MAA Best Practices
Enterprise Manager 10gR2,10gR3 &10gR4

An Oracle White Paper
June 2009

Maximum Availability Architecture

Oracle Best Practices for High Availability

ORACLE

Enterprise Manager MAA Best Practices

INTRODUCTION

Highly Available systems are critical to the success of virtually every business today. It is equally important that the management infrastructure monitoring these mission-critical systems are highly available. Oracle's Enterprise Manager Grid Control (EM GC) has an architecture that is engineered to be scalable and available from the ground up. It is designed to ensure that you concentrate on managing the assets that support your business, while it takes care of meeting your business Service Level Agreements.

This paper draws upon the experience of Oracle's High Availability experts to list the best practices that will allow you to deploy a highly available EM by following Maximum Availability Architecture (MAA) recommendations. Maximum Availability Architecture is a best practices blueprint based on proven Oracle high availability technologies and recommendations.

Note: The MAA best practices for Enterprise Manager 10gR5 and beyond are documented in 'Oracle® Enterprise Manager Advanced Configuration 10*g* Release 5 (10.2.0.5)'

EM Maximum Availability Architecture facilitates:

1. Scalability.
2. No Perceived loss of Service.
3. Automated Failover
4. Disaster Recovery

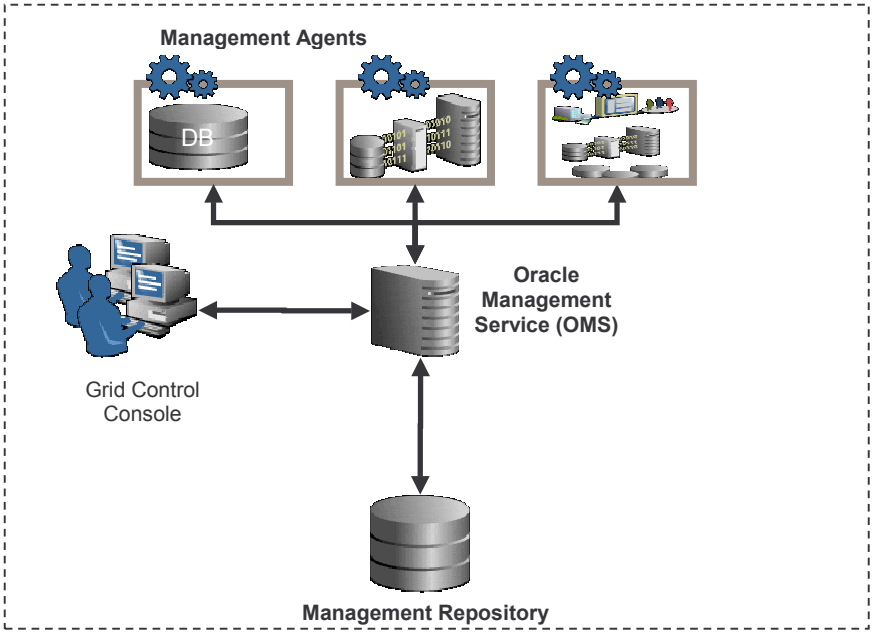
ENTERPRISE MANAGER COMPONENT REVIEW

The three main components of Enterprise Manager are

- **Management Agent**- A native process responsible for monitoring your data center resources such as Database, Application servers etc, and communicating with the Oracle Management Service.
- **Oracle Management Service** (OMS) – A J2EE application that processes the information collected by the agents, renders the EM Grid Control Console GUI and uses the Repository to store the data.
- **Management Repository** – An Oracle database that stores EM data within a special schema.

The *figure* 1 shows the basic components of EM

Figure 1:Enterprise Manager Architecture



This paper assumes familiarity with EM GC architecture. Review 'Enterprise Manager Concepts' in online documentation library (http://www.oracle.com/technology/documentation/oem.html) to brush up on EM GC Architecture

CONFIGURING ENTERPRISE MANAGER FOR HIGH AVAILABILITY

MAA provides a highly available Enterprise Manager (EM) implementation by guarding against failure at each component of EM.

The impacts of failure of the different EM components are:

- Management agent failure or failure in the communication between management agents and OMS: This results in targets no longer monitored by EM, though the EM console is still available and one can view historical data from the repository.
- Oracle Management Service (OMS) failure: This results in the unavailability of EM console as well as unavailability of almost all EM services.
- Repository failure: This results in failure on the part of EM to save the uploaded by the agents as well as unavailability of almost all EM services.

