Backup and Recovery Scenarios for Oracle WebLogic Server: 10.3

An Oracle White Paper
January, 2009

Maximum Availability Architecture

Oracle Best Practices For High Availability

Backup and Recovery Scenarios for Oracle WebLogic Server

INTRODUCTION

The goal of this document is to provide backup and recovery procedures for Oracle WebLogic Server 10.3 deployments. It discusses the mechanism, frequency, and mode for performing backups. It also provides the recovery steps for protection from the most common failure scenarios.

TERMINOLOGY

The following sections describe the terminology used in this document.

Backup Modes

Typical modes are online and offline. All the servers in the domain should be down while performing offline backups.

Oracle WebLogic Server Components

Components in Oracle WebLogic Server (WLS) refer to:

Administration Server

Managed Server

JMS Server

Application artifacts (ear/war files)

Application Customizations (such as datasources.xml)

BACKUP AND RECOVERY APPROACH

Any file system copy mechanism can be used to backup the suggested artifacts. You can also take incremental backups if it is desired.

CONCEPTS

The following sections describe concepts related to backup and recovery.

Administration Server and Console

The Administration Console is a Web browser-based, graphical user interface that you use to manage an Oracle WebLogic Server domain. An Oracle WebLogic Server domain is a logically related group of Oracle WebLogic Server resources that you manage as a unit. A domain includes one or more Oracle WebLogic Servers and may also include Oracle WebLogic Server clusters. Clusters are groups of Oracle WebLogic Servers instances that work together to provide scalability and high availability for applications. You deploy and manage your applications as part of a domain.

One instance of Oracle WebLogic Server in each domain is configured as an Administration Server. The Administration Server provides a central point for managing an Oracle WebLogic Server domain. All other Oracle WebLogic Server instances in a domain are called Managed Servers. The Administration Server hosts the Administration Console, which is a Web application accessible from any supported Web browser with network access to the Administration Server.

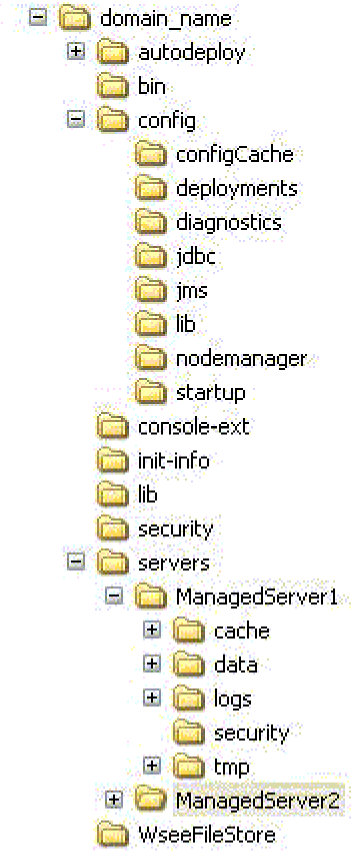
Node Manager

Node Manager is a Java utility that runs as separate process from Oracle WebLogic Server and allows you to perform common operations for a Managed Server, regardless of its location with respect to its Administration Server. While use of Node Manager is optional, it provides valuable benefits if your WebLogic Server environment hosts applications with high-availability requirements.

If you run Node Manager on a machine that hosts Managed Servers, you can start and stop the Managed Servers remotely using the Administration Console or the command line. Node Manager can also automatically restart a Managed Server after an unexpected failure.

WebLogic Domain Structure

The following figure shows the WebLogic domain directory structure:



```
domain_name
    autodeploy
    bin
    config
        configCache
        deployments
        diagnostics
        jdbc
        jms
        lib
        nodemanager
        startup
    console-ext
    init-info
    lib
    security
    servers
        ManagedServer1
            cache
            data
            logs
            security
            tmp
        ManagedServer2
    WseeFileStore
```

Please refer to the WebLogic Server Understanding Domain Configuration for more details. If the Managed Server resides in a host different from the Administration Server, then, at every Managed Server restart, the latest `servers` and `config` directory under the domain directory is pulled from the Administration Server.

