Automating Oracle Commerce
High Availability and
Disaster Recovery
Using Oracle Site Guard

ORACLE WHITE PAPER | AUGUST 2015
# Table of Contents

Executive Overview ........................................... 3

Overview of Oracle Commerce MAA .................... 4
- Oracle Commerce ........................................ 4
- Oracle Site Guard ....................................... 4
- Oracle Commerce Platform MAA .................... 5
- Oracle Site Guard Capabilities ....................... 7

Configuring Oracle Site Guard .............................. 8
- Prerequisites to Configuring Oracle Site Guard .... 8
- Oracle Site Guard Configuration .................... 8

Use Cases ......................................................... 16
- Prechecks .................................................. 16
- Use Cases for Active/Passive Applications and Database 16
  - Applications and Database Switchover .......... 16
  - Applications and Database Failover ............ 16
  - Applications and Database Start and Stop ..... 17
- Use Cases for Active/Active Applications With Active/Passive Database 17
  - Database Switchover ............................... 17
  - Database Failover .................................. 17
  - Applications and Database Start and Stop ..... 17

Results – Site Guard Operations vs Manual Operations .... 18

Best Practices for Disaster Readiness and Recovery ... 19
<table>
<thead>
<tr>
<th>Sample Scripts</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prescript</td>
<td>20</td>
</tr>
<tr>
<td>Postscript</td>
<td>21</td>
</tr>
<tr>
<td>Unmount</td>
<td>22</td>
</tr>
<tr>
<td>Mount</td>
<td>22</td>
</tr>
<tr>
<td>ZFS Storage</td>
<td>22</td>
</tr>
<tr>
<td>References</td>
<td>23</td>
</tr>
</tbody>
</table>
Executive Overview

Oracle Maximum Availability Architecture (MAA) is Oracle’s best practices blueprint based on proven Oracle high availability technologies and recommendations. The goal of MAA is to achieve the optimal high availability architecture at the lowest cost and complexity. Papers are published on the Oracle Technology Network (OTN) - [http://www.oracle.com/goto/maa](http://www.oracle.com/goto/maa).

This paper describes the architecture along with installation, configuration, and operational best practices for deploying Oracle Site Guard to aid in high availability and disaster recovery of Oracle Commerce with MAA best practices. For the purpose of this paper, Oracle Commerce is comprised of Oracle Commerce Platform, Oracle Guided Search, and Oracle Commerce Merchandising.

Oracle Commerce MAA is implemented in two different MAA configurations: 1) fully Active/Passive and 2) Active/Active application with Active/Passive databases (also known as Active/Active/Passive). Each configuration is tested to validate MAA best practices and to measure and observe application impact in various outage scenarios. The results of this vigorous testing are presented in this paper. A third configuration exists, which is fully Active/Active. Due to the many business rules required for this type of configuration to be constructed, it is not in the scope of this document.

The Oracle Fusion Middleware Disaster Recovery solution uses storage replication technology for disaster protection of middle tier components, while Oracle Data Guard provides disaster protection for the Oracle databases that are part of Oracle Fusion Middleware deployments. Disaster Recovery operations are typically time consuming, manual, and prone to errors. Oracle Site Guard, a part of Oracle Enterprise Manager, will help you build, manage, and execute reliable Disaster Recovery plans. Oracle Site Guard helps your systems meet the Recovery Time Objective (RTO) through the automation of Disaster Recovery procedures and reduces costs by achieving predictable and timely results for the recovery of a production environment.