Enterprise Manager should be as available as the highest available application that you are monitoring.

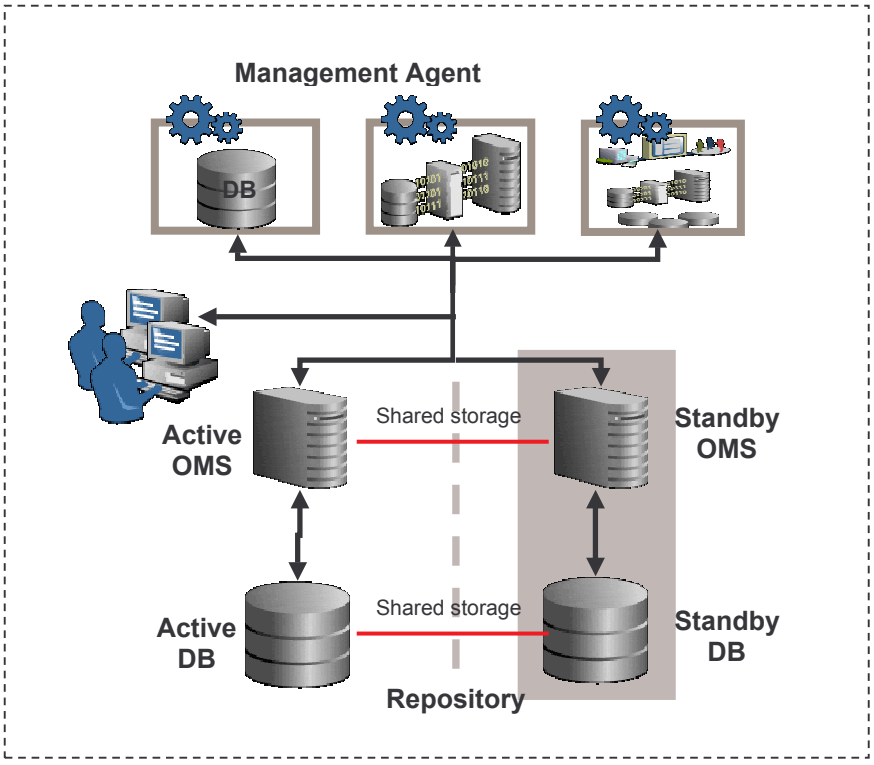
Overall, failure in any component of EM can result in substantial service disruption and therefore it is essential that each component be hardened using a highly available architecture. EM can be configured to run in either active-active or active-passive mode using a single instance database as the repository. The two architectures are summarized below:

Active/Passive: An active-passive configuration involves two hardware nodes with a single node running an OMS instance (active) at a time. The node that primarily hosts OMS is called the active node; the node or sets of nodes that can potentially host the OMS are called the passive nodes. When OMS or any resources upon which it depends (such as disk or the node itself) crashes, the OMS, along with all required resources, is relocated and restarted on a passive node. *Figure* 2 shows the key components of EM configured in active/passive mode. Advantages include:

- Easy to configure, setup and maintain
- Server Load Balancer (SLB) not required

The primary disadvantage of this solution is the inability to scale beyond a single OMS and database instance. In addition, outages caused by component failure take longer to resolve as EM is restarted on the standby hardware.

