ORACLE
Cloud Infrastructure

Best Practices for Disaster Recovery in Oracle Cloud Infrastructure

ORACLE WHITE PAPER | AUGUST 2018

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Revision History

The following revisions have been made to this white paper since its initial publication:

Date	Revision
August 31, 2018	Initial publication

You can find the most recent versions of the Oracle Cloud Infrastructure white papers at https://cloud.oracle.com/iaas/technical-resources.

Table of Contents

Overview

Disaster recovery (DR) is the process of planning to protect your applications from a disaster. A disaster can be anything that puts your applications at risk, from network outages to equipment failures to natural disasters. When an unforeseen disaster happens, DR enables your applications to recover as quickly as possible and to continue to provide services to your users.

Oracle Cloud Infrastructure provides highly available and scalable cloud infrastructure and services that enable the DR for your applications to be reliable, secure, and fast. This white paper outlines best practices for how to design and implement your application DR on Oracle Cloud Infrastructure.

DR Concepts

To understand DR planning, it's important to understand two commonly used terms: *recovery time objective* (RTO) and *recovery point objective* (RPO).

- The RTO is the target time that is required to restore your application functionality after a disaster happens. The goal is to measure how quickly you must recover from a disaster. Typically, the more critical the applications, the lower the RTO.
- The RPO is the acceptable timeframe of lost data that your applications can tolerate. RPO is about how much data your applications can afford to lose in a disaster scenario.

To build a DR plan that guarantees the survival of your applications after a disaster and is also cost effective, you must consider both RTO and RPO. Ensure that both RTO and RPO goals can be achieved to recover your applications effectively from a disaster.

Oracle Cloud Infrastructure DR Foundational Services

To design and implement DR solutions on Oracle Cloud Infrastructure, it's important to know which Oracle Cloud Infrastructure features and services have built-in capabilities for a reliable, secure, and cost-effective DR.

Regions and Availability Domains

An Oracle Cloud Infrastructure *region* is a localized geographic area composed of several *availability domains*.

- Regions are independent of other regions and can be separated by vast distances—across countries or even continents. You can deploy applications in different regions to mitigate the risk of region-wide events, such as large weather systems or earthquakes.

- An availability domain is one or more data centers located within a region. Availability domains are isolated from each other, fault tolerant, and unlikely to fail simultaneously. Because availability domains don’t share physical infrastructure, such as power or cooling, or the internal availability domain network, a failure that impacts one availability domain is unlikely to impact others.

  All the availability domains in a region are connected to each other by a low-latency, high-bandwidth network. This predictable, encrypted interconnection between availability domains provides the building blocks for both high availability (HA) and DR.

Compute

The Oracle Cloud Infrastructure Compute service provides both bare metal and virtual machine compute instances that deliver performance, flexibility, and control. The service is powered by Oracle’s next-generation, internet-scale infrastructure, which is designed to help you develop and run your most demanding applications and workloads in the cloud.

In the context of DR, we recommend deploying your Compute instances across multiple availability domains to protect your applications from failures. The Compute service enables you to share custom images across tenancies and regions by using the image import/export feature.

Storage

The Oracle Cloud Infrastructure Object Storage service is an internet-scale, high-performance storage platform that offers reliable and cost-efficient data durability. With Object Storage, you can safely and securely store or retrieve data directly from the internet or from within the cloud platform. The elasticity of the platform lets you start small and scale seamlessly, without experiencing any degradation in performance or service reliability.

Storage Gateway is a cloud storage gateway that lets you connect your on-premises applications with Oracle’s cloud. You can use Storage Gateway to move files to Oracle Cloud Infrastructure Archive Storage as a cost-effective backup solution. You can move individual files and compressed or uncompressed zip or tar archives. Storing secondary copies of data is an ideal use case for Storage Gateway. Storage Gateway lets traditional applications move data to a highly durable object storage. When there is a need to recover data, a new instance of Storage Gateway is created and data can be easily recovered.