Impact of Administration Server Failure

The failure of an Administration Server does not affect the operation of Managed Servers in the domain but it does prevent you from changing the domain’s configuration. If an Administration Server fails because of a hardware or software failure on its host machine, other server instances on the same machine may be similarly affected.

If an Administration Server for a domain becomes unavailable while the server instances it manages—clustered or otherwise—are running, those Managed Servers continue to run. Periodically, these Managed Servers attempt to reconnect to the Administration Server. For clustered Managed Server instances, the load balancing and failover capabilities supported by the domain configuration continue to remain available.

You can start a Managed Server even if the Administration Server is not running. In this case, the Managed Server uses a local copy of the domain’s configuration files for its starting configuration and then periodically attempts to connect with the Administration Server. When it does connect, it synchronizes its configuration state with that of the Administration Server.

MSI (Managed Server Independence) Mode

Managed Servers maintain a local copy of the domain configuration. When a Managed Server starts, it contacts its Administration Server to retrieve any changes to the domain configuration that were made since the Managed Server was last shut down. If a Managed Server cannot connect to the Administration Server during startup, it can use its locally cached configuration information—this is the configuration that was current at the time of the Managed Server's most recent shutdown. A Managed Server that starts up without contacting its Administration Server to check for configuration updates is running in *Managed Server Independence (MSI)* mode. By default, MSI mode is enabled. However a Managed Server cannot be started even in MSI mode for the first time if the Administration Server is down due to non-availability of the cached configuration.

Configuration Changes in Managed Server

Configuration changes are updated in Managed Server during the following events:

On each Managed Server restart, the latest configuration will be pulled from the Administration Server. This happens even when the Node Manager is down in the node where the Managed Server is running. If the Administration Server is unavailable during the Managed Server restart and if the MSI (Managed Server Independence) mode is enabled in the Managed Server, it starts up reading its local copy of the configuration and synchronizes with the Administration Server when it is available. By default MSI mode is enabled.

Upon activating every administrative change like configuration changes, deploy or redeploy of applications and topology changes, the Administration Server pushes the latest configuration to the Managed Server.

Existing Tools and Their Capabilities

The following sections describe the existing tools and their capabilities.

Configuration File Archiving

You can configure Oracle WebLogic Server to make backup copies of the configuration files. This facilitates recovery in cases where configuration changes need to be reversed or in the unlikely case that configuration files become corrupted. When the Administration Server starts up, it saves a JAR file named config-booted.jar that contains the configuration files. When you make changes to the configuration files, the old files are saved in the configArchive directory under the domain directory, in a JAR file with a sequentially numbered name such as config-1.jar. The configuration archive is always local to the Administration Server host. It is a best practice to back up the archives to an external location.

Pack and Unpack Utility

The pack command creates a template archive (.jar) file that contains a snapshot of either an entire domain or a subset of a domain. You can use a template that contains a subset of a domain to create a Managed Server domain directory hierarchy on a remote machine

BACKUP ARTIFACTS

It is important to understand how to back up critical data to protect the system against different failures. You can save backup artifacts in various ways—by using periodic backups to tape or fault-tolerant disks, or by manually copying files to another machine. The following sections describe the artifacts that you should back up.

Static Artifacts

Static artifacts are those that change less frequently. These include:

BEA_HOME (except USER_PROJECTS/domains/*domain_name*) for the Administration Server and all the Managed Servers

WLS product home (by default, it resides in BEA_HOME and it can be configured by the user to point to a different location) for the Administration Server and all the Managed Servers

This data is changed only while patching or upgrading the environment.

Runtime Artifacts

Runtime artifacts are those that change more frequently. These include:

USER_PROJECTS directory in all the servers (By default, it resides in BEA_HOME, but it can be configured by the user to point to a different location.)