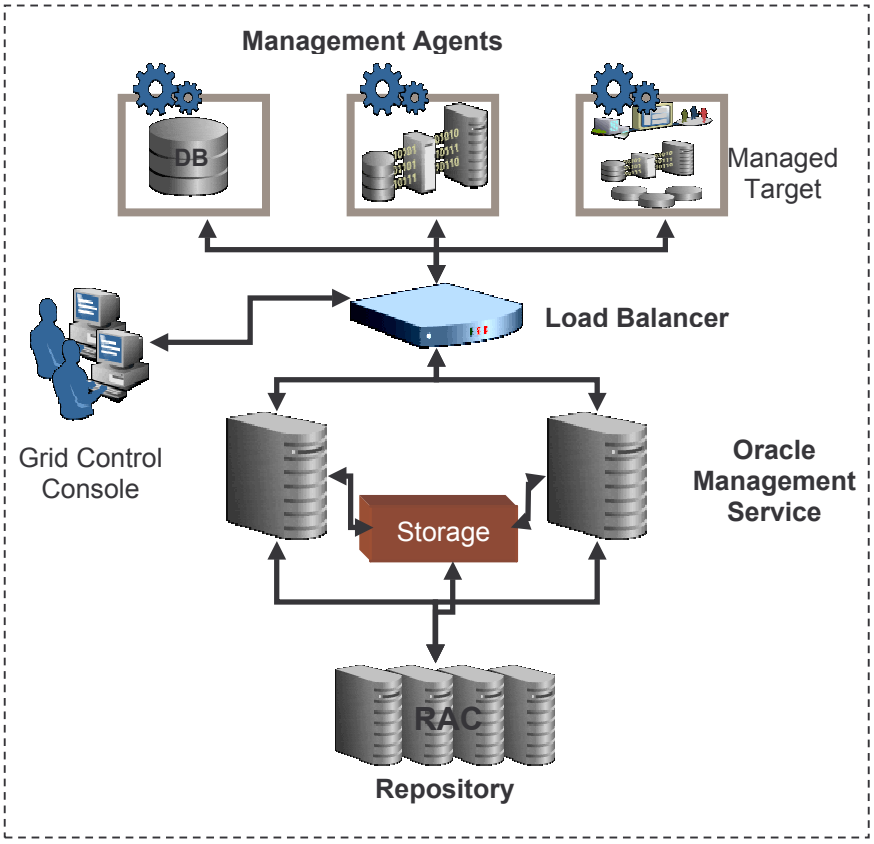
Figure 2:EM Maximum Availability Architecture (Active/Passive)



- **Active/Active (MAA) Configuration:** In an active-active configuration, two or more OMS instances are configured to serve the same application workload. These instances can reside on the same machine or on different machines. The active instances are front-ended by a load balancer router, which can redirect requests to any of the active instances. When any of the nodes of active OMS fails, the remaining nodes of OMS take over the workload. *Figure* 3 shows the key components of EM configured in active/active mode. Advantages include:
    - High level of hardware utilization resulting in better performance (higher throughput) when all nodes are operating
    - Scalability
    - Faster Failover

One disadvantage of this configuration includes possibly reduced performance when a node fails.

Figure 3:EM Maximum Availability Architecture (Active/Active)



The following sections document the best practices for making each component of EM adhere to MAA (an Active/Active HA architecture). While these best practices follow the sequence of a fresh EM install, many of the best practices can also used to retrofit MAA architecture into an existing Enterprise Manager installation.

Note:: Most of the best practices outlined in this paper apply to configuring EM in both Active/Active and Active/Passive mode. The complete outline of the steps required to configure OMS & Repository in Active/Passive mode is published in Web IV Note: 405642.1 and Web IV Note: 405979.1 respectively.

Management Repository Configuration:

Before installing EM, you should prepare the database, which will be used for setting up Management Repository. Install the database using OUI/DBCA to make sure that you inherit all Oracle install best practices.

Automatic Storage Management (ASM): a feature in Oracle Database 10g that provides the database administrator with a simple storage management interface that is consistent across all server and storage platforms

- **Configure Database**:
  - For both high availability and scalability, you should configure the repository in the latest certified database version, with the RAC option enabled. Check for the latest version of database certified for EM from the certify tab on Oracle's Metalink website.
  - Choose Automatic Storage Management (**ASM**) as the underlying storage technology.
  - When the database installation is complete,
    - Go to $ORACLE_HOME/rbdms/admin directory of the database home and execute the 'dbmspool.sql'

      This will install the DBMS_SHARED_POOL package, which will help in improving throughput of the Management Repository.

Number of RAC Nodes: In case you are unsure about the number of RAC nodes to configure for your repository, you may start by configuring your repository in a single node RAC and scale out later to multi-node architecture as needed

- **Install Enterprise Manager**: While installing EM using Oracle Universal Installer (OUI), you will be presented with two options for configuring the repository:
  - *Option 1*:Install using a new database (default install)
  - *Option 2*:Install using an existing database.

