ORACLE

SOA PaaS DR Overview

SOAMP on OCI Disaster Recovery

PaaS MAA team

2023 July

Program agenda

1. Introduction
2. SOA Cloud Service & SOA Marketplace
3. SOAMP DR Topology
4. SOAMP DR Setup
5. SOAMP DR main Lifecycle operations
6. Links

Program agenda

1. **Introduction**
2. SOA Cloud Service & SOA Marketplace
3. SOAMP DR Topology
4. SOAMP DR Setup
5. SOAMP DR main Lifecycle operations
6. Links

INTRODUCTION
Maximum Availability Architecture

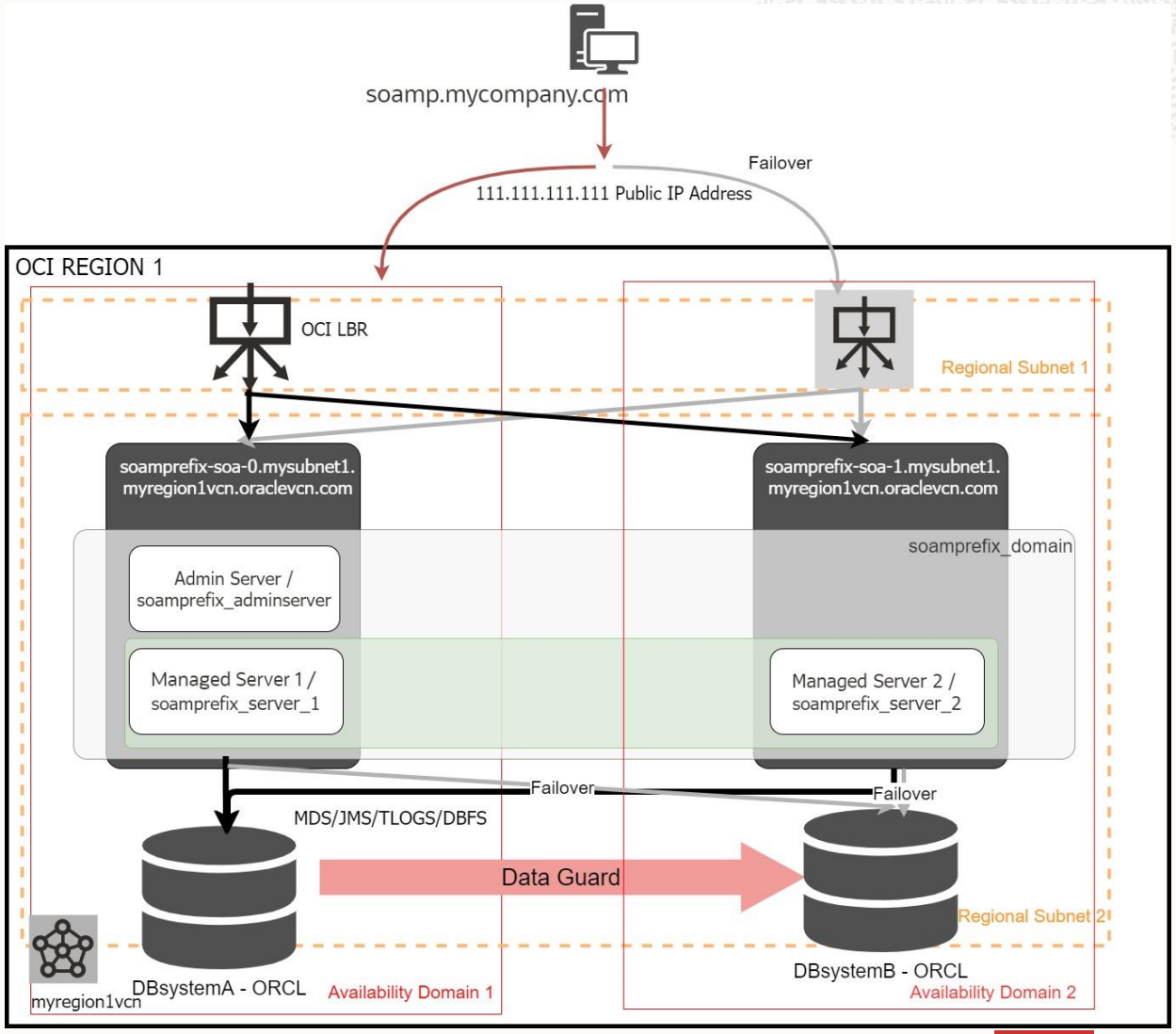
- Oracle Maximum Availability Architectures (MAA)
  - Oracle's best practices blueprint that use Oracle's proven technologies to provide Disaster Recovery solutions for all the Oracle Stack.
  - The key goal of MAA is to achieve optimal high availability, data protection and disaster recovery for Oracle customers at the lowest cost and complexity, by minimizing the RPO and RTO of the system
  - MAA consists of Reference Architectures, configuration practices and HA Life Cycle operational best practices applicable for non-engineered systems, engineered systems, non-cloud and cloud deployments.

- Disaster Recovery (DR) solutions are **MAA architectures** intended to protect critical mission systems by providing a secondary system in another geographical area.
- Disaster Recovery protection is also required for systems running in the Cloud, like WLS for OCI and Oracle SOA Suite on Marketplace (SOAMP).
  - DR is **additional protection** to High Availability. SOAMP and WLS for OCI provide High Availability by default

INTRODUCTION

High Availability in the scope of a single OCI Region

- Oracle SOA Cloud Service uses the Active **high availability** (HA) policy **for compute** when it provisions instance compute nodes: virtual machines (VM) fail over automatically to another physical compute node in the same compute zone in case the primary compute node fails.
- A **different Fault Domain** is used by default in SOACS and SOAMP for each compute instance used by the WLS cluster
- In **SOAMP**, when using **regional subnets**, the provisioning process places **each compute** instance used by the WLS cluster in a **different Availability Domain**
- Additionally, the **front-end LBR** in OCI used by SOAMP **is regional and failover** across ADs provided **OOTB** for regions with more than one AD
- The **Database** can also be protected **against AD failures** by using **Oracle Data Guard** and placing the standby in a different ADs (see on-prem MDC AA for Datasource configuration)
- This configuration, however, **does not provide protection against** disasters that affect an **entire region**



INTRODUCTION
MAA topology for SOA on Cloud

- The Disaster Recovery solution for SOA in Cloud was initially released in 2016 and has been implemented by many customers.
- 3 documents released to address each SOA Cloud service type and infrastructure:
  - For SOA Marketplace — SOA Suite on Oracle Cloud Infrastructure Marketplace Disaster Recovery
  - ~~For SOACS on OCI~~ — SOA Cloud Service Disaster Recovery on OCI - Production and DR in the Cloud
  - ~~For SOACS on OCI Classic~~ — SOA Cloud Service Disaster Recovery on OCI Classic - Production and DR in the Cloud

- The solution provided by each paper consists of:
  - A recommended **Disaster Recovery topology**
  - A list of steps and automation tools for the **initial DR setup**
  - A list of a recommendations and steps for the system's **lifecycle management**

INTRODUCTION
MAA topology for SOA on Cloud

- The DR solution for SOAMP systems involves setting up a standby system in a “geographically-separated” Oracle Cloud Data Center. It uses an **active-passive** model.

Based on solid and proven DR technologies

- While there are some unique considerations to a cloud disaster recovery configuration, it follows the same Oracle MAA best practices as any Oracle Fusion Middleware (FMW) and Oracle Database deployment
- Based on Data Guard (more than 20 years providing DR)

Cross-region

- The DR solution for SOAMP and WLS for OCI systems involves setting up a standby system at a **geographically** different Oracle Cloud Data Center, in a **active-passive** model.
- Cross-region DR is a real protection for any unforeseen (natural or man-made) event that can put your organization at risk

Provides the best RTO and RPO

- By utilizing high availability and disaster protection capabilities provided by Oracle Fusion Middleware and Oracle Database. RTO for a typical switchover: 15-30 min*

INTRODUCTION
Customer experiences

- SOAMP DR paper defines the **reference topology for disaster recovery**
- However, variations on the reference topology have been implemented by customers to address particular customer cases:
  - Cross AD instead cross Region
  - Cross ADs using single frontend LBR
  - Setup custom DB systems in non-OCI managed DG configuration
  - DR Setup integrated with customer's automations tools
  - Integration with JMS client applications
  - …

Program agenda

1. Introduction
2. **SOA Cloud Service & SOA Marketplace**
3. SOAMP DR Topology
4. SOAMP DR Setup
5. SOAMP DR main Lifecycle operations
6. Links

SOA Cloud Service & SOA Marketplace
Introduction

- Both Oracle SOA Cloud Service (SOACS) and Oracle SOA Suite on Marketplace (SOAMP) provide a PaaS (Platform as a Service) computing platform solution for running the SOA applications in the cloud.
- SOACS
  - It was initially released for OCI Classic and then migrated to OCI
  - It is based on **PSM** (Platform Service Manager), hence it is deprecated solution
- SOAMP
  - It is a **OCI native solution**, provisioned via Marketplace images
  - **Recommended** for new deployments

- Complete list of differences Between Oracle SOA Cloud Service and Oracle SOA Suite on Marketplace:

https://docs.oracle.com/en/cloud/paas/soa-cloud/soa-marketplace/soamp-differences-soa-cloud-service-and-oracle-soa-suite-marketplace.html

SOA Cloud Service & SOA Marketplace

Comparison in Disaster Recovery area

Similarities

- The **DR topology is the same** (frontend can differ, OTD/LBR in SOACS and LBR in SOAMP)
- **Setup** procedure is almost the same
- **Main lifecycle operations** are the same

Differences

- **WLS config replica methods:**
  - SOACS supports only the DBFS method
  - SOAMP supports DBFS method, FSS with rsync, and Block Volume cross-region replica
- **New features/improvements** are introduced only in the **SOAMP** solution. Examples: FSS with rsync, scale-out steps, tnsalias etc.
- **DR setup documents are different**
  - To accommodate better the specifics (provisioning menus, resource naming convention, differences in lifecycle operations, setup, etc.) and for future changes affecting only to one of them.
- **SOAMP uses an improved DRS framework**
  - Main features aligned, but differences between each other (FSS with rsync method support, new runtime options, etc.)
- **SOACS can automate switchover tasks with Oracle Site Guard**
- **SOAMP can automate switchover tasks with Full Stack DR**