The Oracle Cloud Infrastructure Block Volumes service lets you dynamically provision and manage block storage volumes. You can create, attach, connect, and move volumes as necessary to meet your storage and application requirements. The service’s backup feature lets you make a point-in-time backup of data on a block volume. This capability provides you with a spare copy of a volume and gives you the ability to successfully complete DR within the same region. You can perform manual backups or implement automated policy-driven backups.

The Oracle Cloud Infrastructure File Storage service provides a durable, scalable, distributed, enterprise-grade network file system. The File Storage service is designed to meet the needs of applications and users that need an enterprise file system across a wide range of use cases. You have redundant storage for resilient data protection.

Networking

Networking is a key component of a DR solution. Oracle Cloud Infrastructure provides several network-related services and features to meet your application DR requirements.

A virtual cloud network (VCN) is a software-defined network that you set up in Oracle data centers, with firewall rules and specific types of communication gateways that you can choose. You can control whether subnets are public or private, and whether instances get public IP addresses. You can set up your VCN to have access to the internet. You can also privately connect your VCN to public Oracle Cloud Infrastructure services such as Object Storage, to your on-premises network, or to another VCN.

Reserved public IP addresses enable you to unassign an IP address and then reassign it to another instance if there is failover or failback, which simplifies the DR process.

Oracle Cloud Infrastructure FastConnect provides an easy way to create a dedicated, private connection between your on-premises data center and Oracle's cloud infrastructure. FastConnect provides higher-bandwidth options and a more reliable and consistent networking experience compared to internet-based connections.

The Oracle Cloud Infrastructure Load Balancing service provides automated traffic distribution from one entry point to multiple servers reachable from your VCN. The service offers a load balancer with your choice of a public or private IP address, and provisioned bandwidth. The load balancer can reduce your maintenance window by draining traffic from an unhealthy application server before you remove it from service for maintenance.

Database

The Oracle Cloud Infrastructure Database service offers several types of Oracle databases, enabling you to quickly launch a database system that meets your needs. You have full access to the features and operations available with the database, but Oracle owns and manages the infrastructure.

The Database service supports several types of DB systems, ranging in size, price, and performance. For details about each type of system, start with the following links:

- Exadata DB Systems
- Bare Metal and Virtual Machine DB Systems

Oracle's Autonomous Data Warehouse provides you with a fully managed, preconfigured data warehousing environment. Autonomous Data Warehouse is designed to run your business intelligence applications and help you discover important insights about your business.

Common Disaster Scenarios on Oracle Cloud Infrastructure

In your DR solution design and planning, consider a full spectrum of possible disaster scenarios. This section describes a few common disaster scenarios that can help you to design and implement your DR solution.

Application Failure

An application can fail because of its own exceptions, changes in underlying resources, and so on. It’s important to include monitoring capability in your DR solution design so that your application failures are detected and alerts are sent. Depending on your requirements, your DR solution can range from simply backing up your applications to using a fully active-to-active failover setup.

Network Failure

For DR, consider potential network outage in your cloud environment. For example, if you use an IPSec VPN to connect your on-premises data centers to Oracle Cloud Infrastructure, you could encounter potential network performance or outage issues for this IPSec VPN connection. We recommend setting up multiple IPSec VPN connections or using both FastConnect and IPSec VPN connections so that you have sufficient redundancy for your network connections.

Data Center Impact in Region Failure

An unexpected event could affect an entire data center (availability domain). In your DR solution design, plan for this kind of failure. This potential is one of the reasons that each Oracle Cloud Infrastructure region consists of three availability domains. We recommend deploying your applications across multiple availability domains to accommodate potential issues for a particular data center.