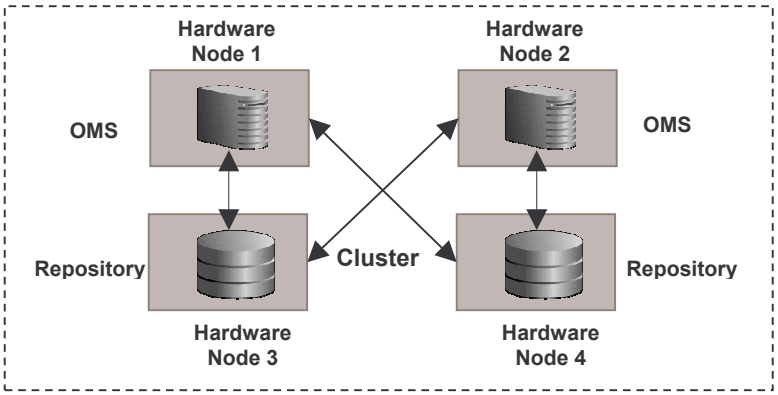
  For MAA you should chose '*Option 2*:Install using an existing database'. When prompted for the 'existing database', you can point to the database configured in the previous step to setup the repository.

Oracle Management Service(OMS) Configuration

Once you configure the repository, the next step is to install and configure the EM Grid Control mid-tier, the OMS, for greater availability. Before discussing steps that add mid-tier redundancy and scalability, it is worthwhile to note that the OMS itself has a built in restart mechanism based on the Oracle Process Management and Notification Service (OPMN). This service will attempt to restart an OMS that is down.

- **OMS Install Location:** If you are managing a large environment with multiple OMS and repository nodes, then consider installing the OMS on hardware nodes that are different from repository nodes (*Figure* 4). This will allow you to scale out OMSs in the future

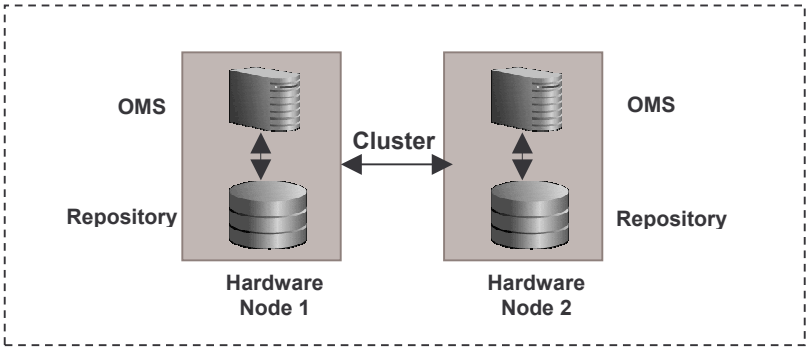
Figure 4:OMS & Repository on separate hardware



You should also consider the network latency between the OMS & the repository while determining OMS install location. The distance between the OMS & the repository may be one of the factors that effect network latency and hence determine EM performance.

If the network latency between the OMS and repository tiers is high or the hardware available for running EM is limited, then install the OMS on the same hardware as the repository (*Figure* 5). This will allow for EM high availability as well as keep the costs down.

Figure 5:OMS & Repository on same hardware



Note: starting with EM 10g release 10.2.0.2, you can install the OMS onto the same nodes as the RAC repository. See the diagram (figure 3) and refer to the instructions specified in the README for doing the same

- **Install Additional OMS:** Install at least one additional OMS using the OUI option 'Add Additional Management Service'. While you need two OMS at the minimum for High Availability, additional OMS processes can be installed depending on anticipated workload or based on system usage data.

See Chapter 9 of the Enterprise Manager Advanced Configuration Guide for sizing recommendations.

- **Configure OMS to Repository communication:** Once all the OMS processes have been installed, they need to be configured to communicate with each node of the RAC repository in a redundant fashion. To accomplish this,
  - Modify the field 'emdRepConnectDescriptor' in the file $ORACLE_HOME/sysman/config/emoms.properities for each installed OMS. The purpose of this configuration is to make the OMS aware of all instances in the database cluster that are able to provide access to the repository through the database service 'EMREP'.

  A sample of this modification script is shown below:

  ```
  oracle.sysman.eml.mntr.emdRepConnectDescriptor=(DESCRIPTION\=(ADDRESS
  _LIST\=(FAILOVER\=ON)
  (ADDRESS\=(PROTOCOL\=TCP)(HOST\=hostname.oms1.com)
  (PORT\=1521))(ADDRESS\=(PROTOCOL\=TCP)(HOST\=hostname.oms2.com)
  (PORT\=1521)) (CONNECT_DATA\=(SERVICE_NAME\=EMREP)))
  ```

  Further information on Oracle Database networking and the 'FAILOVER' parameter can be found in the "Section 13,Enabling Advanced Features of Oracle Net Services" section of the **Oracle® Database Net Services Administrator's Guide 10g Release 2 (10.2)** Part Number B14212-02