Oracle Site Guard provides a means by which Oracle Commerce MAA can be maintained automatically with only a couple of steps. It pulls the error-prone human element out of the reconfiguration to ensure error-free changes. It also includes the ability to test the outcome of any changes before you need to commit them.
Overview of Oracle Commerce MAA

Oracle Commerce

Oracle Commerce MAA is a high availability (HA) architecture – providing local HA – layered on top of the Oracle MAA best practices for Oracle Database and Oracle Fusion Middleware. Operating out of multiple data centers is increasingly important to maintain some form of high availability. The full platinum MAA architecture includes two sites to provide business continuity in the event of a single site failure. The scope of this document covers two types of configurations:

» Active/Passive applications and databases
» Active/Active applications and Active/Passive databases

Oracle Site Guard

Oracle Site Guard, a part of Oracle Enterprise Manager, provides flexible and seamless orchestration of switchovers and failovers between disaster recovery sites, minimizing downtime for enterprise deployments. The disaster recovery automation features in Oracle Site Guard eliminate the need for human intervention and prevent human-induced errors in the switchover or failover process. Oracle Site Guard is flexible and easily integrates with various platforms including Oracle Exalogic and Oracle Exadata Database Machine. Oracle Site Guard is part of the Oracle Enterprise Manager Plug-in for Oracle Fusion Middleware, which allows you to control Oracle WebLogic Managed Server applications, Oracle Database operations, and execute custom scripts to switch over and fail over all or part of the applications in a particular site.

While many variations in disaster recovery topologies are possible, Oracle strongly recommends using a topology similar to the one described in this paper, even though they may vary in configuration and capacity. The topology described in this paper is designed to maintain SLAs through ease of management, maintenance, and automated disaster recovery operations.

For the purpose of this document, Oracle Exalogic and Oracle Exadata Database Machine engineered systems were used in the configuration of two separate environments. The ZFS storage scripts can be used on any ZFS appliance, whether used with Oracle engineered systems or not. Unmounting and mounting scripts can be used by any Unix-based system, as they are simple command-line scripts to run umount and mount operations. The Oracle WebLogic Server and database configurations can apply to both engineered systems and commodity hardware, as both are fully supported for both software configurations. The key element is to maintain the proper Enterprise Manager versions throughout your environments to ensure proper configuration and operation.
Oracle Commerce Platform MAA

Oracle Commerce MAA can be achieved by configuring applications in two separate sites or data centers. A typical active/passive MAA configuration is shown below in Figure 1: Oracle Commerce Active/Passive MAA Configuration. In this type of environment configuration, both the applications and the database have a primary set of servers and a standby set of servers. The standby servers act in what could be considered a disaster recover model. They are used in the event of a primary site failure or a planned outage of the complete site. To see the details of the Commerce MAA environment setup, see the "Oracle Commerce MAA Configuration Best Practices" white paper.

Figure 1: Oracle Commerce Active/Passive MAA Configuration
A typical MAA configuration with active/active applications and active/passive database is shown in Figure 2: Oracle Commerce Active/Active/Passive MAA Configuration. In this type of environment configuration, all application hardware and software is up and running. They are both configured to be using the one set of database servers in one of the sites at any given time. In the event of a database failure, the database is failed over to the standby database in the other site. This configuration allows customers to be using all of their application hardware and software. However, hardware and software upgrades need to be timed in such a way, as to take servers offline, either by site or individually, to perform maintenance and upgrades.

Figure 2: Oracle Commerce Active/Active/Passive MAA Configuration
Oracle Site Guard Capabilities

Oracle Site Guard can handle several different types of operations, which include:

» Starting an entire site  
» Stopping an entire site  
» Failing over an entire site to another site  
» Switching over an entire site to another site

These operations are accomplished with several built-in and custom scripts. Customizing and combining these scripts create operation plans, which perform the aforementioned site operations. Details of each operation plan are shown in the “Configuring Oracle Site Guard” section of this document. For use with the Oracle Commerce products, they include:

» WebLogic domain scripts  
  » Node Manager scripts  
  » Admin Server scripts  
  » Managed Server scripts

» Storage scripts  
  » ZFS storage replication scripts  
  » Mount/Unmount scripts

» Database scripts

» Custom scripts  
  » Prescripts (scripts run at the beginning of the operation plan)  
  » Postscripts (scripts run at the end of the operation plan)

Oracle Site Guard also has the capability of performing operations on Oracle HTTP Server (OHS) and can handle scripting used for Oracle Traffic Director (OTD) operations. As the Commerce MAA environments do not have OHS or OTD as part of the architecture, they are not covered in this paper.
Configuring Oracle Site Guard

Prerequisites to Configuring Oracle Site Guard

Ensure that the following prerequisites are met before configuring Oracle Site Guard.