Application artifacts (ear, war files, property files) which reside outside of the domain directory on each of the servers (in case of nostage or external_stage application staging modes)

This data changes frequently while updating the domain configurations, deploying an application, and while performing other administrative changes.

PERSISTENT STORES

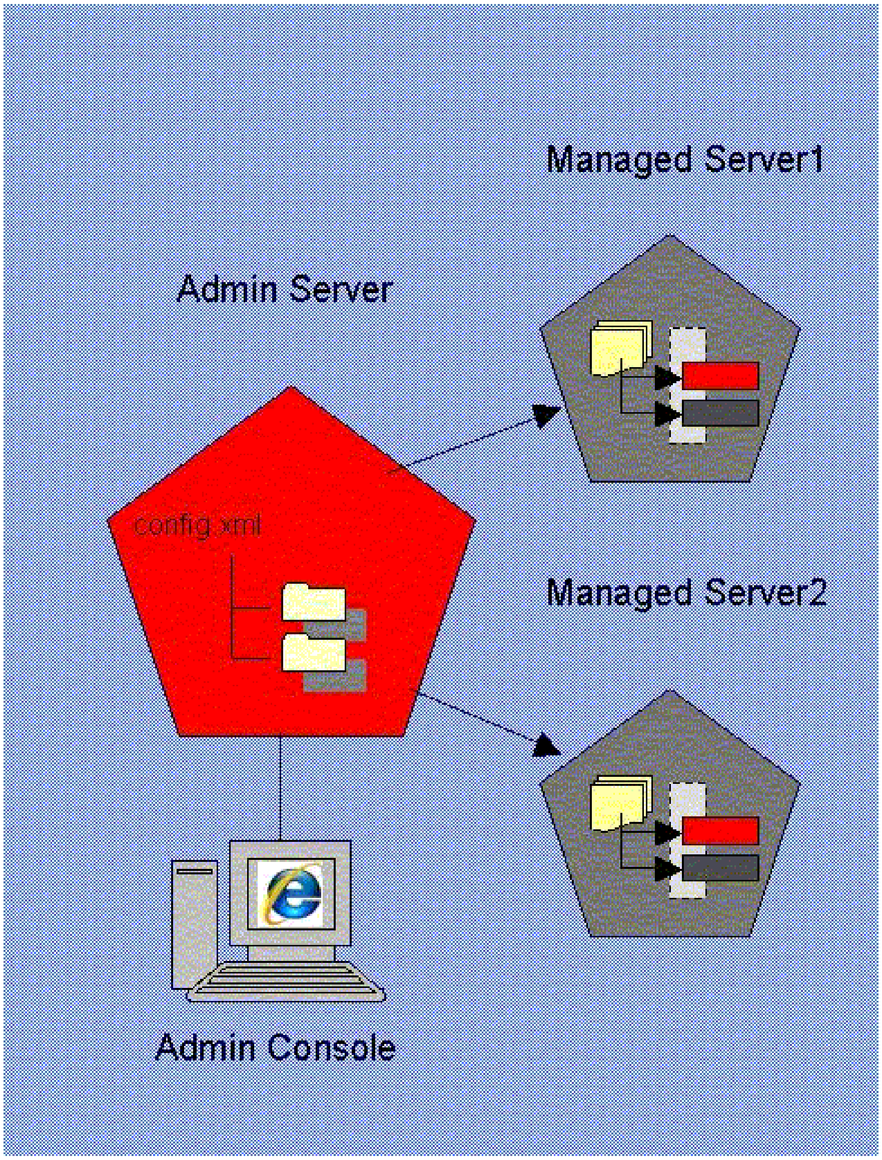
A persistent store provides a built-in, high-performance storage solution for WebLogic Server subsystems and services that require persistence. For example, it can store persistent JMS (Java Messaging Service) messages or durable subscriber information, as well as temporarily store messages sent to an unavailable destination using the Store-and-Forward feature. The persistent store supports persistence to a file-based store (File Store) or to a JDBC-enabled database (JDBC Store). The default store maintains its data in a data\store\default directory inside the *`servername`* subdirectory of a domain's root directory

EXTERNAL DATABASE DEPENDENCIES

The WebLogic Server environment may depend upon some external databases such as, Application database, JMS, and Oracle Internet Directory. Proper backup and recovery procedures should be in place for such databases to ensure proper functioning of the environment. Also, the consistency between domain configuration and database-specific configuration should be maintained wherever applicable. This document does not address database backup and recovery procedures.