- **Configure the shared file system load directory:** A new enhancement in EM 10gR2 allows all OMS processes to persist the information uploaded by Management Agents to a shared directory. This has two benefits:

  I. Allow all OMS(s) to process the agent data and take better advantage of available resources

  II. The ability of another OMS to process agent data in the event of a failure of an OMS.

  To configure the Management Service to use Shared File system Loader, you must run the following steps:

  1. Stop all Oracle Management Services.
  2. Configure a shared receive directory that is accessible by all Management Services using redundant file system storage.
  3. execute: emctl config oms loader -shared yes -dir <loaderdirectory>'

     individually on all OMS hosts, where <loader directory> is the full path to the shared receive directory created in step 2.

Note: Enterprise Manager will fail to start if all the OMSs are not configured to point to the same shared directory. This shared directory should be on redundant storage.

- **Post OMS-Install Repository Configuration**: There are some parameters that should be configured during the repository database install (as mentioned above) and some parameters that should be set after the OMS has been installed. Now that EM console is available, it can be used to configure these best practices in the repository. These best practices fall in the area of:
  - Configuring Storage
  - Configuring Oracle Databse 10g with RAC for High Availability and Fast Recoverability
    - Enable ARCHIVELOG Mode
    - Enable Block Checksums
    - Configure the Size of Redo Log Files and Groups Appropriately
    - Use a Flash Recovery Area
    - Enable Flashback Database
    - Use Fast-Start Fault Recovery to Control Instance Recovery Time
    - Enable Database Block Checking
    - Set DISK_ASYNCH_IO

The details of these settings are beyond the scope of this whitepaper but are described in detail in Section 2.1 and 2.2 of **Oracle® Database High Availability Best Practices 10g Release 2 (10.2)** (Part Number B25159-01)

AGENT CONFIGURATION

Management Agents:

- the real worker drones in the EM infrastructure
- Agent availability is key to getting the best out of EM Grid Control.

The final piece of EM High Availability is the Agent configuration. Before we jump into Agent configuration, it is worthwhile to note that the agent has high availability built into it out of the box. A 'watchdog' process, created automatically on agent startup, monitors each agent process. In the event of a failure of the agent process, the 'watchdog' will try to automatically re-start the agent process.

Communication between the Agent and OMS tiers in a default EMGrid Control install is a point-to-point set up. Therefore, the default configuration does not protect from the scenario where the OMS becomes unavailable. In that scenario, an agent will not be able to upload monitoring information to the OMS (and to the

Repository), resulting in the targets becoming unmonitored until that agents is manually configured to point to a second OMS.

To avoid this situation, use hardware Server Load Balancer (SLB) between the agents and the OMSes. The Load Balancer monitors the health and status of each OMS and makes sure that the connections made through it are directed to surviving OMS nodes in the event of any type of failure. As an additional benefit of using SLB, the load balancer can also be configured to manage user communications to EM. The Load Balancer handles this through the creation of 'pools' of available resources.

Server Load Balancer (SLB): usually a piece of hardware that distributes traffic efficiently among OMSs so that no individual OMS is overburdened

Some of the vendors manufacturing this piece of hardware are: BIG-IP F5, Radware WSD/CT100c, Nortel Alteon, Foundry ServerIron, NetScaler, Cisco ACE/CSM,

- **Configure Server Load Balancer (SLB):** For EM High Availability we create 'pools' in the SLB that correspond to three external services that are provided by the OMS. These services allow:
  1. Access for the agent to upload data,
  2. Access for securing the agent communication
  3. Access to the EM Console GUI.

  The physical locations of the OMS nodes are in effect 'virtualized' by the load balancer through these pools.
- **Configure Agent to communicate through SLB:** The load balancer provides a virtual IP address that all agents can use. Once the load balancer is setup, the agents need to be configured to route their traffic to the OMS through the SLB. This can be achieved through a couple of property file changes on the agents. Refer to the Web IV Note listed below.
- **Configure Agent to allow Retrofitting a SLB:** Some installations may not have access to an SLB during their initial install, but may foresee the need to add one later. If that is the case, consider configuring the Virtual IP address that will be used for the SLB as apart of the initial installation and having that IP address point to an existing OMS. Secure communications between agents and OMS are based on the host name. If a new host name is introduced later, each agent will not have to be re-secured as it is configured to point to the new Virtual IP maintained by the SLB.
- **Configure OMS to direct traffic through SLB:** Finally, modify the OMS to take advantage of the capabilities of the Server Load Balancer. These modifications will cause the all the OMS nodes to redirect EM console traffic through the server load balancer, thereby presenting a single URL to EM user.
  - Modify the ServerName property defined in the Oracle HTTP Server configuration file at $ORACLE_HOME/Apache/Apache/conf/ssl.conf to point to the Virtual host name being managed by the Load Balancer

