Data Security In Oracle Internet Directory

Integration with Oracle Database Vault and Transparent Data Encryption

An Oracle White Paper
November 2007

ORACLE

Data Security In Oracle Internet Directory

INTRODUCTION

Oracle Internet Directory (OID) is Oracle's LDAPv3 Directory Server implementation, which leverages Oracle Database as its backend data store. OID has a rich set of directory security features that includes support for comprehensive Access Control Policies, secure authentication mechanisms, encrypted attributes, password policies and features that help harden the Directory Server deployment. OID Access Control Policies can be setup to restrict access to the Directory super user (cn=orcladmin) as well. In addition to these application security features, we require superior data security features to protect the directory data from privileged users who have direct access to the data store and also to protect data on disk as well as on backups. In this paper, we describe OID uptake of two key Oracle Database data security features viz. Database Vault and Transparent Data Encryption. The use of these two data security features ensure that the data stored in OID is secure and cannot be compromised either due to insider threats or due to loss of physical data backups.

Oracle Database is the leading Database product in the industry with 30 years of innovation in the areas of data management and security. Oracle Database Vault feature helps protect data against "insider threats" and Transparent Data Encryption help protect data on the physical files.

Oracle Database Vault

Oracle Database Vault helps protect data against insider threats, meet regulatory compliance requirements and enforce separation of duty. This enabled via the following key features –

- Restricting the DBA and other privileged users from accessing application data
- Preventing application administrators from manipulating the database and accessing data of other applications
- Providing better control on who, when and where an application can be accessed

By defining Realms around application schema, one can prevent privileged users from accessing application data. Oracle Database Vault Rules and

Factors can be used in a flexible and adaptable manner to enforce authorization requirements.

Transparent Data Encryption

This Oracle Database feature enables the protection of sensitive data by encrypting data in physical operating system files, preventing unauthorized decryption and managing encryption keys. Thus, straightforward data encryption/decryption without requiring users to manage encryption keys is enabled thereby allowing key regulatory compliance requirements and protection of data on disk as well as backups to be addressed quickly, easily and effectively.

PROTECTING OID DATA USING ORACLE DATABASE VAULT

Oracle Database Vault addresses some of the most difficult security problems present in modern corporate IT deployments. With Oracle Database Vault, Realms and Rules can be created to enforce separation of duties, apply fine-grained access control on sensitive data and thus reduce the risk of insider threats.

A Database Vault Realm can be set up around the 'ODS' database schema used by OID. Only the 'ODS' database account has the privilege to access this data while other administrators with SELECT ALL privileges cannot. OID enforces access control in the LDAP protocol layer through its Access Control Framework. However, when data is directly queried from the database using SQL*PLUS, the OID Access Control Framework is bypassed. Oracle Database Vault can be used to restrict access in such scenarios. For instance, while an OID administrator should not be allowed to query any data from the database directly, the OID server, which uses the same database 'ODS' account, should have complete access to the same data.

In addition to the above, the OID server allowed to access the database should be restricted to a known host. This prevents a malicious program on a different host gaining access to the database using correct OID credentials.

All of the above can be achieved by creating **Oracle Database Vault Rules**. A summary of the security features Oracle Database Vault brings to OID can be seen in the comparison Table 1 below:

Table 1: Database Vault And OID

	With Oracle Database Vault	Without Oracle Database Vault
OID Database DBA reading sensitive information stored in OID by directly accessing the Database	×	✓
Other Database privileged users reading sensitive information stored in OID by directly accessing the Database	×	✓
Malicious hosts accessing information using compromised OID database credentials	×	✓

How to Configure Oracle Database Vault For OID

This section details the steps required in configuring Oracle Database Vault to protect OID data.

Software Requirements

Oracle Database – RDBMS v10.2.0.3

Oracle Internet Directory – OID v10.1.4.2

OracleAS Repository Creation Assistant – RepCA v10.1.4.0.1

Oracle Database Vault v10.2.0.3

Installation And Configuration – Database, OID and Database Vault

1. Install Oracle Database v10.2.0.1
    a. Install Oracle Database v10.2.0.1
    b. RepCA requires Ultra Search schema i.e. WKSYS and WKPROXY schemas to be present in the Database. Hence, after Database 10.2.0.1 installation is done, install the Ultra Search option from the RDBMS 10.2 companion CD.
        i. Choose the option "Oracle Database 10g Products 10.2.0.1.0" when installing the database options from the companion CD.
        ii. Once the installation is complete, install the Ultra Search option into the Database using $ORACLE_HOME/bin/dbca as follows –

