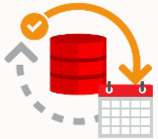
ORACLE

Oracle Cloud
Maximum Availability Architecture

August 30th, 2021 Update

Types of downtime and recovery objectives

Types of downtime



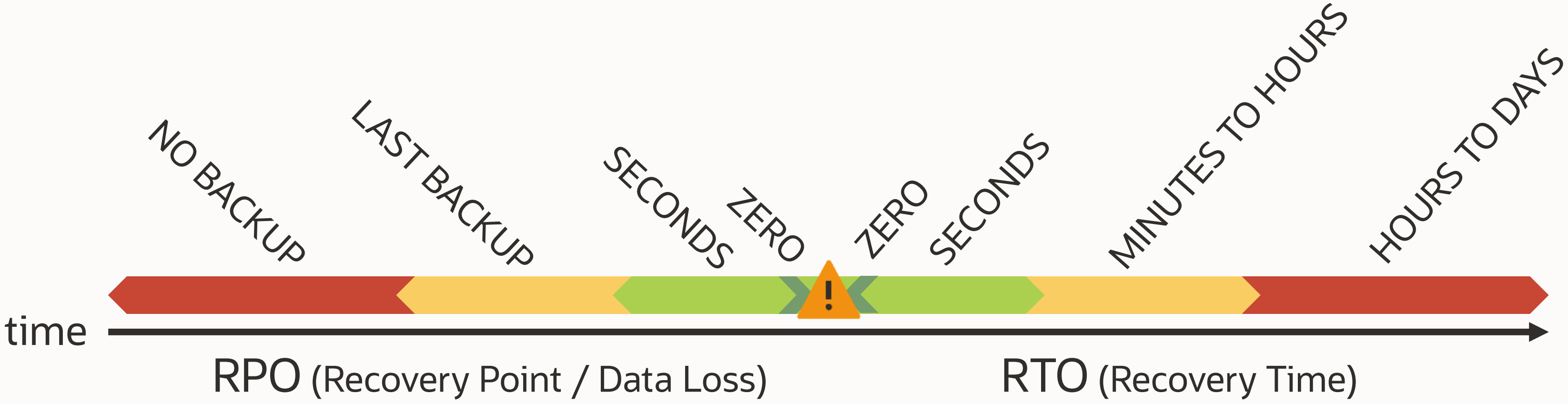
PLANNED MAINTENANCE

UPGRADE

RECOVERABLE LOCAL FAILURE

UNRECOVERABLE OR SITE FAILURE

Recovery objectives



From Single Instance to 99.999%

Maximum Availability Reference Architectures

Single instance protection

Underlying Technologies

SINGLE INSTANCE

- ACID transactions
- Standard protection
- Automatic Restart

ONLINE REORGANIZATION

- Online table redefinition and partition maintenance
- Less planned downtime

RESOURCE MANAGEMENT

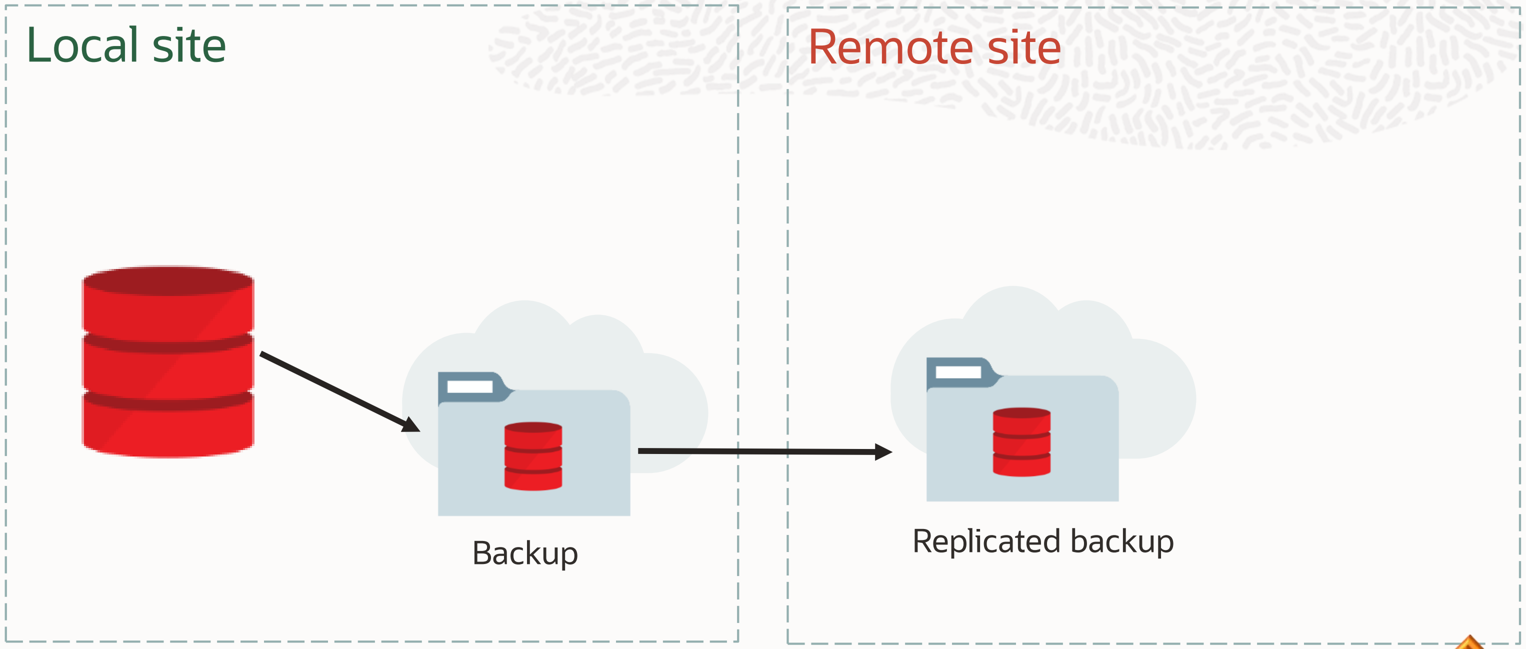
- PDB and CDB isolation
- Protection from noisy neighbors

FLASHBACK

- Protection from wrong transactions

RMAN

- Basic DB protection
- Protection from data loss



Outage Matrix

PLANNED MAINTENANCE	Zero ! Mins/Hours
UPGRADE	Zero ! Hours
RECOVERABLE FAILURE	Zero ! Mins/Hours
UNRECOVERABLE FAILURE	Last backup ! Hours/Days

BRONZE

Protection from recoverable failures

Underlying Technologies

RAC

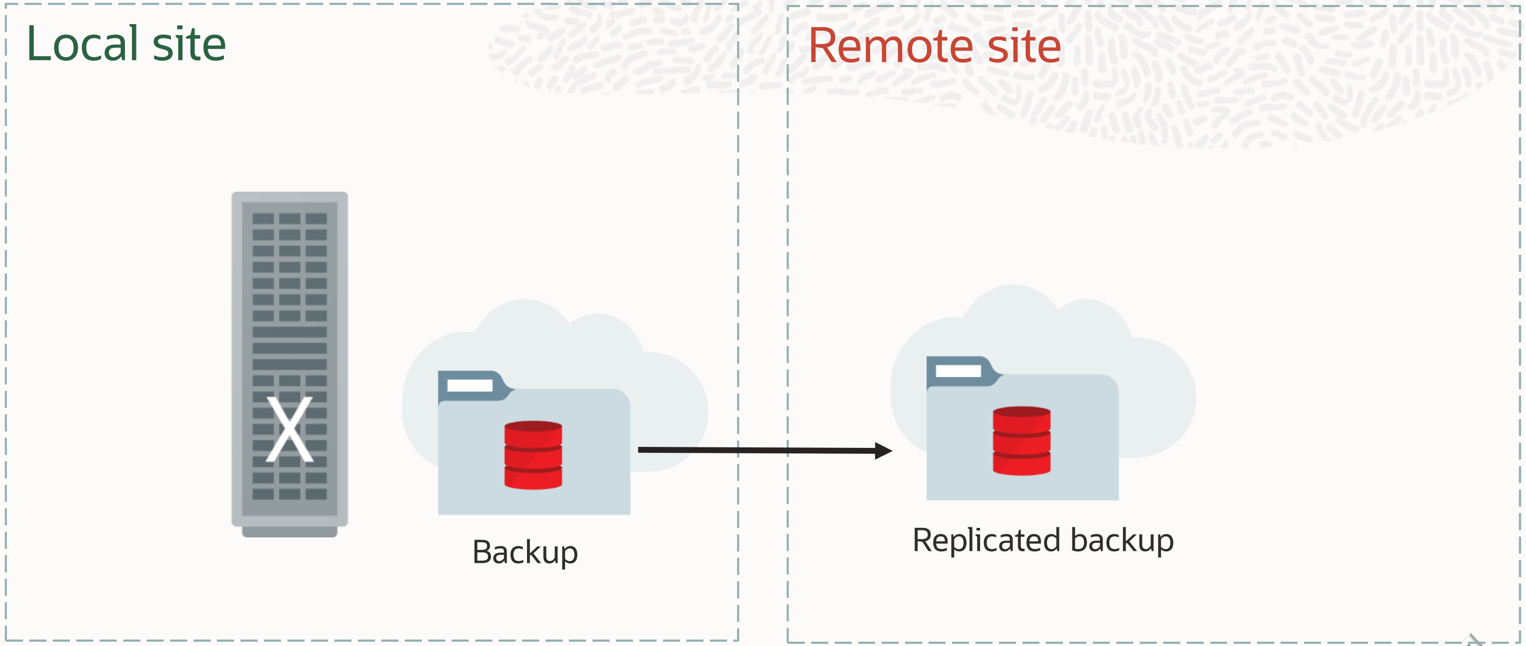
- Node failure protection
- Zero downtime maintenance
- Elastic changes (CPU, mem, storage) with no downtime

APPLICATION CONTINUITY

- (Almost) Transparent unplanned maintenance

ENGINEERED SYSTEMS

- Exadata scalability, performance and availability
- Data protection and Exadata QoS for DB operations



Local site

Backup

Remote site

Replicated backup

Outage Matrix

PLANNED MAINTENANCE	Zero	⚠	Zero
UPGRADE	Zero	⚠	Hours
RECOVERABLE FAILURE	Zero	⚠	Secs
UNRECOVERABLE FAILURE	Last backup	⚠	Mins/Hours

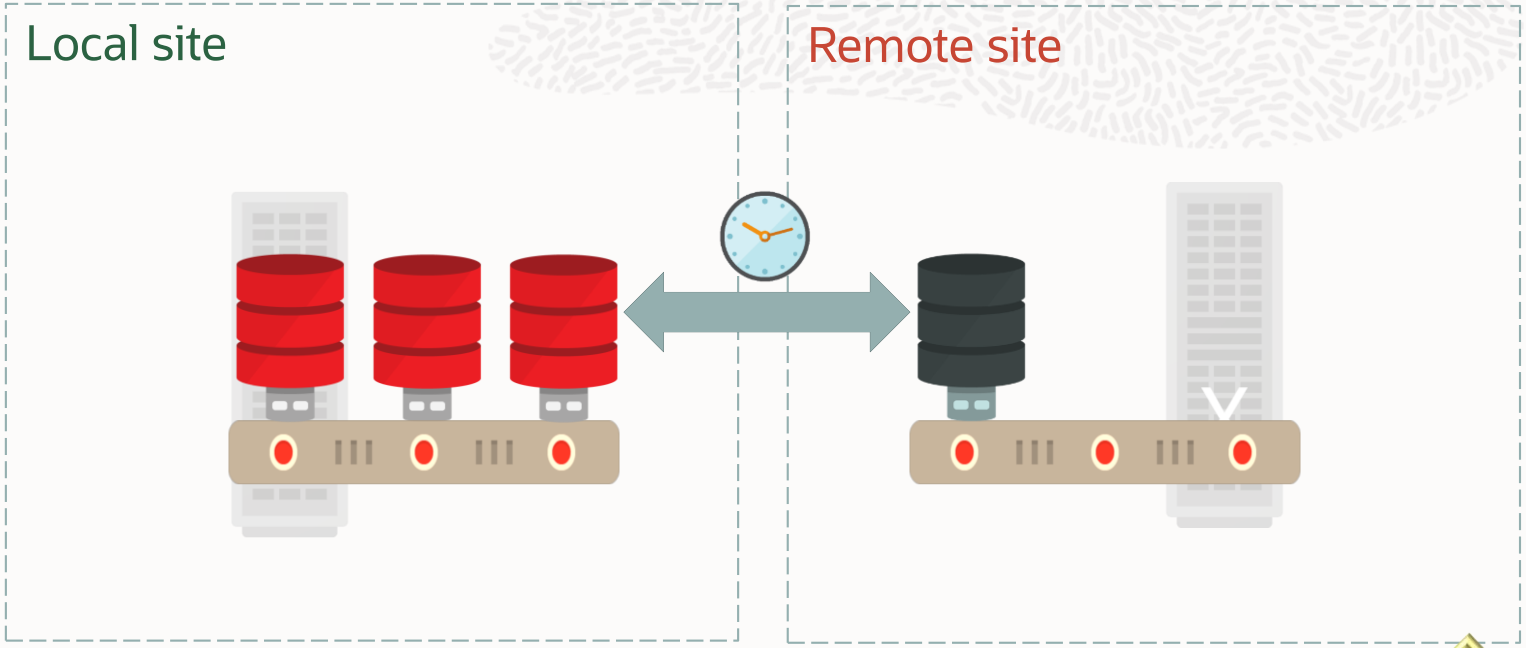
SILVER

Protection from unrecoverable and site failures

Underlying Technologies

REFRESHABLE PDB SWITCHOVER

- Site failure protection
- Partial corruption prevention
- Switchover and failover capability
- One click setup
- PDB relocate to upgraded database



Outage Matrix

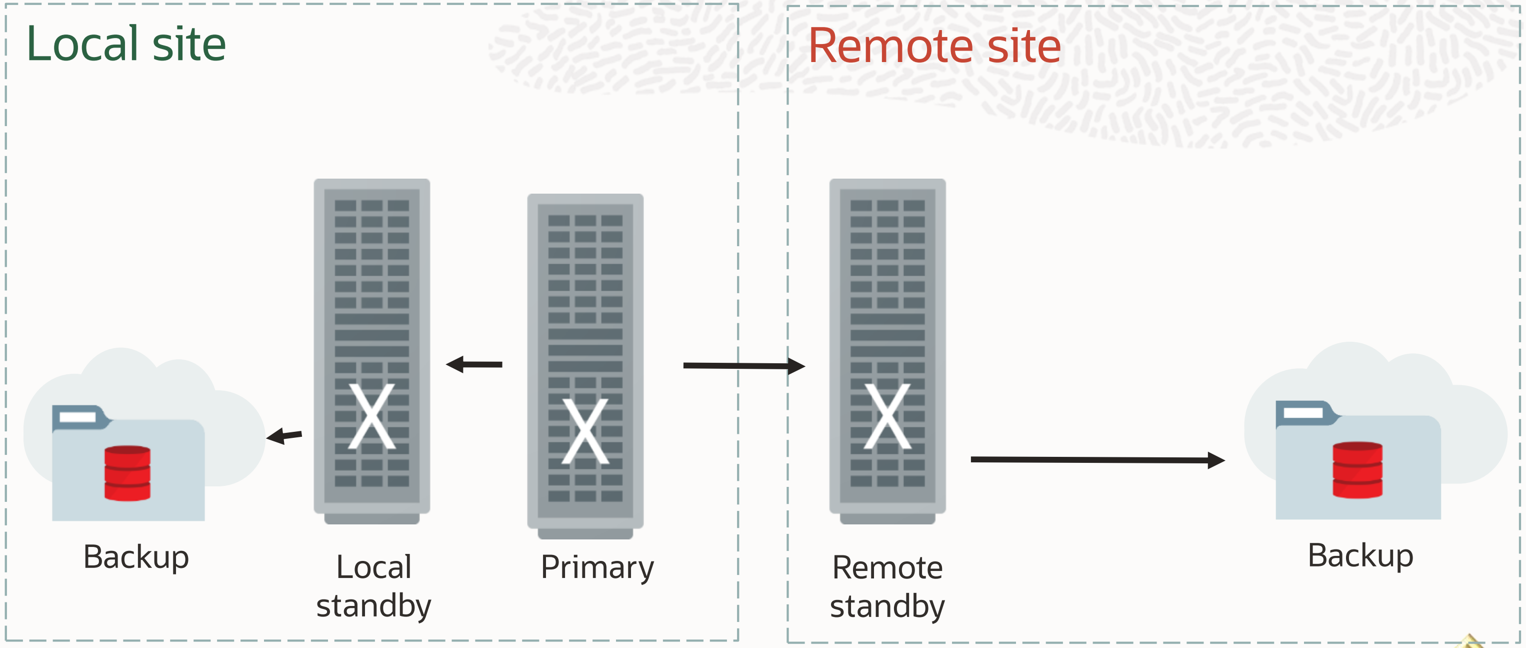
PLANNED MAINTENANCE	Zero ! Zero
UPGRADE	Zero ! Minutes
RECOVERABLE FAILURE	Zero ! Secs
UNRECOVERABLE FAILURE	Last refresh ! Minutes