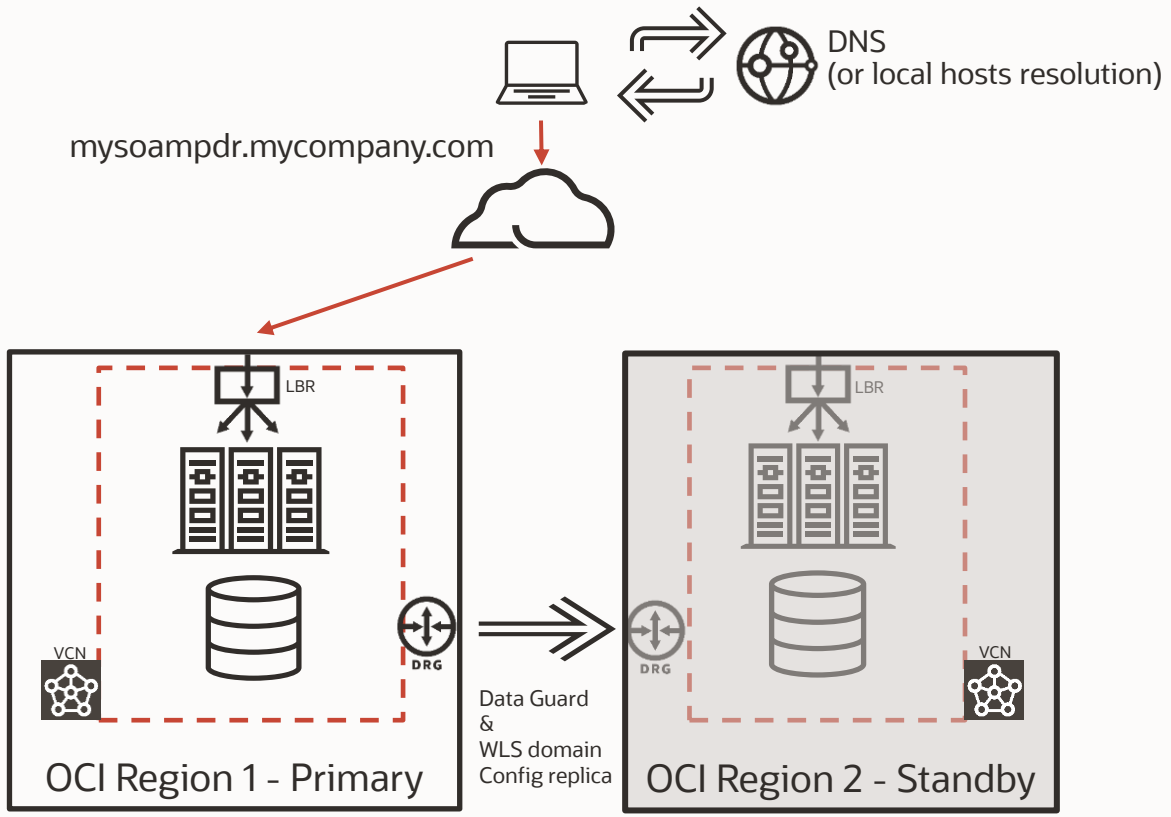
Program agenda

1. Introduction
2. SOA Cloud Service & SOA Marketplace
3. **SOAMP DR Topology**
4. SOAMP DR Setup
5. SOAMP DR main Lifecycle operations
6. Links

SOAMP DR Topology

Overview

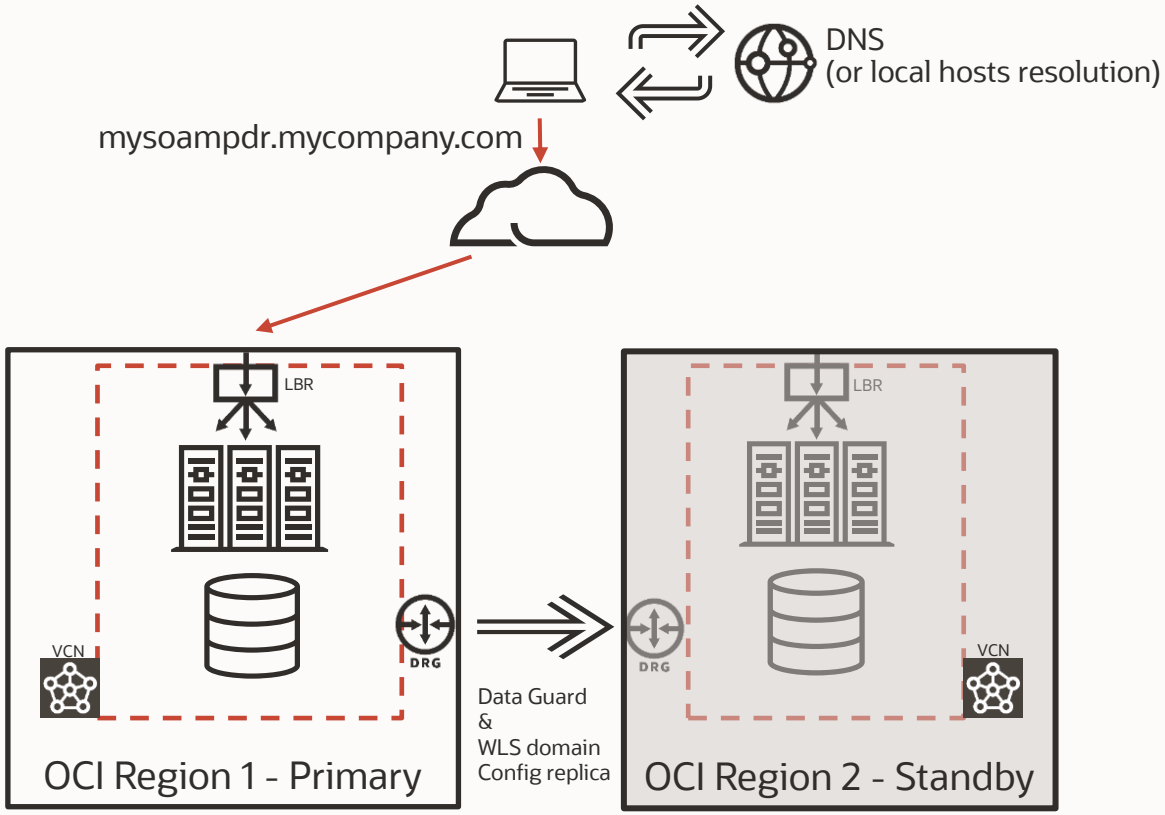
- **Active-Passive** model:
  - Primary SOA & DB system in one region
  - Standby SOA & DB system in a different region
- DB systems configured with **Data Guard**
- **Standby WLS domain is a replica** of the primary domain (same name, schemas, passwords, etc., only db connect string is different, now with tnsalias). Three options for the WLS config replica:
  - DBFS based method
  - FSS with RSYNC method
  - Block Volume replication
- **Unique frontend hostname** to access to the system. Is a “virtual name” that points to the IP of the LBR of the site with primary role
- Network communication between primary and secondary networks via **Dynamic Routing Gateway** (recommended)