- Step 1: - select "Configure Database Options" and click "Next"
- Step 2: - select the database that you want to configure and click "Next"
- Step 3: - select "Oracle Ultra Search" component and respective tablespace and click "Next"
- Step 4: - specify WKSYS password and click "Next"
- Step 5: - select database connection mode and click "Finish"

2. Install Oracle Database patch-set v10.2.0.3
3. Use RepCA v10.1.4.0.1 to install OID schema into the Database
    a. Please refer *"Oracle® Application Server Metadata Repository Creation Assistant User's Guide 10g (10.1.4.0.1) for UNIX"*
    b. In step 2 of RepCA configuration, choose the "load" option to load OracleAS Metadata Repository schemas into the database.
    c. RepCA checks for specific db parameter values and these are documented in the user's guide stated in a. above. You should set these properly to ensure that RepCA is successful.

    Note: Note that using SGA tuning using sga_max_size and sga_target doesn't seem to work for RepCA. db_cache_size is required to be greater than 144 MB. You can revert back to SGA tuning if you choose to once RepCA execution is successfully completed.
4. Install OID v10.1.4.0.1 with "IM only" option against the Database created above
5. Install OID v10.1.4.2 patch-set
6. Install Oracle Database Vault

    Please refer to "**Oracle® Database Vault Installation Guide 10*g* Release 2 (10.2) for Linux x86"** for details on the installation of Oracle Database Vault. If you are using platforms other than Linux x86, please refer to the appropriate platform documentation on Oracle Database Vault. There are several pre-requisites and pre-installation steps documented in this installation guide, please ensure that everything is adhered to carefully.

    Note: Ensure that you set and remember the Database Vault Owner account name and password.

Enabling Oracle Database Vault For OID Database

Please refer to Appendix B of "**Oracle® Database Vault Administrator's Guide 10*g* Release 2 (10.2)"** for the procedure to enable Database Vault. Please refer to this guide for details on Database Vault administration.

Adding Database Vault Policies For OID

Oracle provides scripts to apply the required Database Vault policies for OID. These scripts are located in the OID 10.1.4.2 installation under $ORACLE_HOME/ldap/datasecurity.

To apply the Database Vault policies to OID Database, all you need to do is step 1 and optionally step 2.a. given in this section below:

1. To create the default Database Vault Realm for OID, follow the steps given below –
    a. Open `dbv_oid_rule.sql` and replace the dummy IP address in "Check ods connections" and "Check ods connections 2" Rules with the hostname or IP address that OID binaries are active on. Create a backup copy of dbv_oid_rule.sql before editing it.
    b. Execute `dbv_create_oid_policies.sql` by connecting to the Database as the Database Vault Owner
2. Note that the above policies will disable SQL*PLUS access to the OID Database altogether. However, you may require SQL*PLUS access to the OID Database for some tasks to be performed as 'ODS' user. If so, you can enable SQL*PLUS access to the OID Database from specific host or hosts only.
    a. To enable connectivity to the OID Database using SQL*PLUS tool, follow the steps given below –
        i. Open `dbv_oid_rule_sqlplus.sql` , replace the dummy IP address in "Check ods connections 3" Rule with the hostnames or IP addresses from where you desire to allow SQL*PLUS access to OID Database.
        ii. Execute `dbv_oid_rule_sqlplus.sql` by connecting to the Database as the Database Vault Owner
    b. If you want to block SQL*PLUS access completely to the OID Database at some point, then follow the step given below –
        i. Execute `dbv_oid_delete_rule_sqlplus.sql` by connecting to the Database as the Database Vault Owner

Note: Once the Database Vault policies for OID is installed, disabling and enabling Database Vault does not require deleting and adding the OID policies, once added the policies will be in effect whenever Database Vault is enabled.

Deleting Database Vault Policies For OID

To remove the Database Vault policies for OID installed in the prior section, execute `dbv_delete_oid_policies.sql` by connecting to the Database as the Database Vault Owner

Disabling Oracle Database Vault For OID Database

Please refer to Appendix B of "**Oracle® Database Vault Administrator's Guide 10*g* Release 2 (10.2)"** for the procedure to disable Database Vault.

OID And Database Vault – Limitations And Best Practice Recommendations

Product Upgrades and Patch-set Installs

It is strongly recommended that the Database Vault be disabled before performing OID or Database upgrades or patch-set installations. One-off patch installation should normally not have this requirement.