Protection from unrecoverable and site failures

Underlying Technologies

ACTIVE DATA GUARD

- Site failure protection
- Comprehensive corruption prevention
- Rolling upgrades
- Offload work to standby with read-mostly scale-out



Outage Matrix

	PLANNED MAINTENANCE	Zero ! Zero
	UPGRADE	Zero ! Secs
	RECOVERABLE FAILURE	Zero ! Secs
	UNRECOVERABLE FAILURE	Zero ! Secs

99.999% Availability

Underlying Technologies

GOLDENGATE

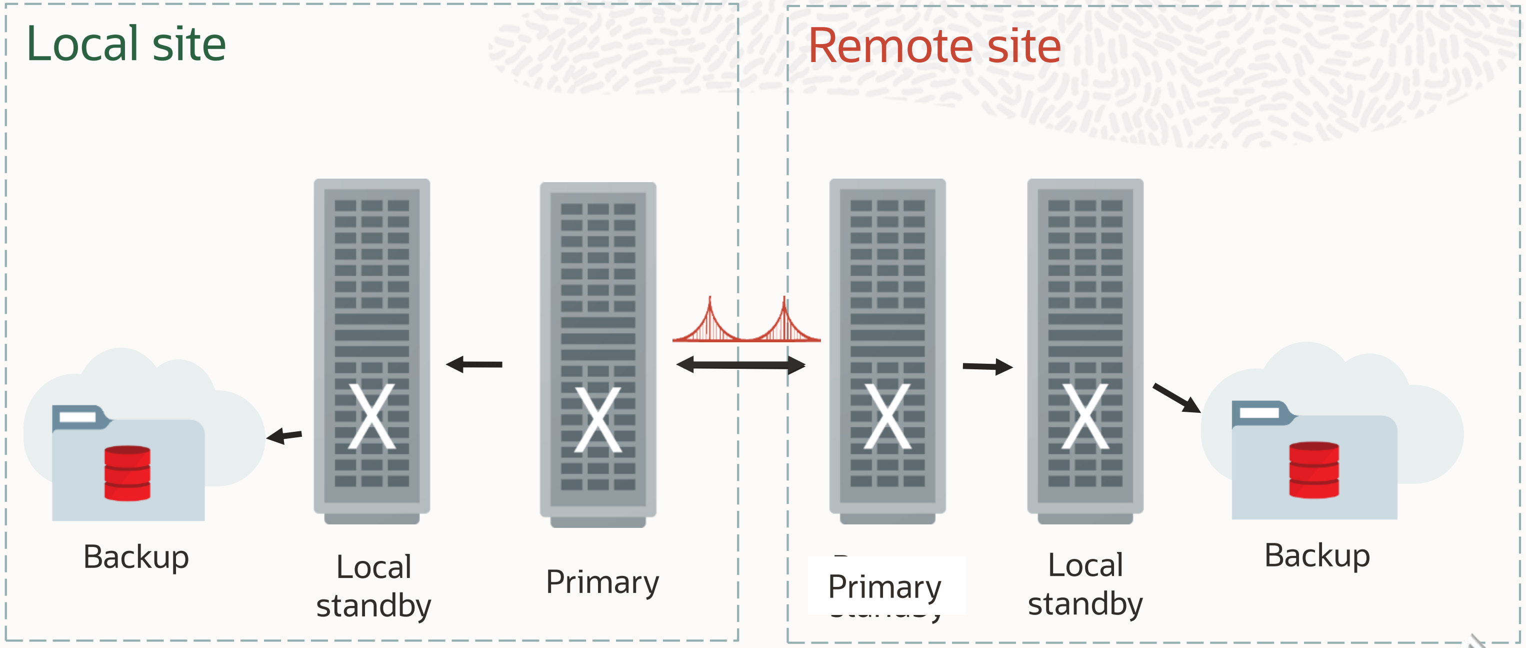
- Active/Active
- Always online
- Online database upgrades
- Site switch with zero database downtime
- Read-write scale-out
- The application must be aware of the replica(s)

EDITION BASED REDEFINITION

- Online application upgrades

SHARDING

- Distributed
- Best scale-out



Outage Matrix

PLANNED MAINTENANCE	Zero	⚠	Zero
UPGRADE	Zero	⚠	Zero
RECOVERABLE FAILURE	Zero	⚠	Zero
UNRECOVERABLE FAILURE	Zero	⚠	Zero

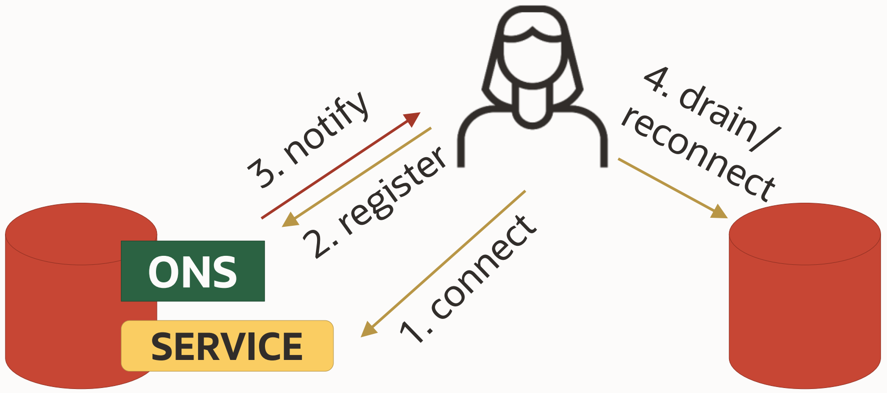
PLATINUM

Client-side required technologies

Client draining/failover is a crucial part of high availability for applications connecting to the database.

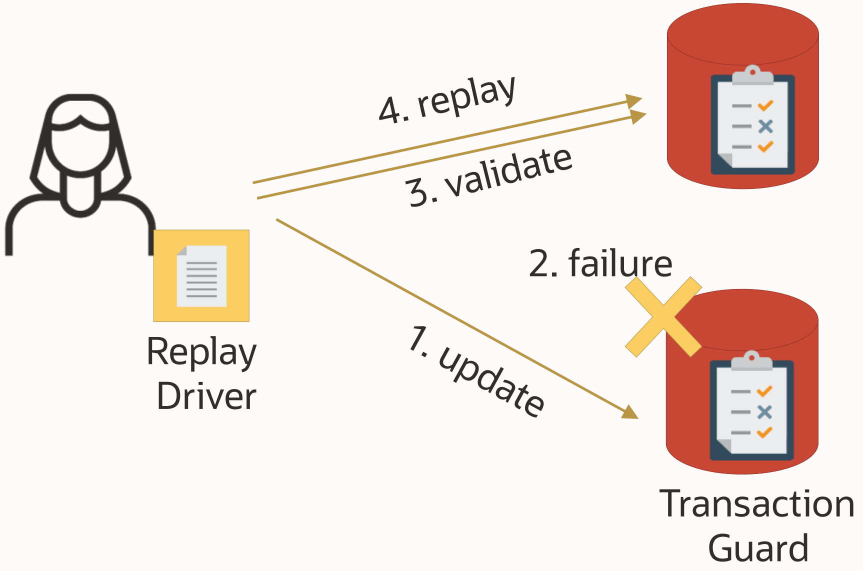
PLANNED MAINTENANCE

Fast Application Notification
(Session Draining)



UNPLANNED MAINTENANCE

Application Continuity [1]
(Transaction Replay)

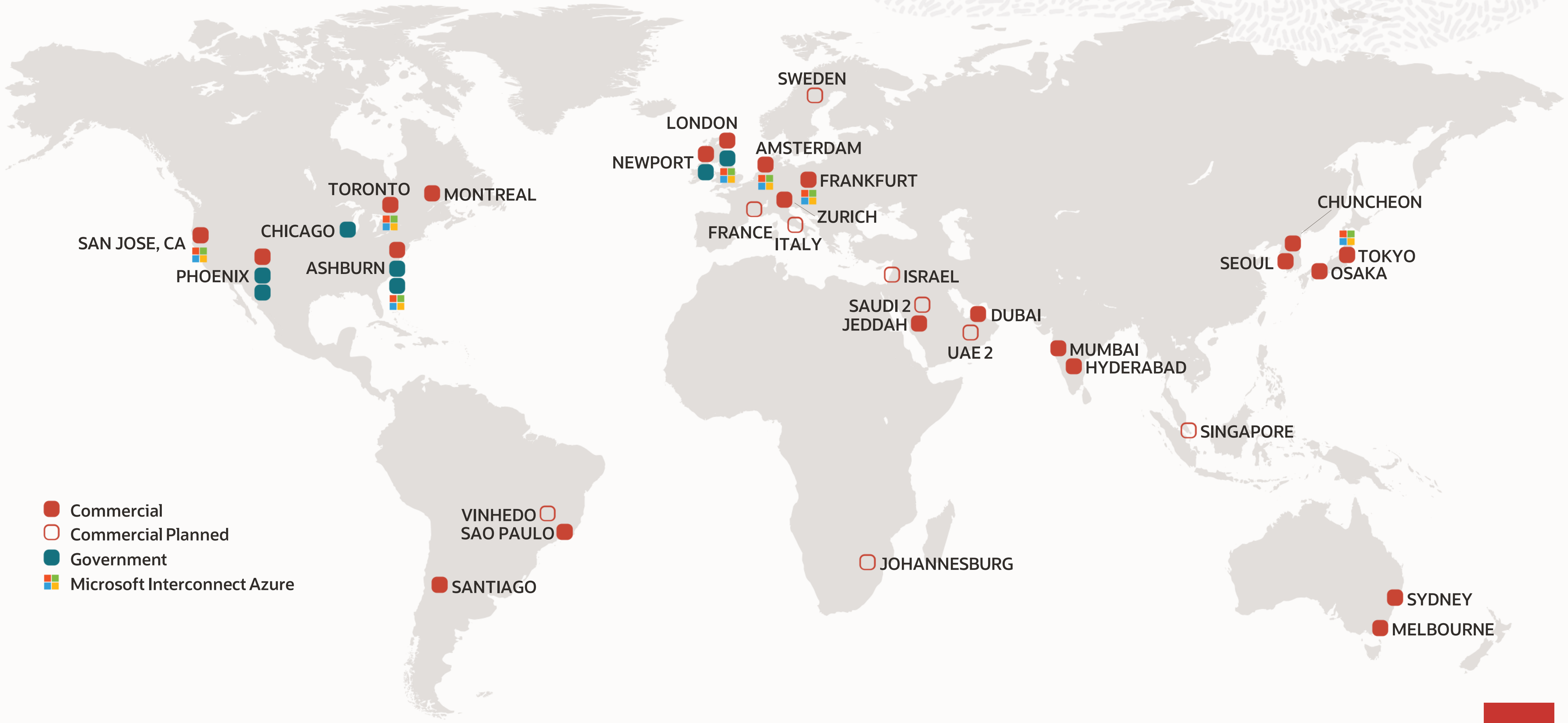


[1] Application Checklist for Continuous Service for MAA Solutions
https://www.oracle.com/technetwork/database/clustering/checklist-ac-6676160.pdf