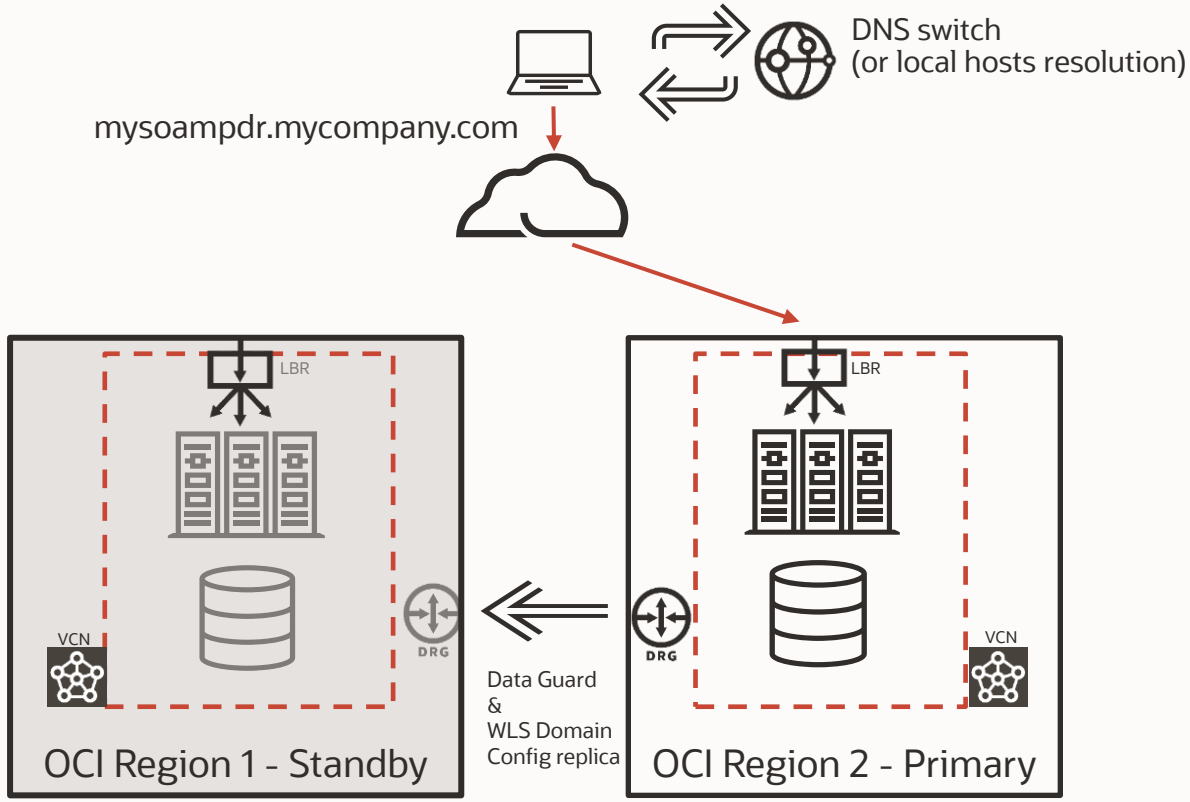
SOAMP DR Topology

Overview

Normal Operation



After a Switchover



SOAMP DR Topology

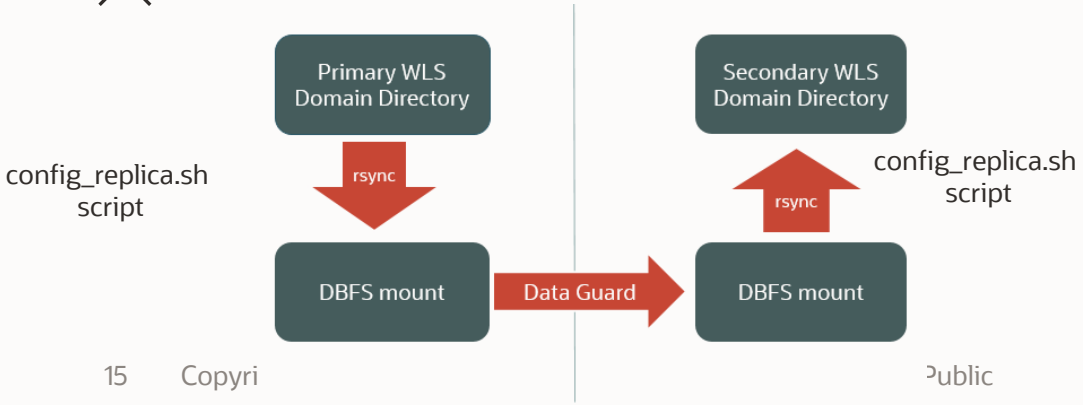
WebLogic Domain config replica using a staging location

DBFS based method

- DBFS mount as staging file system for a copy of the WLS domain.
- Uses underlying Data Guard replica to copy the domain to standby region.
- Recommended for any latency (high or low).
- Supported in SOACS and SOAMP DR.

✓ Takes advantage of the robustness of the DG replica
More resilient behavior through Oracle Driver's retry logic

✗ More complex to configure (db client required) and maintain

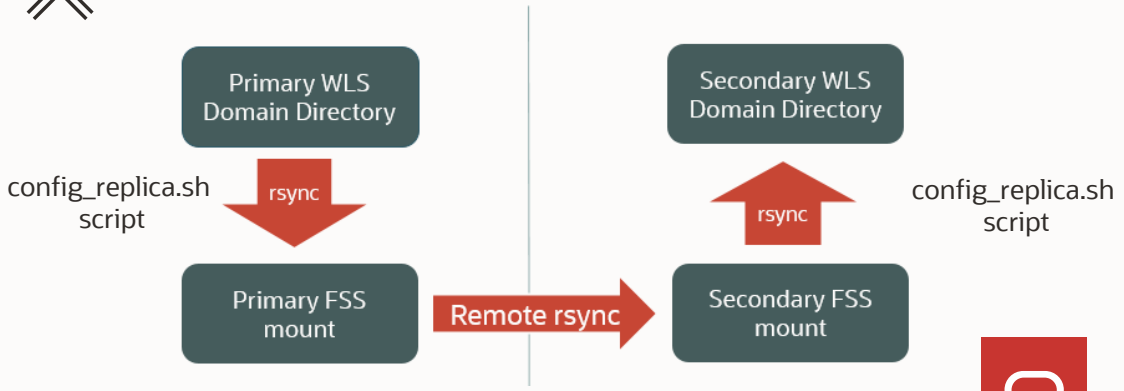


FSS with RSYNC

- File Storage Service (FSS) as staging file system for a copy of the WLS domain.
- Uses rsync to copy the domain to standby region and additional checksum verifications added by the MAA team.
- Recommended when latency is low.*
- Supported only in **SOAMP DR.**

