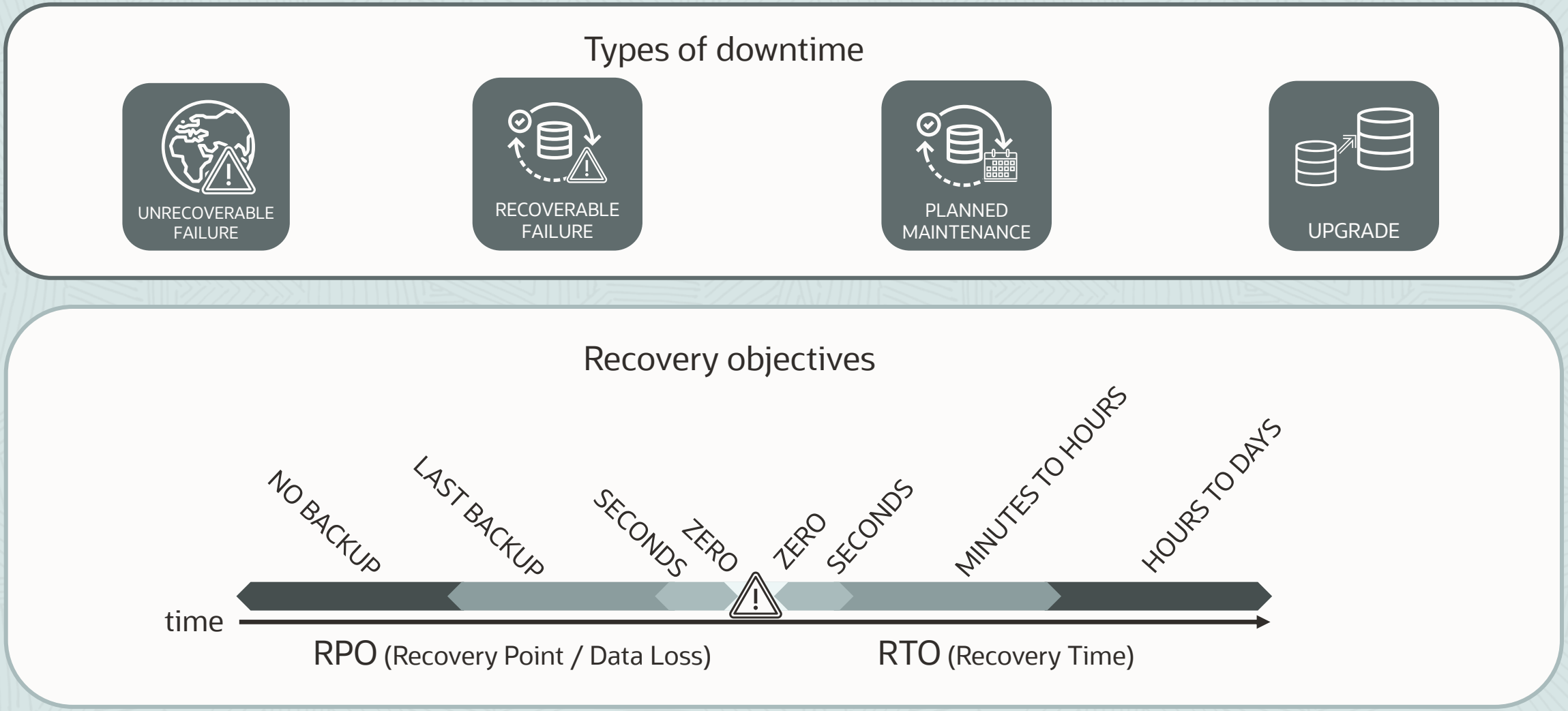
ORACLE

Oracle Cloud
Maximum Availability Architecture

Oracle Database High Availability, Scalability, and Maximum Availability Architecture team