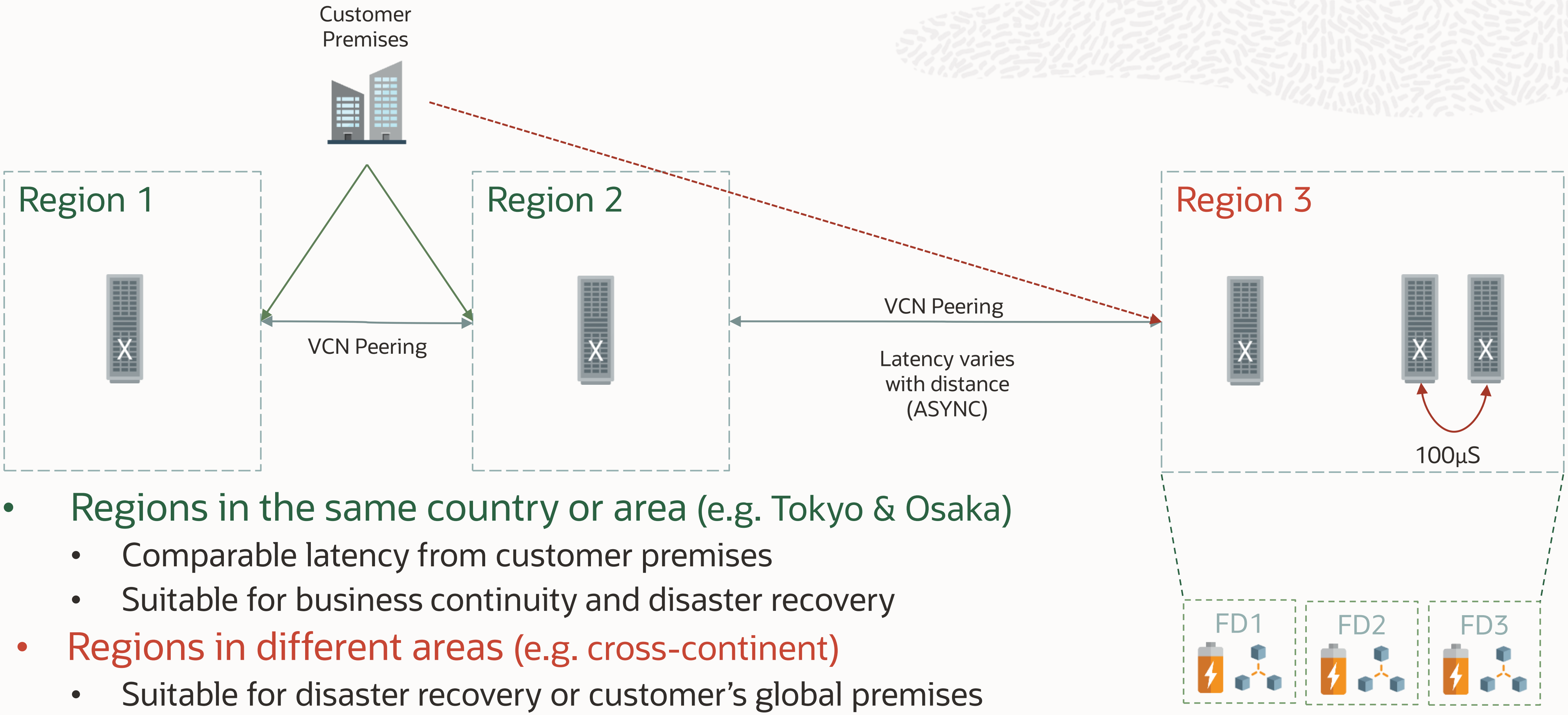
Oracle Cloud Infrastructure Topology

Maximum Availability Architecture

Oracle Cloud Infrastructure regions – April 2021



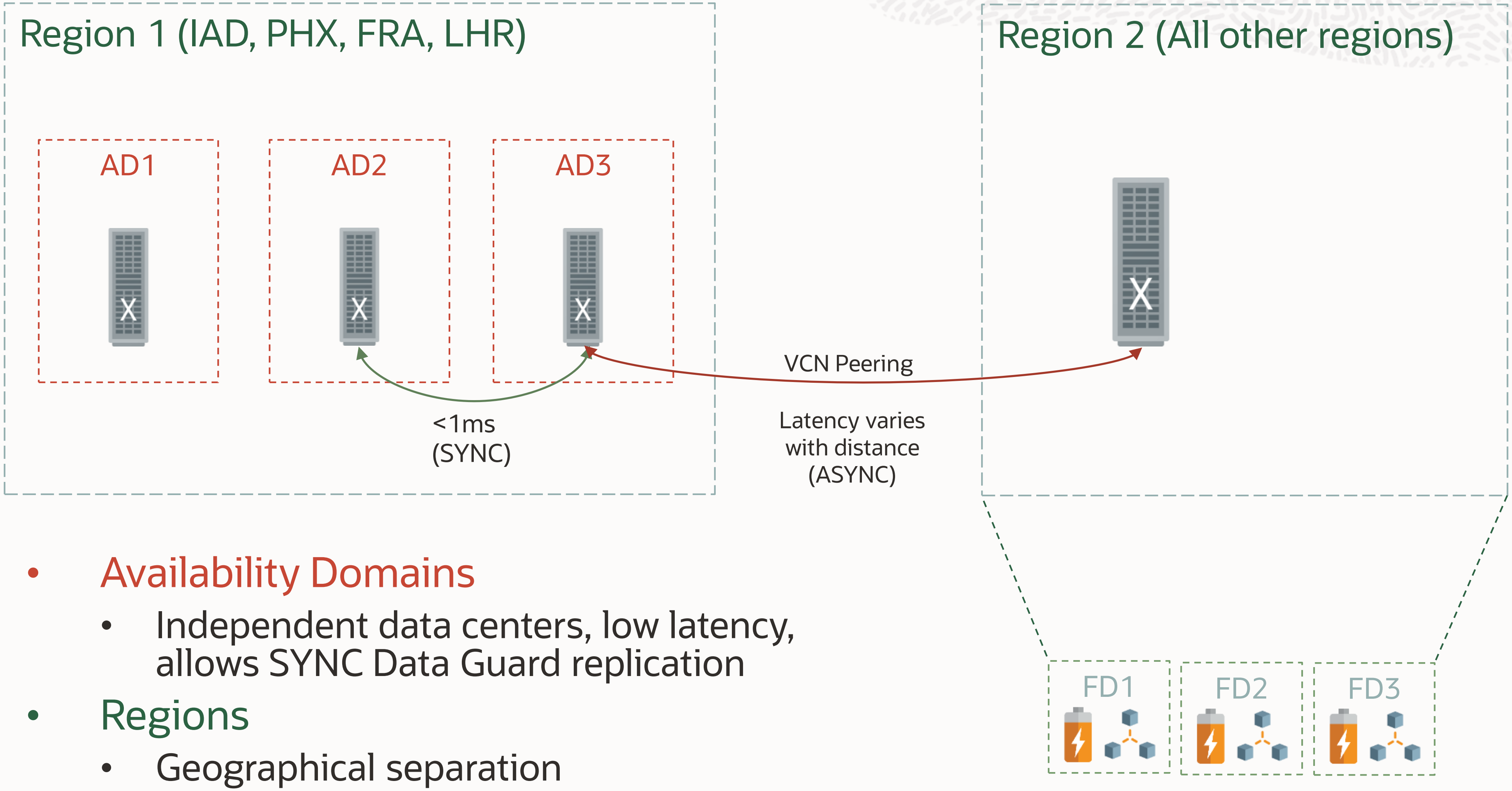
Oracle Cloud Infrastructure topology



- Regions in the same country or area (e.g. Tokyo & Osaka)
  - Comparable latency from customer premises
  - Suitable for business continuity and disaster recovery
- Regions in different areas (e.g. cross-continent)
  - Suitable for disaster recovery or customer's global premises
- Fault Domains
  - Isolated Power & Network

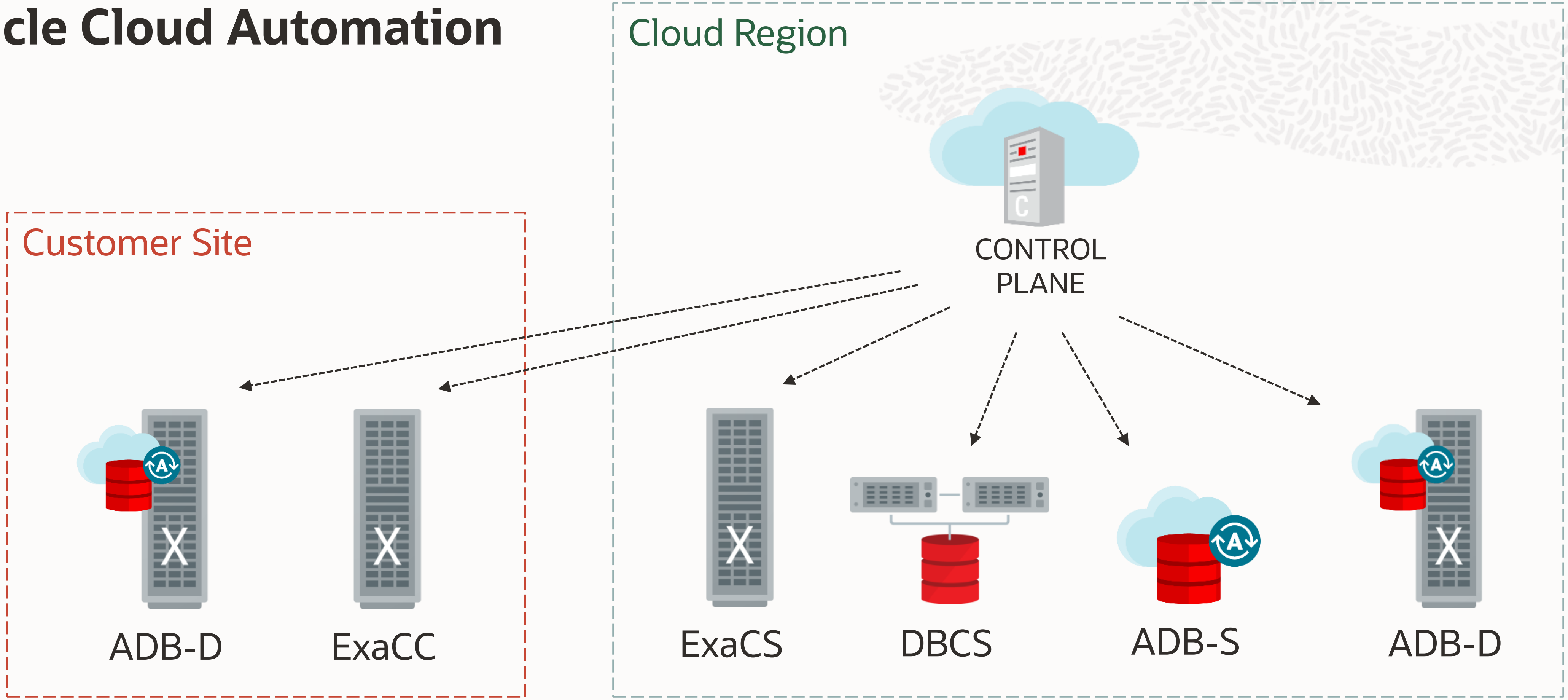
Oracle Cloud Infrastructure Topology

Ashburn, Phoenix, Frankfurt and London only



- Availability Domains
  - Independent data centers, low latency, allows SYNC Data Guard replication
- Regions
  - Geographical separation

Oracle Cloud Automation



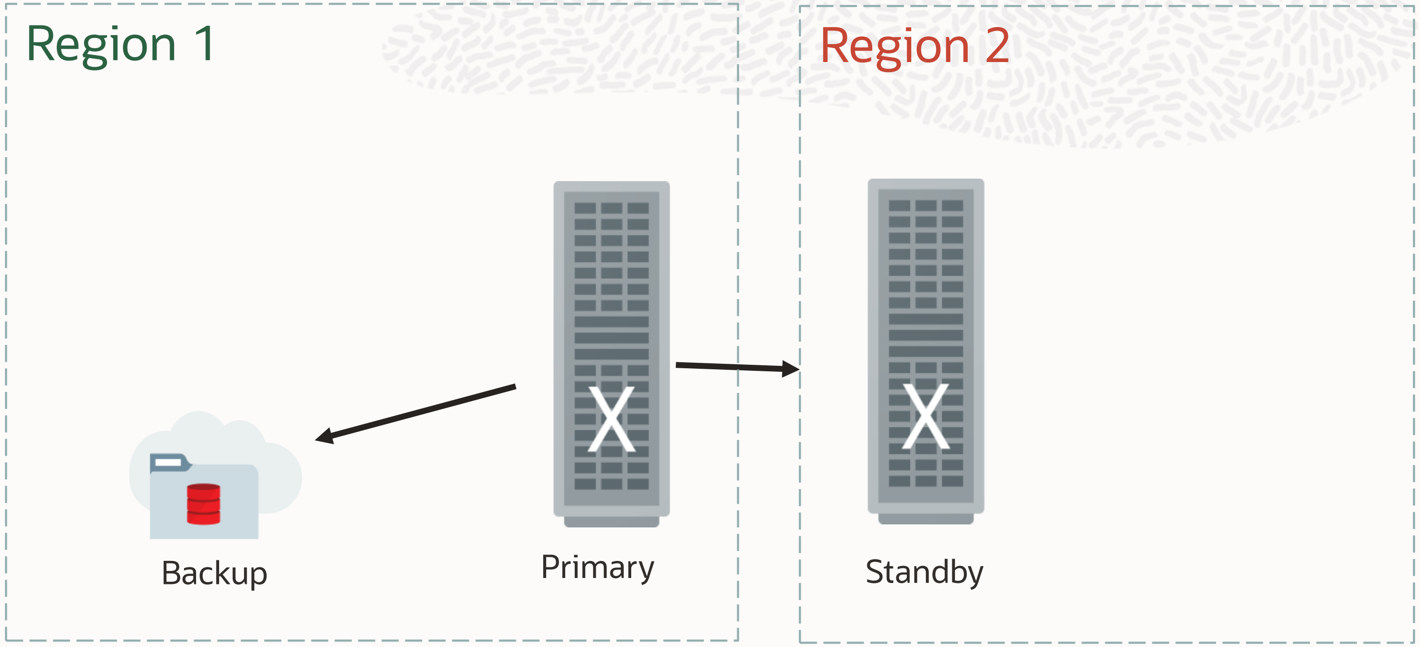
- Cloud Automation can be either:
  - 100% managed by the service
  - Achieved with the OCI Tooling, through the Control Plane:
    OCI User Interface, OCI Rest API, SDK, OCI CLI, Terraform OCI Provider, etc.

Exadata Cloud Services (ExaCS)

Maximum Availability Architecture

Exadata Cloud Services: protection out of the box

	AVAILABILITY / AUTOMATION *	
✓	RMAN	1 copy to 3-way mirrored object storage via automated OCI backups or bkup_api
✓	RAC	Exadata inherent HA, QoS and Performance benefits
✓	ACTIVE DATA GUARD	Via console or DBaaS API (Single Standby only, ExaCS only, cross-region possible, no DBMS_ROLLING OOTB)
✓	GOLDEN GATE	Manual (Capture & Delivery)
	MAA LEVEL	Out of the Box SILVER + Data Guard GOLD



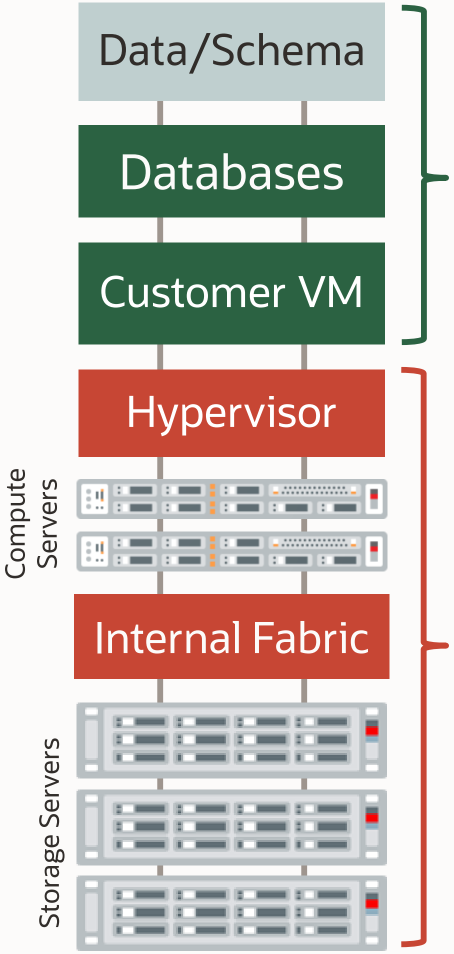
OOTB + ADG Outage Matrix

PLANNED MAINTENANCE	Zero	Zero
UPGRADE	Zero	Hours
RECOVERABLE FAILURE	Zero	Secs
UNRECOVERABLE FAILURE	Secs	Minutes [1]

[1] No FSFO, based on time after customer action

*
- ✓ Out of the box
- ✓ Automated via control plane
- ✓ Manual setup
- ✗ Not available/possible

Exadata Cloud Services: responsibility overview



Customer owns everything inside database

- Data, schema, encryption keys

Customer subscribes to database services

- Customer manages VMs, GI and Databases using Cloud Automation (UI / APIs)
- Automation to create, delete, patch, backup, scale up/down, etc.
- Runs all supported Oracle Database versions from 11.2.0.4 to 19c
- Customer controls access to customer VM

Oracle owns and manages infrastructure

- Database servers/VM hosts, storage servers, fabric network
- Patching, security scans, security updates
- Monitoring and maintenance

Exadata Cloud Services: control plane automatic RMAN backup

1-click configuration automatic RMAN backup

RMAN

SCHEDULING	• Done by control plane, ability to change backup time • Automatic archivelog backup via cron job every 30 minutes
DESTINATION	• DBCS-managed bucket only, no direct control by the customer • No support for archive storage
REPLICAS	• 3-ways mirrored backup • No backup replicas across ADs or object storage buckets
CREDENTIALS	• Managed by the control plane • Automatic password rotation done by control plane
WALLET	• No requirement for wallet backup if using KMS • TDE wallet backed up automatically, but not its password or the autologin Wallet
RESTORE	• Restore CDB capabilities • No capability to restore across ADs or regions via control plane • No duplicate on the same host via control plane
FAILOVER	• Backup runs independently of node availability
STANDBY	• No backup of standby database but can be configured to backup once role is primary
CHARGING	• Only for object storage space (not number of requests or backup module)

Exadata Cloud Services: RMAN backups with `bkup_api`

RMAN

RMAN backup via bkup_api

SCHEDULING	• Scheduled by cron job, runs from first node • Automatic archivelog backup every 30 minutes • Ability to change default backup time and L0 backup day
DESTINATION	• Customer bucket (fully controlled by the customer, including replication) • No support for archive storage
REPLICAS	• Possible to set up backup replication
CREDENTIALS	• Customer responsible for password rotation
WALLET	• TDE wallet backed up, but not its password or the autologin wallet
RESTORE	• Restore CDB and PDB capabilities • No duplicate on the same host via bkup_api
FAILOVER	• Backup initiated on a specific node. • Failure of the node will fail the current backup api call.
STANDBY	• No backup for standby database but can be configured to backup once role is primary
CHARGING	• For object storage space and number of requests (not for the backup module)

Exadata Cloud Services: manual RMAN backups

RMAN

Direct RMAN backup with customer downloaded and configured backup module

SCHEDULING	• No database backup scheduling
DESTINATION	• Use latest Cloud backup module with native API support to access all capabilities (replication, archive storage, …) of OCI object storage
REPLICAS	• Possible to set up backup replication • RMAN catalog possible
CREDENTIALS	• Bucket credentials must be fully managed by customer
WALLET	• TDE wallet backup is customer responsibility
RESTORE	• Anywhere the backups reside (local OSS bucket, remote bucket across AD, remote bucket across region)
FAILOVER	• Customer must configure where the backup executes
STANDBY	• Possible to backup standby databases or offload backups to the standby
CHARGING	• For backup module, object storage and number of requests

