

# Enterprise Manager 10g Backup, Recovery and Disaster Recovery Considerations

*An Oracle White Paper*  
*March 2004*

# Enterprise Manager 10g Backup, Recovery and Disaster Recovery Considerations

Introduction .....	3
Best Practices for Backup and Recovery .....	3
Repository .....	3
Oracle Management Service (OMS) .....	4
Agent .....	4
Best Practice for Disaster Recovery (DR) .....	5
Repository .....	5
OMS .....	5
Agent .....	6

# Enterprise Manager 10g Backup, Recovery and Disaster Recovery Considerations

## INTRODUCTION

The newest release of Oracle Enterprise Manager Grid Control presents a dramatic architectural departure from the previous releases, incorporating a portable browser based interface to the management console and Oracle's application server technology to serve as the middle-tier Management Service (OMS). The foundation of the tool remains rooted in database server technology to manage the repository and historical data. This new architecture requires a different approach to backup, recovery and Disaster Recovery (DR) planning. This article will review practical approaches to these availability topics and discuss different strategies when practical for each tier of Enterprise Manager.

## Best Practices for Backup and Recovery

### Repository

For the database, the best practice is to use the standard database tools for any database backup. Have the database in archivelog mode, and perform regular online backup using RMAN or OS commands.

When considering recovery there are two cases to consider:

- Full recovery of the repository is possible: No special considerations for EM. When the database is recovered, restart the database and OMS processes. Agents will then upload pending files to the repository.

- Only point in time/incomplete recovery is possible: EM agents will be unable to communicate to the repository correctly until they are reset. This is a manual process that is accomplished by shutting down the agent, deleting the agntstmp.txt and lastupld.xml files in the \$AGENT\_HOME/sysman/emd directories and then going to the /state and /upload subdirectories and clearing the contents. The agent can then be restarted. This would need to be done for each agent.

For the case of incomplete recovery, agents may not be able to upload data until there above steps are completed. Additionally, there is no indication in the UI that the agents may not communicate with the OMS after this type of recovery. This information would be available from the agent logs or command line agent status. If incomplete recovery is required, it is best to perform this procedure for each agent.

### **Oracle Management Service (OMS)**

As the OMS is stateless, the task is to restore the binaries and configuration files in the shortest time possible. There are two alternatives in this case.

- Backup the entire software directory structure and restoring that in the event of failure to the same directory path. The agent associated with this OMS install should also be backed up at the same time and restored with the OMS files if a restore is required.
- Reinstall from the original media.

For any highly available OMS install it is a recommended practice to make sure the /recv directory is protected with some mirroring technology. This is the directory the OMS uses to stage files send to it from agents before writing their contents to the database repository. After the agent finishes transmission of its XML files to the OMS, it will delete its copy. In the event of an OMS disk failure, this data would be lost. Warnings and alerts sent from the agents would then be lost. This may require agent resynchronization steps similar to those used with an incomplete database recovery

### **Agent**

This is a similar case to the OMS except that the agent is not stateless. There are two strategies that can be used

- A disk backup and restore is sufficient, assuming the host name has not changed. Delete the agntstmp.txt and the lastupld.xml files from the /sysman/emd directory. The /state and /upload sub-directories should be cleared of all entries before restarting. Starting the agent will then force a rediscovery of targets on the host.
- Reinstall from the original media.

As with the OMS, it is a recommended best practice to protect the /state and /upload directories with some form of disk mirroring.

## Best Practice for Disaster Recovery (DR)

### Repository

In the event of a node failure the database can be restored using RMAN or OS commands. To speed this process, implement Data Guard to replicate the repository to a different hardware node.

If restoring the repository to a new host, restore a backup of the database and modify the emoms.properties file for each OMS manually to point to the new repository location. In addition, the targets.xml for each OMS will have to be updated to reflect the new repository location. If there is a data loss during recovery, see the notes above on incomplete recovery of the repository.

To speed repository re-connection from the OMS in the event of a single OMS failure, configure the OMS with a TAF aware connect string. The OMS can be configured with a TAF connect string in the emoms.properties file that will automatically redirect communications to another node using the 'FAILOVER' syntax. An example is provided below:

```
EM=
(description=
  (failover=on)
  (address_list=
    (failover=on)
    (address=(protocol=tcp)(port=1522)(host=EMPRIM1.us.oracle.com))
    (address=(protocol=tcp)(port=1522)(host=EMPRIM2.us.oracle.com)))
  (address_list=
    (failover=on)
    (address=(protocol=tcp)(port=1522)(host=EMSEC1.us.oracle.com))
    (address=(protocol=tcp)(port=1522)(host=EMSEC2.us.oracle.com)))
  (connect_data=(service_name=EMrep.us.oracle.com)))
```

### OMS

Preinstall the OMS and agent on the hardware that will be used for DR. This eliminates the step of restoring a copy of the EM binaries from backup and modifying the OMS and agent configuration files.

Note that it is not recommended to restore the OMS and agent binaries from an existing backup to a new host in the event of a disaster as there are host name dependencies. Always do a fresh install.

### **Agent**

In the event of a true disaster recovery, it is easier to reinstall the agent and allow it to do a clean discovery of all targets running on the new host



White Paper Title  
March 2004  
Author: Jim Viscusi  
Contributing Authors:

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  
[www.oracle.com](http://www.oracle.com)

Copyright © 2004, Oracle. All rights reserved.

This document is provided for information purposes only  
and the contents hereof are subject to change without notice.

This document is not warranted to be error-free, nor subject to  
any other warranties or conditions, whether expressed orally  
or implied in law, including implied warranties and conditions of  
merchantability or fitness for a particular purpose. We specifically  
disclaim any liability with respect to this document and no  
contractual obligations are formed either directly or indirectly  
by this document. This document may not be reproduced or  
transmitted in any form or by any means, electronic or mechanical,  
for any purpose, without our prior written permission.

Oracle is a registered trademark of Oracle Corporation and/or its  
affiliates. Other names may be trademarks of their respective owners.