Whole Region Failure (Natural Disaster)

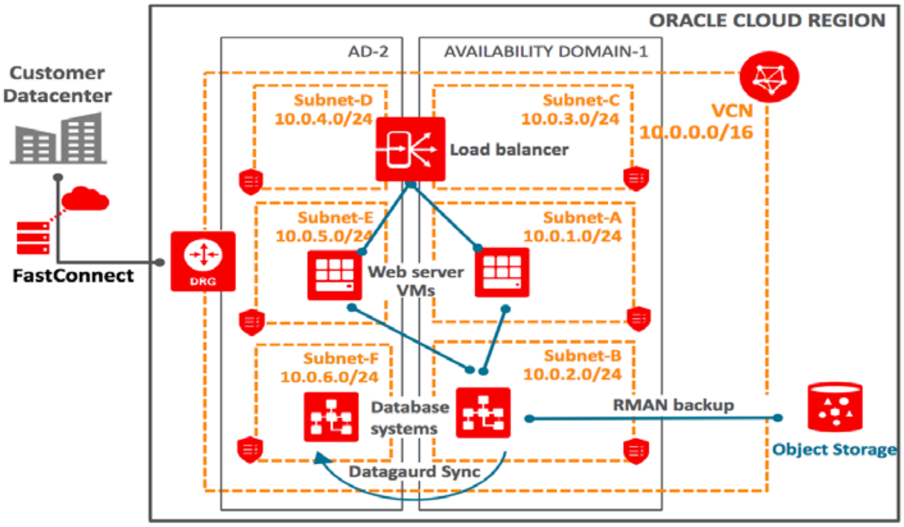
Although it would be rare, a natural disaster could cause an entire Oracle Cloud Infrastructure region to be out of service. This scenario could be the one of the most severe cases in your DR design. In this scenario, we recommend using multiple Oracle Cloud Infrastructure regions for your DR solution. Depending on your DR requirements (RTO and RPO), you can either back up or replicate your data to another region, or set up a fully active-to-active standby in another region.

Deployment Strategies for Disaster Recovery

To protect your applications from the possible disasters described in the previous section, it's important to define your application deployment strategy based on your RTO and RPO requirements. This section provides different deployment strategies for your DR solution design.

Single Region with Multiple Availability Domains

Depending on the criticality of your applications, you could deploy the applications in a single region. Because each region has multiple availability domains, you can deploy your applications across multiple availability domains to accommodate potential failures in a single availability domain. We recommend using the Oracle Cloud Infrastructure Load Balancer service in your DR solution design to minimize the downtime to your applications. If your application stack contains a database component, we recommend deploying a standby DB system in a different availability domain from your primary database and setting up Data Guard between them. We also recommend setting up your database backup to Oracle Cloud Infrastructure Object Storage to further protect your application data. The following figure illustrates this deployment:

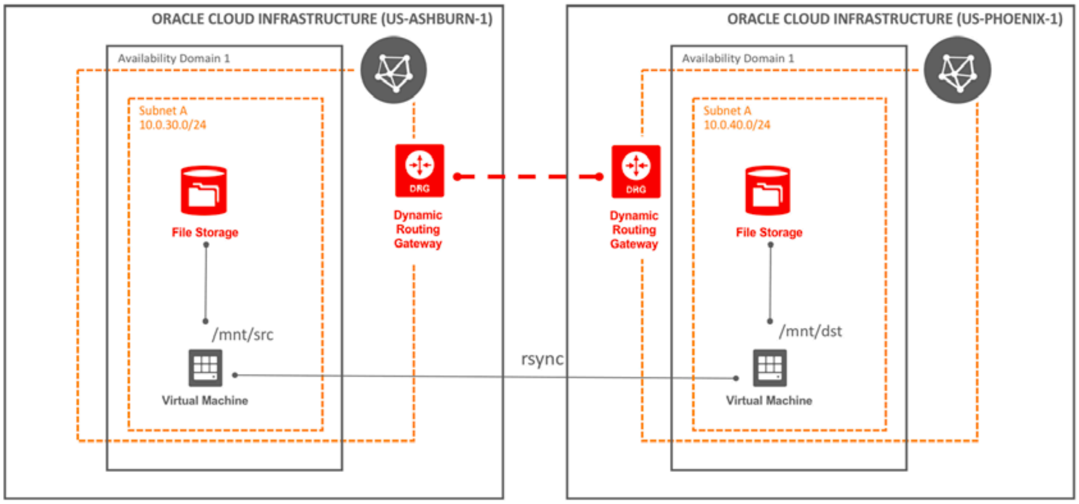


Consider that a single-region deployment doesn't provide full protection if an entire region experiences a failure.