SAMPLE TOPOLOGY

The following figure shows the topology that is referred to in the scenarios in subsequent sections. The sample topology has a domain with an Administration Server and two Managed Servers. All the servers reside in the same host.



BACKUP RECOMMENDATIONS

The following lists some of the common scenarios in a typical deployment that require performing a backup. It also describes the recommendations for backup and the type of backup mode (online or offline) for each scenario. All online backups can be done offline as well.

After WLS is installed and a domain is created

Backup: All of the static and runtime backup artifacts
Mode: Offline

Scheduled backups on a nightly basis or as needed, or both

Backup: All of the runtime backup artifacts

Mode: Online

Before and after making configuration changes to a component or cluster

Backup: All of the runtime backup artifacts

Mode: Online

Prior to deploying a custom pure Java EE application to a Managed Server or cluster

Backup: All of the runtime backup artifacts

Mode: Online

After any major architectural changes to deployment architecture (such as scale out, creation of servers, or creation of clusters)

Backup: All of the runtime backup artifacts

Mode: Online

Before and after product binary files (such as the WebLogic Home) are patched or upgraded

Backup: All of the backup artifacts

Mode: Offline

Before and after patching or upgrading (which may impact BEA home and database)

Backup: All of the backup artifacts

Mode: Offline

LDAP backup

If you are using the embedded LDAP server, then do not update the configuration of a security provider while a backup of LDAP data is in progress. If a change is made—for instance, if an administrator adds a user—while you are backing up the ldap directory tree, the backups in the ldapfiles subdirectory could become inconsistent.

Persistent Stores

It is currently not possible to take consistent backup of persistent stores for a system that uses JMS and transaction logs. This is because the transaction logs can only be file-based and the JMS can be either file-based or it can reside in the database. For highest reliability use a highly available fault-tolerant storage (for example, SAN) for JMS and transaction log file stores.

For clustered servers, WebLogic Server enables you to migrate a failing server, including the Transaction Recovery Service, to a new machine. When the server migrates to another machine, it must be able to locate the transaction log records to complete or recover transactions. Transaction log records are stored in the default persistent store for the server.

If you plan to migrate clustered servers in the event of a failure, you must set up the default persistent store so that it stores records in a shared storage system that is accessible to any potential machine to which a failed migratable server might be migrated.

RECOVERY PROCEDURES

The following sections describe recovery procedures.

Recovery from File System Deletion or Corruption

You can recover from file system deletion or corruption, such as when a configuration has been changed, deleted or corrupted, and WebLogic Server is not functioning properly.

The following sections describe how to recover from file system deletion or corruption. For each scenario, the section provides information about whether you can perform recovery in offline or online mode.

Recovery of Administration Server Configuration

Mode: Offline

In this scenario, the Administration Server does not operate properly or cannot be started because the configuration has been deleted or corrupted, or because the configuration was mistakenly changed and you cannot ascertain what was changed.

1. Stop the Administration Server if it is started.
2. Restore the Administration Server configuration (user_projects/domains/domain_name/config directory under Administration Server BEA Home) from the backup.

   Caution: Performing a domain level recovery can impact other aspects of a running system and all of the configuration changes performed after the backup was taken will be lost.
3. Restart the Administration Server.

On the next configuration change, the configuration from the Administration Server will be pushed to the Managed Servers. On each Managed Server restart, the configuration will be pulled from the Administration Server.

