



Oracle EPM Disaster Recovery High Level Overview

Abstract:

Few Enterprise Performance Management (EPM) topics are more discussed and less understood than Disaster Recovery (DR). What does Disaster Recovery really mean? What are the Disaster Recovery options for Oracle EPM? And more importantly what are the nitty gritty details you absolutely have to get right? We will discuss two Disaster Recovery options for the most common EPM components. We will also go into detail on what a Disaster Recovery plan must include to be successful.

What is Disaster Recovery?

What does 'Disaster Recovery' really mean? Disaster Recovery is a nebulous term that can be used to describe or define any number of scenarios or situations. DR is defined by Dictionary.com as "Planning and implementation of procedures and facilities for use when essential systems are not available for a period of time long enough to have a significant impact on the business..." That definition is moderately helpful, except that it still leaves a great deal open to interpretation. What constitutes '...a significant impact on the business' and more importantly who decides for your organization?

Oracle's documentation outlines the following *purpose* for a Disaster Recovery; "Addresses service continuity so that in case of a disaster, service is maintained through a standby site". This begs the question; what constitutes a disaster? In the end each organization or business must decide for itself what constitutes a 'disaster', and who within the organization decides when one has occurred.

Your organization may have a more relaxed view of Disaster Recovery and may intend to initiate a failover plan in the event of performance issues, server failures, network issues, or other unplanned outages. While Disaster Recovery plans can be customized to meet these needs, they can also be mitigated using Fault Tolerant (FT) and Highly Available (HA) solutions.

For the purposes of this document, a 'disaster' is defined as anything that results in a site-wide failure of the primary Data Center. Therefore, Disaster Recovery is the processes and procedures necessary to restore essential systems (Oracle EPM for our purposes) in the event of a site-wide failure of the primary Data Center.

Disaster Recovery Options

There are an unlimited number of options for setting up a Disaster Recovery plan for an EPM 11.1.2.3 environment. They span the field from a simple export/import of your primary EPM application to another environment, to a full replication of Production to a dedicated Disaster Recovery environment. Many of the EPM components have similar recovery requirements or options. However, there are some EPM components with unique recovery requirements. Understanding these is paramount to a successful DR plan.

Putting Together a Disaster Recovery Solution

The critical first step is Requirements Gathering, which identifies the specific requirements for Disaster Recovery. Without requirements, it is impossible to properly design a DR solution. Once requirements are agreed upon, the method used for recovery is identified; replicating the Production Servers in a DR environment, repurposing another environment as the DR environment, or another custom solution can be determined. A detailed plan must then be created to meet every requirement identified; backups, schedule and method of backups, retention plans for backups, storage and replication of backups to the DR site, and owner of each backup, etc. When the backup plan is complete, it must be implemented, independently verified, and documented.

When the backups are in place and documented, a Recovery Plan should be thought out, documented, and any prerequisite pieces put in place (such as creating Essbase applications in the Target environment). A step-by-step recovery guide should then be created. The guide will include a High Level

Checklist - complete with task ownership, overseeing identification, and verification steps. A detailed process for each High Level Task should be included with step-by-step directions for completing each task. These steps should be executable by anyone familiar with Oracle EPM Systems but with zero environment specific knowledge. Finally, verification/validation testing should be documented, including testing owners and pass/fail qualifications.

Once the proper documentation, backups, and processes are in place, a failover test should be executed. The initial test should focus on documentation accuracy and a successful failover from an Infrastructure Perspective. Application availability and 100% functionality should be verified; however data is not a critical part of this initial test. Following a successful infrastructure test, a failover test including data validation and end-to-end testing should be conducted.

During all tests, the DR Failover documentation should be followed step-by-step. Any discrepancies should be noted and documentation updated. This will ensure subsequent tests are successful regardless of the parties involved.

Dedicated Disaster Recovery Environment

Now that we have looked at the different EPM components and their recovery requirements, let us look at a couple of ways to put them all together. First up is a dedicated DR environment solution. In this example, the DR Environment was installed and configured following the same steps that were used to build the Production EPM environment. The server and RDBMS entries were configured using the Production instance names; local host aliases were used to ensure all entries were resolved to the DR components. We will then look at a custom solution that repurposes a Quality Assurance (QA) environment as a DR solution. This solution makes less use of replication and tends to be more complicated. It does however have the benefit of being less expensive, usually!

This first example is an EPM 11.1.2.3 implementation. The DR environment was built by repeating the steps used to install and configure the Production environment. Prior to configuring the DR environment, local host aliases were created on each of the servers, mapping the Production server names and DR server names to the DR server IP addresses. This ensured the EPM configurations could use the Production server names and eliminate a mismatch within the replicated Oracle schemas.

The Production applications must be migrated to the DR environment to 'seed' the environment. Once the DR environment is seeded, replication and other processes are put in place to ensure the RPO and RTO requirements can be met. For example, command scripts are used to take nightly LCM exports of Shared Services, Planning applications, and Native Essbase applications. Shell scripts are used to take Level 0 data exports of all Essbase applications. All exports are stored on either NAS or SAN, which is replicated to the DR environment.