» A single Enterprise Manager Cloud Control instance should be used to manage both the primary and standby Site Guard sites.
» Perform host target discovery for all of the middleware and database hosts in Enterprise Manager
   (Enterprise Manager Cloud Control Administrator's Guide, "Discovering, Promoting, and Adding Targets").
» Perform the Enterprise Manager agent deployment in Enterprise Manager
   (Enterprise Manager Cloud Control Basic Installation Guide, "Installing Oracle Management Agents").
» Discover the middleware targets for both sites in Enterprise Manager
   (Enterprise Manager Cloud Control Administrator's Guide, "Discovering, Promoting, and Adding Middleware Targets").
» Discover the database targets for both sites in Enterprise Manager
   (Enterprise Manager Cloud Control Administrator's Guide, "Discovering, Promoting, and Adding Database Targets").
» Configure the WebLogic managed server Graceful Shutdown Timeout for each managed server in the domain
   (using WebLogic Server Administration Console: [domain] > [server] > Control tab > Start/Stop tab. Default is 0 (indefinite). Because Commerce managed servers do not gracefully shut down, a timeout should be set. A good starting point is 60 seconds.

Remember, the longer the timeout set, the longer it takes to perform a switchover.

Oracle Site Guard Configuration

The Oracle Site Guard configuration is performed in several steps. These include:

1. Create Site Guard sites as generic system targets in Enterprise Manager, making sure to add the correct
   WebLogic servers, WebLogic deployments, database instances, and cluster databases to the sites.

   Set key members appropriately. Key members are the WebLogic elements, which are required to be
   running in order to consider the site to be in a running state.

   Control Console" for more information.

2. Create global named credentials in Enterprise Manager for the following logins:
   » Database instance(s)
   » Middleware server privileged users (make sure to grant sudo access to the user)
   » WebLogic Node Manager users (Oracle Fusion Middleware Administering Node Manager for Oracle
     WebLogic Server)
   » WebLogic server users (Admin and managed servers, set up as host credentials)
   » ZFS users (for both the source and target ZFS appliances).

3. Create software library storage, if there isn’t a software library already.


4. Create custom prescripts and/or postscripts.

   See “Sample Scripts” for more details on prescripts and postscripts.

5. Configure the sites (generic system targets) in Enterprise Manager.


   a. On site 1 only, add site 2 as standby and save the configuration.
b. On both site 1 and 2 do the following steps:
   i. Configure credentials associations for hosts, WebLogic objects, and database in the credentials tab

   **Site Guard Configuration**
   
   Site Guard requires the following credentials for performing operations:
   - Normal Host Credentials
   - Privileged Host Credentials
   - Oracle Node Manager Credentials
   - Oracle WebLogic Administration Credentials
   - SYSDBA Database Credentials
   
   The named or preferred credentials have to be created before they can be associated with a Site Guard configuration.

   **Normal Host Credentials**
   
<table>
<thead>
<tr>
<th>Target</th>
<th>Credential Name</th>
<th>Use Preferred</th>
</tr>
</thead>
<tbody>
<tr>
<td>scan04kn21.us.oracle.com</td>
<td>ORACLE_ATG_2015-04-08-111113</td>
<td>No</td>
</tr>
<tr>
<td>scarn08db03.us.oracle.com</td>
<td>ORACLE_ATG_2015-04-08-111113</td>
<td>No</td>
</tr>
<tr>
<td>scarn04kn23.us.oracle.com</td>
<td>ORACLE_ATG_2015-04-08-111113</td>
<td>No</td>
</tr>
<tr>
<td>scarn08db04.us.oracle.com</td>
<td>ORACLE_ATG_2015-04-08-111113</td>
<td>No</td>
</tr>
</tbody>
</table>