December 2024

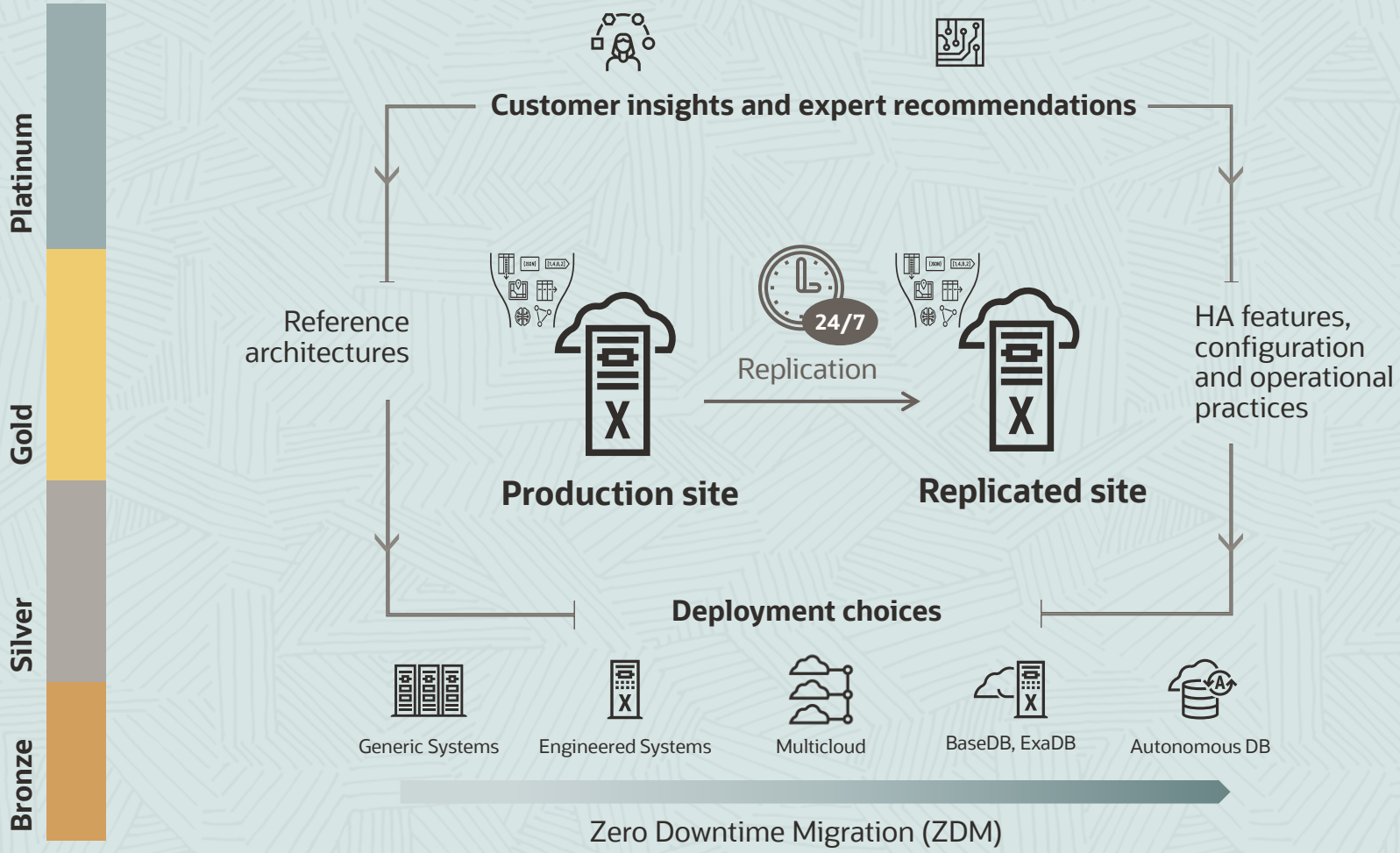
Types of Downtime and Recovery Objectives



From Single Instance to 99.999%

Maximum Availability Reference Architectures

Oracle Maximum Availability Architecture (MAA)