Exadata Cloud Services: RMAN best practices

RMAN

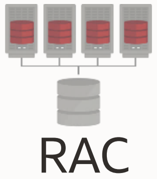
- Use **Control Plane** Automatic Backup for database backup/restore in ExaCS
  - MAA best practices and backup validation are built-in
  - Default settings provide good performance (https://www.oracle.com/a/tech/docs/exacs-oci-backup-restore--oss-performance.pdf)
  - Increase parallelism for higher performance trading off higher CPU processing
  - Ensure data retention settings meets your business requirements (7, 15, 30 or 60 days)
  - For backup monitoring use OCI Events Service
- Customer backup options via **bkup_api**
  - Increase RMAN parallelism for higher performance trading off higher CPU processing
  - TDE wallet needs to be backed up separately
- Use **manual backup** solution for these exceptions
  - Long term (archival) backup retention, backup to remote region or offload backup to standby use cases required

Exadata Cloud Services: Real Application Clusters

RAC

- Out of place patching is built-in with control plane move command
- Software update orchestrates drain, service relocation and instance restart
- RAC uses 192.168.128.0/20 on IB and 100.64.0.0/10 on RoCE for interconnect
- Additional IP addresses can be added
- Changing listener port is not supported, but additional ports can be added

Exadata Cloud Services: RAC best practices



- Create databases only through cloud Control Plane or cloud APIs to include configuration best practices
- Update software using Cloud automation. DB software is out of place update.
- Create a separate application service managed by Oracle Clusterware and follow application failover best practices to achieve zero application downtime
- Run exachk monthly and address alerts
- For “Single Instance”, consider PDB singletons.
- Adjust `hugepages` as you add or resize databases   (set `use_large_pages=ONLY`)
- Avoid DB and system customizations

Exadata Cloud Services: Data Guard via control plane

ACTIVE
DATA GUARD

SETUP	• 1-click setup from control plane • Uses Data Guard broker and MAA practices • Uses optimized Data Guard instantiation
TOPOLOGY	• Supports Data Guard across ADs or across regions • Supports ExaCS to ExaCS only
PROTECTION	• Asynchronous configuration by default (protection level MAX PERFORMANCE) • Synchronous configuration (protection level MAX AVAILABILITY) • Data Guard fast-start failover is a manual setup
ROLE CHANGES	• Supports failover and switchover operations • Out-of-band role transition is not recommended but DB role status will be resynchronized in minutes
OPEN MODE	• Always configured as Active Data Guard (open read-only)
PATCHING UPGRADE	• Control plane understands the role and requires that the standby home is updated first. `datapatch` is run after primary database is updated

Exadata Cloud Services: manual Data Guard setup

ACTIVE
DATA GUARD

SETUP	• Data Guard instantiation and setup are done by the customer • Create Cloud Database and then manually instantiate standby database using standard MAA Data Guard best practices
TOPOLOGY	• Multiple standby databases, far sync and cascade standby • Hybrid Data Guard configurations • These Data Guard topologies are not recognized in the control plane
PROTECTION	• All data protection modes are possible • Setup fast-start failover and incorporate MAA practices manually
ROLE CHANGES	• Recommend using DG broker or Enterprise Manager. • Automatic when Data Guard fast-start failover is setup
OPEN MODE	• Managed by the customer
PATCHING UPGRADE	• Some cloud automation still possible if database is recognized as a cloud database • Customers can manually use standby-first update strategy and `DBMS_ROLLING` for rolling upgrades

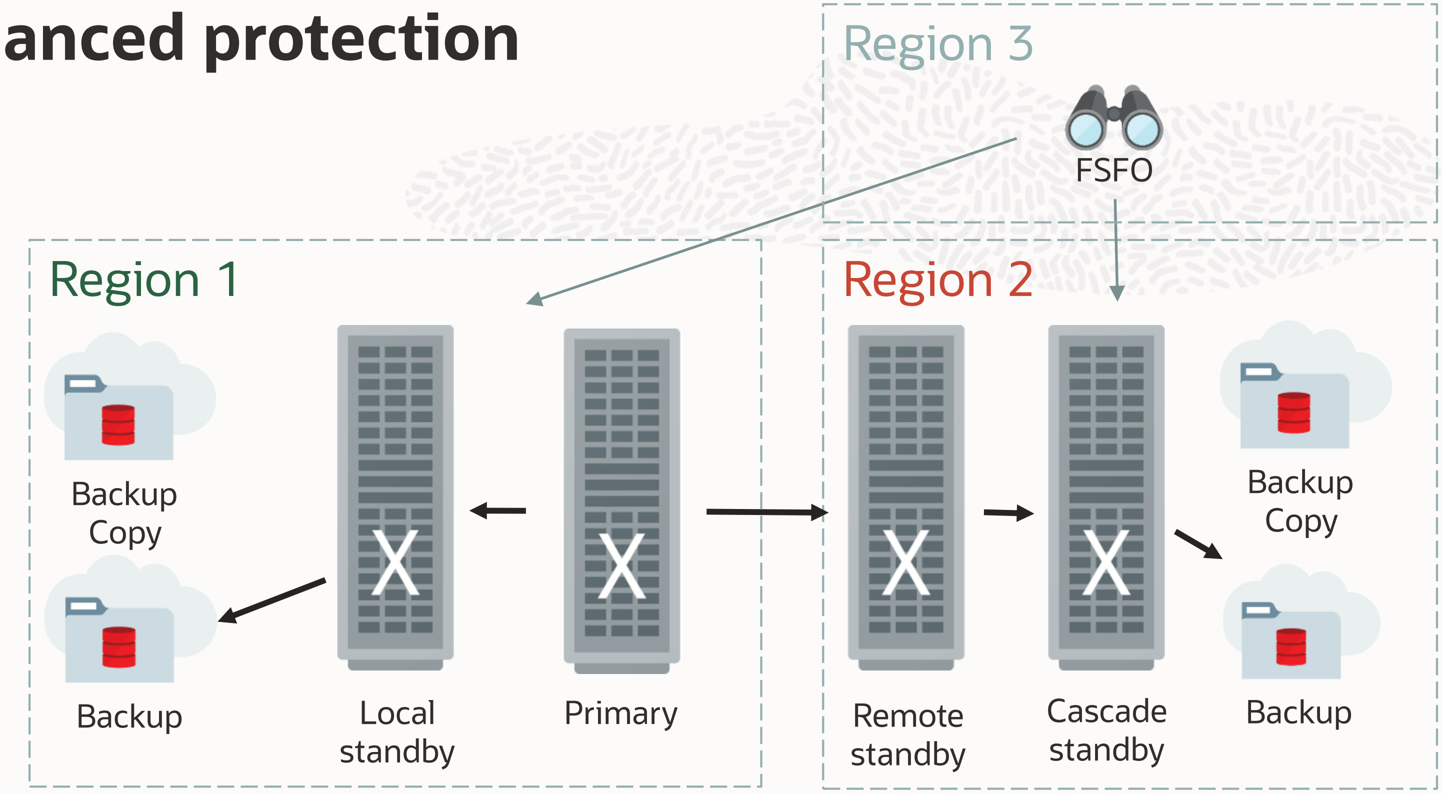
Exadata Cloud Services: Data Guard best practices

ACTIVE
DATA GUARD

- Topology
  - Pick Data Guard topology and protection mode based on SLAs and use cases
  - Use symmetric primary and standby to preserve performance post role transitions
  - Use VCN connectivity (not public cloud) between primary and standby
- Operations
  - Create Data Guard through control plane
    - Pre-create the target Oracle Home with the same version
    - It’s recommended to use Custom Database Software Images for source and target
  - MAA and Data Guard configuration practices incorporated
  - Keep the primary and standby Oracle Home software the same as much as possible
  - Periodically Test and Validate end-to-end DR

Exadata Cloud Services: enhanced protection

AVAILABILITY / AUTOMATION *		
✓ RMAN	Multiple backup copies Backup from the standby	
✓ RAC	Custom application services	
✓ ACTIVE DATA GUARD	Multiple standbys Fast-start failover	
✓ GOLDEN GATE	Manual (capture & delivery) Global Data Service	
MAA LEVEL	ExaCS + Data Guard + Golden Gate	SILVER GOLD PLATINUM



Gold Outage Matrix

PLANNED MAINTENANCE	Zero	! Zero
UPGRADE	Zero	! Secs
RECOVERABLE FAILURE	Zero	! Secs
UNRECOVERABLE FAILURE	Zero	! Secs

*

- ✓ Out of the box
- ✓ Automated via control plane
- ✓ Manual setup
- ✗ Not available/possible

Exadata Cloud Services: Read more

Oracle Maximum Availability Architecture in Exadata DB Systems
https://docs.oracle.com/en-us/iaas/Content/Database/Concepts/maxavailarch.htm#MAA_Exa

ExaCS Database Backup and Restore with Object Storage Performance Observations
https://www.oracle.com/a/tech/docs/exacs-oci-backup-restore--oss-performance.pdf

Managing Exadata Database Backups
https://docs.oracle.com/en-us/iaas/Content/Database/Tasks/exabackingup.htm

Managing Exadata Database Backups by Using bkup_api
https://docs.oracle.com/en-us/iaas/Content/Database/Tasks/exabackingupBKUPAPI.htm

OCI: How To Configure & Manage Database Backups On OCI EXACS DB System (Doc ID 2708469.1)
https://support.oracle.com/epmos/faces/DocumentDisplay?id=2708469.1

Exadata Cloud Services: Read more (cont.)

Autoscaling - Scale-up and Scale-down automation utility for OCI DB System (ExaCS/ExaCC) (Doc ID 2719916.1)
https://support.oracle.com/epmos/faces/DocumentDisplay?id=2719916.1

HowTo configure oci-cli with Instance/Resource Principals (Doc ID 2763990.1)
https://support.oracle.com/epmos/faces/DocumentDisplay?id=2763990.1

Using Oracle Data Guard with Exadata Cloud Service
https://docs.cloud.oracle.com/en-us/iaas/Content/Database/Tasks/exausingdataguard.htm

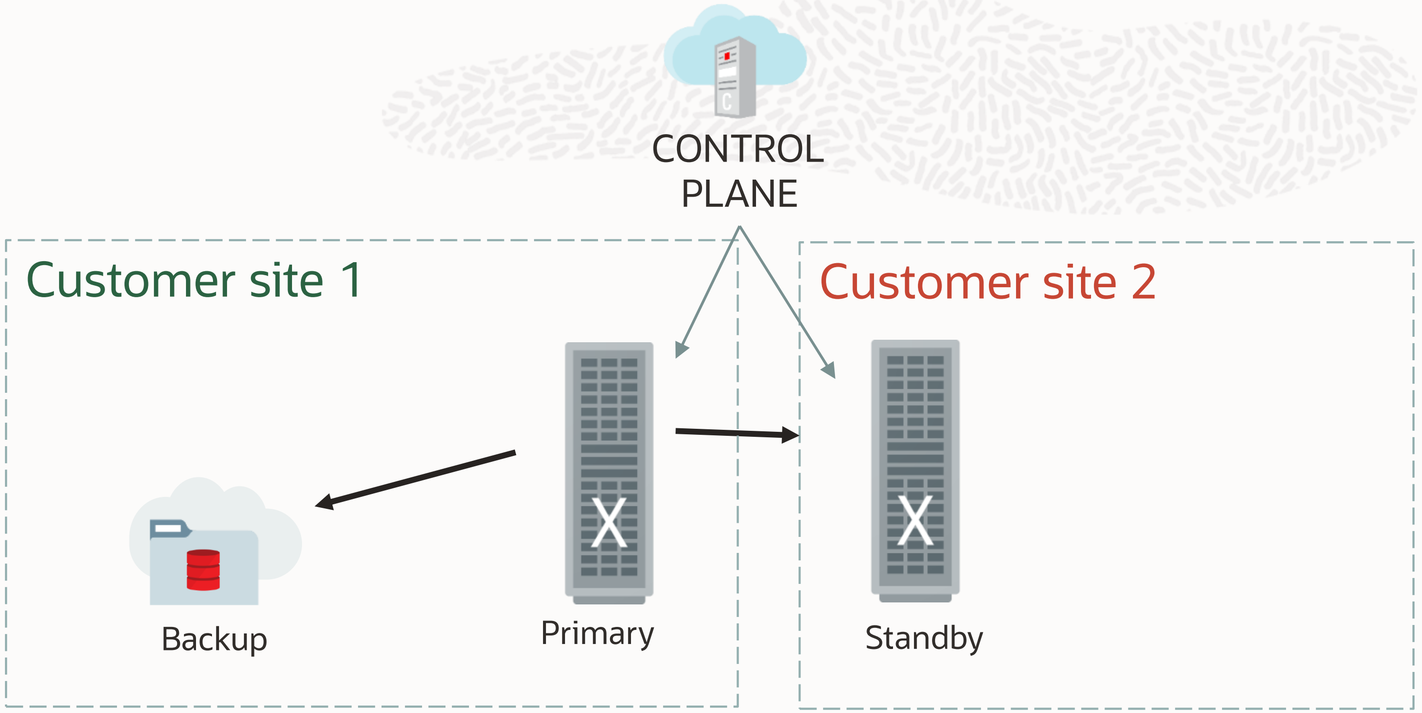
Disaster Recovery using Exadata Cloud (On-Premises Primary to Standby in Exadata Cloud Service or Gen 2 Exadata Cloud at Customer)
https://www.oracle.com/a/tech/docs/hybrid-data-guard-to-exaoci-update-gen2-exacc-exacs.pdf

Exadata Cloud @ Customer

Maximum Availability Architecture

Exadata Cloud @ Customer: protection out of the box

	AVAILABILITY / AUTOMATION *	
✓	RMAN	Customer-defined, to NFS, local object storage, ZDLRA or cloud object storage
✓	RAC	Exadata inherent HA, QoS and Performance benefits
✓	ACTIVE DATA GUARD	Via console or DBaaS API (single standby only, no DBMS_ROLLING OOTB, same control plane)
✓	GOLDEN GATE	Manual (capture & delivery)
	MAA LEVEL	Out of the box SILVER + Data Guard GOLD



OOTB + ADG Outage Matrix

PLANNED MAINTENANCE	Zero	Zero
UPGRADE	Zero	Hours
RECOVERABLE FAILURE	Zero	Secs
UNRECOVERABLE FAILURE	Secs	Minutes[1]

[1] No FSFO, based on time after customer action

*
- ✓ Out of the box
- ✓ Automated via control plane
- ✓ Manual setup
- ✗ Not available/possible

Exadata Cloud @ Customer: control plane automatic RMAN Backup

RMAN

1-click configuration Automatic RMAN backup

	SCHEDULING	• Set up as cron job • Automatic 30 minutes archivelog backup via cron job
	DESTINATION	• To NFS or ZDLRA • To cloud object storage or service-managed bucket
	REPLICAS	• 3-ways mirrored backup for cloud object storage (no replication) • Customer-defined for NFS and ZDLRA
	CREDENTIALS	• Object Storage: managed by the control plane • ZDLRA and NFS: Managed by the customer
	WALLET	• TDE wallet backed up automatically, but not its password (cloud object storage only) • No requirement for wallet backup if using Oracle Key Vault
	RESTORE	• Database restore (from backup, to point-in-time or full) options
	FAILOVER	• Backup initiated on a specific node. It does not run if that node is down.
	STANDBY	• No backup of standby database

Exadata Cloud @ Customer: manual RMAN backups

RMAN

Direct RMAN backup with customer configured backup module

SCHEDULING	• No automatic scheduling. Database and archivelog backups must be scheduled by the customer
DESTINATION	• Any destination possible via RMAN • Use latest Cloud backup module with native API support to access all capabilities (replication, archive storage, …) of OCI object storage
REPLICAS	• Depends on destination capabilities
CREDENTIALS	• Credentials fully managed by customer
WALLET	• TDE wallet backup is customer responsibility • Check backup destination compatibility when using Oracle Key Vault
RESTORE	• Possible everywhere
FAILOVER	• Customer must configure where the backup executes
STANDBY	• Possible to backup standby databases

Exadata Cloud @ Customer: RMAN best practices

RMAN

- Use control plane automatic backup for database backup/restore in ExaCC
- Use ZDLRA for lowest RPO, incremental forever and additional backup/restore benefits
- If NFS is used backup destination, configure DNFS. Tuning is responsibility of the customer
- Increase parallelism for higher performance trading off higher CPU processing
- Ensure backup window is optimum for application cycles
- Choose the backup retention depending on your requirements
  - Object Storage, NFS: 7, 15, 30, 45 or 60 days
  - ZDLRA: controlled by the recovery appliance protection policy
- Use OCI Object Storage and Archive storage for long term backup retention

