Oracle Financial Services Analytical Applications

Installation and Configuration Guide

Version 8.1.0.0.0+

ORACLE®
FINANCIAL SERVICES

DOCUMENT CONTROL

Version Number	Revision Date	Changes Done
1.0	Created: September 2023	Captured the Best Practices for OFSAA Disaster Recovery process.

TABLE OF CONTENTS

ORACLE®

Background

Disaster Recovery (DR) involves a set of policies and procedures to enable the recovery or continuation of vital technology infrastructure and systems, following a natural or human-induced disaster. A Disaster Recovery Plan (DRP) is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster.

Introduction

DRP preparation is an integral part of the contingency planning. This document serves as a reference document for preparation of specific DRP.

Objective

The objective of this document is to establish a process to reconfigure OFSAA instances (PROD and DR) in case of a disaster.

Note: This document is not applicable for setting up a High Availability (HA) instance. It should be used to ensure service continuity through maintenance of a standby site.

Assumptions

This document has been prepared after considering the below assumptions:

1. Considers failure for any single OFSAA component(s)/ sub-system(s) as failure for complete OFSAA system.

2. An appropriate backup strategy for OFSAA File System (`$FIC_HOME` and `FTPSHARE`) and Oracle Database(s) is already in place.

3. Installation of OFSAA platform, applications on PROD and other mandatory software have also been completed on DR instance (Standby site) as outlined in the section Standby Site Setup and DR instance was tested functionally. It is important to note that both the instances should be of the same release version.

4. Considers OFSAA 8.1.0.0.0 as the deployed version.

5. Customer has a valid license for Oracle Data Guard or similar software/ tools.

6. DR database is setup as a Physical Standby Database. (Read in-line with Point 1 in the Exclusions section. For example, OFS Behavior Detection Application requires DB structures to be similar as the Primary DB.)

7. Impact to business due to unscheduled downtime for *n* hours. No real time switch-over to DR setup.

8. Hardware configurations (in terms of RAM/ CPU/ CORE) may vary. It is also mandatory that the file system references such the OS mount and folders, Web Application Server Profiles/ Domains/ Deployed Paths and so on are exactly the same.

   For example, if OFSAA has been installed on PROD instance under `/usr/ofsaa`, ensure it is installed under `/usr/ofsaa` even on DR instance.

9. Deployment architecture is similar for PROD and DR setup. For example, if PROD is installed on a web application server cluster, the DR installation too is expected to be on a web application server cluster.

10. Some of the IP Address/ Host names of systems in the PROD and DR systems are different. The same are stored in OFSAA configuration schema and files of the respective systems.

11. Business user access to DR instance is via a URL, which is different or same from the PROD instance access.

> **NOTE:** The steps in this document consider the OFSAA 8.1.0.0.0 release. Kindly check with Oracle Support if the documented steps are applicable for any other specific OFSAA release.

Exclusions

1. This document is generic to OFSAA suite of applications. It does not consider any OFSAA Application specific configurations.

2. This document does not consider reporting layer configuration for OBIEE. (Can be modified later if anything found.)

3. This document does not propose any detailed Oracle Data Guard/ similar software configuration steps. See the Oracle Data Guard product specific manuals for configuration.

4. Archived Audit Trail Data in DR instance (restored from PROD) does not get updated with the DR instance data such as IP, Port and so on upon restoration.

5. The table `batch_parameter` is not updated with the new IP after you run `portc.jar`. This table holds the batch execution details of batches that were executed earlier. The table `batch_parameter_master` holds the new IP after you run `portc.jar`.

Standby Site Setup

Follow the OFSAA Cloning guide to perform the installation (on DR setup).

> **NOTE:** This document considers symmetric topology between the production and standby sites. However, the document and steps can be enhanced further to support asymmetric topology.
> The Oracle Database setup on DR instance should be performed using `RMAN` *duplicate* feature.
> The storage replication job between production and standby site is to be performed at periodic intervals.

Approach

Though there are various ways in which the DR process can be devised, after discussion on the requirements, following is the recommended approach (to be used as reference only) to devise any further changes/ modifications to the processes as per the use cases.