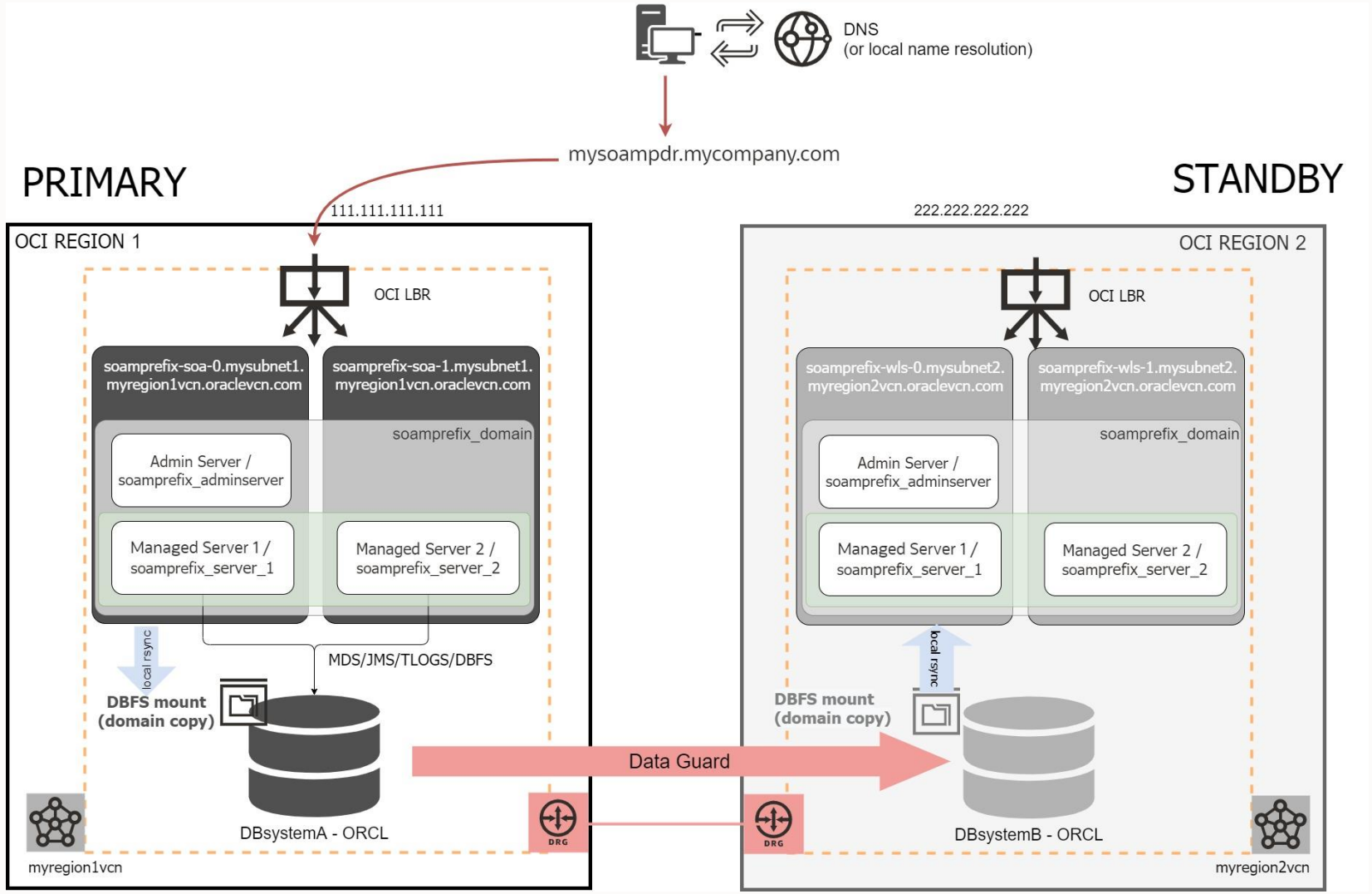
✓ Easy to configure and maintain

✗ More sensible to latency and jitter



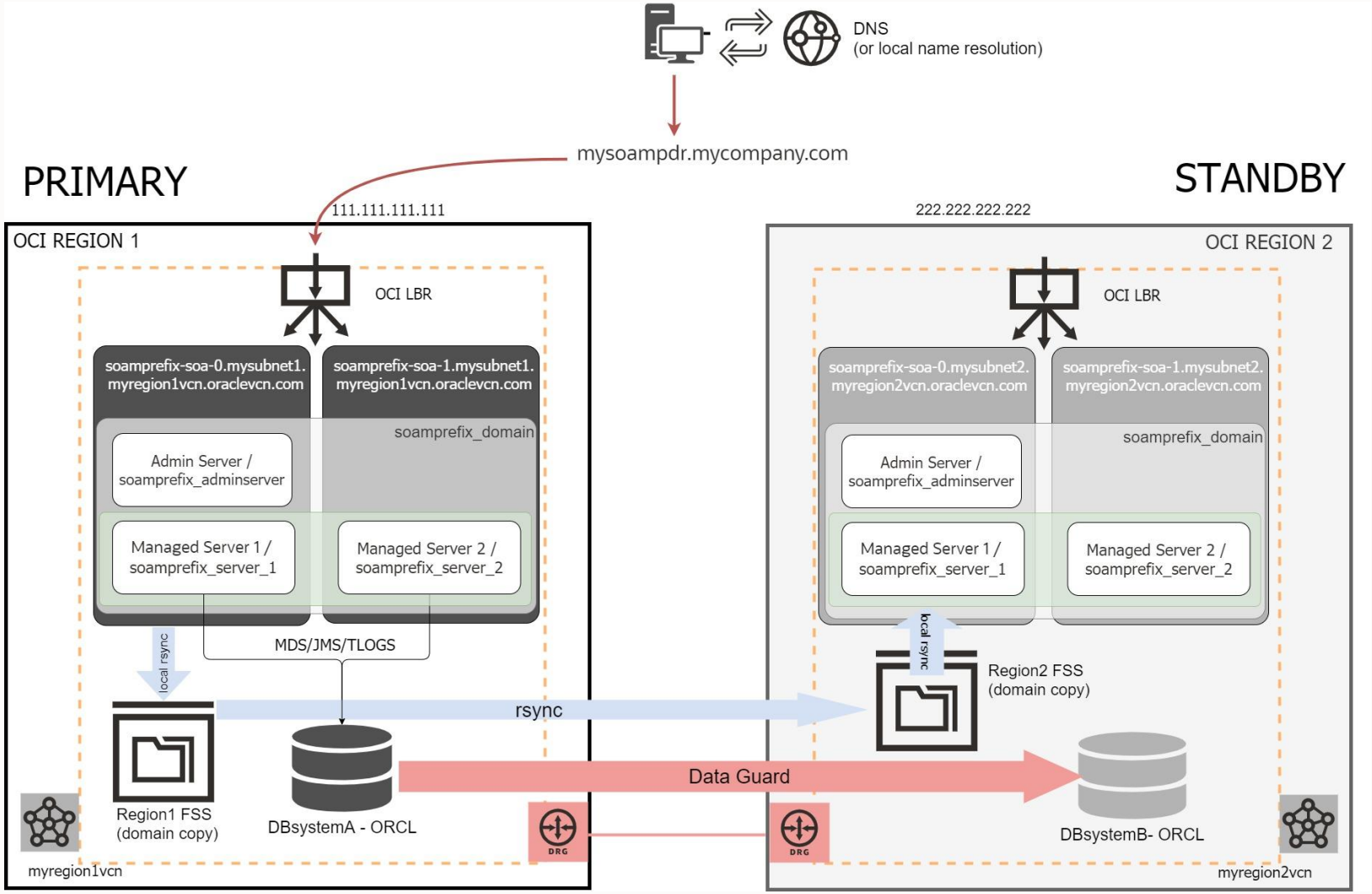
SOAMP DR Topology

Topology - DBFS based method



SOAMP DR Topology

Topology - FSS with RSYNC method



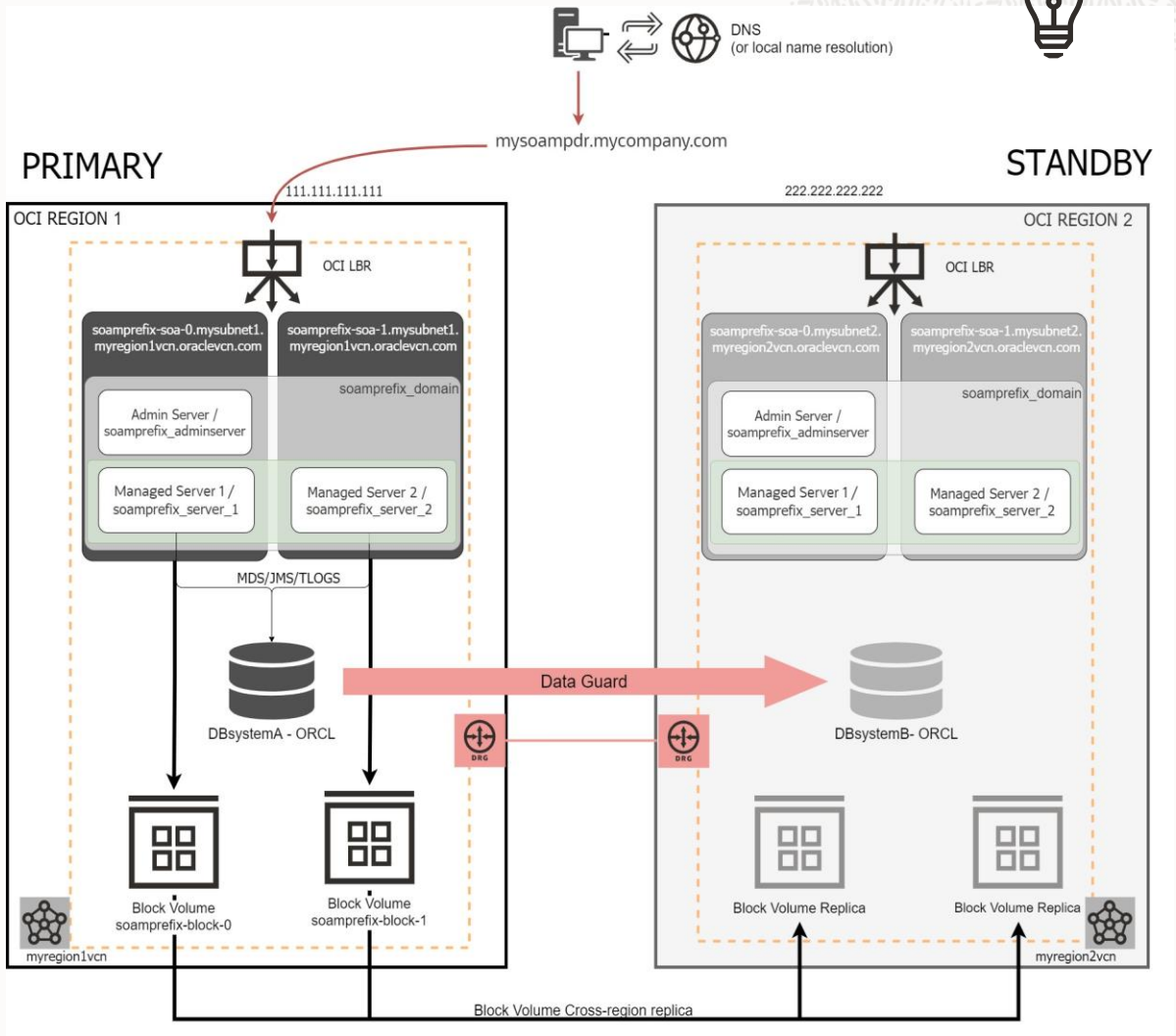
Supported in SOAMP only

SOAMP DR Topology

Topology – Block Volume cross-region replica

Supported in SOAMP only

- The **Block Volume** containing the WLS Domain **is replicated** using Cross-Region Block Volume Replication feature (automatic asynchronous replication to other region)
- No stage location is used, hence, the **setup** and ongoing **replication differs significantly** from the DBFS and FSS-rsync approaches.
- Main Disadvantages of this model:
  - Slightly higher RTO due to BV attachments
  - Slightly more complex Switchover operations
- Main advantages:
  - It is a general-purpose solution applicable not only to FMW- based PaaS services.
  - Provides continuous and automated replica.