Recovery of Managed Server Configuration

Mode: Offline

In this scenario, Managed Server1 (refer to figure 1) does not operate properly or cannot be started because the configuration has been deleted or corrupted, or because the configuration was mistakenly changed and you cannot ascertain what was changed.

If this occurs while the Administration Server is reachable:

Restart the Managed Server1. This will get the latest configuration from the Administration Server. If this is not feasible, use the following procedure to recover the configuration:

1. Stop the Managed Server1 if it is running.
2. Restore the Managed Server1 configuration from the most recent backup. The directory is:

   (user_projects/domains/domain_name/config under the Managed Server1 BEA Home)
3. Restart Managed Server1 to synchronize the configuration with the Administration Server.
4. On each Managed Server restart, the latest configuration will be pulled from the Administration Server.

If this occurs while the Administration Server is not reachable:

1. Stop Managed Server1 if it is running.
2. Restore the Managed Server1 configuration (the directory user projects/domains/domain_name/config under the Managed Server1 BEA Home) from the backup.
3. Restart Managed Server1.

   If the MSI (Managed Server Independence) mode is enabled in Managed Server1, it starts up reading its local copy of the configuration and synchronizes with the Administration Server when it is available.
4. When the Administration Server is available, restart Managed Server1. The latest configuration is pulled from the Administration Server.
5. If Managed Server1 is part of a cluster, restart the cluster.

Recovery of Administration Server BEA Home

Mode: Offline

In this scenario, the Administration Server is running, but the file system for the BEA home is lost or corrupted.

To restore the BEA home:

1. Stop the Administration Server.
2. Recover the BEA home from the backup.
3. Restart the Administration Server.

Recovery of Application Artifacts

Mode: Offline

In this scenario, application artifacts, such as .ear files, have been lost in the target Managed Server1, probably as a result of user error. To recover the application artifacts:

1. Restart the Managed Server1 to synchronize with the configuration with the Administration Server.

   On each Managed Server1 restart, the latest configuration will be pulled from the Administration Server.

If the application is staged, the Administration Server pushes the application artifacts to the stage directories of all the target servers during deployment. For archived applications, the application artifacts are further exploded in the `servers` directory under the domain. If the application artifacts under the `servers` directory is lost, it can be regenerated on every Manager Server restart. If the application artifacts under the stage directory of the target server are lost, the Administration Server pushes the application artifacts to the stage directory of the target Managed Server upon Managed Server restart. The application artifacts can also be found in Administration Server's upload directory (configurable) if the applications are deployed using the `upload` option

This procedure is applicable for staged applications. If the application is not staged, restore the application artifacts from the backup.

Recovery of Managed Server Software Home

Mode: Offline

In this scenario, Managed Server1 is running, but the file system for the Managed Server1 home is lost or corrupted.

To restore the Managed Server home:

1. Stop Managed Server1.
2. Recover Managed Server1 home from the backup.
3. Restart Managed Server1.

Recovery After Configuration Changes

The following sections describe how to recover to an earlier version of the configuration. For example, the configuration was mistakenly changed and WebLogic Server is not operating properly. You cannot ascertain what was changed, but you want to revert to the previous configuration.

For each scenario, the section provides information about whether you can perform recovery in offline or online mode.

Recovery of Managed Server Configuration After Changes

Mode: Offline

In this scenario, the Managed Server1 configuration, such as the JMS configuration or container-level data-sources.xml, was mistakenly changed and committed. The server cannot be started or does not operate properly or the services running inside the server are not starting. You cannot ascertain what was changed.

If the configuration changes are small in scope, then the easiest way is to redo the configuration changes. If that is not feasible, use the following procedure to recover the configuration:

1. Stop the Administration Server.

2. Restore the Administration Server configuration (the directory user_projects/domains/domain_name/config under Administration Server BEA Home) from the backup.

   Caution: Performing a domain level recovery can impact other aspects of a running system and all of the configuration changes performed after the backup was taken will be lost.
3. Start the Administration Server.
4. Start Managed Server1.

   On the Managed Server restart, the configuration will be pulled from the Administration Server.

