Oracle® E-Business Suite Concepts

Security

Introduction

The foundation of security is *access control*, which refers to how the system is being accessed and by whom. User security consists of three principal components: *authentication*, *authorization* and an *audit trail*. Authentication validates the user's identity, authorization controls the user's access based on responsibilities assigned, and the audit trail keeps track of the user's transactions to ensure that the user's privileges are not being misused.

Security Strategies

The Oracle E-Business Suite tables are no different from any other Oracle database tables, as far as a DBA is concerned, and the same security issues that apply to Oracle database installations also apply to Oracle E-Business Suite installations. While the Oracle database provides multiple mechanisms to ensure security, recovery, and high availability of databases, no amount of technology can completely protect against human problems (error or sabotage), or poor disaster recovery and corporate security policies. This section describes a number of factors that should be taken into account when designing and implementing a security policy.

Additional Information: For further details of recommended security practices and strategies, see My Oracle Support Knowledge Document 403537.1, *Best Practices For Securing Oracle E-Business Suite Release 12*.

Basic Strategies

There are several basic steps that can be taken to enhance the security of an Oracle E-Business Suite database, as outlined below.

Simply restricting the availability of the passwords for accounts with DBA privileges is an important first step in implementing security-oriented DBA access policies. This can then be extended by setting up procedures for *auditing* DBA actions, as described later in this section.

DBAs should generally use named accounts at the OS level, and the use of privileged operating system accounts such as root, oracle, applmgr should be tightly regulated. Where named accounts are not feasible, limited access accounts should be used.

Common tasks that require elevated privileges should wherever possible be performed via delegation mechanisms such as Oracle Enterprise Manager or sudo. Where this is not feasible, auditing should be used to track performance of privileged tasks.

For example, Oracle E-Business Suite requires the APPS password and access to the applmgr operating system account to start and stop application tier services such as the Concurrent Processing server. An Oracle Enterprise Manager script or sudo script can be used to start and stop the Concurrent Processing server without requiring the user to know the APPS password or have direct access to the applmgr account.

Note: For further details, see My Oracle Support Knowledge Document 950018.1, *Using Database Vault with Oracle E-Business Suite*.

Patching

Applying patches to Oracle E-Business Suite requires the person performing the patching (normally, the DBA) to provide the passwords for the APPS account and (if on AD-TXK Delta 13 or later) the EBS_SYSTEM account or (if on an earlier AD-TXK release update pack) the SYSTEM account. All these accounts are highly privileged. It is possible to keep the passwords to these accounts secret until just before the patching process begins, at which point the passwords are changed to temporary values that are communicated to the DBA. When patching is complete, the passwords are set back to their previous values. This procedure adds only a few minutes to the patching process, and can help improve security in cases where the DBA is, for example, located in a different country, but it should not be relied on for complete protection of data: the DBA could still carry out unauthorized actions, immediately before or after the patching operation. Therefore, additional safeguards such as auditing and keystroke logging may be advisable during patching operations.

Auditing DBA Activity

Oracle Database 11g includes features that can be used to track DBA actions. The audit trail, mentioned earlier, should not be used in place of procedures for hiring trustworthy DBAs, but can be a useful adjunct to them.

Oracle recommends that you strongly protect your audit trail records wherever they are stored. The most secure location for the audit trail, in terms of keeping the content from DBAs, is the operating system's own audit trail or operating system files. Oracle recommends that the database server should write audit records to the operating system, and the file to which Oracle writes audit records should have suitable operating system file protection.

Using an operating system audit trail requires a simple change of the AUDIT_TRAIL database initialization parameter from "DB" to "OS", and prevents privileged database users from reading, modifying or deleting audit records. However, this strategy is ineffective for users who have extensive operating system privileges. Also, the query advantage that SQL brings to audit analysis is lost, unless you have an operating system audit analysis tool that can read Oracle-generated operating system audit records.

The Human Aspect

While technical measures such as those already mentioned can and should be used to restrict DBA actions and selectively audit DBA activity, it is important to remember that DBAs serve in positions of trust. Organizations must therefore take appropriate steps to ensure that persons assigned to such positions are worthy of trust. A company's data is just as sensitive and valuable as trade secrets; indeed, data should often be treated as the most closely-guarded secret. Therefore, the same checks should be made on DBAs as are made on staff given access to corporate secrets.

DBAs need to have extensive privileges to do their jobs; this also means that they can carry out destructive actions on a database, either by accident or intentionally. Such actions can directly and seriously impair an organization's ability to carry on with its business. For example, if your customer database is accidentally corrupted, and no backups have been made, you may lose vital customer information and not be able to fulfil orders.

If regulatory compliance or other reasons require DBA access to be restricted, optional features such as Oracle Database Vault and Transparent Data Encryption (both described elsewhere in this chapter) may be employed as part of a comprehensive approach to security that includes policies and practices to meet auditing, segregation of duties, and other business requirements.