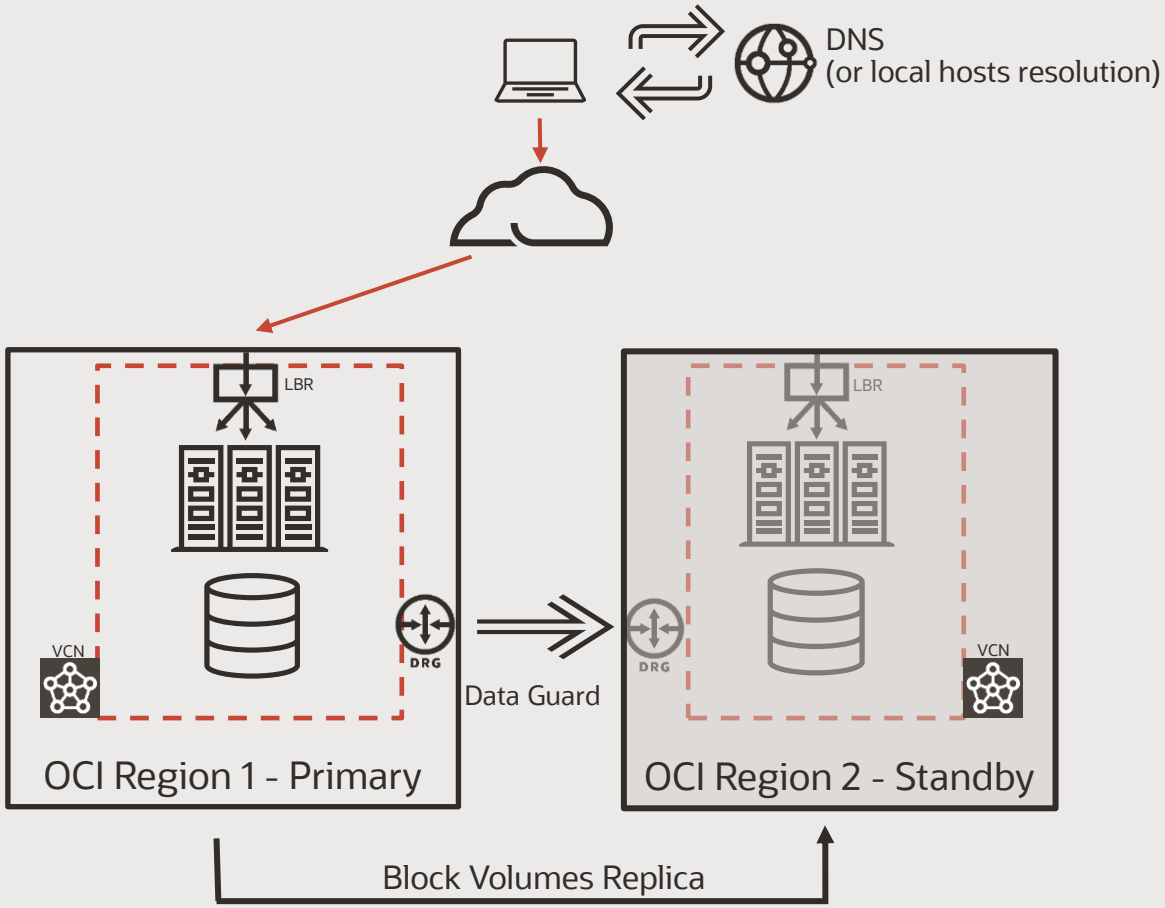


SOAMP DR Topology

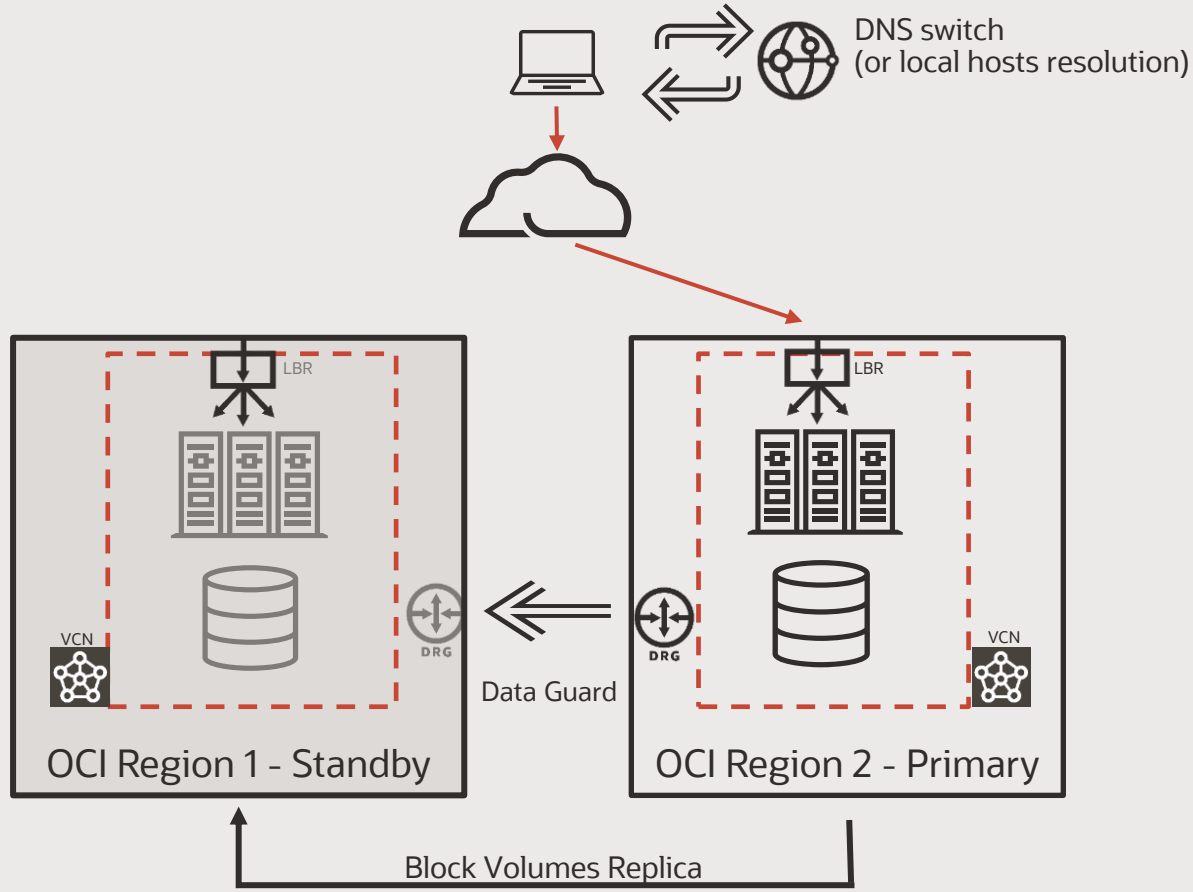
Topology – Block Volume cross-region replica (NEW since July 2021!)

Supported in SOAMP only

Normal Operation



After a Switchover



Program agenda

1. Introduction
2. SOA Cloud Service & SOA Marketplace
3. SOAMP DR Topology
4. **SOAMP DR Setup**
5. SOAMP DR main Lifecycle operations
6. Links

SOAMP DR setup

Setup vs Management

DR Setup

- Initial configuration, **one time operation**
- DR setup has evolved since the initial documents:
  - **Automation level 0: Manual step-by-step:**
    - Initially the DR setup was a very manual step-by-step (copy folders, tar, scp, replacements, etc.)
  - **Automation level 1: DR setup scripts:**
    - When SOACS was released in OCI, disaster recovery setup scripts were created to automate many steps.
  - **Automation level 3: DRS tool:**
    - In 2019, the DRS tool was released to wrap the DR setup scripts in a single operation, orchestrate the execution, and automate some other additional tasks (aliases, etc.).

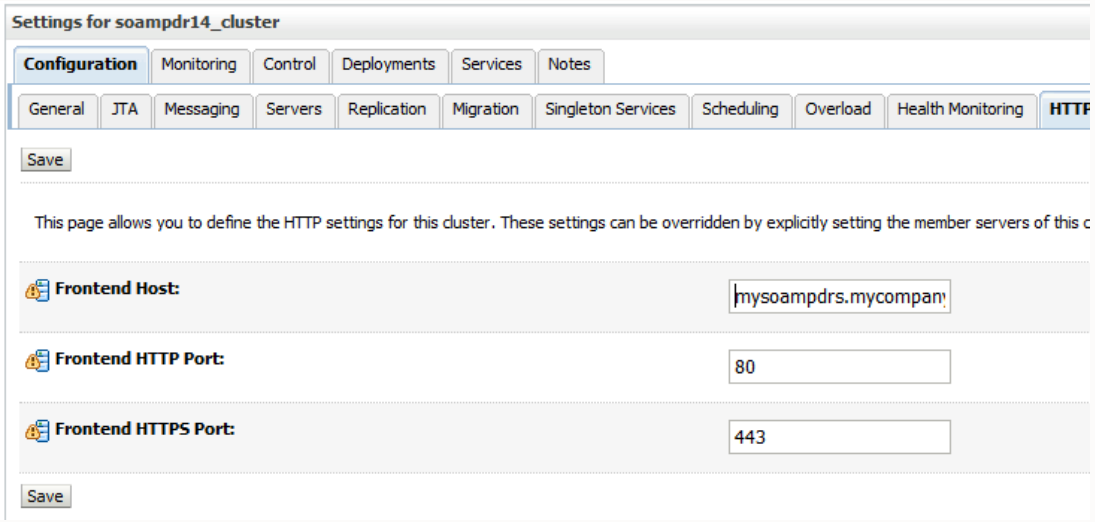
DR Management

- Similar to on premise. Specific DR operations are:
  - **Switchovers/Failover**. They can be done:
    - Manually
    - Oracle FSDR (when configured)
  - **WebLogic config replication**
    - Oracle provides a script to replicate midtier configuration

Regardless how the setup is done (more manually by using DR setup scripts, or more automated by using DRS tool), the resulting DR topology is supported and runtime is the same.

SOAMP DR setup
Starting point

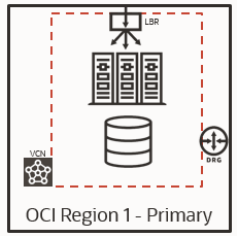
- Starting point assumption: **the primary SOA system already exists** (along with its LBR and DB system)
- The impact of the DR setup on the existing system minimal:
  - Down time needed (a restart of the managed servers) only in case the frontend name was not already configure or frontend is not going to be re-used for DR



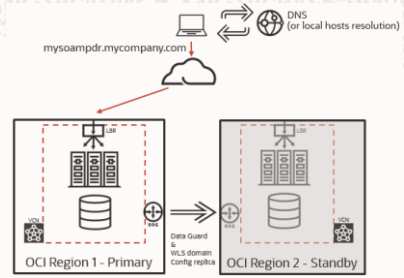
- DR setup process has been designed to be **idempotent**: each step can be retried.

SOAMP DR setup

Steps



Primary SOAMP exists



DR setup complete

1. Choose a virtual frontend name and register in DNS

2. Prepare primary midtier to use the virtual frontend name and TNS alias

3. Setup secondary database

4. Provision secondary SOA

5. Prepare secondary mid-tier for virtual frontend and TNS alias

6. Configure the staging mounts for WebLogic config replication (in FSS method)

7. Download and run DRS

SOAMP DR setup

Details on the step 3

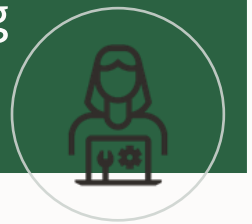
1. Choose a virtual frontend name and register in DNS
2. Prepare primary midtier to use the virtual frontend name and TNS alias
3. Setup secondary database
4. Provision secondary SOA
5. Prepare secondary mid-tier for virtual frontend and TNS alias
6. Configure the staging mounts for WebLogic config replication (in FSS method)
7. Download and run DRS

Option 1) Configuring using OCI Console ("auto DG")

- Since March 2020, OCI console **allows to configure Data Guard cross-region** (before, only cross-ad was supported)
- Some requirements: same tenancy, same compartment, communication between Dynamic Routing Gateway

Option 2) Configuring data guard manually ("manual DG")

- For scenarios where 1) does not apply, it can be done manually.
- First, provision standby database as a regular DB System (same version, shape, password, etc. than primary)
- Second, use scripts provided in the paper to configure it as standby (rman duplicate, dgmgrl commands. etc),
  - *dataguardit_primary*.sh and *dataguardit_standby_root*.sh



The secondary database is created as a Data Guard physical standby of the primary database. Two ways to do this.

SOAMP DR setup

Details on the step 4

- Convert secondary database into **SNAPSHOT STANDBY** (fully updatable database, any modification is lost when it is converted to physical standby again)

```
[oracle@drDBa ~]$ dgmgrl sys/your_sys_password@primary_db_unqname

DGMGRL> CONVERT DATABASE secondary_db_unqname to SNAPSHOT STANDBY;
Converting database "secondary_db_unqname " to a Snapshot Standby
 database, please wait...
Database "secondary_db_unqname" converted successfully
```

- Provision secondary SOA as usual, pointing to the secondary database

SOAMP DR setup

Details on the step 7

- **The Disaster Recovery Setup (DRS) framework** is written in python and wraps the fmw_dr_setup scripts, orchestrates the execution of the DR setup, and runs prechecks and post checks.
- To run DRS tool:
  - Choose a host that has SSH access to all the hosts in the DR (primary and secondary midtier and db hosts)
  - Download DRS tool, upload to the host, untar
  - Review README.md and customize drs_user_config.yaml with environment values
  - Run "sh drs_run.sh --config_dr"

- DRS tool can be re-run:
  - Before, shutdown secondary processes if they are running (admin, wls, nodemanagers)
  - Restore the domain backup that DRS does in secondary hosts
  - Verify that standby database is in snapshot standby mode
  - Re-run "sh drs_run.sh --config_dr –skip_checks"