   **Privileged Host Credentials**
   
<table>
<thead>
<tr>
<th>Target</th>
<th>Credential Name</th>
<th>Use Preferred</th>
</tr>
</thead>
<tbody>
<tr>
<td>scan04kn21.us.oracle.com</td>
<td>ORACLE_ATG_SUDO_2015-05-05-07</td>
<td>No</td>
</tr>
<tr>
<td>scarn08db03.us.oracle.com</td>
<td>ORACLE_ATG_SUDO_2015-05-05-07</td>
<td>No</td>
</tr>
<tr>
<td>scarn04kn23.us.oracle.com</td>
<td>ORACLE_ATG_SUDO_2015-05-05-07</td>
<td>No</td>
</tr>
<tr>
<td>scarn08db04.us.oracle.com</td>
<td>ORACLE_ATG_SUDO_2015-05-05-07</td>
<td>No</td>
</tr>
</tbody>
</table>

   See *Oracle Site Guard Administrator's Guide, "Creating Credential Associations"* for more information.
ii. Configure unmount scripts for switchover and failover, and automatically configure the scripts as primary role.

**Site Guard Configuration**

Configure unmount scripts for switchover and failover, and automatically configure the scripts as primary role.

See unmount sample scripts and *Oracle Site Guard Administrator's Guide, “Configuring Mount and Unmount Scripts”*. 
iii. Configure mount scripts for switchover and failover, automatically set as standby role (see "Mount" for the sample script).

iv. Configure ZFS storage scripts for switchover and failover, automatically set as standby role (see “ZFS Storage” for a sample script).

v. Configure prescripts and postscripts.

**Site Guard Configuration**

Pre and Post Scripts are custom scripts associated with a site. A script can be associated with more than one host target in the site. These are executed as part of the operation plan - Pre-Scripts are executed as the first step and Post-Scripts are executed as the last step in the operation plan.

- For example, script.sh param1=value1 param2=value2

Switchover and Failover operation types will be shown when a Site Guard configuration has a primary site and one or more standby sites.

<table>
<thead>
<tr>
<th>Add</th>
<th>Add Like</th>
<th>Edit</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image.png" alt="Image" /></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


6. Create Site Guard operation plans for both sites.

The role that you selected (or that was selected automatically) will determine which pieces of the configurations appear on the operation plan and in what order. The following graphic is an example of a listing of completed operation plans:

**Site Guard Operations**

An operation plan needs to be created in order to execute any Site Guard operation. It contains the list of steps to be executed for this Site Guard operation. For example, stopping Oracle HTTP Servers, stopping the Managed Servers and Administration Server in a WebLogic domain, and so on. You can either use the default operation plan or update it to change order of targets within their corresponding steps.

An operation plan can be saved in the repository and executed as needed.

The following graphic is an example of a switchover plan created for an active/passive applications and database configuration. Note that it has WebLogic, Commerce, and database operations.