- Modify the 'Port' in the Oracle HTTP Server configuration file at $ORACLE_HOME/Apache/Apache/conf/ssl.conf to be '443. This assumes you are running in the default secured configuration between the OMS and agent

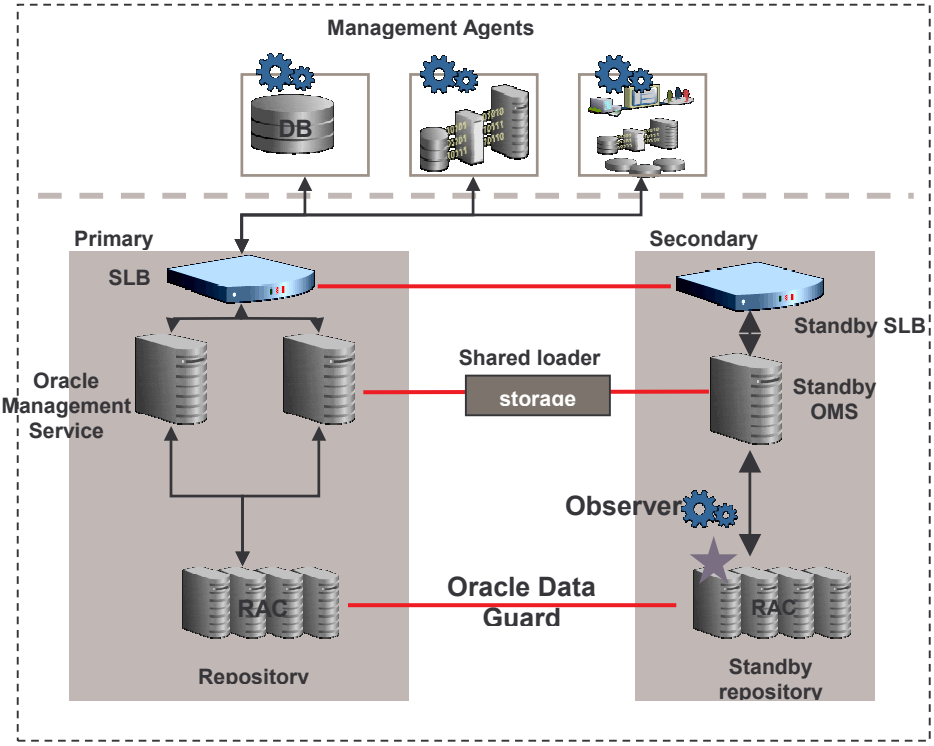
Note:: complete outline of the steps required to configure a hardware Load Balancer for EM High Availability is published on Web IV:Note 353074.1:How to configure Grid Control 10.2 Management Servers behind a Server Load Balancer (SLB)

DISASTER RECOVERY

While high availability typically protects against local outages such as application failures or system-level problems, disaster tolerance protects against larger outages such as catastrophic data-center failure due to natural disasters, fire, electrical failure, evacuation, or pervasive sabotage. For Maximum Availability, the loss of a site cannot be the cause for outage of the management tool that handles your enterprise.

Maximum Availability Architecture for EM mandates deploying a remote failover architecture that allows a secondary datacenter to take over the management infrastructure in the event that disaster strikes the primary management infrastructure.

Figure 6:EM Disaster Recovery Architecture



As can be seen in *Figure* 6, setting up disaster recovery for Enterprise manager essentially consists of installing a standby RAC, a standby OMS and a standby Server Load Balancer and configuring them to automatically startup when the primary components fail.

The following section lists the best practices to configure the key EM components for disaster recovery:

Note: To set up the Standby Database, you should use the command line for executing each of the following steps, as the initial set up of Data Guard requires bounces of the primary database at install-time.