High performance

- Resource Management
- Database In-Memory
- True Cache

Continuous availability

- Application Continuity
- Online Redefinition
- Edition-based Redefinition

Data protection

- Flashback
- RMAN
- ZDLRA+ ZRCV

Active replication

- Active Data Guard
- Full Stack DR
- GoldenGate

Scale out & Lifecycle

- RAC
- Globally Distributed Database
- FPP
- Real Application Testing

Single Instance Protection

Underlying Technologies

SINGLE INSTANCE

- ACID transactions
- Standard protection
- Automatic Restart

ONLINE REORG

- Online table redefinition and partition maintenance
- Less planned downtime

RESOURCE MANAGER

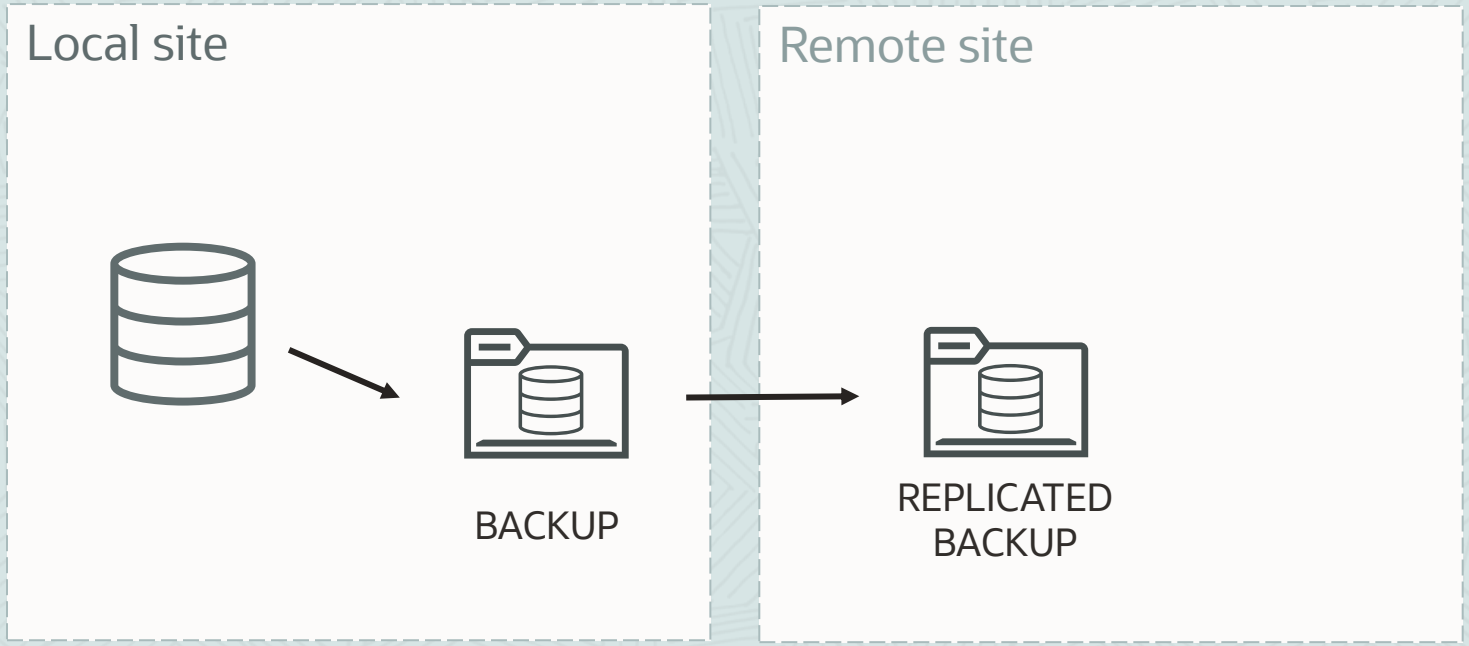
- PDB and CDB isolation
- Protection from noisy neighbors

FLASHBACK

- Protection from wrong transactions

RMAN

- Basic DB protection
- Protection from data loss



Bronze Outage Matrix

PLANNED MAINTENANCE	ZERO / MINS/HOURS
RECOVERABLE FAILURE	ZERO / MINS/HOURS
UNRECOVERABLE FAILURE	LAST BACKUP / HOURS (1)
UPGRADE	ZERO / MINS/HOURS

BRONZE

(1) RPO can be seconds with Autonomous Recovery Service (ZRCV)

