way as the APPS password.

- **Encrypt SQLNET traffic from APPS Tier to RDBMS.**

  We should use encryption to protect the APPS password from networks, tracing SQLNET connection packets.

- **Allow only specific IP addresses to access RDBMS via SQLNET.**

  Restricting the IP addresses that can access the Oracle Apps database will help minimize the risk. Oracle recommends upgrading to server-based equivalent tools or shared desktop technologies such as Citrix, so desktop clients no longer need direct access.