Cross Region

For your mission-critical applications, consider a cross-region design for your DR solution. Oracle Cloud Infrastructure provides robust and high-performance backbones between Oracle Cloud Infrastructure regions. You can use remote VCN peering to establish secure and reliable connections between different VCNs across regions.

For example, to accomplish cross-regional data protection, you can use rsync to asynchronously copy your file system or snapshot data to another region.



Disaster Recovery Solutions

This section describes several DR solutions to consider as you plan your DR design.

Backup and Restore

The primary use of backups is to support business continuity, disaster recovery, and long-term archiving. When you are determining a backup schedule, your backup plan and goals should cover the following considerations:

- **Frequency**: How often you want to back up your data.
- **Recovery time**: How long you can wait for a backup to be restored and accessible to the applications that use it. The time for a backup to complete depends on several factors,

such as the size of the data being backed up and the amount of data that has changed since the last backup, but it generally takes a few minutes.

- **Number of stored backups**: How many backups you must keep available, and the deletion schedule for those you no longer need. You can create only one backup at a time; if a backup is underway, it must finish before you can create another one. For details about the number of backups that you can store, see Block Volume Capabilities and Limits.

Following are some common use cases for using backups:

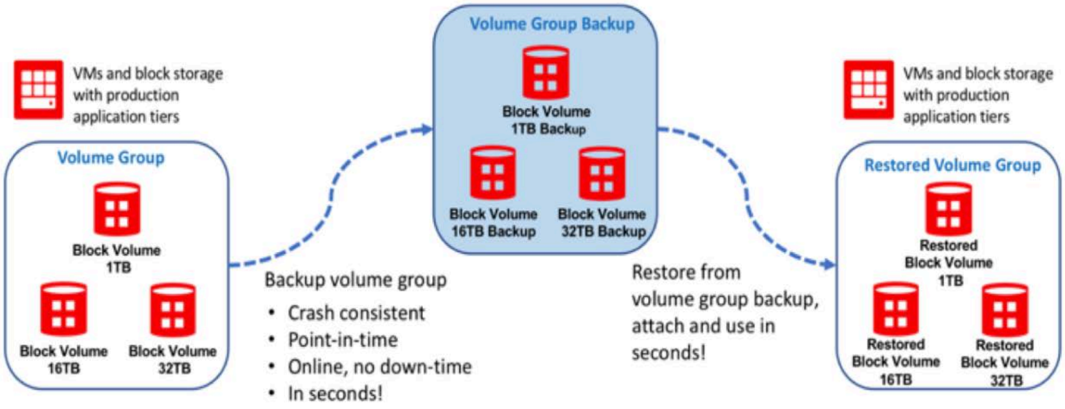
- Creating multiple copies of the same volume. Backups are highly useful when you must create many instances with many volumes that must have the same data formation.
- Taking a snapshot of your work that you can restore to a new volume at a later time.
- Ensuring that you have a spare copy of your volume in case something goes wrong with your primary copy.

Best Practices When Creating Block Volume Backups

When creating and restoring from backups, consider the following best practices:

- Before creating a backup, ensure that the data is consistent: sync the file system, unmount the file system if possible, and save your application data. Only the data on the disk is backed up. When creating a backup, after the backup state changes from REQUEST_RECEIVED to CREATING, you can return to writing data to the volume. While a backup is in progress, the volume that is being backed up can’t be deleted.
- If you want to attach a restored volume that has the original volume attached, consider that some operating systems don’t allow you to restore identical volumes. To resolve this issue, change the partition IDs before restoring the volume. How to change an operating system's partition ID varies by operating system; for instructions, see your operating system's documentation.
- Don’t delete the original volume until you have verified that the backup you created of it completed successfully.