Protection from Recoverable Failures

Underlying Technologies

RAC

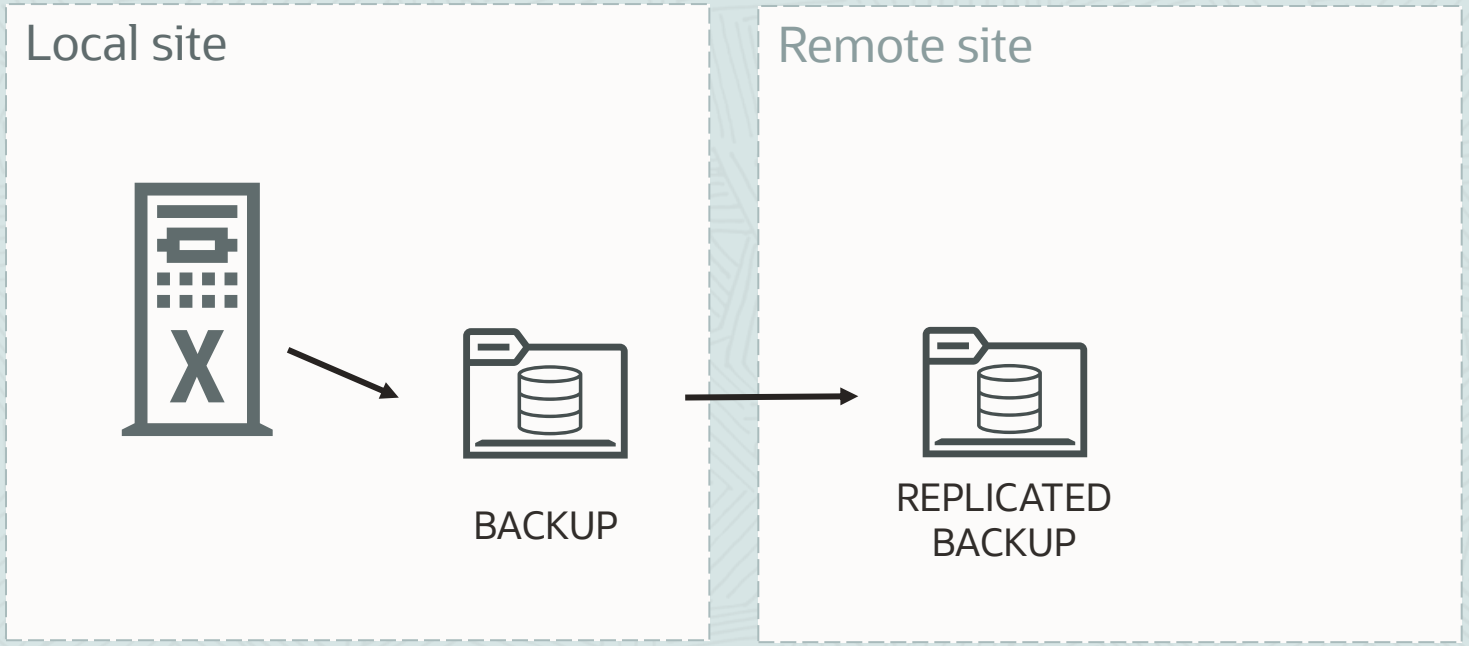
- Node failure protection
- Zero downtime software maintenance
- Elastic changes (CPU, mem, storage) with no downtime

APP CONTINUITY

- (Almost) Transparent unplanned maintenance

ENGINEERED SYSTEMS

- Exadata scalability, performance and availability
- Exadata agility with changing number of VMs, storage, compute resources
- Data protection and Exadata QoS for DB operations



Silver Outage Matrix

PLANNED MAINTENANCE	ZERO	ZERO
RECOVERABLE FAILURE	ZERO	SECONDS
UNRECOVERABLE FAILURE	LAST BACKUP	HOURS (1)
UPGRADE	ZERO	MINS/HOURS