After the upgrade or patch-set installation is complete, the Oracle Database Vault can be enabled once again.

Using OID Bulkload Tool

Using OID 'bulkload' tool is the fastest way to load data in bulk into OID. Due to some limitations, the performance of 'bulkload' is poor when the Database Vault policies are active for OID. This is due to the fact that SQL*LDR "direct path" mode does not work when Database Vault is enabled. Hence, if there is a requirement to load a large amount of data (ex. several 100K or Millions of entries), then it is recommended that the Database Vault be disabled before performing the bulk load. The Database Vault can be enabled after bulk load is successful.

OID Multi-master Replication Setup

During the "add-node" and "delete-node" procedures of OID Multi-master replication setup, Oracle Database Vault must be disabled on the node that is either being added to the multi-master ring or being deleted from the multi-master ring. Once the setup is complete, the Database Vault can be enabled.

PROTECTING OID DATA USING TRANSPARENT DATA ENCRYPTION

Transparent Data Encryption enables us to encrypt sensitive data stored in Oracle Database. OID stores all directory data in Oracle Database, and this data can be protected by using Transparent Data Encryption. No one, including the most privileged system administrators, can retrieve the information directly from the encrypted operating system files.

How to Configure TDE For OID

This section details the steps required in configuring Transparent Data Encryption to protect OID data.

Software Requirements

Oracle Database – RDBMS v10.2.0.3

Oracle Internet Directory – OID v10.1.4.2

OracleAS Repository Creation Assistant – RepCA v10.1.4.0.1

Installation And Configuration

1. Install Oracle Database v10.2.0.1
    a. Install Oracle Database v10.2.0.1
    b. RepCA requires Ultra Search schema i.e. WKSYS and WKPROXY schemas to be present in the Database. Hence, after Database 10.2.0.1 installation is done, install the Ultra Search option from the RDBMS 10.2 companion CD.
        i. Choose the option “Oracle Database 10g Products 10.2.0.1.0” when installing the database options from the companion CD.
        ii. Once the installation is complete, install the Ultra Search option into the Database using $ORACLE_HOME/bin/dbca as follows –
            - Step 1: - select "Configure Database Options" and click "Next"
            - Step 2: - select the database that you want to configure and click "Next"
            - Step 3: - select "Oracle Ultra Search" component and respective tablespace and click "Next"
            - Step 4: - specify WKSYS password and click "Next"
            - Step 5: - select database connection mode and click "Finish"

2. Install Oracle Database patch-set v10.2.0.3
3. Use RepCA v10.1.4.0.1 to install OID schema into the Database
    c. Please refer *"Oracle® Application Server Metadata Repository Creation Assistant User's Guide 10g (10.1.4.0.1) for UNIX"*
    d. In step 2 of RepCA configuration, choose the "load" option to load OracleAS Metadata Repository schemas into the database.
    e. RepCA checks for specific db parameter values and these are documented in the user's guide stated in a. above. You should set these properly to ensure that RepCA is successful.

       Note: Note that using SGA tuning using sga_max_size and sga_target doesn't seem to work for RepCA. db_cache_size is required to be greater than 144 MB. You can revert back to SGA tuning if you choose to once RepCA execution is successfully completed.
4. Install OID v10.1.4.0.1 with "IM only" option against the Database created above
5. Install OID v10.1.4.2 patchset

Encrypting OID Data Using Transparent Data Encryption

Oracle provides scripts that enable the use of OID with Transparent Data Encryption. These scripts are included in the OID 10.1.4.2.0 Patch-set and they can encrypt and decrypt all the columns containing OID data.

For details on Transparent Data Encryption, please refer to "Oracle® Database Advanced Security Administrator's Guide 10*g* Release 2 (10.2)"

To encrypt the data in OID, follow the steps given below –

1. Set the Database wallet location in the Database ORACLE_HOME. Oracle recommends that a separate wallet be used exclusively for Transparent Data Encryption.
    a. To use a separate Database Wallet for Transparent Data Encryption, set the parameter `ENCRYPTION_WALLET_LOCATION` in sqlnet.ora. For example –

```
ENCRYPTION_WALLET_LOCATION=
      (SOURCE=(METHOD=FILE)(METHOD_DATA=
        (DIRECTORY=/install/db1023/dbs)))
```

b. To use the same Database Wallet shared by all Oracle components, set the parameter `WALLET_LOCATION` in sqlnet.ora. For example –

```
WALLET_LOCATION=
      (SOURCE=(METHOD=FILE)(METHOD_DATA=
        (DIRECTORY=/install/db1023/dbs)))
```