If your application consists of multiple volumes that span multiple compute instances, use the volume group backup feature to conduct volume backups and restores. This feature provides an end-to-end solution for creating, managing, and restoring backups for applications by using and extending the existing single-volume backup and restore features that are already available for block storage volumes. This feature simplifies the process of creating backups and clones of running enterprise applications that span multiple storage volumes across multiple instances. You can then restore an entire group of volumes from a volume group backup.



Pilot Light

The term *pilot light* refers to a small flame in a traditional gas heater that is always lit and can quickly ignite the heater when triggered by temperature sensors in the house. The same concept applies to pilot light DR, in which a whole production-sized environment (heater) is deployed when DR is activated by an application owner. The pilot light is the critical core components of your application that get deployed on the DR site and keep all the latest application configuration and critical data. Following are the critical components of the pilot light on the DR site.

Database Tier

The Oracle Cloud Infrastructure Database service offers a unique feature, CPU scaling, that lets you provision your entire database in your DR site (availability domain, region, or both) but *not* enable all production-sized CPUs. When DR is activated, you can enable additional CPUs with just one REST API call to the service without restarting the database server.

Application Tier

You deploy only one application server in your DR site (availability domain, region, or both) that keeps all your latest configuration at hand. You can use the custom images feature in Oracle Cloud Infrastructure to back up your OS on applications periodically and then use these images to provision new servers when the DR site is activated. For example, if a production site contains eight application servers, you deploy only one application server in the DR site and keep it synchronized with the primary site by using rsync or another tool. You create a custom image from this server in the DR site daily that can be used to provision the remaining seven servers when DR is activated.

Networking Tier

Use the following services on Oracle Cloud Infrastructure in your pilot light DR solution:

- IP addresses (private and public)
- DNS service
- Load Balancer service

Warm Standby

A warm standby is a scaled-down version of a full production environment that is always running on a DR site. The warm standby solution is an extension of the pilot light solution. It reduces the DR activation time because some services are always running on the DR site and they can start taking the workload while rest of the services are coming up. This solution is not scaled to take a full-production load, and it can be used for nonproduction work such as testing, quality assurance, and internal use.

Like other cloud providers, Oracle Cloud Infrastructure offers traditional horizontal scaling, which is a key element of the warm standby DR configuration. However, it’s not easy to scale a database horizontally unless you have deployed database sharding in your solution. Oracle Cloud Infrastructure offers CPU scaling, in which you can deploy the Database service with a minimum of two OCPUs and enable more OCPUs when you activate the DR site. This feature applies only to bare metal and Exadata database shapes. With this nonintrusive feature, you don’t have to restart the database and more CPUs are available almost instantly (in less than 30 seconds).

Database Strategies for Disaster Recovery

Oracle Active Data Guard and Oracle GoldenGate are two strategic capabilities within Oracle's software portfolio.

- Active Data Guard provides data protection and availability for Oracle Database in a simple and economical manner by maintaining an exact physical replica of the production copy at a remote location that is open read-only while replication is active.
- GoldenGate is an advanced logical replication product that supports multi-master replication, hub and spoke deployment, and data transformation. GoldenGate provides customers flexible options to address the complete range of replication requirements, including heterogeneous hardware platforms.

Active Data Guard

Data Guard provides a comprehensive set of services that create, maintain, manage, and monitor one or more standby databases to enable production Oracle databases to survive disasters and data corruptions. Data Guard maintains these standby databases as transactionally consistent copies of the production database. If the production database becomes unavailable because of a planned or an unplanned outage, Data Guard can switch any standby database to the production role, minimizing the downtime associated with the outage. Data Guard can be used with traditional backup, restoration, and cluster techniques to provide a high level of data protection and data availability.