### Site Guard Operations

#### Operation Plan - scan04 to scan03 site switchover

<table>
<thead>
<tr>
<th>Target Name</th>
<th>Target Host</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-Scripts</td>
<td></td>
<td>Run Script</td>
</tr>
<tr>
<td>/home/oracle_ats/bin/SiteGuard/swap03Apps_swap04_m21.sh</td>
<td>scan04_m21.us.oracle.com</td>
<td>Run Script</td>
</tr>
<tr>
<td>/home/oracle_ats/bin/SiteGuard/swap03Apps_swap04_m22.sh</td>
<td>scan04_m22.us.oracle.com</td>
<td>Run Script</td>
</tr>
<tr>
<td>Oracle Weblogic Domains</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/Commerce_11_1_Primary_WLS_Domain_atg_domain/atg_domain</td>
<td></td>
<td>Stop Domain</td>
</tr>
<tr>
<td>Oracle Weblogic Servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oracle Weblogic Administration Servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oracle Weblogic Node Managers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage Unmount Scripts</td>
<td></td>
<td>Run Script</td>
</tr>
<tr>
<td>sh mount_umount.sh -o umount -f J01/apporacle_atg/product/fmw,J01/app/appDomain/atg, scan04_m21.us.oracle.com</td>
<td>scan04_m21.us.oracle.com</td>
<td>Run Script</td>
</tr>
<tr>
<td>sh mount_umount.sh -o umount -f J01/apporacle_atg/product/fmw,J01/app/appDomain/atg, scan04_m22.us.oracle.com</td>
<td>scan04_m22.us.oracle.com</td>
<td>Run Script</td>
</tr>
<tr>
<td>sh mount_umount.sh -o umount -f J01/apporacle_atg/product/fmw,J01/app/appDomain/atg, scan04_m23.us.oracle.com</td>
<td>scan04_m23.us.oracle.com</td>
<td>Run Script</td>
</tr>
<tr>
<td>sh mount_umount.sh -o umount -f J01/apporacle_atg/product/fmw,J01/app/appDomain/atg, scan04_m24.us.oracle.com</td>
<td>scan04_m24.us.oracle.com</td>
<td>Run Script</td>
</tr>
<tr>
<td>Storage Scripts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sh db2_storage_role_reversal.sh - scan03m-fe.us.oracle.com - root -n scan04m01.us.oracle.com</td>
<td>scan03m0019-es02.us.oracle.com</td>
<td>Run Store</td>
</tr>
<tr>
<td>sh mount_umount.sh -o umount -f J01/apporacle_atg/product/fmw,J01/app/appDomain/atg, scan03m0019-es02.us.oracle.com</td>
<td>scan03m0019-es02.us.oracle.com</td>
<td>Run Script</td>
</tr>
<tr>
<td>sh mount_umount.sh -o umount -f J01/apporacle_atg/product/fmw,J01/app/appDomain/atg, scan03m0021-es02.us.oracle.com</td>
<td>scan03m0021-es02.us.oracle.com</td>
<td>Run Script</td>
</tr>
<tr>
<td>sh mount_umount.sh -o umount -f J01/apporacle_atg/product/fmw,J01/app/appDomain/atg, scan03m0027-es02.us.oracle.com</td>
<td>scan03m0027-es02.us.oracle.com</td>
<td>Run Script</td>
</tr>
<tr>
<td>Database Instances</td>
<td></td>
<td>Switchover</td>
</tr>
<tr>
<td>commerce_swap04_commerce1</td>
<td>scan01edn01.us.oracle.com</td>
<td>Switchover</td>
</tr>
<tr>
<td>Oracle Weblogic Domains</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/Oracle Weblogic Servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/Oracle Weblogic Administration Servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oracle Weblogic Node Managers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Post-Scripts</td>
<td></td>
<td>Run Script</td>
</tr>
<tr>
<td>/home/oracle_ats/bin/sysGuidesSearchContent.sh</td>
<td>scan03m0019-es02.us.oracle.com</td>
<td>Run Script</td>
</tr>
<tr>
<td>/home/oracle_ats/bin/SiteGuard/swap03Apps_swap03m0019.sh</td>
<td>scan03m0019-es02.us.oracle.com</td>
<td>Run Script</td>
</tr>
<tr>
<td>/home/oracle_ats/bin/SiteGuard/swap03Apps_swap03m0020.sh</td>
<td>scan03m0020-es02.us.oracle.com</td>
<td>Run Script</td>
</tr>
</tbody>
</table>

The following graphic is an example of a switchover operation plan created for an active/active applications, active/passive database configuration. Note that it is only a database switchover operation.

### Site Guard Operations

#### Operation Plan - scan08 to scan01 DB switchover

<table>
<thead>
<tr>
<th>Target Name</th>
<th>Target Host</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Instances</td>
<td></td>
<td>Switchover</td>
</tr>
<tr>
<td>commerce_swap01_commerce1</td>
<td>scan01edn01.us.oracle.com</td>
<td>Switchover</td>
</tr>
</tbody>
</table>

The following graphic is an example of a switchover plan created for an active/passive applications and database configuration. Note that it has WebLogic, Commerce, and database operations.
Use Cases

The following sections describe the individual use cases which can be followed for the Oracle Commerce applications and database in both active/passive applications and database and active/active applications, active/passive database environment configurations.