Authentication

Identifying and verifying who is allowed to access the system is the first line of defense. The most common approach is *password-based authentication:* if the legitimate user is the only one who knows the password, then whoever just entered the correct password is very likely to be the person authorized to use the account.

A number of practical problems can arise with passwords. These include:

- Passwords that are allowed to be too short, and thus vulnerable to being observed on entry
- Passwords that are forced to be too long, and which the user might decide to write down
- Easy-to-guess passwords, chosen as being easy to remember
- Rarely changed passwords
- Passwords that are used for multiple accounts

In a single-sign on environment (see Chapter 8), a single password allows access to more than one application, so the consequences of it being discovered or divulged are proportionately much more serious.

An attacker will generally focus on identifying the password of a powerful user such as a system administrator. Such users are generally more aware of security risks, and can be persuaded to take more care in their choice of password and to change it regularly. The Oracle E-Business Suite features various password management policies that can be enabled to secure key user accounts.

Authorization

On entering the system, the user should only be granted access to the features and specific data needed to perform his job. Routine access to highly sensitive data should only be given to trusted users who need that level of access. The *Function Security* feature allows the System Administrator to manage the access privileges of individual users. By enforcing tighter security policies for more sensitive accounts, Function Security can mitigate the risk of unauthorized users' access to highly sensitive information.

Audit Trail

Even the most carefully planned user authentication and authorization policies cannot eliminate the risk of exploitation when the attacker is an authorized user. An *audit trail* can be used to keep track of a user's transactions to verify that the user is not misusing his access privileges. Oracle E-Business Suite can record details of every user's login, including time stamp, session ID, and information about the Function Security rules applying to that session. Information about the identity of the user is also attached to all transactions. This provides a method for detecting the party responsible for any transaction, or determining which users viewed sensitive data in a given time period.

If a valid user password has been compromised, and becomes known to an unauthorized person, it can be difficult to trace the intrusion back to the attacker. However, knowing the particular account that was used can help to identify other people who may have learned that user's password.

Additional Information: For further details of Audit Trail, see *Oracle E-Business Suite Security Guide*.

Network Security

An organization may or may not have physical control over the network infrastructure in use. The Internet is the best example of a network where it will not have control, and where extra steps must be taken to ensure security is not compromised.

A common concern regarding use of a public network such as the Internet is the possibility of someone eavesdropping on password transmissions by using a network sniffer. In such a case, though, the concern should be wider, and reflect the possibility of someone eavesdropping on sensitive information in general. In such cases, HTTPS (Secure HTTP) connection to Oracle E-Business Suite is recommended. All current browser-based password login screens send the password as a parameter in the HTTP form submission. Using an HTTPS connection will encrypt this information. The best practice is therefore to use HTTPS for all web-based access. On the other hand, if you have control over your network to the point where you can rule out eavesdropping, then password interception should not be an issue.

Oracle User Management

Oracle User Management (UMX) is a secure and scalable system that enables organizations to define administrative functions and manage users based on specific requirements such as job role or geographic location.

With Oracle User Management, instead of exclusively relying on a centralized administrator to manage all its users, an organization can, if desired, create *functional administrators* and grant them sufficient privileges to manage a specific subset of the organization's users. This provides the organization with a more granular level of security, and the ability to make the most effective use of its administrative capabilities.

A login assistance mechanism is easily accessed from the Oracle E-Business Suite Login Page. A user simply clicks on the "Login Assistance" link located below the Login and Cancel buttons, and can then go to a Forgot Password section or Forgot User Name section to have the necessary action taken automatically, without the need for an administrator to become involved.

Another feature allows users with the relevant privileges to enable other users to act on their behalf, as delegates, without having to share the account password. For example, managers may need to grant peers or subordinates limited authority to act on their behalf while they are out of the office. This *Proxy User* feature allows control over the pages, functions, and data security policies that can be granted, and includes an on-screen display that indicates when a user is acting on behalf of another user.

Role Based Access Control

Oracle User Management implements several different layers of security, requiring organizations to specify:

- The set of users that will be granted access to specific areas of Oracle E-Business Suite
- The information these users will require to do their jobs
- The extent to which the users can use this information

Oracle's function and data security models constitute the base layers of this system, and contain the traditional system administrative capabilities.

Organizations can optionally add more layers to the system depending on the degree of flexibility they require. *Role Based Access Control* (RBAC) enables organizations to create roles based on specific job functions, and to assign these roles the appropriate permissions. With RBAC, administrative privileges and user access are determined by assigning individuals the appropriate roles.

Key features of RBAC include:

- **Delegated Administration** - Enables system administrators to delegate some of their administrative privileges to individuals that manage a subset of the organization's users.
- **Registration Processes** - Enable organizations to provide end-users with a method for requesting various levels of access to the system, based on their eligibility.
- **Self-Service Requests and Approvals** - Enable end users to request initial access or additional access to the system by clicking on links embedded in a Web application.