Data Guard Benefits

Active Data Guard offers the following benefits:

- Secure physical replication. The standby database is open read-only so your data consistency is guaranteed.
- Simple, fast, one-way replication of a complete Oracle Database. The default configuration handles most workloads so there’s little administrative overhead.
- No restrictions. Oracle Data Guard Redo Apply supports all Oracle features and transparently replicates all data and storage types, PL/SQL packages, and DDL without special considerations.
- Best data protection. Replication direct from memory isolates the standby database from I/O corruption that can occur at the primary database. Detects silent lost-write corruption that can occur independently on the primary or standby database. Automatically detects and repair physical block corruption that can occur independently on the primary or standby database.
- Choice of synchronous with zero data loss, or asynchronous with near-zero data loss protection.
- Simple to improve ROI by offloading read-only workloads or backups to a synchronized physical standby.
- Transparency of backups. An Oracle Data Guard primary database and standby database are physically exact copies of each other. RMAN backups are interchangeable.
- A single command converts a physical standby database as a test system open read-write. A second command converts it back to a physical standby database and resynchronizes it with the primary database. Primary data is always protected.
- Integrated management of a complete configuration with Oracle Data Guard Broker command line or Oracle Enterprise Manager Cloud Control, integrated automatic database, and client failover.

- Supported for single-node database or multiple-node database (Real Application Cluster) configuration.

Data Guard Configuration Modes

Data Guard supports the following protection modes:

Maximum Protection: This protection mode provides zero data loss if the primary database fails. To ensure that data loss can’t occur, the primary database shuts down if a fault prevents it from writing its redo stream to the standby redo log of at least one standby database.

Maximum Availability: This protection mode provides the highest level of data protection that is possible without compromising the availability of the primary database. Like the Maximum Protection mode, a transaction doesn’t commit until the redo needed to recover that transaction is written to the local online redo log and to the standby redo log of at least one transactionally consistent standby database. Unlike the Maximum Protection mode, the primary database doesn’t shut down if a fault prevents it from writing its redo stream to a remote standby redo log. Instead, the primary database operates in maximum performance mode until the fault is corrected, and all gaps in redo log files are resolved. When all gaps are resolved, the primary database automatically resumes operating in Maximum Availability mode.

Maximum Performance: This protection mode (the default) provides the highest level of data protection that is possible without affecting the performance of the primary database. This is accomplished by allowing a transaction to commit when the redo data needed to recover that transaction is written asynchronously to the local online redo log. When network links with sufficient bandwidth are used, this mode provides a level of data protection that approaches that of Maximum Availability mode with minimal impact on primary database performance.

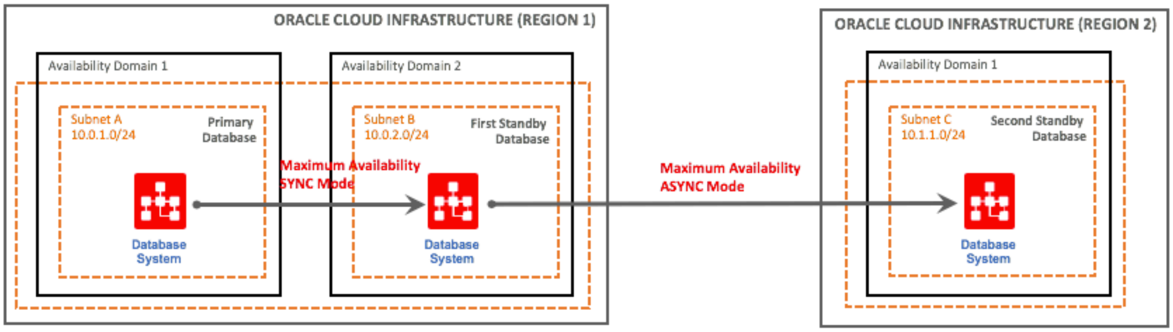
Oracle Cloud Infrastructure Best Practice for Data Guard Configuration

All three Data Guard configurations are fully supported on Oracle Cloud Infrastructure. However, because of a high risk of production outage, we don’t recommend using the Maximum Protection mode for your Data Guard configuration.

Oracle Cloud Infrastructure recommends using the Maximum Availability mode in SYNC mode between two availability domains (same region), and using the Maximum Availability mode in ASYNC mode between two regions. This architecture provides you the best RTO and RPO without causing any data loss.

