Enterprise Manager 10gR2/R3 Backup, Recovery and Disaster Recovery Considerations

An Oracle White Paper
February 2007

Maximum Availability Architecture

Oracle Best Practices for High Availability

ORACLE

Enterprise Manager 10gR2/R3 Backup, Recovery and Disaster Recovery Considerations

Enterprise Manager 10gR2/R3 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 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.

For an overview of the Enterprise Manager Architecture, refer to **Enterprise Manager Grid Control Installation and Basic Configuration 10*g* Release 2 (10.2)**

Best Practices for Backup and Recovery

Backing up the 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 hot backup using RMAN using the Recommended Backup Strategy option through Grid Control. This strategy will create a full backup and then create incremental;

backups on each subsequent run. The incremental changes will then be rolled up into the baseline, creating a new full backup baseline.

Using the Recommended Backup strategy also takes advantage of the capabilities of Grid Control to execute the backups. Jobs will be automatically scheduled through the job sub-system of Grid Control. This history of the backups will then be available for review and the status of the backup will be displayed on the Repository database target home page

Use of this job along with achiving and flashback technologies will provide a restore point in the event of the loss of any part of the repository. This backup along with archive and online logs will allow the repository to be recovered to the last completed transaction.

First, enable Archive Logging then Flashback Database through the Recovery Setting Screen of Enterprise Manager. Each of these configuration changes will require a bounce of the database and a restart of any OMS processes. Then enable Block Change Tracking to speed up backup operations

A thorough summary of how configure backups using Enterprise Manager is available in the 'Database 2 Day DBA' manual

For additional information on Database high availability best practices, review the Oracle Database High Availability Best Practices 10*g* Release 2 documentation

The frequency of the backup job can be set depending on how much data is generated in the Grid Control environment and how much outage time can be tolerated if a restore is required. If the outage window is small and the Service Level Agreement can not be satisfied by restoring the database, consider additional strategies for repository availability such a RAC or Data Guard. Additional High Availability options for the Repository are documented in the 'Configuring Enterprise Manager for High Availability' Paper available from the MAA page on OTN

Recovering the Repository

In the event that something happens to affect the Repository, Grid Control will not be available to provide the management interface to RMAN. A sample syntax for database recovery using RMAN is included below. Please review the chapter on database recovery in the Oracle Database Backup and Recovery Basics for detailed information.

```
RMAN> STARTUP MOUNT

RMAN> RESTORE DATABASE;
RMAN> RECOVER DATABASE;

RMAN> ALTER DATABASE OPEN;
```

When considering repository recovery there are two cases to consider:

- Full recovery of the repository is possible: No special considerations for EM. Use the backups created with RMAN to recovery to the last saved transaction. 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: Some EM agents will be unable to communicate to the OMS 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 that is unable to upload data to the repository.

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 if a restore is required. This should be done while the OMS is down to ensure a consistent backup.
- Reinstall the OMS and the agent 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, the agent will delete its copy. In the event of an OMS disk failure, this data would be lost. Warnings and alerts and metric data sent from the agents would then be lost. This may require agent resynchronization steps similar to those used with an incomplete database recovery

Grid Control 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. Like the OMS, this should be done while the agent is down to ensure a consistent backup.
- 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.

If an agent fails, any jobs that are in process will be marked as failed and any future steps cancelled. As a best practice, multi-step jobs should be created with retry logic or with consistent rollback points.

Best Practice for Disaster Recovery (DR)

Repository

In the event of a node failure the database can be restored using RMAN commands. To speed this process, consider implementing Data Guard to replicate the repository to a different hardware node. Information on configuring Data Guard for the Grid Control Repository is documented in the 'Configuring Enterprise Manager for High Availability' Paper available from the MAA page on OTN

If restoring the repository to new hosts restore a backup of the database and modify the emoms.properities 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.

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
Febuary2007
Author: 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