JDEtips
JD Edwards Knowledge. Transferred. Sustained.

December 2013 Technical / Security

Restricting Access Privileges on an Oracle Database

By Carlos Sebaaly

Editor's Note: OK, everybody out of the pool. All it takes is a simple SQL script to go from wide open to shut down tight. Protecting the data is Mission One for any ERP system, and this article shows you how to close the gaps left in place after a default JDE installation with Oracle Database.

Introduction

Security is one of the highest concerns in today's ERP environments to protect the essential data silo in a company: the ERP database. Therefore, one of the main post-installation practices is setting a well-planned security strategy that tightens infrastructure, application, and especially database security to minimize, if not to eliminate access breaches.

Besides the various available recommended and documented practices for securing a JD Edwards database, such as changing default user passwords and disabling user accounts this article will go a step further and provide guidelines for managing and restricting access privileges for existing database user accounts by granting them only the necessary privileges they should be assigned.

In the first section, we will review how Oracle database manages privileges and how those privileges are assigned to JD Edwards users during installation. Then we'll look at some useful SQL statements to refine the applied configuration.

The examples in this article are based on JD Edwards EnterpriseOne 9.1 naming conventions, but they are also applicable to most of JD Edwards versions, especially 8.9x and 9.x versions.

Default JD Edwards and Oracle Database Security

By default, users do not have any access permissions to any object in the Oracle database other than the objects they own unless they are granted a privilege explicitly. They cannot run a particular type of SQL statement, or access an object that belongs to another user, run a PL/SQL package, and so on.

A user can receive a privilege in the following ways:

- **System privileges**. These privileges allow the grantee to perform a particular action or to perform an action on any schema objects of a particular type. (ALTER ANY TABLE, DROP ANY INDEX, UPDATE ANY TABLE, …).
- **Object privileges**. Each type of object has privileges associated with it (SELECT, DELETE, EXECUTE, …).
- **User roles**. A role groups several privileges and roles, so that they can be granted to and revoked from users simultaneously (CONNECT, RESOURCE, DBA, …).
- **PUBLIC**. This is a logical user group that represents all users in the database. Any privilege granted to PUBLIC is automatically granted to all users in the database.

Copyright © 2013 by Klee Associates, Inc.

www.JDEtips.com

During JD Edwards installation, several users are created that own objects for the different JD Edwards environments. The table below shows the four default environments with their associated schemas.

EnterpriseOne Environment	**Business Data Owner**	**Control Tables Owner**	**Central Objects Owner**	**Versions Owner**
PS910 (*Pristine Environment*)	PS910DTA	PS910CTL	PS910	PS910
DV910 (*Development Environment*)	TESTDTA	TESTCTL	DV910	DV910
PY910 (*Prototype Environment*)	CRPDTA	CRPCTL	PY910	PY910
PD910 (*Production Environment*)	PRODDTA	PRODCTL	PD910	PD910
Common Schemas	DD910, OL910, SY910, SVM910			
Other users *	JDE, APPLEAD, JDEDBA, PRODUSER, DEVUSER			

Default EnterpriseOne Environments with Their Respective Schemas

In fact, JD Edwards default installation grants full access control to all users on all schemas, unlike the access supposed to be granted as per the above table. This gets applied during JD Edwards installation by granting all system privileges and all roles to each JD Edwards database user and by providing PUBLIC all object privileges to all schemas. Let's review the different privileges assigned for an EnterpriseOne 9.1 database.

To list system privileges granted for a specified user, use the following SQL statement:

```
SELECT * FROM sys.dba_sys_privs WHERE GRANTEE = 'username';
```

While checking the system privileges for JD Edwards database users, you can notice that all system privileges are granted to all these users. Figure 1 shows the output of the above script when using 'PS910DTA' as *username*.

JDEtips Knowledge Express

This Article Continues…

Subscribers, log in from our main search page to access the full article:

www.JDEtips.com/MyAccess.html

Not a Subscriber? Gain access to our full library of JDE topics:

www.JDEtips.com/JD-Edwards-Library

Visit **www.JDEtips.com** for information on the JDEtips University schedule, private training and consulting, and our Knowledge Express Document Library.

License Information: The use of JDE is granted to JDEtips, Inc. by permission from J.D. Edwards World Source Company. The information on this website and in our publications is the copyrighted work of JDEtips, Inc. and is owned by JDEtips, Inc.

NO WARRANTY: This documentation is delivered as is, and JDEtips, Inc. makes no warranty as to its accuracy or use. Any use of this documentation is at the risk of the user. Although we make every good faith effort to ensure accuracy, this document may include technical or other inaccuracies or typographical errors. JDEtips, Inc. reserves the right to make changes without prior notice.

Oracle and J.D. Edwards EnterpriseOne and World are trademarks or registered trademarks of Oracle Corporation. All other trademarks and product names are the property of their respective owners.

Copyright © by JDEtips, Inc.