Database Security Features

The Oracle database has always included mechanisms to protect its contents from unauthorized access, without hindering access by legitimate users. Details of these can be found in the standard database documentation.

Optional database features can be used to enhance and customize security to meet the specific needs of a site:

- *Transparent Data Encryption*, - a feature that can be used either to encrypt all content stored in a particular tablespace, or only the data stored in specific database columns.
- *Oracle Database Vault* - a feature that can be used to help address security issues such as insider threats, regulatory compliance requirements, and enforced separation of duties.

These two features will be discussed next.

Oracle Database Vault

Oracle E-Business Suite Release 12.0.4 and higher support *Oracle Database Vault*, a feature that can be used to help address security issues such as insider threats, regulatory compliance requirements, and enforced separation of duties. A number of flexible options enable you to apply fine-grained access control to sensitive data. In particular, Oracle Database Vault can be employed to protect sensitive data from unauthorized access by privileged users, while still allowing them to maintain your Oracle databases.

Oracle Database Vault uses realms (groupings of Oracle objects) to provide an internal firewall that prevents unauthorized access to specific application data. These realms can be supplemented with command rules - for example, classes of commands (such as INSERT, UPDATE, DELETE, DROP) can be prohibited. The command rules can, in the form of rule sets, help ensure that DBAs do not perform DML within the realm.

Effective use of Oracle Database Vault requires an initial evaluation of the privileges required for the various roles involved in administering the database and applications. These roles should be chosen to minimize the requirement to use generic database accounts (APPS, APPLSYS, EBS_SYSTEM, SYSTEM, and the product schema accounts). Use of Oracle Database Vault should be combined with organization-specific processes to provide a more complete security solution. For example, DBAs should use specific named accounts wherever possible, which assists with the provison of realms and simplifies the ability to audit activities.

Some DBAs will require little or no access to applications data.These include roles that focus on administration of third-party software, or database administration and tuning. The default realms shipped with Oracle E-Business Suite prevent DBAs from viewing any applications objects.

Oracle E-Business Suite DBAs who need access to a defined subset of applications data (for example, the FND tables) can be given access to a realm that provides access to this subset of tables. The are two strategies for accomplishing this. The most controlled way to do this is by defining specific objects in the Oracle E-Business Suite application to which DBAs are allowed access so they can perform particular roles. The named DBA accounts should be granted access to a realm that provides access to that data specifically.

An alternative approach, which is easier to maintain if the DBAs need access to a large number of applications tables, involves modification of the shipped realms to create a list of tables that contain sensitive information to which DBAs are *not* permitted to have access. However, this strategy is less rigorous as by default it allows rather than denies access to objects.

Oracle E-Business Suite delivers pre-defined realms for the integration with Oracle Database Vault. With AD-TXK Delta 13 and later, integration with Oracle Database Vault is simplified with two predefined realms. With earlier AD-TXK release update packs, five predefined realms were recommended.

Additional Information: For further details, see the following My Oracle Support knowledge documents as applicable:

- Doc ID 2727580.1, *Integrating Oracle E-Business Suite Release 12.2 with Oracle Database Vault using EBS_SYSTEM*
- Doc ID 2617770.1, *Integrating Oracle E-Business Suite Release 12.2 with Oracle Database Vault 19c*
- Doc ID 2131435.1, *Integrating Oracle E-Business Suite Release 12.2 with Oracle Database Vault 12c*

Transparent Data Encryption

For fields containing sensitive information (such as credit card numbers), it may be desirable to encrypt the data stored.

Currently, Oracle E-Business Suite does not automatically encrypt data. Optionally, *Transparent Data Encryption* (TDE) functionality can be used to encrypt selected areas of the database. As the encryption is transparent to the application, code does not have to be rewritten to provide the encryption, and existing SQL statements should work without modification.

Two encryption strategies are available:

- **TDE Tablespace Encryption** is used to encrypt all content stored in a particular tablespace.
- **TDE Column Encryption** is used to encrypt only specific database columns, typically those that contain sensitive data.

Note: For further details, see My Oracle Support Knowledge Documents 828229.1, *Using TDE Tablespace Encryption with Oracle E-Business Suite Release 12*, and 732764.1, *Using TDE Column Encryption with Oracle E-Business Suite Release 12*.

(#)

About Oracle (http://www.oracle.com/corporate/index.html) | Contact Us (http://www.oracle.com/us/corporate/contact/index.html) | Legal Notices (http://www.oracle.com/us/legal/index.html) | Terms of Use (http://www.oracle.com/us/legal/terms/index.html) | Your Privacy Rights (http://www.oracle.com/us/legal/privacy/index.html) | Cookie Preferences (#) | Ad Choices (https://www.oracle.com/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html#12) |

Copyright © 2025, Oracle and/or its affiliates. (http://www.oracle.com/pls/topic/lookup?ctx=cpyr&id=en)