For the purpose of this topic, let us consider the below OFSAA deployment scenario for PROD and DR instance:
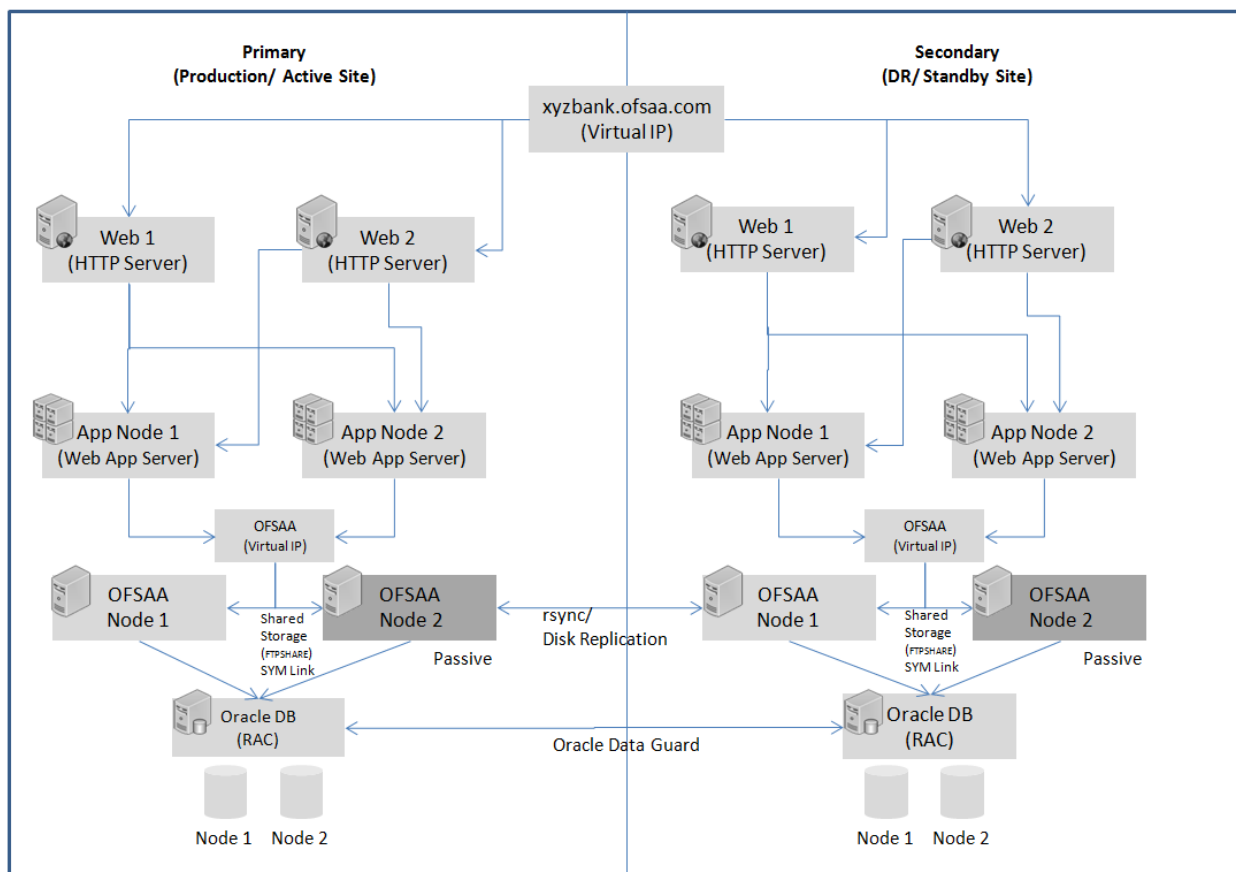
In the above diagram, the DR setup is proposed to be a mirror of the PROD setup. Noted below are the different components of an OFSAA instance and their respective configuration recommendations for a DR scenario.

1. **Database Schemas**:

    An OFSAA instance consists of one CONFIGURATION schema (CONFIG) and one or more data schemas.

    For data replication of all schemas from PROD to DR, install and configure Oracle Data Guard. Thus, any DML/ DDL operations performed on PROD are replicated on DR Database.

ORACLE®

Note: Contact your DBA for Oracle Data Guard installation and configuration. See Oracle Data Guard Configurations for reference on ODG configurations.

2. **File System**:

An OFSAA instance consists of one installation folder (FIC_HOME) where the product binaries and configuration files get deployed. Additionally, the OFSAA instance also consists of one data staging / metadata repository / downloads area (FTPSHARE).