2. Login to SQL*PLUS as a user who has the ALTER SYSTEM privilege and execute the following command –

   ```
   ALTER SYSTEM SET ENCRYPTION KEY IDENTIFIED BY
   <yourwalletpassword>;
   ```

3. Shutdown all OID processes in the OID ORACLE_HOME

   a. If you are using OPMN for process control -

      ```
      $ORACLE_HOME/opmn/bin/opmnctl stopproc
      ias-component=OID
      ```

   b. If you are using OIDMON/OIDCTL instead of OPMN for process control –

      ```
      OIDMON connect=<db-conn> stop
      ```

4. In the OID ORACLE_HOME, deploy the 'tdeoid' package by connecting to the OID Database as 'ODS' user and executing the SQL script $ORACLE_HOME/ldap/admin/oidttde.sql

5. Encrypt OID data by executing the following command by connecting to the OID Database as 'ODS' user –

   SET SERVEROUTPUT ON SIZE 1000000;

   EXECUTE ODS.TDEOID.ENCRYPT();

   Note: This step may take a while depending on the number of entries existing in OID. Please also see the "Performance" section later in this paper.

   Note: If you hit ORA-01555 during the execution of ods.tdeoid.encrypt(), increase the UNDO tablespace and re-run ods.tdeoid.encrypt() which will encrypt only the tables that are not encrypted.

   Note: If there are attribute values that are of length greater than 3932 characters, the above command will error out. Please see "Limitations" section later in the paper for more details.

   Note: Every time the Database is bounced (stopped and restarted), the database wallet must be opened. To open the Database wallet, login to SQL*PLUS as a user who has ALTER SYSTEM privilege and execute the following command –

```
ALTER SYSTEM SET ENCRYPTION WALLET OPEN
IDENTIFIED BY <yourwalletpassword>;
```

6. Startup all OID processes
7. Subsequently, every time an attribute is indexed or cataloged in OID using the OID tool 'catalog', step 4 above must be executed to encrypt the data in the added catalog table. The tdeoid.encrypt() procedure takes care of encrypting only the unencrypted tables.

Disabling Transparent Data Encryption

To disable encryption of OID Data and to decrypt the encrypted data, execute the following command by connecting to the OID Database as 'ODS' user –

EXECUTE ODS.TDEOID.DECRYPT();

Note: This step may take a while depending on the number of entries existing in OID. Please also see the "Performance" section later in this paper.

TDE And OID – Limitations And Best Practice Recommendations

Dynamic Groups

Dynamic Group membership can be specified using two methods in OID viz. using a 'labeledURI' attribute or by using the 'CONNECT_BY' assertion. When OID Data is encrypted, then the 'CONNECT_BY' assertion is not supported. For more details on Dynamic Groups in OID, please refer to OID Administrator's Guide 10g (10.1.4.0.1).

Maximum Attribute Value Length

Attributes other than binary attributes, are limited to a maximum value length of 4000 in OID. When OID Data is encrypted, the maximum value length of non-binary attributes is reduced to 3932. The tdeoid.encrypt() procedure will take care of ensuring that the reduced size comes into effect.

Using OID Bulkload Tool

Using OID 'bulkload' tool is the fastest way to load data in bulk into OID. Due to some limitations, the performance of 'bulkload' is slower when OID Data is encrypted. However, using 'bulkload' tool to populate the directory after encryption is enabled is still the faster approach, especially if the number of entries in OID exceeds several hundreds of thousands.

Enabling encryption first and then performing 'bulkload' is more optimal for run time LDAP operations as well as minimizing Database tablespace size overhead.

CONCLUSION

Given the mission critical nature of modern corporate IT deployments, the importance of data security and adherence to regulatory requirements is heightened. Keeping with Oracle's commitment to enabling customers keep abreast with these requirements, this paper described how the Database Vault and Transparent Data Encryption features for Oracle Database could be leveraged to further harden Oracle Internet Directory deployments.

First, the potential issues in existing deployment practices were identified and briefly described. Next, the means to address those issues using were identified and the steps to do so were described in detail. Best practices and Limitations were also discussed. Finally, a brief analysis of the performance implications was provided.

Oracle Internet Directory v10.1.4.2 Integration with Oracle Database Vault and Transparent Data Encryption
November 2007
Authors: Paul Li, Ajay Keni
Contributors: Buddhika Kottahachchi

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com