Exadata Cloud @ Customer: RAC best practices

RAC

- Create databases only through cloud control plane or cloud APIs to include configuration best practices
- Update software using Cloud automation. DB software is out of place update.
  - Cloud orchestrates service drain, service relocation and instance restart transparently
- Create a separate application service managed by Oracle Clusterware and follow application failover best practices to achieve zero application downtime
- Avoid DB and system customizations
- Run exachk monthly and address alerts
- Adjust `hugepages` as you add or resize databases (set `use_large_pages=ONLY`)
- For Single Instance or RAC sub-setting, administrator has to change startup options

Exadata Cloud @ Customer: Data Guard via control plane

ACTIVE
DATA GUARD

	SETUP	• 1-click setup from same control plane • Uses Data Guard Broker and MAA practices • Uses `Optimized Data Guard Instantiation`
	TOPOLOGY	• Supports Data Guard across ADs or across regions • Supports ExaCC to ExaCC only • Far sync, cascade or multiple standby databases require manual configuration
	PROTECTION	• Asynchronous configuration by default (protection level MAX PERFORMANCE) • Synchronous configuration (protection level MAX AVAILABILITY) • Data Guard fast-start failover is a manual setup
	ROLE CHANGES	• Supports failover and switchover operations with Control Plane • Out-of-band role transition is not recommended but DB role status will be resynchronized in minutes
	OPEN MODE	• Always configured as Active Data Guard (open read-only)
	PATCHING UPGRADE	• Control Plane understands the role and requires that the standby home is updated first. Data Patch is run after primary database is updated. • DB rolling upgrade (DBMS_Rolling) is not available yet

Exadata Cloud @ Customer: manual Data Guard setup

ACTIVE
DATA GUARD

SETUP	• Data Guard instantiation and setup are done by the customer • Create Cloud Database and then manually instantiate standby database using standard MAA Data Guard best practices
TOPOLOGY	• Multiple standby databases, far sync and cascade standby are available • Hybrid configurations • Data Guard topology is not recognized in the control plane
PROTECTION	• All data protection modes are possible • Setup Fast-start failover and incorporate MAA practices
ROLE CHANGES	• Recommend using DG broker or Enterprise Manager. • Automatic if Data Guard Fast-Start Failover is setup
OPEN MODE	• Managed by the customer
PATCHING UPGRADE	• Some Database Cloud Automation still possible • Customers can manually use standby-first approach and DBMS_ROLLING for rolling upgrades

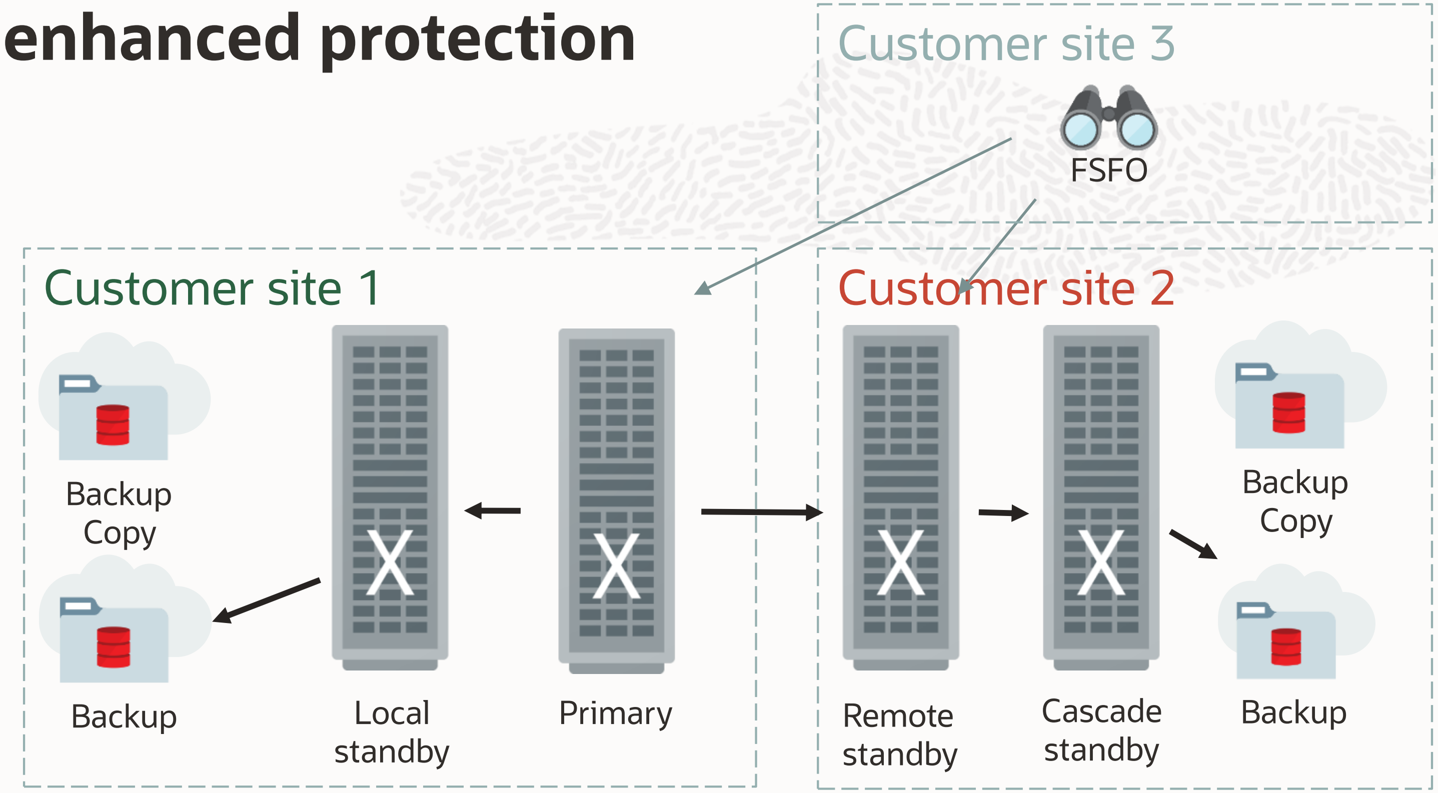
Exadata Cloud @ Customer: Data Guard best practices

ACTIVE
DATA GUARD

- Topology
  - Pick Data Guard topology and protection mode based on SLAs and use cases
  - Use symmetric primary and standby to preserve performance post role transitions
- Operations
  - Create Data Guard through control plane
    - Pre-create the target Oracle Home with the same version
    - It's recommended to use Custom Database Software Images for source and target
  - MAA and Data Guard configuration practices incorporated
  - Keep the primary and standby Oracle Home software the same as much as possible
  - Periodically Test and Validate end-to-end DR

Exadata Cloud @ Customer: enhanced protection

AVAILABILITY / AUTOMATION *		
✓	RMAN	Backup from the primary or/and standby. Offload backups to the standby.
✓	RAC	Custom application services
✓	ACTIVE DATA GUARD	Multiple standbys Fast-start failover
✓	GOLDEN GATE	Manual (capture & delivery)
	MAA LEVEL	Out of the box — SILVER + Data Guard — GOLD + GoldenGate — PLATINUM



Gold Outage Matrix

PLANNED MAINTENANCE	Zero	Zero
UPGRADE	Zero	Secs
RECOVERABLE FAILURE	Zero	Secs
UNRECOVERABLE FAILURE	Zero	Secs

*

- ✓ Out of the box
- ✓ Automated via control plane
- ✓ Manual setup
- ✗ Not available/possible

Exadata Cloud @ Customer MAA: Read more

Oracle Maximum Availability Architecture in Exadata DB Systems
https://docs.oracle.com/en-us/iaas/Content/Database/Concepts/maxavailarch.htm#MAA_Exa

Using Oracle Data Guard with Exadata Cloud at Customer
https://docs.oracle.com/en-us/iaas/exadata/doc/eccusingdataguard.html

Guidelines When Using ZFS Storage in an Exadata Environment (2087231.1)
https://support.oracle.com/epmos/faces/DocumentDisplay?id=2087231.1

Set Up and Configure Exadata X8M Backup with ZFS Storage ZS7-2 (2635423.1)
https://support.oracle.com/epmos/faces/DocumentDisplay?id=2635423.1

Database Cloud Services – Virtual Machines

Maximum Availability Architecture

Database Cloud Services VM: basic information

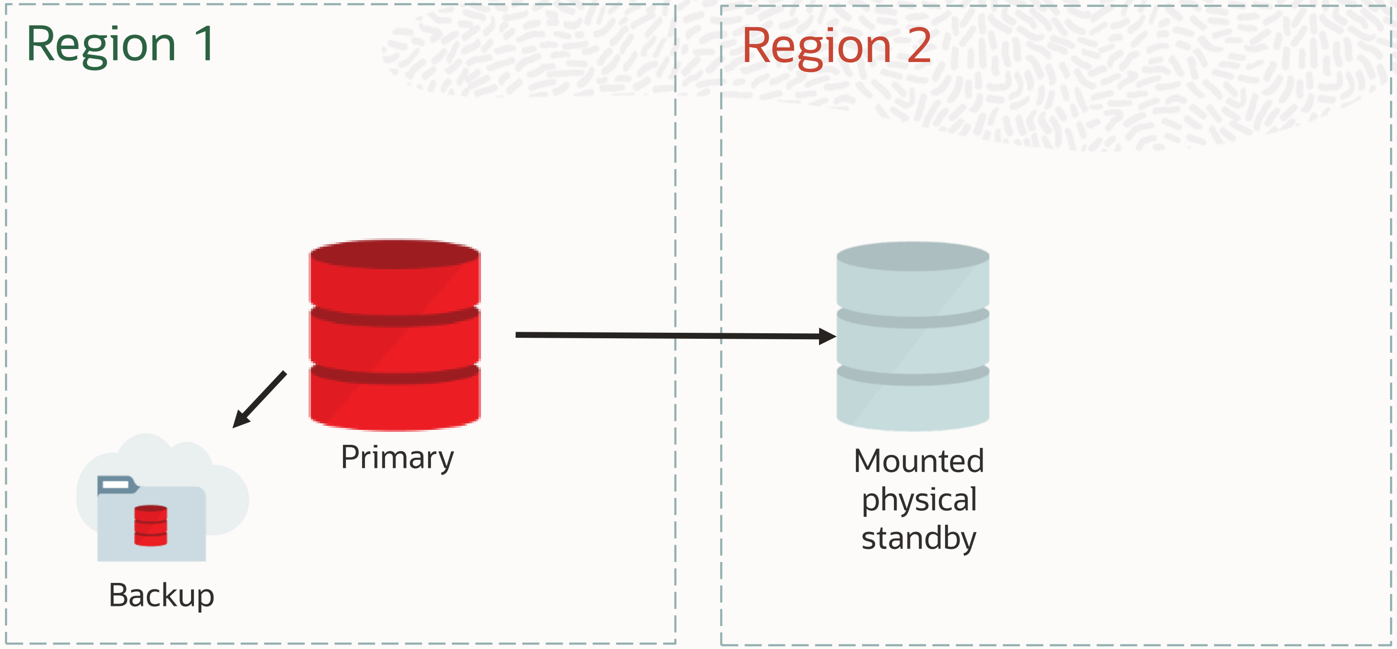
- DBCS uses standard Intel Compute with block storage
  - Block storage is triple-mirrored automatically
  - Either on LVM or ASM (Grid Infrastructure)
    - ASM uses external redundancy
- VMs are automatically restarted on failure
- VMs are automatically relocated to a different hypervisor on HW failure
- RAC nodes use different fault domains per node
- Support for «VM reboot» migrations

Database Cloud Services VM: software editions

	SE	EE	EE HP	EE EP 1n	EE EP 2n
Flashback	Only Flashback Query	✓	✓	✓	✓
Backup & Recovery	Non parallel only	✓	✓	✓	✓
Multitenant / Refresh Clone	Single CDB per VM DB System, Max 3 PDBs starting with 19c	Single CDB per VM DB System, Max 3 PDBs starting with 19c	Single CDB per VM DB System	Single CDB per VM DB System	Single CDB per VM DB System
RAC	✗	✗	✗	✗	✓
Data Guard	✗	✓ Standard Data Guard	✓ Standard Data Guard	✓ Active Data Guard	✓ Active Data Guard
Application Continuity	✗	✗	✗	✓	✓

Database Cloud Services VM 1-Node: protection out of the box

	AVAILABILITY / AUTOMATION *	
✓	RMAN	1 copy to 3-way mirrored object storage via automated OCI backups
✗	RAC	Only for 2 nodes EE Extreme Performance
✓	ACTIVE DATA GUARD	Standard Data Guard only, via console or DBaaS API (1 SB only, symmetric only)
✓	GOLDEN GATE	Manual (capture & delivery)
	MAA LEVEL	Out of the box BRONZE



OOTB + ADG Outage Matrix

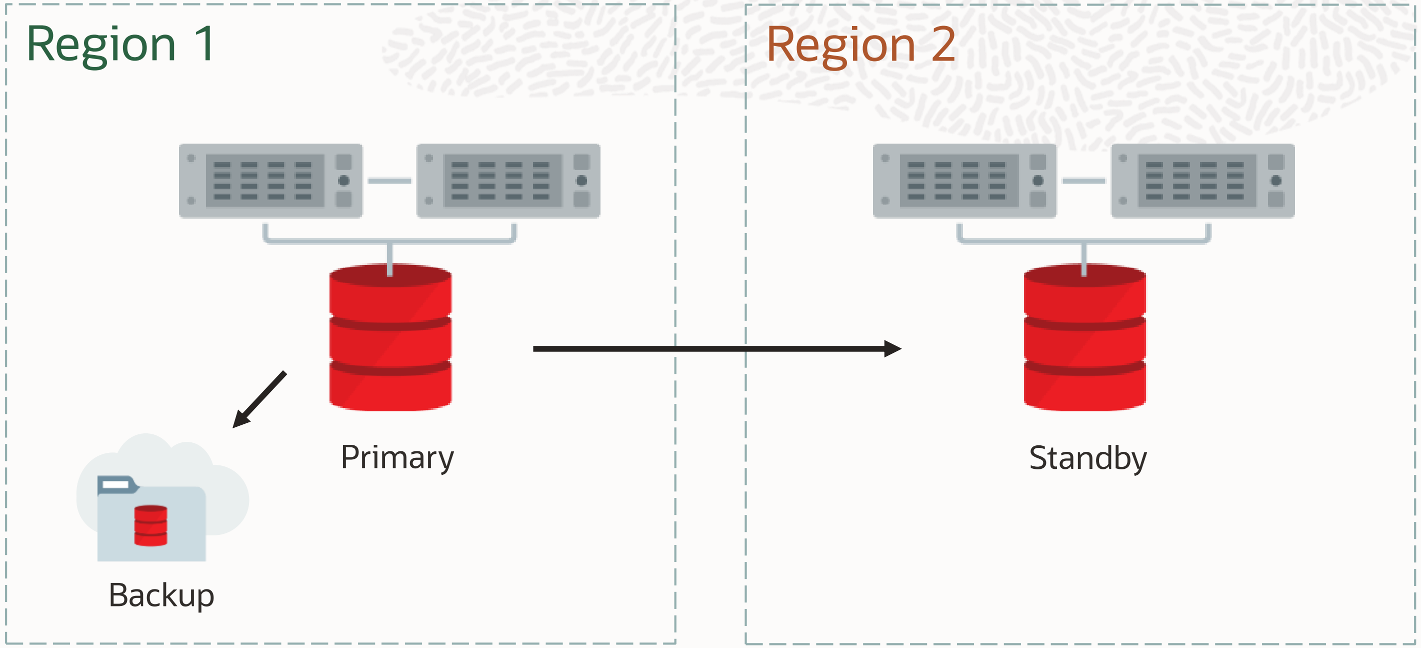
PLANNED MAINTENANCE	Zero	Mins/Hours
UPGRADE	Zero	Hours
RECOVERABLE FAILURE	Secs	Minutes
UNRECOVERABLE FAILURE	Secs	Mins/Hours