Program agenda

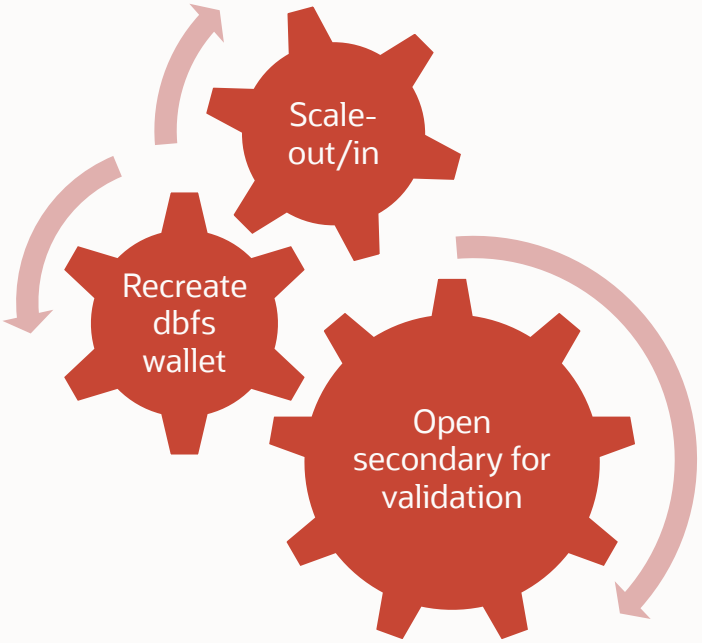
1. Introduction
2. SOA Cloud Service & SOA Marketplace
3. SOAMP DR Topology
4. SOAMP DR Setup
5. **SOAMP DR main Lifecycle operations**
6. Links

SOAMP DR Lifecycle Operations

Main lifecycle operations in DR

- WLS Config replication
- Switchover
- Failover

Other lifecycle operations



SOAMP DR Lifecycle Operations

WLS Config Replication

OPTION 1)

WHEN DOMAIN CHANGES ARE **INFREQUENT**

- Apply the configuration **manually twice**

	STEP
1	Apply the configuration change normally in the primary site
2	Convert the standby database to a snapshot standby
3	Start (if it wasn't started) the WebLogic Administration Server on the secondary site
4	Repeat the configuration change in the secondary site
5	Revert the database to physical standby

OPTION 2)

WHEN DOMAIN CHANGES ARE **FREQUENT**

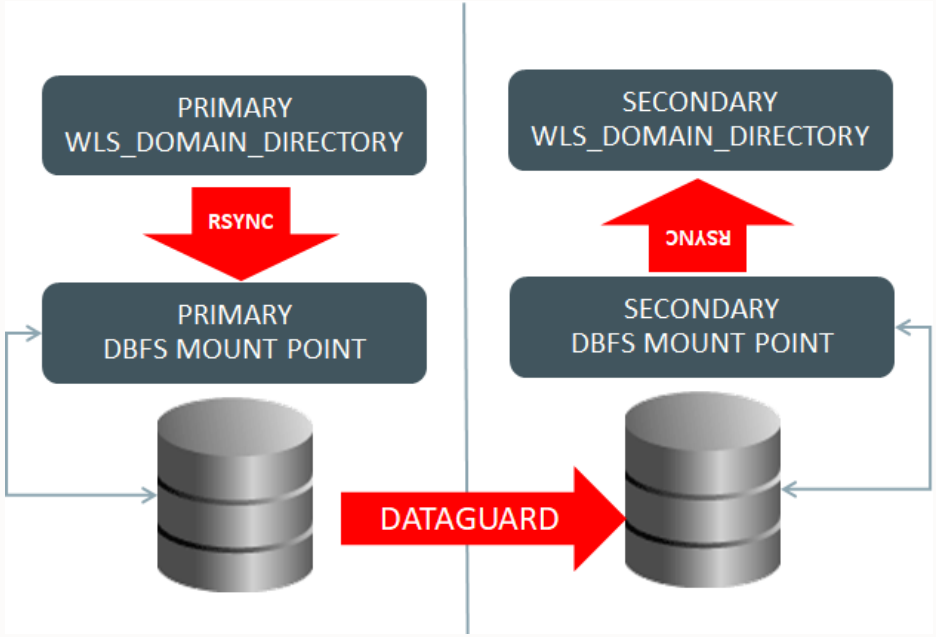
- Use the provided script to replicate changes:
  - Run the script in **primary WLS Administration host:**
    - It copies primary domain to the staging mount (DBFS or FSS), skipping some specific folders.
    - In FSS with rsync approach, the script rsyncs the copy to the secondary FSS too.
    - In DBFS approach, DBFS content is automatically replicated to secondary site by DG.
  - Run script in **secondary WLS Administration host:**
    - It copies from the secondary staging mount (DBFS or FSS) to secondary domain

SOAMP DR Lifecycle Operations

WLS Config Replication

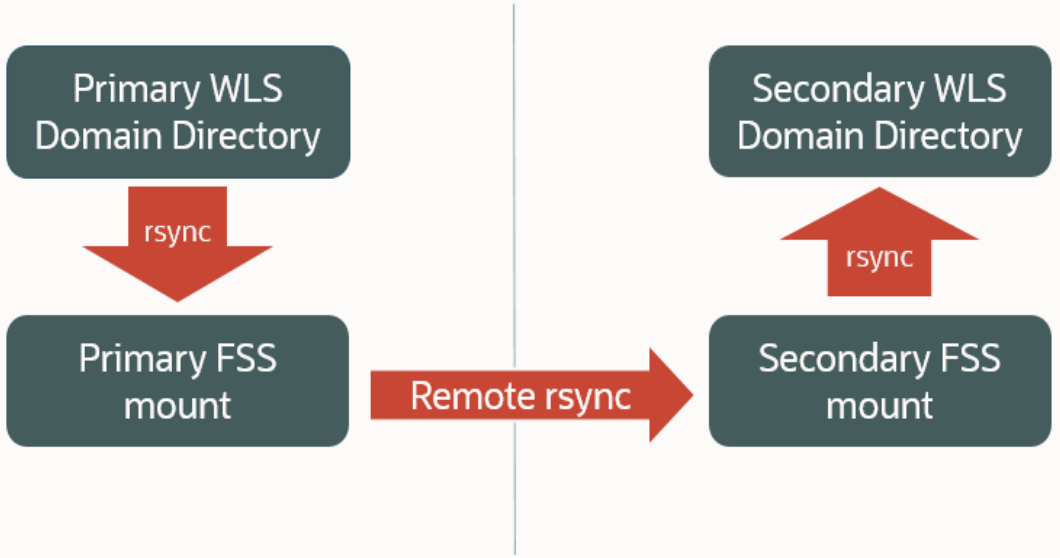
DBFS approach

- Script config_replica.sh



FSS with rsync approach

- Script config_replica.sh

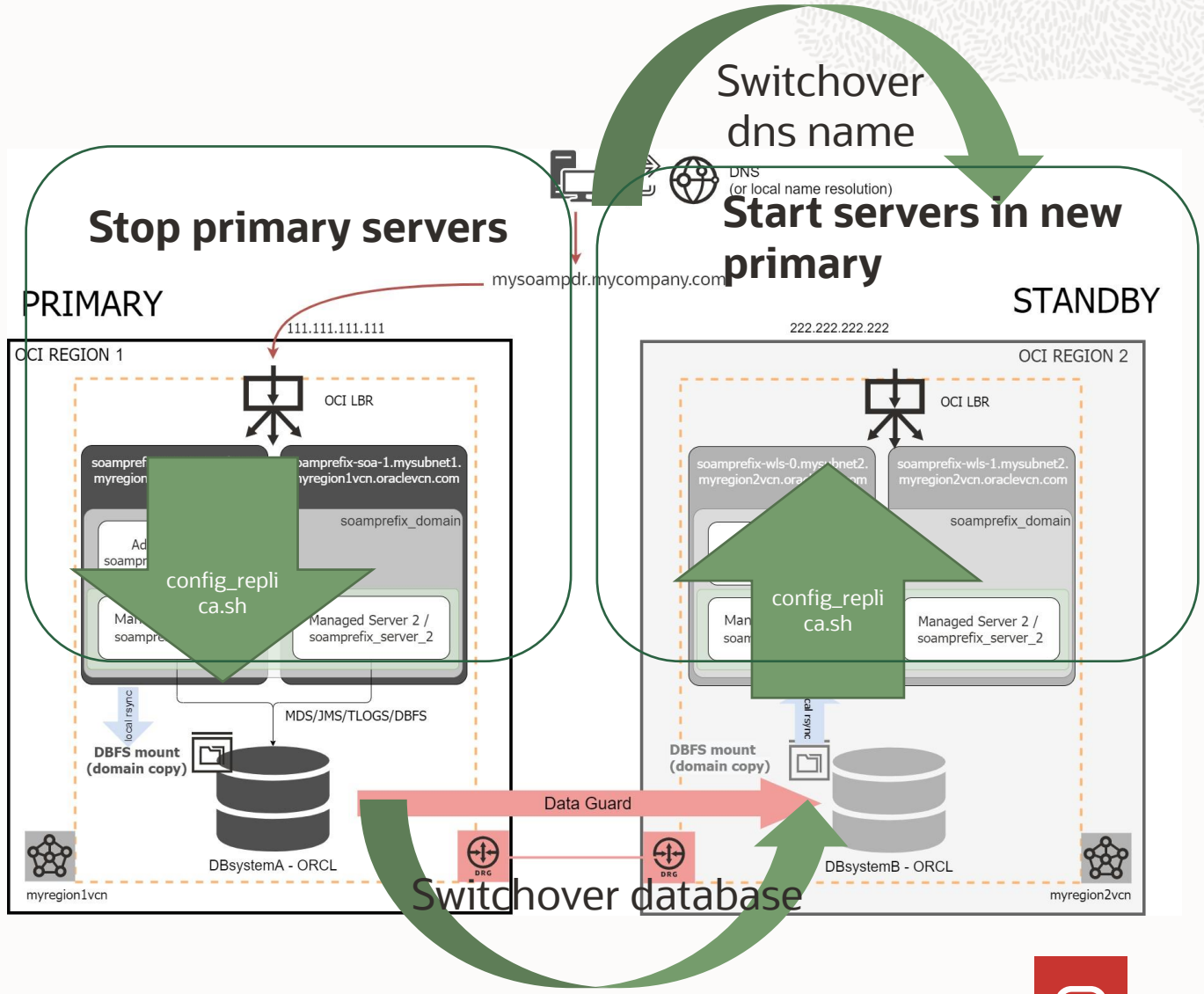


SOAMP DR Lifecycle Operations
Switchover

A switchover is a planned operation where an administrator reverts the roles of the two sites.