Recovery of Cluster-Level Configuration After Changes

Mode: Offline

In this scenario, the cluster-level configuration, such as the JMS configuration or container-level data sources, was mistakenly changed and committed. The server cannot be started or does not operate properly or the services running inside the server are not starting. You cannot ascertain what was changed.

If the configuration changes are small in scope, then the easiest way is to redo the configuration changes. If that is not feasible, use the following procedure to recover the configuration:

1. Stop the Administration Server.

   For changes in container-level services like JDBC data sources, the Administration Server needs to be stopped, then later restarted.
2. Restore the Administration Server configuration (the directory user_projects/domains/domain_name/config under Administration Server BEA Home) from the backup.

   Caution: Performing a domain level recovery can impact other aspects of a running system and all of the configuration changes performed after the backup was taken will be lost.
3. Start the Administration Server.
4. Restart the cluster.

   The latest configuration will be pulled from the Administration Server to every member of the cluster.

Recovery After Cluster Is Deleted

Mode: Offline

In this scenario, the cluster has been erroneously deleted.

If the configuration changes are small in scope, then the easiest way is to redo the configuration changes. If that is not feasible, use the following procedure to recover the configuration:

1. Stop the Administration Server.

This prevents inconsistencies because the Administration Server periodically flushes the configuration to disk.

2. Restore the Administration Server configuration (the directory user_projects/domains/domain_name/config under Administration Server BEA Home) from the backup.

   Caution: Performing a domain level recovery can impact other aspects of a running system and all of the configuration changes performed after the backup was taken will be lost.

3. Restart the Administration Server.

   The deleted cluster is back.

4. Start the cluster.

Recovery After Cluster Membership Mistakenly Modified

Mode: Offline

In this scenario, the cluster membership has been mistakenly modified. For example, a member has been deleted from the cluster.

You can create a new Managed Server by cloning an existing Managed Server that is a part of cluster. If that is not feasible, then use the following procedure to restore the membership:

1. Stop the Administration Server.

   This prevents inconsistencies because the Administration Server periodically flushes the configuration to disk.

2. Restore the Administration Server configuration (user_projects/domains/domain_name/config directory under Administration Server BEA Home) from the backup.

   Caution: Performing a domain level recovery can impact other aspects of a running system and all of the configuration changes performed after the backup was taken will be lost.

3. Restart the Administration Server.

   The deleted member will be back in the cluster.

4. Start the member of the cluster if it is not started.

Recovery After Provisioning or Deprovisioning

The following sections describe how to recover to an earlier state after provisioning or deprovisioning applications. For each scenario, the section provides information about whether you can perform recovery in offline or online mode.

Recovery of Redeployed Application

Mode: Online

In this scenario, a Java EE application was redeployed to a Managed Server1 (that is not a part of a cluster), but the application is no longer functional.

To recover the application you can use one of the following approaches:

If the new application is versioned, then un-target the new version from the cluster and re-target the old version to the cluster.

If application is not versioned then redeploy the old version of the application from the backup.

Recovery of Redeployed Application in Cluster

Mode: Online

In this scenario, a Java EE application was redeployed to a cluster), but the application is no longer functional. Use the procedures in the previous section.

Recovery of Undeployed Application

Mode: Online

In this scenario, a Java EE application was undeployed to a Managed Server1 (that is not a part of a cluster) and you want to redeploy it.

To recover the application, you can redeploy the old version of the application (application bits can either be used from source control or obtained from the backup).

Loss of Host: Recovery to Same Host

If you lose your original operating environment, you can recover to the same host. For example, you could have a serious machine malfunction or loss of media. You correct the problem and want to restore WebLogic Server to this host.

The following sections describe how to recover to the same host. For each scenario, the section provides information about whether you can perform recovery in offline or online mode.

Recovery After Loss of Managed Server Host

Mode: Offline

In this scenario, the host that contains Managed Server1 is lost. Managed Server1 may or may not be in a cluster.