*

- ✓ Out of the box
- ✓ Automated via control plane
- ✓ Manual setup
- ✗ Not available/possible

Database Cloud Services VM RAC: protection out of the box

	AVAILABILITY / AUTOMATION *
✓ RMAN	1 copy to 3-way mirrored object storage via automated OCI backups
✓ RAC	Only for 2 nodes EE Extreme Performance
✓ ACTIVE DATA GUARD	Via console or DBaaS API (1 SB only, symmetric only)
✓ GOLDEN GATE	Manual (capture & delivery)
MAA LEVEL	Out of the box SILVER + Data Guard GOLD



OOTB + ADG Outage Matrix

PLANNED MAINTENANCE	Zero	Zero
UPGRADE	Zero	Hours
RECOVERABLE FAILURE	Zero	Minutes
UNRECOVERABLE FAILURE	Secs	Minutes [1]

[1] No FSFO, based on time after customer action

*

- ✓ Out of the box
- ✓ Automated via control plane
- ✓ Manual setup
- ✗ Not available/possible

Database Cloud Services VM: control plane automatic RMAN backup

RMAN

1-click configuration Automatic RMAN backup

SCHEDULING	• Done by control plane • Automatic hourly archivelog backup via DBCS agent
DESTINATION	• DBCS-managed bucket only, no direct control by the customer • No support for archive storage
REPLICAS	• 3-ways mirrored backup • No backup replicas across ADs or object storage buckets
CREDENTIALS	• Managed by the control plane • Automatic password rotation done by control plane
WALLET	• TDE wallet backed up automatically, but not its password or the autologin wallet • Separated manual backup recommended
RESTORE	• No capability to restore across ADs or regions via control plane • No duplicate on the same host (only 1 CDB supported per DB system)
FAILOVER	• Backup runs independently of node availability (only for RAC)
STANDBY	• No backup of standby database
CHARGING	• Only for object storage space (not number of requests or backup module)

Database Cloud Services VM: RMAN backups with `dbcli`

RMAN

RMAN backup via dbcli

SCHEDULING	• Scheduled by DBCS scheduler • Automatic hourly archivelog backup
DESTINATION	• Customer bucket (fully controlled by the customer) • No support for archive storage
REPLICAS	• Possible to set up backup replication
CREDENTIALS	• Customer responsible for password rotation
WALLET	• TDE wallet backup is customer responsibility
RESTORE	• No duplicate on the same host (only 1 CDB supported per DB system)
FAILOVER	• Backup runs independently of node availability (only for RAC)
STANDBY	• No backup for stand-by
CHARGING	• For object storage space and number of requests (not for the backup module)

RMAN

Database Cloud Services VM: manual RMAN backups

Direct RMAN backup with customer downloaded and configured backup module

	SCHEDULING	• No automatic scheduling. Database and archivelog backups must be scheduled by the customer
	DESTINATION	• Use latest Cloud backup module with native API support to access all capabilities (replication, archive storage, …) of OCI object storage
	REPLICAS	• Possible to set up backup replication • RMAN catalog possible
	CREDENTIALS	• Bucket credentials must be fully managed by customer
	WALLET	• TDE wallet backup is customer responsibility
	RESTORE	• Possible everywhere
	FAILOVER	• Customer must configure where the backup executes
	STANDBY	• Possible to backup standby databases
	CHARGING	• For backup module, object storage and number of requests

Database Cloud Services VM: RMAN best practices

RMAN

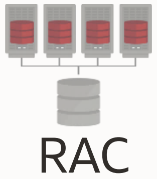
- The performance of the RMAN backup is defined by the network.
  - Depending on VM shape (network bandwidth is correlated to the number of CPUs)
  - Network is used for reading datafiles (block storage) and writing backup pieces (object storage)
  - Monitor network for RMAN backups impact on running applications
- Standard Edition allows just 1 backup channel
- Number of backup channels depends on VM shape and should be adapted manually
- Backup compression (LOW/MEDIUM) can be changed manually
- Other RMAN configuration parameters should not be changed when using automated backup
- Additional separated manual backup of TDE wallet recommended
- Backup retention can be set to 7, 15, 30 or 60 days
- For backup monitoring use OCI Events Service
- Use standalone backups (full) through control plane for long-term backups with longer retention requirements
  - Automatic backups are deleted when the instance is terminated
  - Standalone backups will stay until deleted manually

RAC

Database Cloud Services VM: Real Application Clusters

- Software update orchestrates drain, service relocation and instance restart
- RAC uses `192.168.16.0/24` for interconnect
- Additional IP addresses can be added
- Changing listener port is not supported, but additional ports can be added

Database Cloud Services VM: RAC best practices



- Create databases only through cloud Control Plane or cloud APIs to include configuration best practices
- Update software using Cloud automation. DB software is out of place update.
- Create a separate application service managed by Oracle Clusterware and follow application failover best practices to achieve zero application downtime
- For “Single Instance”, consider PDB singletons.
- Adjust `hugepages` as you add or resize databases   (set `use_large_pages=ONLY`)
- Avoid DB and system customizations

Database Cloud Services VM: Data Guard via control plane

ACTIVE
DATA GUARD

SETUP	• 1-click setup from control plane • Uses Data Guard broker • Only via `DUPLICATE FROM ACTIVE DATABASE`
TOPOLOGY	• No far sync, cascade or multiple standby databases • Possible only between DBCS VMs • Not supported between RAC and single instance
PROTECTION	• Asynchronous configuration by default (protection level MAX PERFORMANCE) • Synchronous configuration (protection level MAX AVAILABILITY) • Data Guard fast-start failover is a manual setup
ROLE CHANGES	• Out-of-band role transition is not recommended but DB role status will be resynchronized in minutes
OPEN MODE	• It depends on Database software edition (ADG only with Extreme Performance)
PATCHING UPGRADE	• No guided patching of databases but control plane understands the role and does not apply datapatch on a standby • No support for rolling upgrade

ACTIVE
DATA GUARD

Database Cloud Services VM : manual Data Guard setup

SETUP	• Data Guard instantiation and setup are done by the customer • Create Cloud Database and then manually instantiate standby database using standard MAA Data Guard best practices
TOPOLOGY	• Multiple standby databases, far sync and cascade standby are available • Hybrid configurations • Data Guard topology is not recognized in the control plane
PROTECTION	• All data protection modes are possible • Setup Fast-start failover and incorporate MAA practices
ROLE CHANGES	• Recommend using DG broker or Enterprise Manager. • Automatic if Data Guard Fast-Start Failover is setup
OPEN MODE	• Managed by the customer
PATCHING UPGRADE	• Some Database Cloud Automation still possible • Customers can manually use standby-first approach and DBMS_ROLLING for rolling upgrades

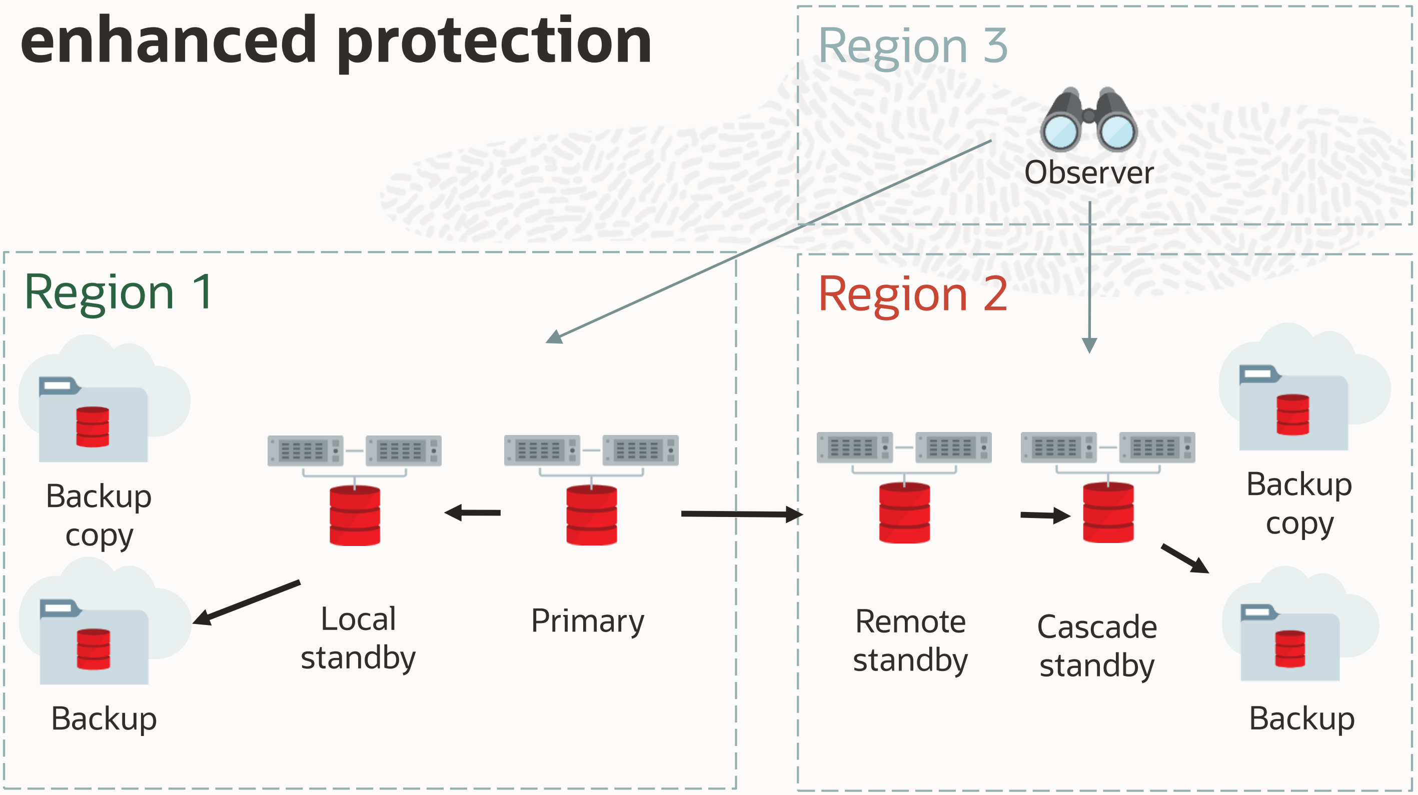
ACTIVE
DATA GUARD

Database Cloud Services VM: Data Guard best practices

- Always use Grid Infrastructure storage management (ASM) for Data Guard environments
  - It includes Oracle Notification Services (ONS)
  - No static listener entries required
  - Service control (`srvctl`)
- Data Guard on LVM is supported but lacks above functionalities
- Always use custom application services
- Changing listener port is not supported (but additional ports can be added)
- `db_block_checking` is set by default to:
  - `FULL` on Grid Infrastructure, consider performance implications when migrating
  - `TYPICAL` on LVM
- Custom DB software images are recommended
- Only use VCN connectivity and not public network
- Put FSFO observer with the applications or in a 3rd region

Database Cloud Services VM: enhanced protection

	AVAILABILITY / AUTOMATION *		
✓	RMAN	Multiple backup copies Backup from the standby	
✓	RAC	Custom application services	
✓	ACTIVE DATA GUARD	Multiple standbys Fast-start failover	
✓	GOLDEN GATE	Manual (capture & delivery)	
	MAA LEVEL	Out of the box	SILVER
		+ Data Guard	GOLD
		+ GoldenGate	PLATINUM



Gold Outage Matrix		
PLANNED MAINTENANCE	Zero	Zero
UPGRADE	Zero	Secs
RECOVERABLE FAILURE	Zero	Secs
UNRECOVERABLE FAILURE	Zero	Secs

*

- ✓ Automated via control plane
- ✓ Manual setup
- ✗ Not available/possible

Database Cloud Services VM: read more

Backing Up a Database to Oracle Cloud Infrastructure Object Storage
https://docs.oracle.com/en-us/iaas/Content/Database/Tasks/backingupOS.htm

Using Oracle Data Guard
https://docs.oracle.com/en-us/iaas/Content/Database/Tasks/usingdataguard.htm

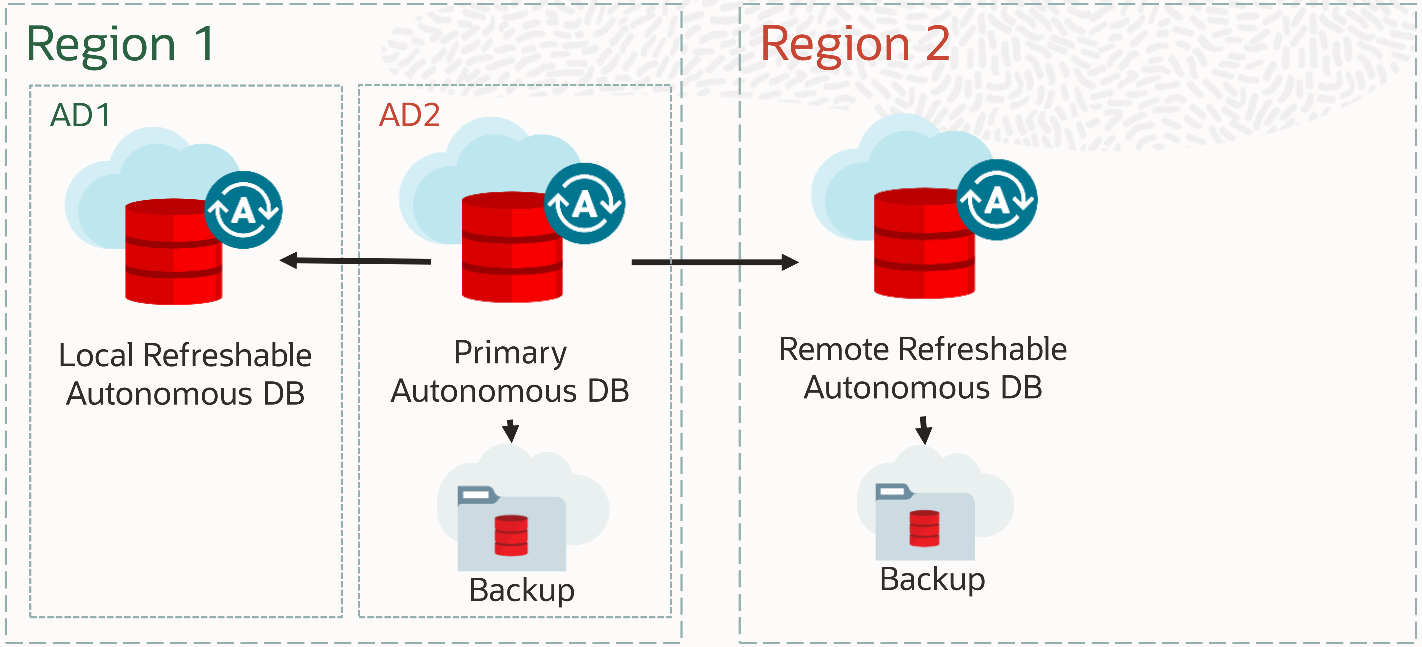
HowTo configure oci-cli with Instance/Resource Principals (Doc ID 2763990.1)
https://support.oracle.com/epmos/faces/DocumentDisplay?id=2763990.1

Autonomous Database – Shared

Maximum Availability Architecture

Autonomous Database - Shared: protection out of the box

	AVAILABILITY / AUTOMATION *	
✓	RMAN	Backup from primary and standby to 3-way mirrored object storage via Autonomous Backups
✓	RAC	Exadata inherent HA, QoS and Performance benefits Services out of the box
✓	AUTONOMOUS DATA GUARD	Via console (2 StandBys: 1 local and 1 remote, ADB-S only) [1] Automatic failover if zero data loss
✓	GOLDEN GATE	Manual (capture & delivery)
	MAA LEVEL	Out of the box SILVER + AuDG AUROUS



Region 1
AD1
Local Refreshable Autonomous DB
AD2
Primary Autonomous DB
Backup
Region 2
Remote Refreshable Autonomous DB
Backup

Outage Matrix

PLANNED MAINTENANCE	Zero ! Zero
UPGRADE	Zero ! Minutes
RECOVERABLE FAILURE	Zero ! Secs
UNRECOVERABLE FAILURE	Last refresh ! Minutes