	SWITCHOVER STEP	DETAILS
1	Propagate any pending configuration changes	Run config_replica.sh in primary admin node and then in secondary admin node
2	Stop servers in primary Site	Use WebLogic Administration Server Console or scripts to stop managed servers in primary Site (the admin server can remain up).
3	Switchover DNS name	Perform the required DNS push in the DNS server hosting the names used by the system or alter the file host resolution in clients to point the front end address of the system to the public IP used by LBR in site2
4	Switchover Database	Use DG broker in primary db host to perform the switchover. As user oracle: # dgmgrl sys/your_sys_password@primary_db_unqname DGMGRL> switchover to “secondary_db_unqname”
5	Start the servers in secondary site (new primary)	Restart secondary Admin Server if configuration changes were replicated while this was standby, so they take effect. Start secondary managed servers (using the WebLogic Console or scripts)

Switchback consists of the same steps, but in the other way



SOAMP DR Lifecycle Operations
Switchover

RTO time based on our latest tests in SOAMP:

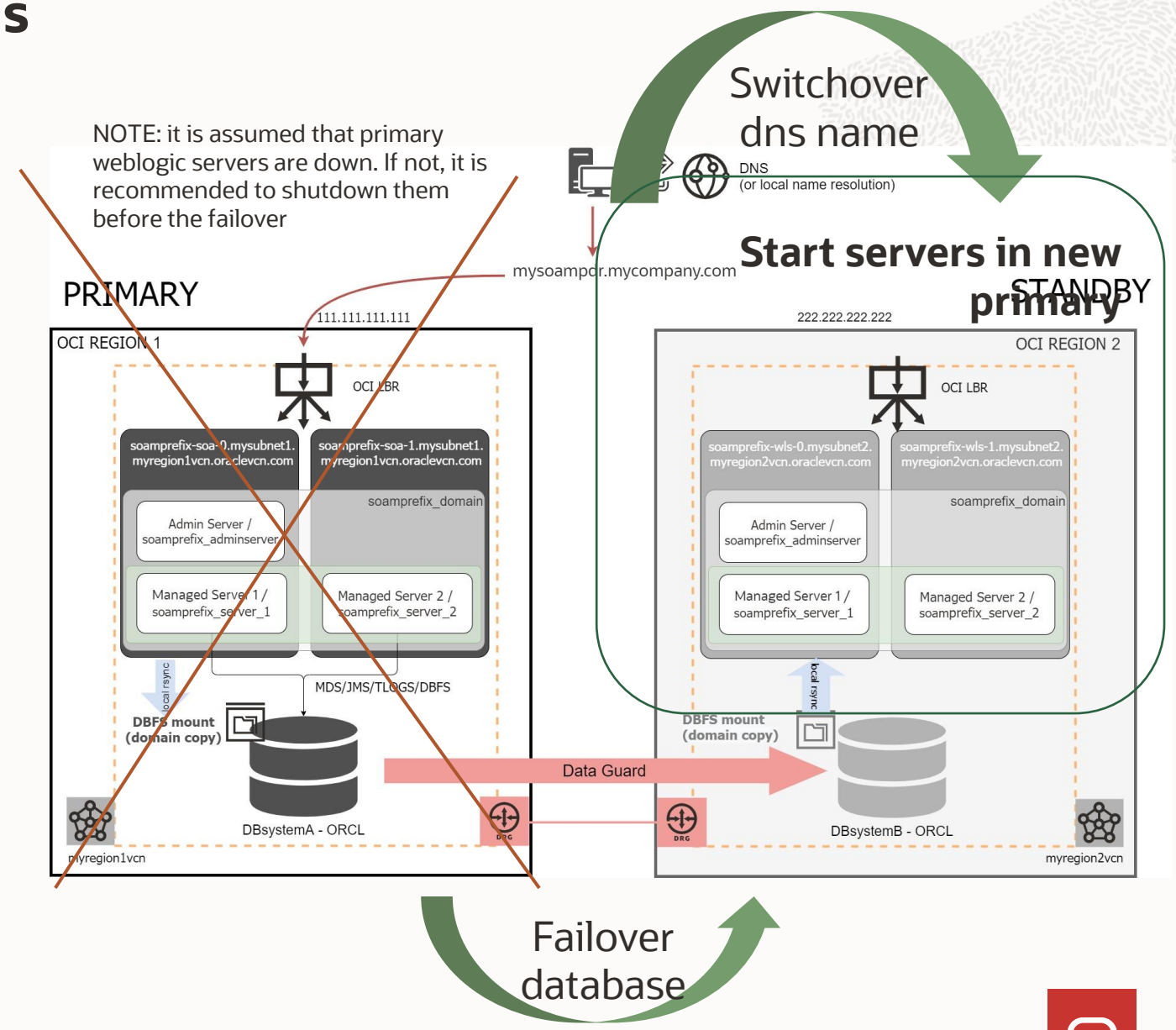
	SWITCHOVER STEP	DETAILS	
1	Propagate any pending configuration changes	Run config_replica.sh in primary admin node and then in secondary admin	→ ~ 6 min
2	Stop servers in primary Site	Use WebLogic Administration Server Console or scripts to stop managed servers in primary Site (the admin server can remain up).	→ ~ 4 min (complete normal shutdown)
3	Switchover DNS name	Perform the required DNS push in the DNS server hosting the names used by the system or alter the file host resolution in clients to point the front end address of the system to the public IP used by LBR in site2	→ (depends on DNS, TTL)
4	Switchover Database	Use DG broker in primary db host to perform the switchover. As user oracle: # dgmgrl sys/your_sys_password@primary_db_unqname DGMGRL> switchover to “secondary_db_unqname”	→ ~ 3 min
5	Start the servers in secondary site (new primary)	Restart secondary Admin Server if configuration changes were replicated while this was standby, so they take effect. Start secondary managed servers (using the WebLogic Console or scripts)	→ ~ 10 min (starting admin first and then managed)

Of course these times can vary depending on the hosts shapes, tuning, etc., but:
TOTAL SWITCHOVER time in 15-30 min range

SOAMP DR Lifecycle Operations
Failover

A failover operation is performed when the primary site becomes unavailable, and it is commonly an unplanned operation.

	FAILOVER STEP	DETAILS
1	Switchover DNS name	Perform the required DNS push in the DNS server hosting the names used by the system or alter the file host resolution in clients to point the front end address of the system to the public IP used by LBR in site2
2	Failover Database	Use DB broker in secondary db host to perform the failover. As user oracle: $ dgmgrl sys/your_sys_password@secondary_db_unqname DGMGRL> failover to “secondary_db_unqname”
3	Start the servers in secondary site	Restart secondary admin server if configuration changes were replicated while this was the standby, so they take effect. Start secondary managed servers (use the WebLogic Console or scripts)

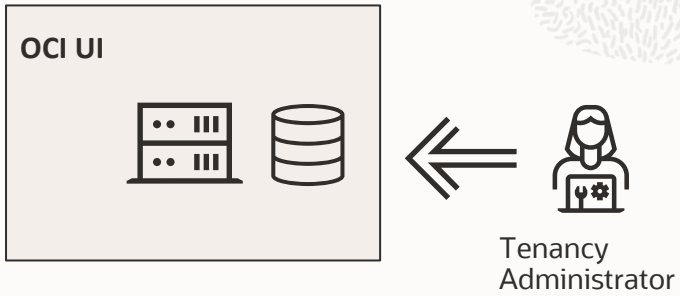


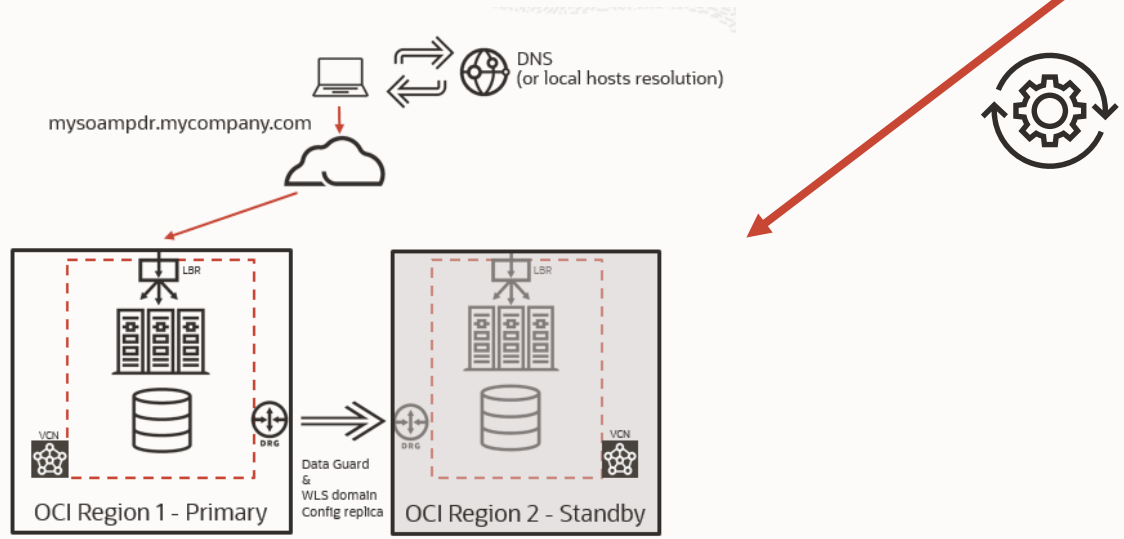
SOAMP DR Lifecycle Operations

Using Oracle FSDR for Switchover/Failover

Full stack switchover can be orchestrated by Oracle **Full Stack DR**

Required setup documented in separated playbook





Perform switchover/failover using FSDR

SOAMP DR latest features/updates

- Updated manual Data Guard setup scripts
- RTO and RPO considerations
- Patching recommendations
- Using OCI DNS views for hostname “aliasing”
- Added support to additional local standby database (besides remote DG standby)
- End-to-End Validation for Configuration Replication
- Using TNS alias in the Datasources
- Support for Autonomous Database Dedicated/Shared
- ExaCS details

Program agenda

1. Introduction
2. SOA Cloud Service & SOA Marketplace
3. SOAMP DR Topology
4. SOAMP DR Setup
5. SOAMP DR main Lifecycle operations
6. **Links**