Prechecks

Each operation plan that you create should be tested, using the Site Guard “Run Prechecks” feature, to verify that it succeeds. This feature is found on the Operations page of your site’s generic system target at Target > Generic System [lower top nav] > Site Guard > Operations.

Prechecks check all scripts and the credentials that are configured to execute the scripts. Additionally, Site Guard also checks the disaster recovery readiness of both database and underlying ZFS. Prechecks are configured by default to run at the beginning of any operation plan execution to ensure that all of its scripts and credentials are in the proper condition to execute successfully. This option can be disabled for each execution, if desired.

Use Cases for Active/Passive Applications and Database

The following are use cases that are specific to an active/passive applications and database environment configuration.

Applications and Database Switchover

An Oracle Commerce active/passive site switchover swaps the entire Oracle Commerce site from site 1 to site 2. It can be used for exercises, such as software or hardware upgrades, where you may need to take applications, the database, or hardware offline. A site switchover should probably be performed during off-hours or slow traffic periods, because it takes the first site offline before it brings up the second. Depending on the size of the site, this may take some time to complete.

You can also create switchover operation plans to switchover only applications or databases individually. When a switchover is initiated in this manner, Site Guard will consider the roles of both sites 1 and 2 as switched. Care should be taken when switching back to make sure that the site which the switchover is initiated from is set as the primary role.

Applications and Database Failover

An Oracle Commerce active/passive site failover swaps the entire Oracle Commerce site from site 1 to site 2. It is used in the event of a disaster recovery, when the primary site fails and needs to be completely failed over to the other site’s applications and database.

You can also create failover operation plans to fail over only applications or databases individually. When a failover is initiated in this manner, Site Guard will consider the roles of both sites 1 and 2 as switched. Care should be taken when bringing the original primary site back up to make sure that the site which is initiating the failover reversal is set as the primary role.
Applications and Database Start and Stop
Operation plans can be created in Site Guard to stop and start the entire site, all applications or all database instances only, or individual application servers or individual database instances. This eliminates the need to log in to consoles to stop some or all servers or instances. To create operation plans for some of the application servers or database instances, you must create a site stop or start plan and then remove those servers or instances that you do not wish to include in the plan.

Use Cases for Active/Active Applications With Active/Passive Database
With this type of environment configuration only the database must be switched over or failed over, because all applications in both sites are always active.

Database Switchover
This type of operation plan is set up just as you would set up a database-only switchover operation plan in an active/passive applications and database environment configuration. This operation is used when performing maintenance on hardware or upgrading software. As with the entire site switchover, it should be performed during off-hours or slow traffic periods, because the operation briefly takes the primary database offline while it switches over to the standby database. When a switchover is initiated in this manner, Site Guard will consider the roles of both sites 1 and 2 as switched. Care should be taken when switching back to make sure that the site which the switchover is initiated from is set as the primary role.

Database Failover
This type of operation plan is set up just as you would set up a database-only failover plan in an active/passive applications and database environment configuration. This operation is used for disaster recovery, when the primary database fails and must be completely failed over to the standby database on the other site. When a failover is initiated in this manner, Site Guard will consider the roles of both sites 1 and 2 as switched. Care should be taken when bringing the original primary database back up to make sure that the site which is initiating the failover reversal is set as the primary role.

Applications and Database Start and Stop
As with the start and stop operation plans in the active/passive applications and database environment configuration, operation plans can be created in Site Guard to stop and start the entire site, all applications or all database instances only, or individual application servers or individual database instances. This eliminates the need to log in to consoles to stop some or all servers or instances. As with the other start and stop plans, to create operation plans for some of the application servers or database instances, you must create a site stop or start plan and then remove those servers or instances that you do not wish to include in the plan.
Results – Site Guard Operations vs Manual Operations

Testing was performed on the Commerce MAA environments. For specific configuration details, see the "Oracle Commerce MAA Configuration Best Practices" white paper. Because switchover operations consume the most time, they were used as the testing criteria for comparisons of Site Guard operations to those performed manually. In addition to the extra time it takes to run commands manually, manual operations are extremely error prone. Therefore, a comparison of automated switchover processes to manual switchover processes was run. Table 1 shows the difference that Site Guard makes in executing operations.