For replication of file system from PROD to DR, use storage replication technologies. For example, install and configure any OS utility such as **Remote Sync** (*rsync*). Thus, any file updates, add or delete operations performed on PROD are replicated on DR file system.

Note the following points:

- You may need to configure a CRON job to sync-up the file system at frequent/ desired intervals.

- Only one-way sync-up has been configured, that is from PROD to DR.

- Refer the OS specific documentation on configuring rsync over SSH for added security.

    Example of rsync command:

    ```
    rsync –uavzP /scratch/ofsaaapp/ftpshare
    ofsaauser@drserver:/scratch/ofsaaapp/ftpshare
    ```

- OFSAA patch installations should be performed only on PROD instance. Promotions of patches to DR instance are taken care as part of the sync-up processes for Database and File System components.

Steps to Bring Up the DR Instance

In the event of a disaster, perform the following steps to bring up the DR instance in use:

Assumption: It is assumed that the DB and File System sync-up processes have been completed before beginning with the following steps.

Step 1 – Ensure a latest snapshot/ backup of the OFSAA DR instance File System and DB is available. This can be useful for rollback in case of a failure to bring up the DR instance.

Step 1a – Shutdown the OFSAA PROD services such as the web/ web app servers and OFSAA services. Ensure the OFSAA application is not accessible to business users by accessing the URL.

Step 1b – Stop the file system replication from PROD site to the STANDBY site.

NOTE: One or more of the OFSAA PROD services/ replication service may have already been stopped due to the failure.

ORACLE

Step 1c – Perform a failover or switchover of the Oracle databases using Oracle Data Guard.

Step 2 – Login to the OFSAA DR setup and navigate to the `$FIC_HOME/` folder.

Step 3 - Execute the command:

```
java –jar PortC.jar DMP
```

NOTE: In case Production Database goes down, the `DynamicServices.xml` file should be updated with the DR database JDBC URL before executing the above command.

Step 4 – Edit the **DefaultPorts.properties** file generated from the previous step. Specify the IP Address/ Hostname, Ports and Path changes in this file as per the DR instance. Save the file.

Step 5 – Execute the following command to update the details in DR file system/ database:

```
java –jar PortC.jar UPD
```

Step 6 - Navigate to $FIC_WEB_HOME and execute the command:

```
./ant.sh.
```

This generates the OFSAA web archive (.ear/ .war) file(s). For information on generating application archives, see *OFS AAAI Application Pack Installation and Configuration Guide* available in OTN.

Step 7 – Navigate to `$FIC_HOME/ficapp/common/FICServer/bin/` and start the OFSAA DR services. For information on start/ stop of OFSAA services, see *OFS AAAI Application Pack Installation and Configuration Guide* available in OTN.

Step 8a – Start the DR Web Server/ Web Application Server services. Access the Admin/ Deployment Console and deploy the archive(s) generated in Step 6. For information on deploying application archives, see *OFS AAAI Application Pack Installation and Configuration Guide* available in OTN.

Step 8b – Configure the Global/ Network Load Balancer to reroute requests to the standby site.

Step 9 – Access the OFSAA DR application from browser by entering the URL.

Step 10 – At this point the standby site/ DR site has assumed the production role and the site "switchover" is complete.

Oracle Data Guard Configurations

This section outlines the configurations performed while executing the DRP. The configuration of Oracle Data Guard and/or the replication should be devised in consultation with your DBA and referring to Oracle Data Guard Documentation.

- Enable `archivelog` mode on primary database if it is not already enabled.

- Create Standby database on standby DB server using `RMAN` duplicate.

- Modify Primary database to write archive logs on both primary and standby database.

- Modify Primary database to enable swapping of roles, that is, primary to standby and vice-versa.

- Entries for the primary and standby databases are required in the `tnsnames.ora` files on both servers.

- Create standby redo logs on both primary and stand by database to allow switchover of roles.

- Start redo apply on the standby database either using real-time apply or delayed apply based on company policy.

- There are three options for Protection mode such as Maximum Availability, Maximum Performance (default), and Maximum Protection. This should be set according to company policy.

- After setup is complete, test log transport by forcing a log switch on the primary. Then confirm whether the new archived redo log has arrived at the standby server and has been applied.

ORACLE®

ORACLE®

OFSAA

Disaster Recovery Process Best Practices Guide

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/us/industries/financial-services/