Oracle Cloud Infrastructure recommends building this architecture in daisy-chain mode, in which the primary database ships redo logs to the first standby database in another availability domain in SYNC mode, and then the first standby database ships the redo logs to another region in ASYNC mode. This method ensures that your primary database is not doing the double work of shipping redo logs, which can cause performance impact on a production workload.

The following figure shows the recommended architecture for Data Guard on Oracle Cloud Infrastructure:



This configuration offers the following benefits:

- No data loss within a region.
- No overhead on the production database to maintain standbys in another region.
- Option to configure lagging on the DR site if needed for business reasons.
- Option to configure multiple standbys in different regions without any additional overhead on the production database. A typical use case is a CDN application.

Oracle GoldenGate

Oracle GoldenGate is a comprehensive software package for real-time data integration and replication in heterogeneous IT environments. The product set enables high availability solutions, real-time data integration, transactional change data capture, data replication, transformations, and verification between operational and analytical enterprise systems.

Use Oracle GoldenGate when a replica database must be open read-write while replication is active, including in the following scenarios:

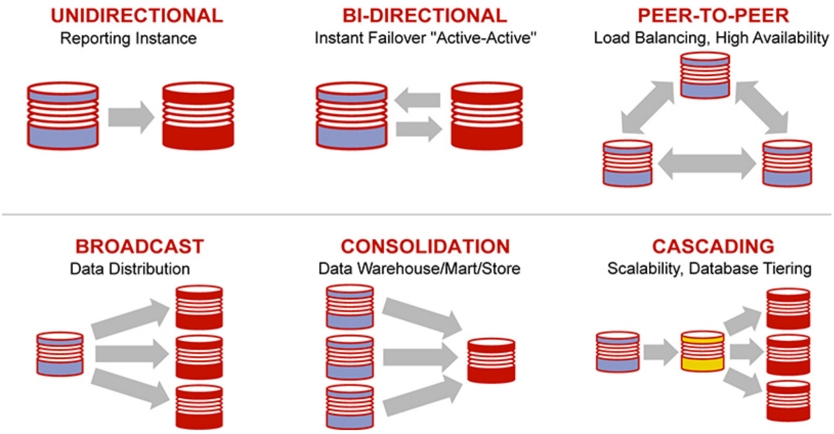
- Advanced replication requirements, such as multi-master and bidirectional replication, subset replication, many-to-one replication, cross-endian replication, and data transformations.
- Maintenance and migrations that require zero downtime using bi-directional replication.

- Cross-platform migration that is not supported by Data Guard (for example, cross-endian platform migration).
- When the primary database and the live standby database are on different operating systems or are different types (for example, DB2/MySQL to Oracle and vice versa).
- When you replicate from a more recent version of Oracle Database to an earlier version of Oracle Database (for example, from Oracle Database 11g to Oracle Database 10g).

Golden Gate Configuration Modes

GoldenGate supports the following topologies, and they are fully supported on Oracle Cloud Infrastructure:

- Unidirectional
- Bi-directional
- Peer-to-peer
- Broadcast
- Consolidation
- Cascading