*

- ✓ Out of the box
- ✓ Automated via control plane
- ✓ Manual setup
- ✗ Not available/possible

Autonomous Database - Shared: automatic backup

RMAN

SCHEDULING	• Automatically done by the service (full every 60 days, daily incremental, weekly cumulative, hourly archivelog)
DESTINATION	• Service-managed bucket, no direct customer access
REPLICAS	• 3-ways mirrored backup • Backup replication available with Autonomous Data Guard
CREDENTIALS	• Managed internally • Automatic password rotation
WALLET	• TDE wallet managed and backed up by Oracle
RESTORE	• In-place restore only • Duplicate from backup is supported if the source is available or if within the retention window
FAILOVER	• Backup runs independently of node availability
STANDBY	• Backup of standby database is automatic with AuDG
CHARGING	• No charge for automatic backups • For object storage and number of requests, when doing manual backups

Autonomous Database - Shared: automatic backup best practices

RMAN

- Backup retention is always 60 days
- Automatic backups are unavailable when the ADB instance is terminated
- Manual backup to customer object storage:
  - Used for fast PITR only
  - Follows backup retention
  - Cannot be used to create a new database

Autonomous Database - Shared: Real Application Clusters

RAC

- Services are automatically created
  - ATP and ADW: `_high, _medium, _low`
  - ATP only: `_tp, _tpurgent`
- Client access only via TLS
- Application Continuity can be enabled and configured via `DBMS_CLOUD_ADMIN` package
- No configuration requirement for Fast Application Notification
  - FAN events are handled by Connection Manager (CMAN)
- Databases with lower OCPU count only opened on a single node
- Databases with higher OCPU count opened on two nodes
- Patching is rolling and announced in the user interface (No database downtime . Zero application downtime for short transactions, long transactions might have impact)

Autonomous Database - Shared: Autonomous Data Guard via control plane

Autonomous
DATA GUARD

	SETUP	• 1-click setup from control plane • Only via PDB hot clone
	TOPOLOGY	• Setup of 1 standby within region (across ADs where applicable) and 1 across regions • Remote region destinations predefined based on latency • Only possible between ADB-S
	PROTECTION	• Asynchronous configuration (RPO up to 5 minutes, RTO up to 2 minutes) • Automatic failover available if no data loss can be guaranteed • RTO does not include detection time
	ROLE CHANGES	• Switchover and failover available through control plane • Connection string does not change
	OPEN MODE	• No access to standby database • Additional read-only clones can be created and refreshed manually
	PATCHING UPGRADE	• Primary and standby are patched independently • PDB can be relocated to upgraded database

Autonomous Database - Shared: read more

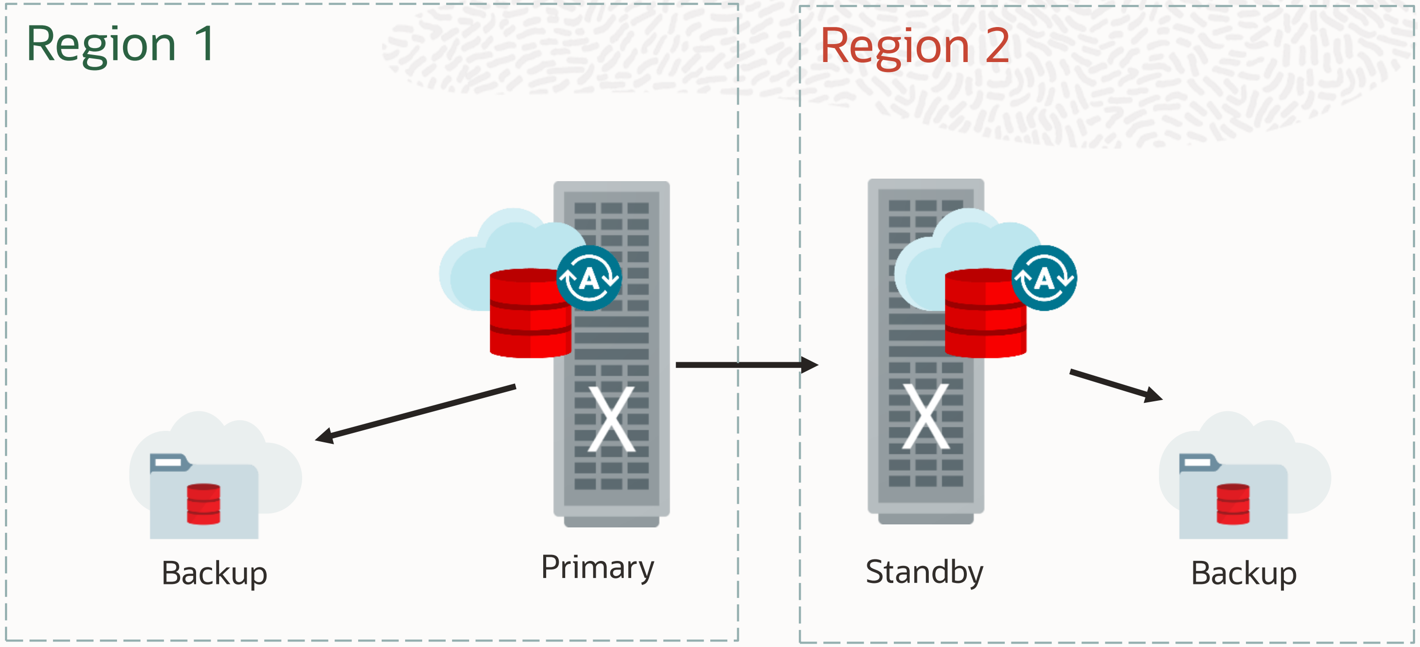
Oracle Maximum Availability Architecture and Autonomous Database Cloud
https://docs.oracle.com/en-us/iaas/Content/Database/Concepts/maxavailarch.htm#MAA_auto

Autonomous Database – Dedicated

Maximum Availability Architecture

Autonomous Database - Dedicated: protection out of the box

	AVAILABILITY / AUTOMATION *		
✓	RMAN	1 copy to 3-way mirrored object storage via automated OCI backups ExaCC: also ZDLRA, NFS, local	
✓	RAC	Exadata inherent HA, QoS and Performance benefits Services out of the box	
✓	AUTONOMOUS DATA GUARD	1 SB ADB-D only, cross-region possible ADB on ExaCC: same control plane only, ADB ExaCC only	
✓	GOLDEN GATE	Manual (Capture & delivery)	
	MAA LEVEL	Out of the box + AuDG + GoldenGate	SILVER GOLD PLATINUM



Gold Outage Matrix

PLANNED MAINTENANCE	Zero	Zero
UPGRADE	Zero	Minutes
RECOVERABLE FAILURE	Zero	Secs
UNRECOVERABLE FAILURE	Secs	Minutes [1]

[1] No FSFO, based on time after customer action

*

- ✓ Out of the box
- ✓ Automated via control plane
- ✓ Manual setup
- ✗ Not available/possible

Autonomous Database - Dedicated: automatic backup

RMAN

	SCHEDULING	• Automatically done by the service (weekly full, daily incremental, 15 mins archivelog)
	DESTINATION	• Internal object storage bucket, no direct customer access • ADB on ExaCC: NFS, ZDLRA (recovery appliance) or local • For ZDLRA, real time redo transport not available yet
	REPLICAS	• Object storage, 3-ways mirrored backup • ADB on ExaCC: ZDLRA backup replication available (manual)
	CREDENTIALS	• Object Storage: managed internally • ZDLRA, NFS: managed by the customer
	WALLET	• TDE wallet managed and backed up by Oracle • ADB: Oracle Vault (KMS) supported • ADB on ExaCC: Oracle Key Vault supported
	RESTORE	• In-place restore only • Duplicate (clone) is supported
	FAILOVER	• Backup runs independently of node availability
	STANDBY	• Automatic backup of standby database
	CHARGING	• No charge for automatic backups

Autonomous Database - Dedicated: automatic backup best practices

RMAN

- Backup retention
  - Object Storage, NFS: 7, 15, 30, 45 or 60 days
  - ZDLRA: controlled by the recovery appliance protection policy
  - Local: 7 days
- On-demand PDB backup:
  - Used for fast PITR only
  - Follows backup retention
  - Cannot be used to create a new database

Autonomous Database - Dedicated: Real Application Clusters

RAC

- RAC uses 192.168.128.0/20 on IB and 100.64.0.0/10 on RoCE for interconnect
- Client network configured on customer’s subnet. The only available connection is SCAN
- Client connection via TCP or TLS
- Databases with lower OCPU count only opened on a single node
- Databases with higher OCPU count opened on two or more nodes
- Patching is rolling and scheduled by the customer
- Fast Application Notification must be configured, ONS ports need to be opened

Autonomous Database – Dedicated: RAC services

RAC

High priority OLTP [1]	tpurgent	tpurgent_tls	tpurgent_ro	tpurgent_ro_tls
Typical OLTP [1]	tp	tp_tls	tp_ro	tp_ro_tls
High priority Reporting [2]	high	high_tls	high_ro	high_ro_tls
Typical Reporting [2]	medium	medium_tls	medium_ro	medium_ro_tls
Low priority Reporting [2]	low	low_tls	low_ro	low_ro_tls

[1] Transparent Application Continuity enabled by default

[2] Use DBMS_APP_CONT_ADMIN.ENABLE_TAC to enable TAC for the non TP services

Autonomous Database - Dedicated: Autonomous Data Guard via control plane

Autonomous
DATA GUARD

SETUP	• Setup from control plane on CDB creation • A protected CDB can be chosen at ADB creation
TOPOLOGY	• Single primary-standby setup across ADs or regions • Only possible between ADB-D of the same type (On-Prem to On-Prem or OCI to OCI) • MAA practices integrated
PROTECTION	• Max Availability or Max Performance possible at CDB level • Automatic failover not available yet
ROLE CHANGES	• Switchover and Failover at CDB level available through control plane • Connection string is aware of Autonomous Data Guard • Role based services available
OPEN MODE	• Standby database is open read-only • Standby role services available
PATCHING UPGRADE	• Customer controls when primary and standby are patched • No database downtime for any software or hardware updates

Autonomous Database - Dedicated: Read more

Continuous Availability Best Practices for Applications Using Autonomous Database – Dedicated
https://www.oracle.com/technetwork/database/options/clustering/applicationcontinuity/continuous-service-for-apps-on-atpd-5486113.pdf

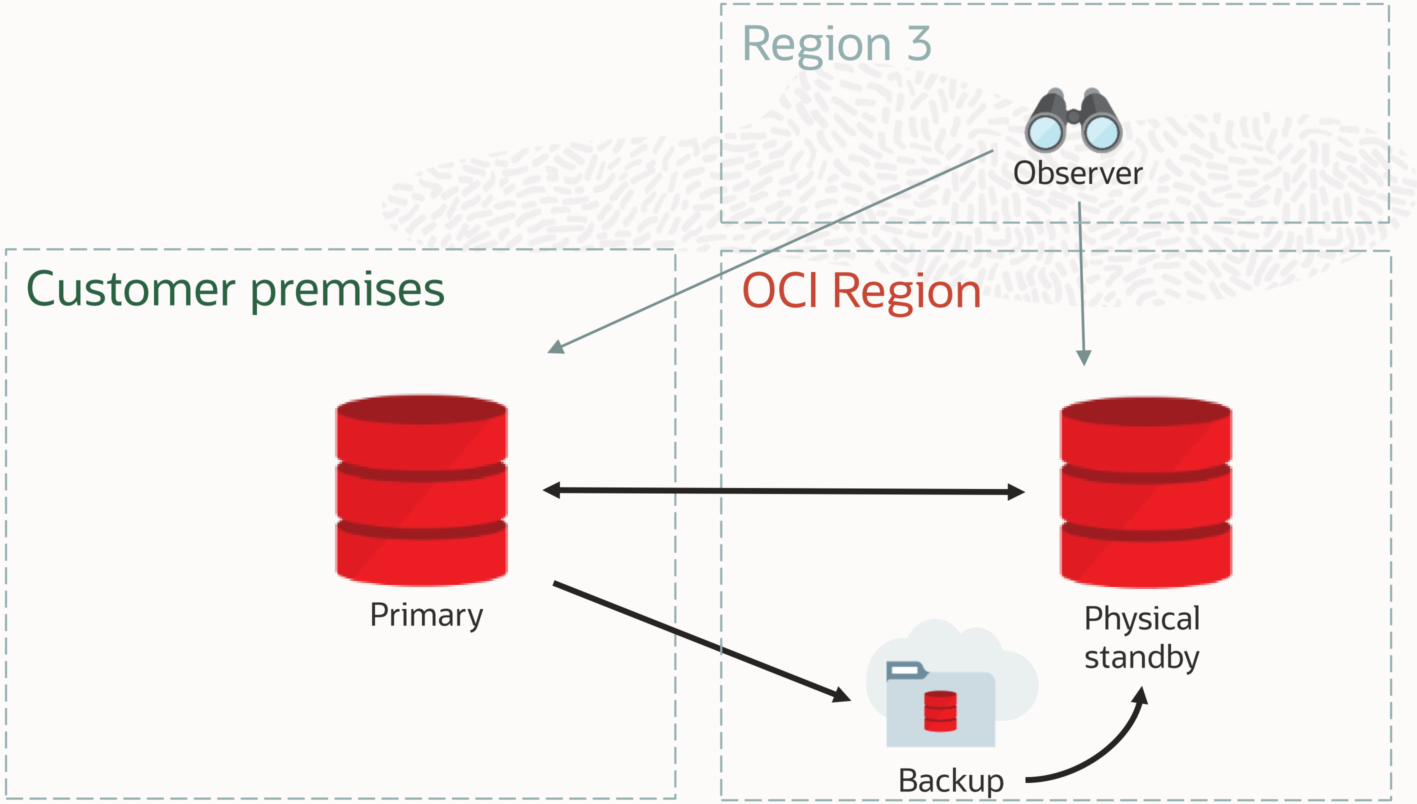
Oracle Maximum Availability Architecture and Autonomous Database Cloud
https://docs.oracle.com/en-us/iaas/Content/Database/Concepts/maxavailarch.htm#MAA_auto

Hybrid Cloud

Maximum Availability Architecture

Hybrid Cloud: overview

AVAILABILITY / AUTOMATION [1]		
RMAN	Backup to the cloud	
RAC	Customer-specific	
ACTIVE DATA GUARD	Instantiate & operate Data Guard configuration	
GOLDEN GATE	Manual (capture & delivery)	
MAA LEVEL	Customer responsibility	BRONZE GOLD PLATINUM