The testing criteria were:

» Tests using Site Guard were executed on the Site Guard site’s operations page. Execution started when the confirmation to begin the operation was accepted.

» Tests using manual operations were executed from staged application consoles or staged ssh consoles:
  » Commerce applications were executed from the WebLogic Administration Console.
  » Commerce Guided Search applications were executed from ssh command-line scripts.
  » Database operations were executed from ssh consoles using the Data Guard command-line interface utility.
  » ZFS storage operations were executed from the ZFS Browser User Interface (BUI).

The fastest times of Site Guard operations and manual operations are shown in Table 1.

<table>
<thead>
<tr>
<th>Operation Type</th>
<th>Site Guard Operation Time</th>
<th>Manual Operation Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full site switchover (includes all checks and sub-operations)</td>
<td>20 minutes, 13 seconds</td>
<td>24 minutes, 37 seconds</td>
</tr>
<tr>
<td>Run primary site prescripts (stop Guided Search applications)</td>
<td>46 seconds</td>
<td>58 seconds</td>
</tr>
<tr>
<td>Stop primary WebLogic servers (admin and managed servers)</td>
<td>178 seconds</td>
<td>205 seconds</td>
</tr>
<tr>
<td>Stop primary WebLogic node managers</td>
<td>26 seconds</td>
<td>35 seconds</td>
</tr>
<tr>
<td>Unmount primary file systems</td>
<td>44 seconds</td>
<td>50 seconds</td>
</tr>
<tr>
<td>Reverse ZFS roles</td>
<td>223 seconds</td>
<td>297 seconds</td>
</tr>
<tr>
<td>Mount standby file systems</td>
<td>43 seconds</td>
<td>48 seconds</td>
</tr>
<tr>
<td>Switchover database (including pre/post validations)</td>
<td>137 seconds</td>
<td>140 seconds</td>
</tr>
<tr>
<td>Start standby node managers</td>
<td>61 seconds</td>
<td>58 seconds</td>
</tr>
<tr>
<td>Start standby WebLogic servers (admin and managed servers)</td>
<td>240 seconds</td>
<td>272 seconds</td>
</tr>
<tr>
<td>Run standby postscripts (start Guided Search applications)</td>
<td>50 seconds</td>
<td>63 seconds</td>
</tr>
</tbody>
</table>

When using manual ZFS commands, it is possible for the user to end up seeing multiple zombie replication packages on target appliances. This would make choosing the correct replication package very difficult. Site Guard automatically picks up the correct replication package and converts it into a read/write volume.
Best Practices for Disaster Readiness and Recovery

The following are the best practices for deploying a secondary site and recovery procedures in readiness for a site outage. The below support Site Guard operations:

- Deploy a second, geographically separated site that can run the Oracle Commerce workload in the event that the primary site is down. The environment configuration type determines the distance between the two sites.
- Use Data Guard to replicate all database changes to a standby database located on the secondary site.
- Take advantage of Oracle Active Data Guard to offload read-only queries to the standby database.
- Enable Oracle Flashback Database so that the old primary database can be quickly reinstated as a standby database in the event of a site failover.
- Replicate the Oracle Commerce File System to the secondary site if using an Active/Passive environment configuration. Develop procedures to reverse the direction of replication in the event of failover or switchover and to clone the replica for site testing.
- Export the Oracle Commerce File System primary, standby replica, and clones with different names to avoid mounting the incorrect one.
- Create different role-based database services for the Oracle Commerce database in primary, standby, and snapshot standby mode.
- Develop and document operational procedures that conform to the Oracle Commerce MAA state model and state transitions.
- Use Oracle Data Guard Broker to simplify Data Guard administration.
- Use the snapshot standby to provide an updatable replica of the primary database for temporary site testing.
- Use software, such as Site Guard, rather than manual operations, to remove human error from HA/DR functions.
Sample Scripts