LINKS
Documents in OTN

Summary of SOA on Cloud Disaster Recovery documents:

- SOA on Marketplace DR:

SOA Suite on Oracle Cloud Infrastructure Marketplace Disaster Recovery
(https://www.oracle.com/a/tech/docs/maa-soamp-dr.pdf)

- SOACS on OCI DR:

SOA Cloud Service Disaster Recovery on OCI - Production and DR in the Cloud
(https://www.oracle.com/a/tech/docs/maa-soacs-dr-oci.pdf)

- Oracle FSDR:

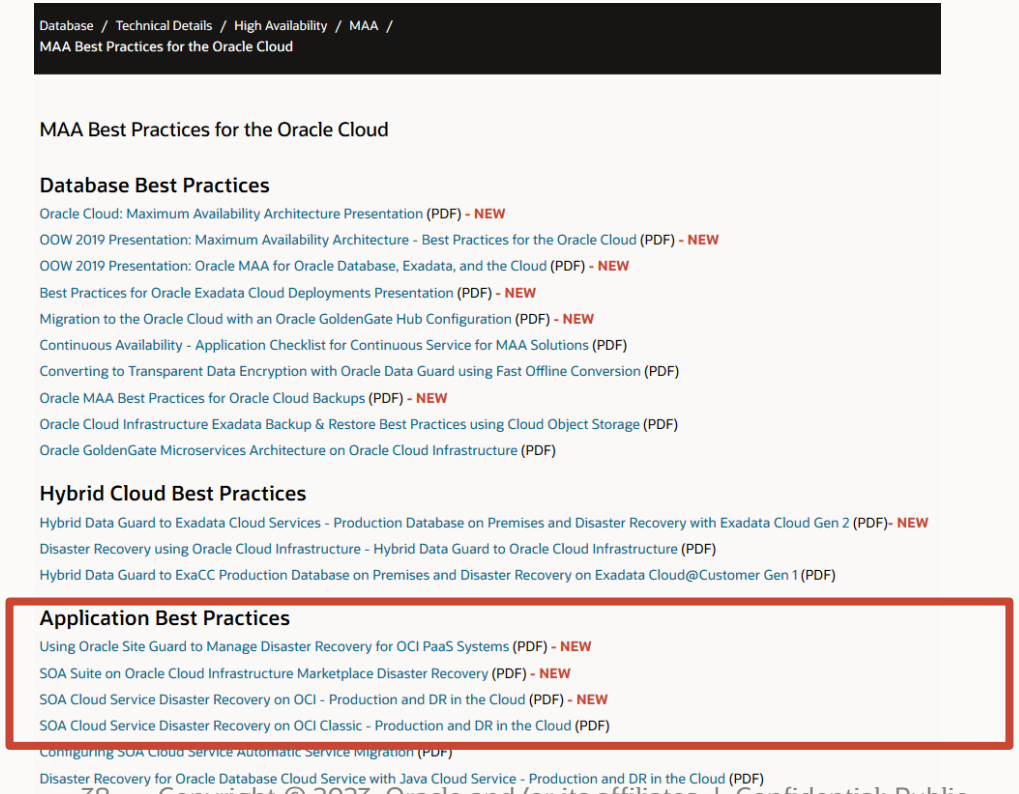
Use OCI Full Stack Disaster Recovery Service with Oracle WebLogic Server domains

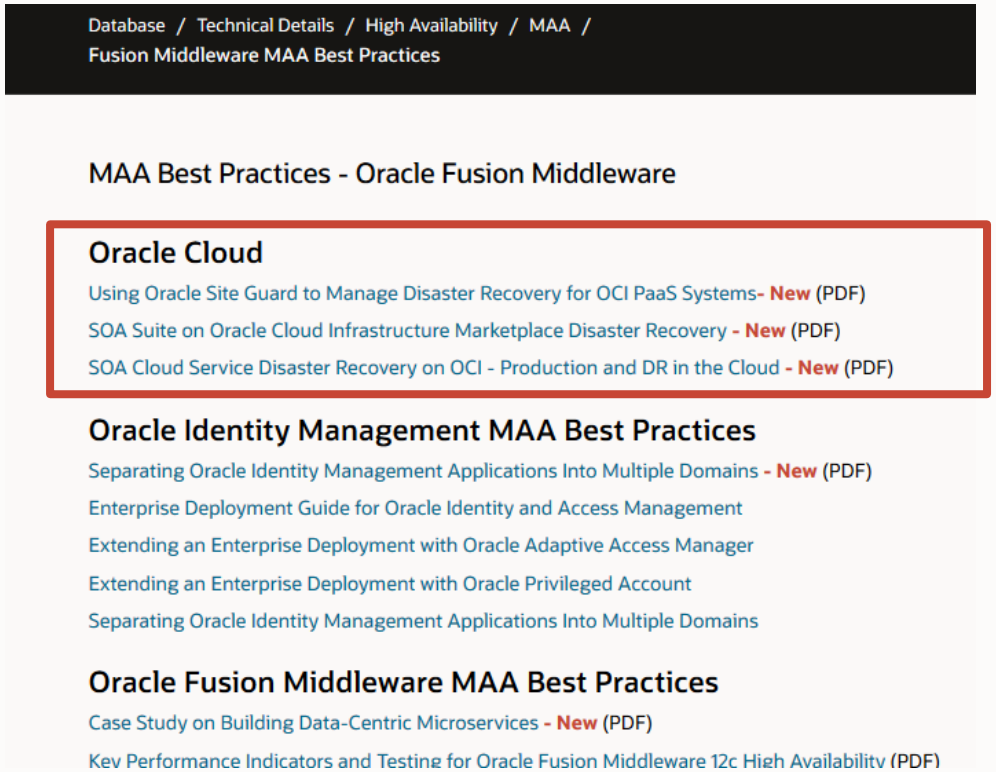
- Configure a DR Solution with an Oracle Autonomous Database

(https://docs.oracle.com/en/solutions/adb-refreshable-clones-dr/index.html)

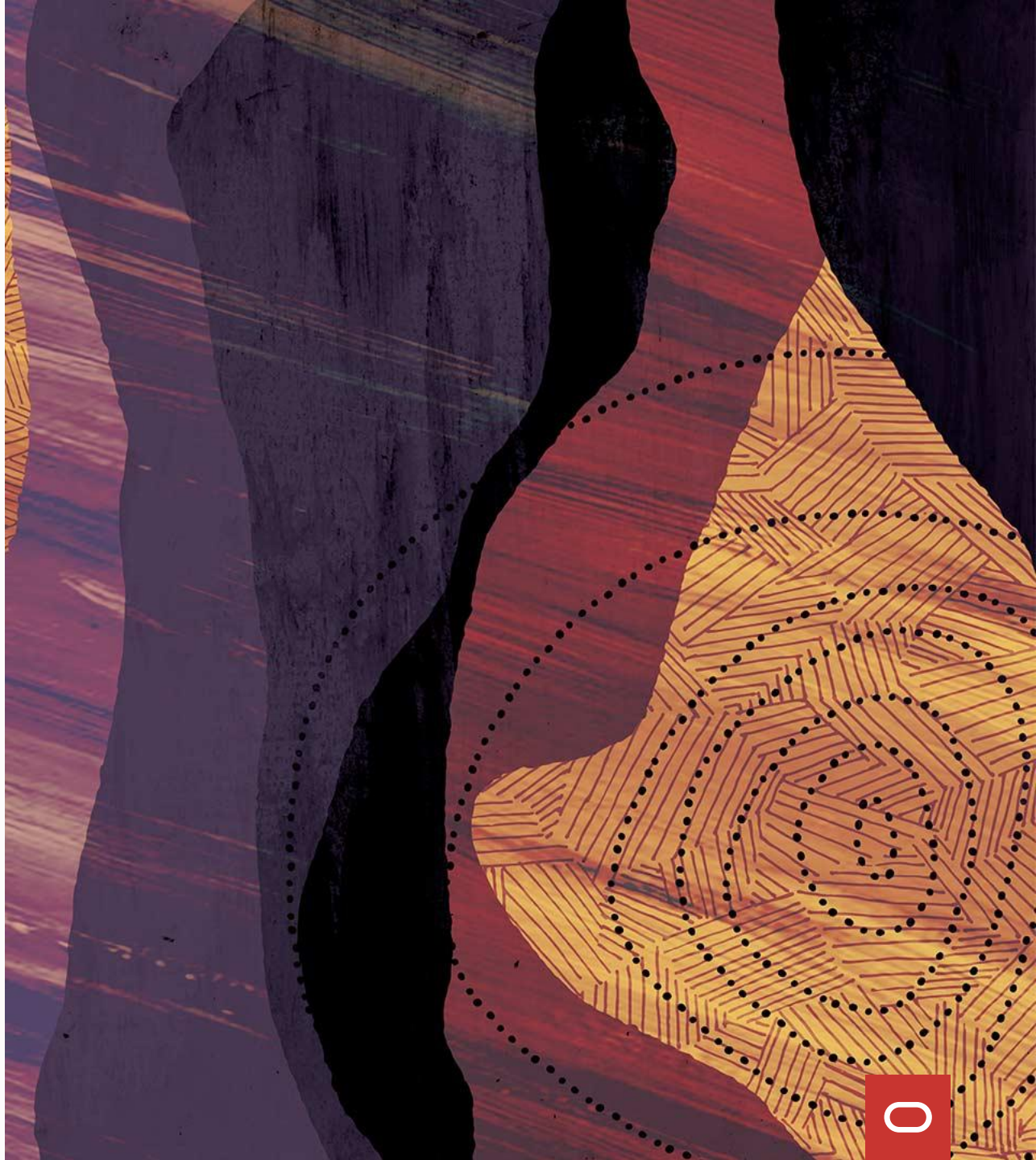
LINKS
Documents in OTN

- The PaaS DR documents are published in MAA OTN pages:
  - MAA Best Practices for the Oracle Cloud (https://www.oracle.com/database/technologies/high-availability/oracle-cloud-maa.html)
  - MAA Best Practices - Oracle Fusion Middleware (https://www.oracle.com/database/technologies/high-availability/fusion-middleware-maa.html)





Thank you



ORACLE