To recover to the same host:

1. If there is a file system loss, restore the Managed Server1 configuration (the directory user_projects /domains/domain_name/config under Managed Server1 BEA Home) from the backup.

   Even though the Administration Server pushes the latest configuration to Managed Server1, Managed Server1 needs Node Manager properties to start up. Those properties reside in the config directory.
2. Whether or not there is a file system loss, start the Node Manager in the host that contains Managed Server1.
3. Whether or not there is a file system loss, start Managed Server1.

Managed Server1 connects to the Administration Server and updates the configuration changes that happened after the Managed Server 1 host crashed.

Recovery After Loss of Administration Server Host

Mode: Offline

In this scenario, the host that contains the Administration Server is lost.

To recover to the same host:

1. If there is a file system loss, restore the Administration Server configuration (user_projects/domains/domain_name/config directory under Administration Server BEA Home) from backup.

   Caution: Performing a domain level recovery can impact other aspects of a running system and all of the configuration changes performed after the backup was taken will be lost.
2. Start the Administration Server.

Loss of Host: Recovery to Different Host

If you lose your original operating environment, you can recover to a different host. For example, you could have a serious machine malfunction or loss of media. You want to restore the files to a different host.

The following sections describe how to recover to a different host. These sections assume that the new host where the environment is restored has same host name and IP address as the previous host. For each scenario, the section provides information about whether you can perform recovery in offline or online mode.

Recovery After Loss of Managed Server Host

Mode: Offline

In this scenario, the host that contains Managed Server1 is lost. Managed Server1 may or may not be in a cluster.

To recover Managed Server1 to a different host:

1. Restore the Managed Server1 BEA home if it is available. If it is not, install the BEA home on the new host.
2. Start the Node Manager in the host that contains Managed Server1.
3. Enroll the Node Manager running in new host with the Administration Server.

   Enrolling Managed Server1 with the Administration Server (using nmEnroll) creates the domain configuration on the new host.
4. Change the Managed Server1 configuration to point to the machine running in the new host. (Home -> Summary of Machines -> your_machine)
5. Start Managed Server1.

Recovery After Loss of Administration Server Host

Mode: Offline

In this scenario, the host that contains the Administration Server is lost.

To recover the Administration Server to a new host:

1. Restore the Administration Server BEA Home, if it is available, on the new host. If it is not, install the software on the new host.
2. Restore the domain directory from the backup.
3. Start the Administration Server.
4. Ensure that additional application artifacts are available. For example, if the deployment mode is no-stage, applications may reside in directories outside of the domain directory. Make your application files available to the new Administration Server by copying them from backups or by using a shared disk. Your application files should be available in the same relative location on the new file system as on the file system of the original Administration Server.
5. Make your configuration and security data available to the new administration machine by copying them from backups or by using a shared disk.

Recovery of Database

Mode: Offline

You can recover your database-based persistent stores, such as JMS, if the database has been corrupted.

Database point-in-time recovery should be used to recover a database to the most recent time to ensure minimum data loss.

CONCLUSION

Backup and recovery of your Oracle WebLogic Server is important to protect data from corruptions, hardware failures, and data failures. To protect the application server environment from potential disaster, backup and recovery is one of the most important aspects of administration. It helps to bring the application server environment to a consistent state.

REFERENCES

Overview of WebLogic Server System Administration:

http://edocs.bea.com/wls/docs103/intro/overview.html

LDAP backup procedures:

WebLogic Server Managing Server Startup and Shutdown

Configuration file archiving and domain structure:

WebLogic Server Understanding Domain Configuration

Pack and unpack commands:

WebLogic Server Creating Templates and Domains Using the pack and unpack Commands

Backup and Recovery Scenarios for Oracle WebLogic Server
January, 2009
Author: Praveen Sampath
Contributing Authors: Shailesh Dwivedi, Pradeep Bhat, Peter Bower, Sunita Sharma,Helen Grembowicz

Oracle USA, Inc.
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