Prescript

#!/bin/sh

if [ `ps -fu oracle_atg | grep "endeca" | grep -v grep | awk '{print $2}' | wc -l` = 0 ]; then
    echo "ENDECA SERVICES ARE NOT RUNNING"
    echo "exit 0"
    exit 0
else
    echo "Stopping Endeca Services"
    /usr/bin/sudo /sbin/service endeca_platform stop
fi

sleep 10

if [ `ps -fu oracle_atg | grep "endeca" | grep -v grep | awk '{print $2}' | wc -l` = 0 ]; then
    echo "exit 0"
    exit 0
else
    echo "exit 1"
    exit 1
fi
Postscript

#!/bin/sh

if [ `ps -fu oracle_atg | grep "endeca" | grep -v grep | awk '{print $2}' | wc -l` = 0 ]; then
    echo "Starting Endeca Services"
    /usr/bin/sudo /sbin/service endeca_platform start
else
    echo "ENDECA SERVICES ALREADY RUNNING"
fi

sleep 10

if [ `ps -fu oracle_atg | grep "endeca" | grep -v grep | awk '{print $2}' | wc -l` = 0 ]; then
    echo "exit 1"
    exit 1
else
    echo "exit 0"
    exit 0
fi
Unmount

sh mount_umount.sh -o umount -f
/u01/app/oracle_atg/product/fmw,/u01/app/wls/atgDomain/atg,/u01/app/oracle_atg/data,/u01/app/oracle_atg/product/oracle_endeca

Mount

sh mount_umount.sh -o mount -f
/u01/app/oracle_atg/product/fmw,/u01/app/wls/atgDomain/atg,/u01/app/oracle_atg/data,/u01/app/oracle_atg/product/oracle_endeca

sh mount_umount.sh -o mount -f
/u01/app/oracle_atg/product/fmw,/u01/app/wls/atgDomain/atg,/u01/app/oracle_atg/data

ZFS Storage

sh zfs_storage_role_reversal.sh -t scan04sn02.us.oracle.com -w MAA -h scan03sn-fe.us.oracle.com -u root -j ATG11 -p exalogic -q exalogic -x Y -c Y -e 600 -f N -z 300 -l Y -o switchover

sh zfs_storage_role_reversal.sh -t scan04sn02.us.oracle.com -w MAA -h scan03sn-fe.us.oracle.com -u root -j ATG11 -p exalogic -q exalogic -x Y -c N -f N -z 300 -l Y -o failover

sh zfs_storage_role_reversal.sh -t scan03sn-fe.us.oracle.com -w root -h scan04sn02.us.oracle.com -u MAA -j ATG11 -p exalogic -q exalogic -x Y -c Y -e 600 -f N -z 300 -l Y -o switchover

sh zfs_storage_role_reversal.sh -t scan03sn-fe.us.oracle.com -w root -h scan04sn02.us.oracle.com -u MAA -j ATG11 -p exalogic -q exalogic -x Y -c N -f N -z 300 -l Y -o failover
References
» Oracle MAA Best Practices
» Oracle Commerce MAA with a Case Study On Exadata and Exalogic
» Oracle Commerce MAA Configuration Best Practices
» Oracle Site Guard Documentation
» Oracle Fusion Middleware Documentation
» Automating Disaster Recovery using Oracle Site Guard
» Oracle Enterprise Manager 12c Cloud Control Documentation
» Oracle Commerce Platform Documentation
» Oracle Commerce Guided Search Documentation
» Oracle Database 12c (12.1) High Availability
» Oracle Fusion Middleware 12c High Availability Guide
» Oracle Fusion Middleware Disaster Recovery Guide
» Sun ZFS Storage 7000 System Administration Guide
» Oracle Fusion Middleware Disaster Recovery using Oracle’s Sun ZFS Storage Appliance
Automating Oracle Commerce High Availability and Disaster Recovery - Using Oracle Site Guard
August 2015
Author: Chuck Boucher