- **Install Standby Database for the Repository:**

    1. Create standby database, In version 10.2 of EM, standby database must be **physical standbys only**

> Follow the instructions in chapter 3 of the **Oracle® Data Guard Concepts and Administration 10*g* Release 2 (10.2)** Part Number B14239-04 to create a **physical standby database**

    2. Return to the Enterprise Manager console and discover the new standby database.
    3. Navigate to primary database targets page and follow the instructions (below) to bring the primary and standby database under Data Guard Broker Control.
    4. If the standby database instance is to be a RAC cluster, follow the steps documented in the white paper 'MAA / Data Guard 10g Release 2 Setup Guide –Creating a RAC Logical Standby for a RAC Primary'

> Configure the primary repository and standby repository with the recommendations listed in **Section 2.4 of the Oracle® Database High Availability Best Practices** 10g Release 2 (10.2) Part Number B25159-01.

Data Guard is a product that synchronizes committed database transactions between primary and secondary, thereby maintaining a mirror image of the primary database.

In the event of a '**switchover**' (a planned actions) or a '**failover**' (unplanned outage), Data Guard will:

- Manage moving the last transaction to secondary
- Transfer control to secondary and 'recover' it to be the new primary

- **Configure Data Guard:** Data Guard is key to EM Disaster Recovery strategy. Follow the standard database best practices for Data Guard performance. A full discussion of all the capabilities of Data Guard is available in the Data Guard Concepts Guide.

  Chapter 6 of the **Oracle® Data Guard Broker 10*g* Release 2 (10.2)** Part Number B14230-02 manual gives a detailed overview of how to use Oracle Enterprise Manager graphical user interface (GUI) to create, manage, and monitor a Data Guard configuration.

- **Install additional OMS processes for failover site:** Use the 'Create Additional Management Service' option of the EM Installer to add the secondary OMS processes. As with the primary, the OMS can be installed on the same nodes as the standby database instance if desired. Follow these steps in sequence to configure the secondary OMS

  1. Configure the OMS to point to the repository running on the primary during install.
  2. After the install is complete, shutdown the OMS and edit the $ORACLE_HOME/sysman/config/emoms.properities file to modify the following properties to point the OMS to the standby database:
     - oracle.sysman.eml.mntr.emdRepConnectDescriptor=<database connection string>
     - oracle.sysman.emSDK.svlt.ConsoleServerName=<virtual host name>

     add the following property:

     - em.FastConnectionFailover=true

- **Configure shared loader directory:** Configure the shared loader directory to be replicated at the primary and standby sites. It is possible during a complete site outage that the OMS on the primary side would have received data from the agents, staged it into the shared loader directory, but not have had time to process that data. Under normal circumstances, that data would be lost during an unexpected site outage. This data loss can be controlled by using hardware vendor disk level replication technologies. Then, in the event of a failure, the OMS enabled on the standby side can process agent data up to the last transaction.

  Note: Configure the name of the shared directory used by the OMS to be same on the primary and standby sites.

Data Guard Observer: a process that is configured to monitor the health of the primary and the secondary processes. The Observer is usually installed on a host somewhere in the standby site

- **Configure the Data Guard Observer for Fast Start Failover:** A new feature delivered with Database 10.2 is Fast Start Failover (FSFO) and the Observer process. In the event of a failure of the primary repository database, the Observer triggers a failover of the repository to the standby site. The feature allows for the repository to move quickly without administrator intervention. If the repository database has been configured to be under Data Guard Broker control, the Observer process can be enabled through EM.
- **Configure Triggers to start OMS at standby site:** An ability of the database is the facility to execute Oracle triggers to be fired database startup. Combined with Data Guard these triggers can be configured to start OMS processes at the standby site after a Data Guard switchover or failover occurs. Examples of these triggers as they relate to Enterprise Manager are in the Appendix.

  A complete reference on the underlying technology used to automate these client failovers is documented in the Client Failover Best Practices for Highly Available Oracle Databases: Oracle Database 10g Release 2, located on the OTN on the Maximum Availability Architecture Page.

  Note: The standby OMS processes can be kept ready for service (not started) until the Data Guard failover triggers are initiated or be configured to service requests from the primary if network latency between the primary and standby is low.
- **Add additional hardware Server Load Balancer** For complete redundancy in a Disaster Recovery environment, a second hardware Server Load Balancer should be installed at the standby site.

  1. Secondary SLB should be configured in the same fashion as the primary.
  2. Configure the secondary OMS to be a part of the 'virtual pools' created by the secondary Server Load Balancer.