Repurposed Disaster Recovery Environment

This example is of an EPM 11.1.2.3 implementation. The plan is based on repurposing the Quality Assurance (QA) environment as the Production environment in the event of a DR. The existing QA applications, security, and data are not critical. While efforts will be made to back up the QA objects as part of the failover, their survival is not paramount. The Recovery Point Objective (RPO) and Recovery Time Objective are (RPO: HFM = 0, Planning/Essbase < 24 hours)(RTO < 8 hours). The Recovery Time

Objective is impacted by a number of items beyond the control of the Oracle EPM Team. Some of these include network services, database services, Domain Name Services, and LDAP/MSAD authentication services. The RTO assumes all of these 'required' services are available and does not take into account the time required to restore those services. Limiting its dependencies on these other teams, especially DBAs can help make the DR plan or strategy more efficient when the time comes.

The QA environment was architected to mirror the Production environment and it consists of the same number, size, and configuration of servers. The EPM installation and configuration also mirrors that of Production. However, the instance names, dBs, server names, etc. are all unique to the QA environment. The DR Solution is based on migrating the required objects from Production to QA (DR) in the event of a disaster. The key being that the 'export' portion of the migration must be done prior to the Production environment being lost due to a disaster. Each EPM component is taken individually to ensure its export migration requirements are met. Those steps are then scripted through batch and shell scripts, and automated through third party tools. The import portion of the migrations is primarily a manual effort, although automating some of the pieces should be possible.

The Life Cycle Management utility is the primary tool used for creating the required backups or migration exports needed for DR. LCM export migrations are created for Planning, HFM, as well as Essbase applications and EPM System Security from the Production environment. These are stored on a NAS that is replicated to the QA environment.

A weekly process is run to take cold backups of the entire Essbase volume, including all Essbase application objects, configuration files, and the Essbase.sec (security) file. These Essbase backups and exports are stored on SAN which is replicated to the QA environment.

In the event of a DR failover, the exported content is imported using the same method or tool used for the export. When all objects have been imported, base level functionality testing is completed. This includes a Health Check checklist that ensures basic functionality is working. HFM and Planning/Essbase financial reports are executed to validate security, data source connectivity, HFM and Planning/Essbase functionality, and Foundation and RA Services are working as expected. Following the base level testing, the application owners begin data validation testing. This includes a deeper dive into the full EPM functionality and data validation. This level of testing closely resembles Systems Integration Testing (SIT) to ensure data flows through the entire system properly.

Critical Details

There are many steps in designing and implementing an Oracle EPM Disaster Recovery solution; from choosing dedicated vs. shared environment, to using Life Cycle Management or RDBMS schema exports. None of these is more important and critical to the success of the plan than requirements gathering. Many times a disaster recovery solution is developed without ever having consulted the business or application owners to identify or understand the actual requirements. Are all Production applications required in a DR scenario? What level of resiliency is necessary in a DR environment? Will the upstream and downstream systems change? Will integrations change in DR? Will a full complement of users access the system in a DR scenario? What are the actual Recovery Point Objective (RPO) and Recovery Time Objective (RTO)? And what costs are you willing to accept to meet those requirements? Many of these questions are never asked or not fully answered or understood; by one or both sides. For example, an application owner that insists on an RPO of zero (zero data loss) for an Essbase application, likely doesn't understand the implications in terms of downtime to meet this 'requirement'.

The requirements must be gathered and challenged to ensure 1) that they are truly 'requirements' and 2) that the costs for meeting the requirements are understood.

Another critical piece is the backup strategy employed to meet the Recovery Point Objective. Many EPM components can be properly and easily backed up using the Life Cycle Management's command line utility. LCM migrations can be scripted using the LCM GUI and automated using 3rd party scheduling tools. Most LCM migrations can be run during normal business processes with little or no impact to the end user. They can be scheduled to run as often as necessary to meet defined RPOs.

The use of replication goes hand in hand with a proper backup methodology. Configuring the EPM components to use NAS or SAN simplifies replicating the data to the Disaster Recovery environment.

Lastly, once the DR plan is documented and implemented, it must be tested. Sometimes, the plan must be tested repeatedly to ensure the process, as documented is complete, accurate, and meets the DR requirements. The test should be executed by the individuals tasked with executing the plan in a true Disaster Recovery scenario. The plan should be followed step-by-step to ensure there are no actions or information assumed. This is to ensure the team can complete the test in the time allowed. Updates to the DR plan are typically required during the first few tests. In the end, the plan should be able to be fully executed by individuals outside of the design team, without assistance.

About CheckPoint

CheckPoint Consulting is one of the largest privately held boutique firms focused on providing complete Enterprise Performance Management (EPM) solutions to Fortune 1000 companies. With over 20 years of experience in the Oracle Hyperion space, Managing Partners Timothy J. Halk and Gregory M. Feld lead a team of highly qualified and multi-certified consultants experienced in all aspects of EPM and Business Analytics. As a Certified Oracle Platinum Partner, CheckPoint has successfully implemented hundreds of EPM solutions including Strategy Management, Financial Close and Reporting, Oracle Planning, Budgeting, and Forecasting, Oracle Profitability and Cost Management, and Oracle Business Intelligence Tools and Technology.



100 West Big Beaver | Suite 200
Troy, Michigan 48084
800.601.0760
checkpointllc.com