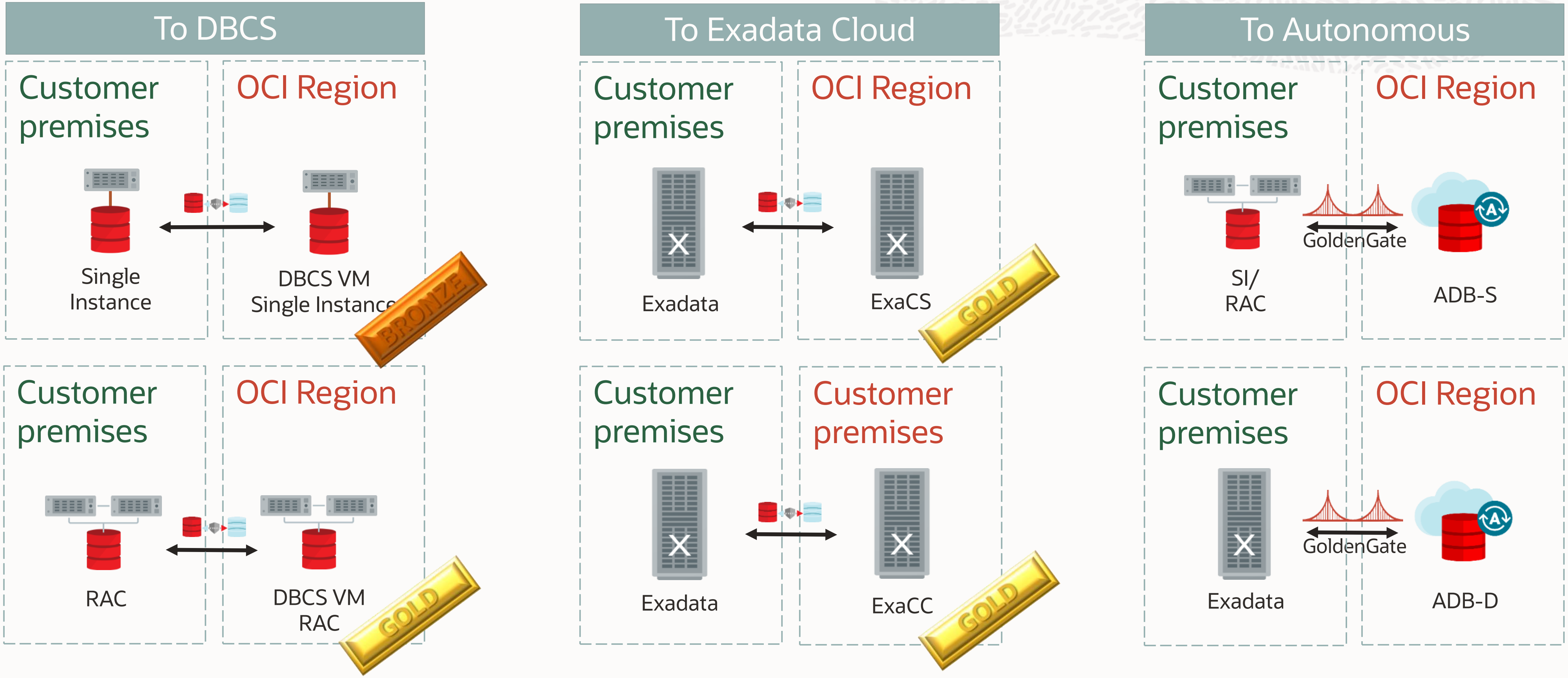


Gold Outage Matrix [2]		
	PLANNED MAINTENANCE	Zero ! Zero
	UPGRADE	Zero ! Secs
	RECOVERABLE FAILURE	Zero ! Secs
	UNRECOVERABLE FAILURE	Zero ! Secs

[1] Customer responsibility

[2] Best case scenario (FSFO + SYNC or FAR SYNC)

Hybrid Cloud: recommended hybrid sources/destinations



To DBCS

Customer premises: Single Instance → OCI Region: DBCS VM Single Instance (BRONZE)

Customer premises: RAC → OCI Region: DBCS VM RAC (GOLD)

To Exadata Cloud

Customer premises: Exadata → OCI Region: ExaCS (GOLD)

Customer premises: Exadata → Customer premises: ExaCC (GOLD)

To Autonomous

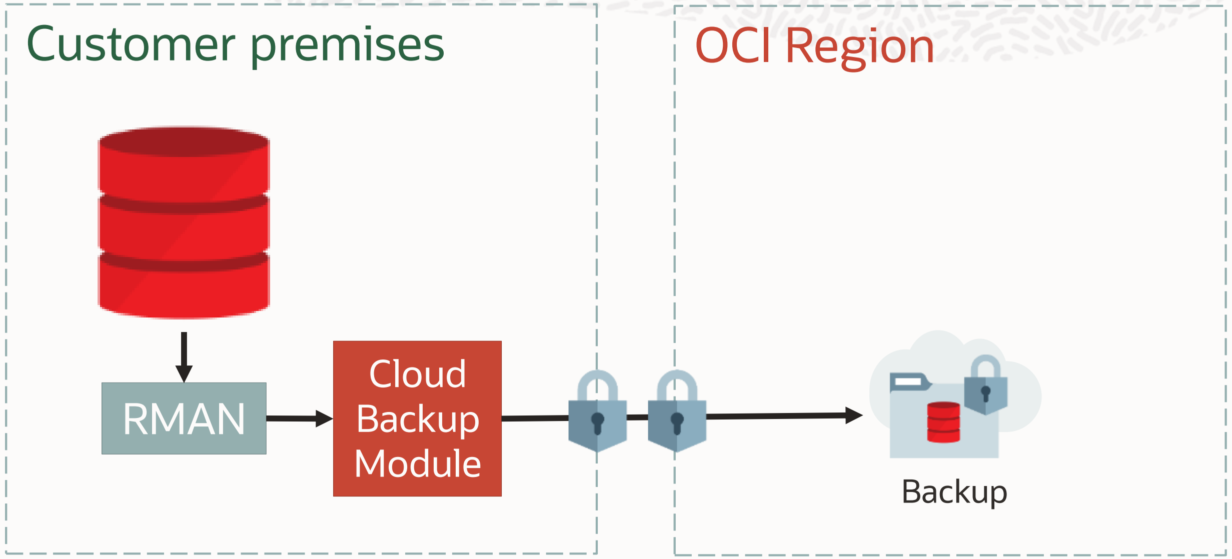
Customer premises: SI/ RAC → GoldenGate → OCI Region: ADB-S

Customer premises: Exadata → GoldenGate → OCI Region: ADB-D

- All Hybrid configurations are achieved manually: no Control Plane automation
- On-premises non-Exadata to ExaCC/ExaCS is possible but beware of exclusive features

Hybrid Cloud: backup to Oracle Cloud Infrastructure

- Cost effective, scalable cloud storage for database backups
- End-to-end enterprise-grade data encryption, compression and protection
- Key based authentication
- Supports multiple compartments
- Object lifecycle policies for archiving
- Multipart upload
- Geo-Replication,
  3-way Protection in the cloud
- RMAN driven backup & recovery



Hybrid Cloud: backup to Oracle Cloud Infrastructure

RMAN

Oracle Database Backup Cloud Service Best Practices for On-Premise Database Backup & Recovery
https://www.oracle.com/technetwork/database/features/availability/twp-oracledatabasebackupservice-2183633.pdf

Use Fast Connect with public peering
https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/fastconnectmultipledrgs.htm

ACTIVE
DATA GUARD

Hybrid Cloud: Data Guard destination matrix

		On-premises DB	DBCS	DBCS RAC	ExaCC	ExaCS
	OS	Linux Windows [1]	Linux	Linux	Linux	Linux
	VERSION	11.2.0.4 to 19c	Same as source	Same as source	Same as source	Same as source
	RELEASE UPDATE	Stay within last 3 RUs	Same as source or Standby first. Use Custom DB Image	Same as source or Standby first. Use Custom DB Image	Same as source or Standby first. Use Custom DB Image	Same as source or Standby first. Use Custom DB Image
	ARCHITECTURE	Same as destination	CDB	CDB	CDB or non-CDB	CDB or non-CDB
	EDITION	DG: EE ADG: +ADG option	DG: EE, EE-HP ADG: EE-EP	EE-EP	Included in ExaCC	Included in ExaCS

[1] Data Guard Support for Heterogeneous Primary and Physical Standbys in Same Data Guard Configuration (Doc ID 413484.1)

Hybrid Cloud: Data Guard checklist

ACTIVE
DATA GUARD

Network

- Measure peak redo rates and ensure enough bandwidth
  - Assessing and Tuning Network Performance for Data Guard and RMAN (Doc ID 2064368.1)
    - Generally recommended:
      `(SDU=65536) (RECV_BUF_SIZE=134217728) (SEND_BUF_SIZE=134217728)`
      `net.core.rmem_max = 134217728 net.core.wmem_max = 134217728`
- Communication must be bi-directional
- Use either IPSec VPN or FastConnect (recommended)
  - For FastConnect use private peering
  - If internet is used, use SQL*Net encryption

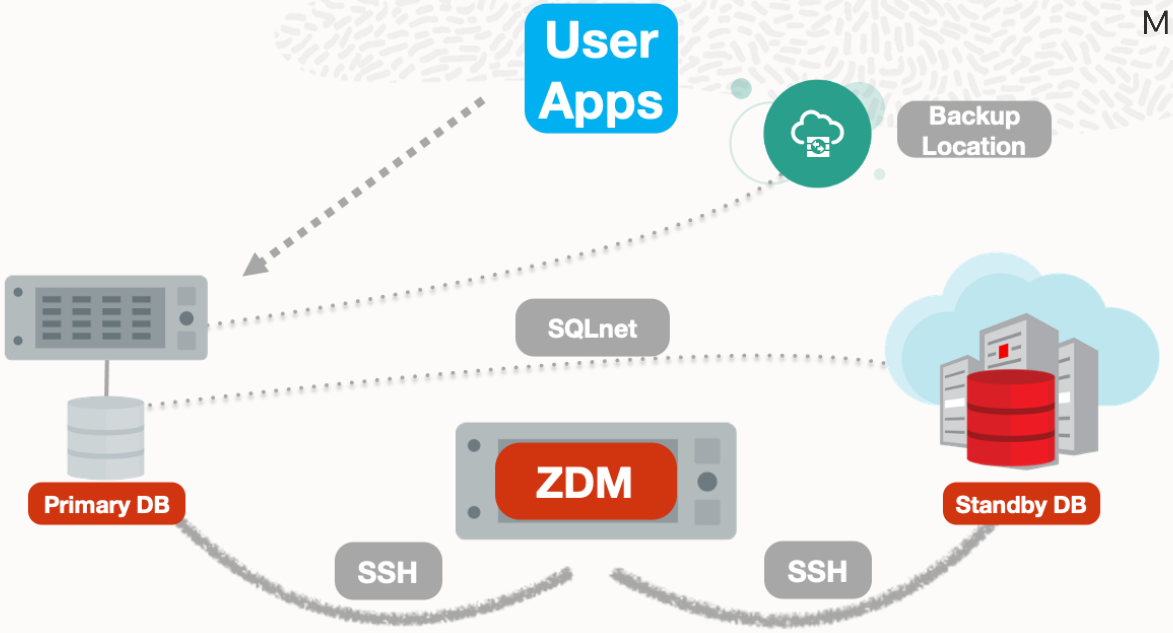
Transparent Data Encryption

- Use TDE on both primary and standby
  - Encrypt primary prior to migration whenever possible
- Master Note for Transparent Data Encryption (TDE) (Doc ID 1228046.1)
- Oracle Database Tablespace Encryption Behavior in Oracle Cloud (Doc ID 2359020.1)

Hybrid Cloud: automatic setup with ZDM

ZERO DOWNTIME MIGRATION

ZDM PHASES	
1	Download & Configure ZDM
2	ZDM Starts Database Migration
3	ZDM Connects the Source to the Object Store
4	ZDM Orchestrates Transfer of Backup Files
5	ZDM Instantiates a Standby DB
6	ZDM Synchronizes Primary & Standby
7	ZDM Switches Over & Swaps Roles
8	ZDM Finalizes the Migration Process



Simple

Leverages Oracle MAA best practices

Zero data loss

Free

https://oracle.com/goto/zdm

Hybrid Cloud: Data Guard high-level implementation steps

ACTIVE
DATA GUARD

- Create Database in the Cloud
  - Same patch level +one-offs as source via Custom DB Software Images
  - Same db_name (db_unique_name defined by the cloud)
- Delete the DB with the drop command (not using cloud tooling)
- Copy passwordfile
- Prepare the new init file (avoid copying parameters from on-premises)
- Copy/create TDE wallet
- Setup SQL*Net communication
- Instantiate standby database (RESTORE FROM SERVICE/DUPLICATE)
- Configure broker and enable configuration
- Validate Switchover, Snapshot Standby, **Client failover**
- Monitor MAA score (ORAchk for DBCS, exachk for ExaCS)
- Monitor DG health: **Monitoring a Data Guard Configuration (Doc ID 2064281.1)**
- Extend configuration with FAR_SYNC and FSFO

- Hybrid Data Guard steps also work for manual DG setup in cloud in general

ACTIVE
DATA GUARD

Patching

- Control plane does not support automatic patching of primary and standby
- Cloud tooling understands the role of the database
  - To patch a Data Guard environment (Cloud control plane setup or manual):
    1. Patch standby first, tooling will not try to run datapatch, it will succeed
    2. Patch primary, tooling runs datapatch, changes will be applied to standby
    3. Patches on RAC are always rolling (no downtime)
  - To patch a Data Guard environment non-RAC with minimum downtime:
    1. Patch standby first, tooling will not try to run datapatch, it will succeed
    2. Switchover to standby
    3. Patch old primary, tooling will not try to run datapatch, it will succeed
    4. Finish patching manually by calling datapatch manually on primary

Hybrid Cloud: Data Guard - read more

ACTIVE
DATA GUARD

Hybrid Data Guard to Oracle Cloud Infrastructure Production Database on Premises and Disaster Recovery with DBaaS BM or VM shapes in Oracle Cloud Infrastructure
https://www.oracle.com/technetwork/database/availability/hybrid-dg-to-oci-5444327.pdf

Disaster Recovery using Exadata Cloud
On-Premises Primary to Standby in Exadata Cloud Service or Gen 2 Exadata Cloud at Customer
https://www.oracle.com/a/tech/docs/hybrid-data-guard-to-exaoci-update-gen2-exacc-exacs.pdf

Best Practices for Corruption Detection, Prevention, and Automatic Repair - in a Data Guard Configuration (Doc ID 1302539.1)
https://support.oracle.com/epmos/faces/DocumentDisplay?id=1302539.1

Oracle Data Guard Best Practices
https://docs.oracle.com/en/database/oracle/oracle-database/19/haovw/oracle-data-guard-best-practices.html

Hybrid Cloud: GoldenGate

Migration to the Oracle Cloud with an Oracle GoldenGate Hub Configuration
https://www.oracle.com/a/tech/docs/maa-database-migration-to-oci-with-a-goldengate-hub.pdf

Additional Information

Maximum Availability Architecture

Cloud MAA configuration

	RMAN			RAC	DATA GUARD			
	Auto Backup	Backup Replicas	Standby Backup	App Services	Auto DG Config	Auto Failover	Cross Region	Auto Patching
ExaCS	🟩	🟨	🟨	🟨	🟩	🟨	🟩	🟩
ExaCC	🟩	🟨	🟨	🟨	🟩	🟨	🟩	🟩
DBCS VM RAC	🟩	🟨	🟨	🟨	🟩	🟨	🟩	🟩
ADB-S	🟦	🟩	🟩	🟦	🟩	🟩	✖	🟦
ADB-D	🟦	✖	🟩	🟦	🟩	🟨	🟩	🟦

*

🟦	Out of the box	🟨	Manual setup
🟩	Automated via control plane	✖	Not yet available

Additional Information: GoldenGate setup

GoldenGate can be set up:

- Manually for on-premises, hybrid and cloud architectures
- Using GoldenGate OCI marketplace to leverage GoldenGate Hub when replicating between 2 databases in the cloud
  - Round-trip latency between GoldenGate Hub and replication target must be <2 ms

Using Oracle GoldenGate on Oracle Cloud Marketplace

https://docs.oracle.com/en/middleware/goldengate/core/19.1/oggmp/getting-started-oracle-goldengate-oracle-cloud-marketplace.html

Migration to the Oracle Cloud with an Oracle GoldenGate Hub Configuration

https://www.oracle.com/a/tech/docs/maa-database-migration-to-oci-with-a-goldengate-hub.pdf

Oracle Maximum Availability Architecture (MAA) GoldenGate Hub

https://www.oracle.com/a/tech/docs/maa-goldengate-hub.pdf

Additional Information: read more

MAA Best Practices for the Oracle Cloud
https://www.oracle.com/database/technologies/high-availability/oracle-cloud-maa.html

MAA Best Practices - Oracle Database
https://www.oracle.com/database/technologies/high-availability/oracle-database-maa-best-practices.html

MAA Best Practices - Exadata Database Machine
https://www.oracle.com/database/technologies/high-availability/exadata-maa-best-practices.html

MV2OCI: move data to Oracle Cloud Database in "one-click" (Doc ID 2514026.1)
https://support.oracle.com/epmos/faces/DocumentDisplay?id=2514026.1

Best Practices for Corruption Detection, Prevention, and Automatic Repair - in a Data Guard Configuration (Doc ID 1302539.1)
https://support.oracle.com/epmos/faces/DocumentDisplay?id=1302539.1

Continuous Availability Best Practices for Applications Using Autonomous Database - Dedicated
https://www.oracle.com/technetwork/database/options/clustering/applicationcontinuity/continuous-service-for-apps-on-atpd-5486113.pdf

ORACLE

Our mission is to help people see data in new ways, discover insights, unlock endless possibilities.