  Some SLB vendors (such as F5 Networks) offer additional services that can be used to pass control of the Virtual IP presented by the SLB on the primary to the SLB on the standby site in the event of a site outage. This can be used to facilitate automatic switching of agent traffic from the primary to the standby site.

CONCLUSION

High-availability and disaster-recovery architecture requires customization to meet the requirements of different environments. The best practices specified in this white-paper will provide you the guidelines to configure a fault-tolerant, highly available management solution for most environments. The complete selection of papers documenting Oracle's Maximum Availability Architecture is available on OTN at:

http://www.oracle.com/technology/deploy/availability/htdocs/maa.htm

APPENDIX:

- **Examples of DB Disaster Recovery Triggers & Scripts:**

The following trigger will be fired on the start up of any instance of a database. The trigger will call the script 'start_oms', which will start an OMS process. This facility can be used to start the OMS for a standby database in the event of an unplanned site outage

```
CREATE OR REPLACE TRIGGER manage_service after startup on
database
    DECLARE
      role VARCHAR(30);
    BEGIN
      SELECT DATABASE_ROLE INTO role FROM V$DATABASE;
      IF role = 'PRIMARY' THEN
        DBMS_SERVICE.START_SERVICE('gcha_oms');
          begin
            dbms_scheduler.create_job(
            job_name=>'oms_start',
            job_type=>'executable',
    job_action=>'<script location>/start_oms.ksh',
            enabled=>TRUE
            );
          end;
      ELSE
        DBMS_SERVICE.STOP_SERVICE('gcha_oms');
      END IF;
    END;
    /
```

The script to start OMS- start_oms.ksh:

```
#!/bin/ksh
<OMS INSTALL LOCATION>/bin/emctl start oms
```

- **References:**
  - Most of the books referenced in this white paper can be found in the 'Documentation' tab at:

    http://www.oracle.com/pls/db102/db102.homepage
  - Enterprise Manager Concepts:

    http://www.oracle.com/technology/documentation/oem.html
  - Orcle Database Networking:

    "Section 13,Enabling Advanced Features of Oracle Net Services" section of the Oracle® Database Net Services Administrator's Guide 10g Release 2 (10.2)

    http://download-west.oracle.com/docs/cd/B19306_01/network.102/b14212/toc.htm
  - Configuring Highly Available repository:

    Section 2.1 and 2.2 of Oracle® Database High Availability Best Practices 10g Release 2 (10.2) (Part Number B25159-01)

    http://download-west.oracle.com/docs/cd/B19306_01/server.102/b25159/configbp.htm - i1014681
  - Setting up Server Load Balancer:

    https://metalink2.oracle.com/metalink/plsql/ml2_documents.showFrameDocument?p_database_id=NOT&p_id=353074.1
  - Setting up OMS in Active/Passive mode

    https://metalink2.oracle.com/metalink/plsql/ml2_documents.showFrameDocument?p_database_id=NOT&p_id=405642.1
  - Setting up Repository in Active/Passive mode

    https://metalink2.oracle.com/metalink/plsql/ml2_documents.showFrameDocument?p_database_id=NOT&p_id=405979.1
  - Creating a physical standby database:

    Oracle® Data Guard Concepts and Administration 10g Release 2 (10.2) Part Number B14239-04 physical standby database

    http://download-west.oracle.com/docs/cd/B19306_01/server.102/b14239/toc.htm

- Databases High Availability

  Section 2.4 of the Oracle® Database High Availability Best Practices 10g Release 2 (10.2) Part Number B25159-01.

  http://download-west.oracle.com/docs/cd/B19306_01/server.102/b25159/configbp.htm - i1007026

- Oracle Enterprise Manager graphical user interface (GUI) to create, manage, and monitor a Data Guard configuration.

  Chapter 6 of the Oracle® Data Guard Broker 10g Release 2 (10.2) Part Number B14230-02

  http://download-west.oracle.com/docs/cd/B19306_01/server.102/b14230/toc.htm

- MAA / Data Guard 10g Release 2 Setup Guide –Creating a RAC Logical Standby for a RAC Primary

  Chapter 6 of the Oracle® Data Guard Broker 10g Release 2 (10.2) Part Number B14230-02

  http://www.oracle.com/technology/deploy/availability/pdf/MAA_WP_10gR2_RACPrimaryRACLogicalStandby.pdf

EM 10g MAA (Maximum Availability Architecture):
Best Practices
September 2008
Author: Anirban Chatterjee,James Viscusi

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