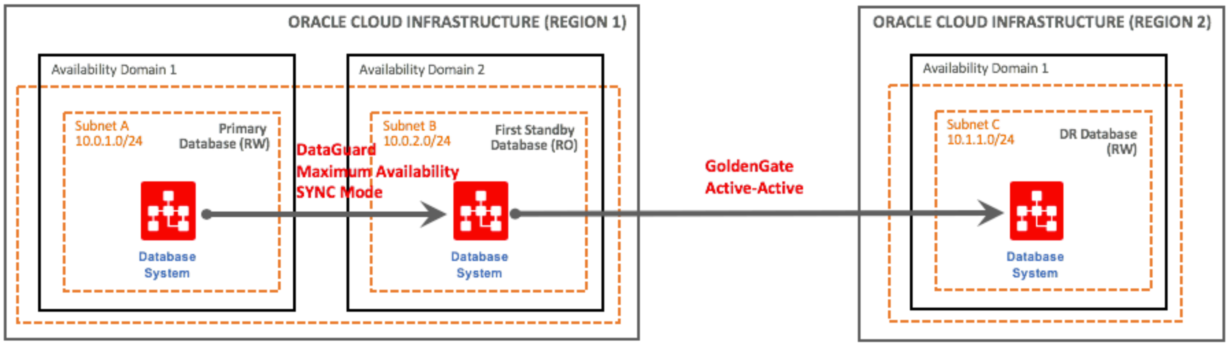

UNIDIRECTIONAL
Reporting Instance
BI-DIRECTIONAL
Instant Failover "Active-Active"
PEER-TO-PEER
Load Balancing, High Availability
BROADCAST
Data Distribution
CONSOLIDATION
Data Warehouse/Mart/Store
CASCADING
Scalability, Database Tiering

Oracle Cloud Infrastructure Best Practice for Golden Gate Configuration

Because GoldenGate replicates data on the transactional level, Oracle Cloud Infrastructure recommends implementing Conflict Detection and Resolution (CDR) for data consistency between two sites. Conflicts are identified immediately and handled with automated scripts.

If you are using GoldenGate primarily for DR purposes and replication is only one way, we recommend adding Data Guard between two regions to provide a zero-data-loss solution with strong data consistency between the primary and Data Guard instance. This configuration also alleviates the overhead of running GoldenGate extract from the primary database.

The following figure show this proposed architecture:



Using Both Active Data Guard and GoldenGate

As indicated in the preceding section, Active Data Guard and GoldenGate are not mutually exclusive. You can use the solutions together in the following scenarios:

- Use an Active Data Guard standby for disaster protection and database rolling upgrades for a mission critical OLTP database. Use GoldenGate to extract data from the Data Guard primary database (or from the standby database using GoldenGate ALO mode) for ETL update of an enterprise data warehouse.
- Use GoldenGate subset replication to extract, transform, and aggregate data from numerous data sources into a central operational data store (ODS). The ODS supports mission critical application systems that generate significant revenue for the company. Use an Active Data Guard standby database to protect the ODS, providing optimal data protection and availability.
- Use GoldenGate multi-master replication to synchronize several databases, each located in different geographies. Each GoldenGate copy has its own local synchronous Data Guard standby database that enables zero-data-loss failover should an outage occur.

Disaster Recovery Planning

As a part of your DR planning, consider the following steps to help you better prepare for different DR scenarios.

Automation

Automation can dramatically reduce the time to redeployment and improve your RTO and RPO goals. It ensures consistency and minimizes human errors during your DR process. Oracle Cloud Infrastructure provides several SDKs and a CLI to help you develop automation scripts. Also, Oracle Cloud Infrastructure provides a Terraform provider to support provisioning and rebuilding your entire cloud environment through Terraform templates.

Failure Detection

For any DR solution, you must have a reliable and timely way to detect failures in your cloud environment. In your application stack, you must be able to monitor the health of your applications. Oracle Cloud Infrastructure provides a service health dashboard that shows the health of Oracle Cloud Infrastructure services. You can subscribe to service health events to get updates on the health of Oracle Cloud Infrastructure services.

Disaster Recovery Testing

To ensure a successful DR solution, you have to periodically conduct DR testing. Testing can help you to find any potential gaps in your DR plan and show the effectiveness of your DR solution. To minimize impacts to your applications, you must carefully choose the test time window and be able to restore to the normal state if a failure occurs in your testing.

Conclusion

Oracle Cloud Infrastructure provides highly available and scalable cloud infrastructure and services that enable reliable, secure, and effective DR for your applications. This white paper highlights a few common disaster scenarios and deployment strategies for your DR solution. It provides best practices for how to design and implement your application DR solutions on Oracle Cloud Infrastructure.

References

- Oracle Maximum Availability Architecture (MAA):
  - Overview
  - Best Practices
  - White paper
- Disaster Recovery to the Oracle Cloud white paper

ORACLE

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Best Practices for Disaster Recovery in Oracle Cloud Infrastructure
August 2018
Authors: Shan Gupta and Changbin Gong