SILVER

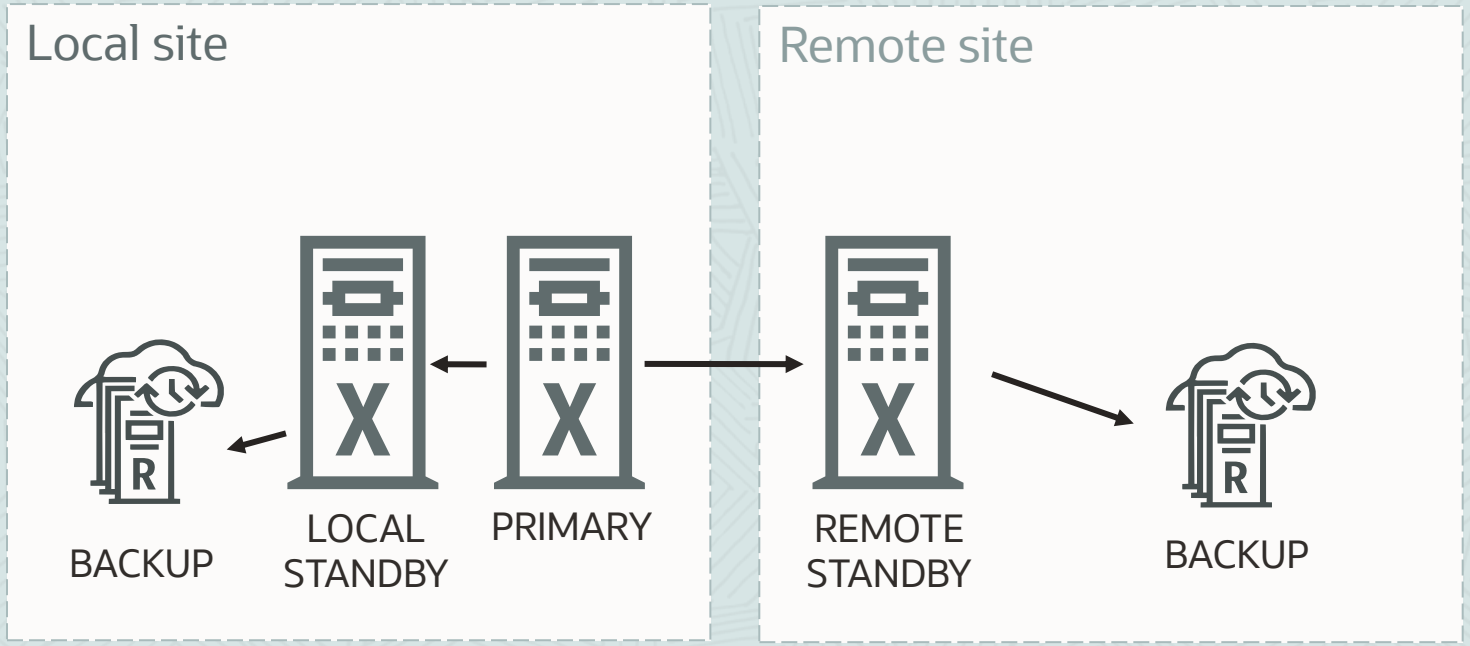
(1) RPO can be seconds with Autonomous Recovery Service (ZRCV)

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



Gold Outage Matrix

PLANNED MAINTENANCE	ZERO ZERO
RECOVERABLE FAILURE	ZERO SECONDS
UNRECOVERABLE FAILURE	ZERO SECONDS
UPGRADE	ZERO SECONDS

GOLD

Highest Availability

Underlying Technologies

GOLDENGATE

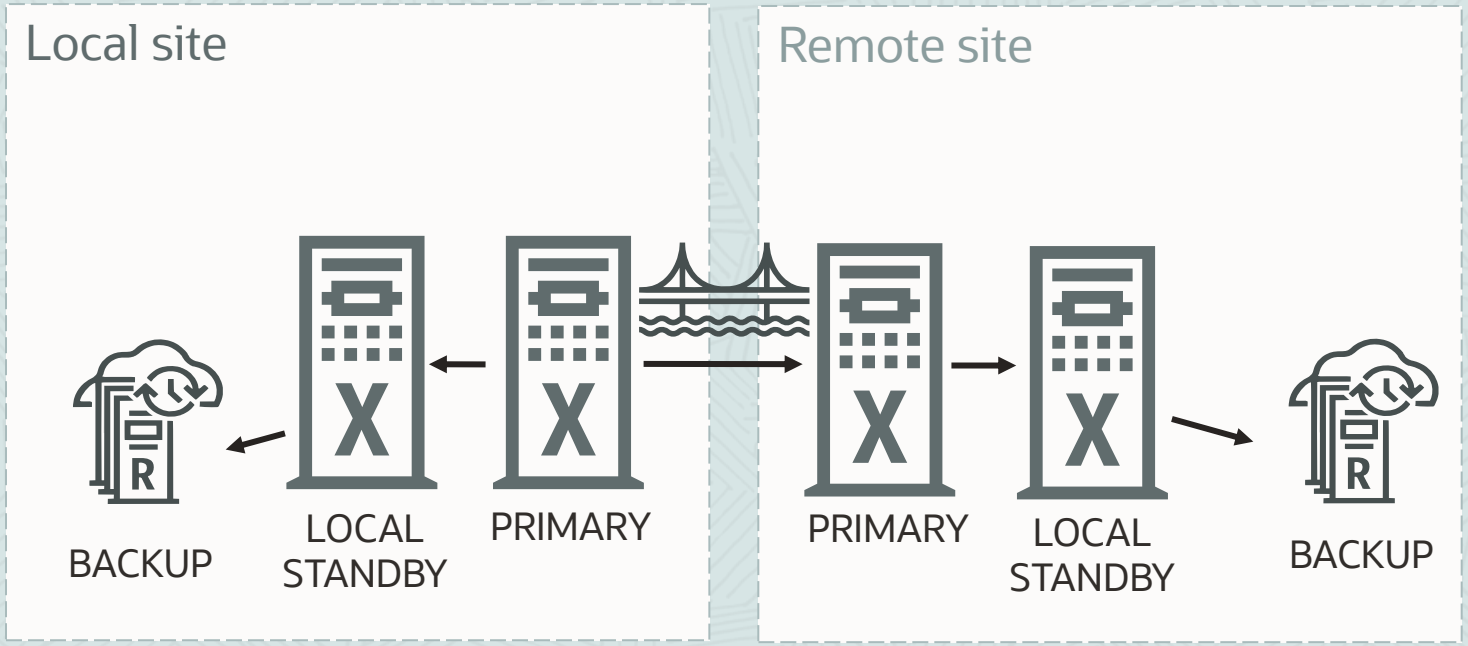
- Active/Active
- Always online
- Online database upgrades
- Site switch with zero database downtime
- Read-write scale-out
- The application must be aware of the replica(s)

EDITION-BASED REDEFINITION

- Online application upgrades

SHARDING

- Distributed
- Best scale-out



Platinum Outage Matrix

	PLANNED MAINTENANCE	ZERO	ZERO
	RECOVERABLE FAILURE	ZERO	ZERO
	UNRECOVERABLE FAILURE	ZERO	ZERO
	UPGRADE	ZERO	ZERO

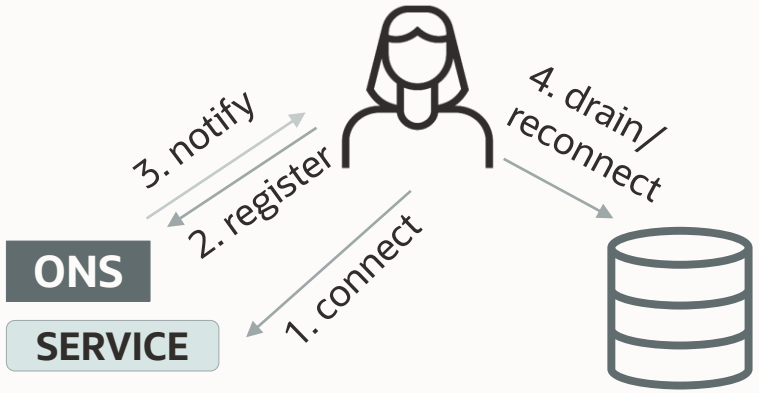
PLATINUM

Client-side Required Technologies

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

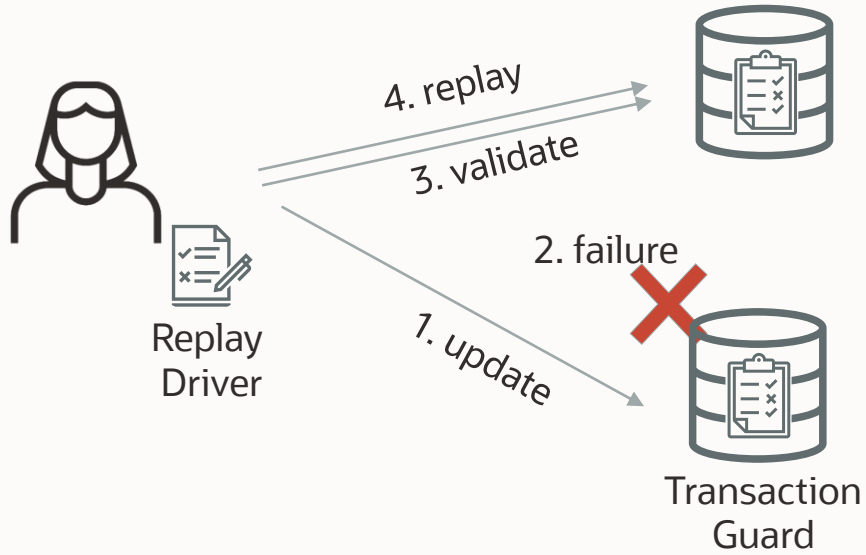
PLANNED MAINTENANCE

Fast Application Notification
(Session Draining)



UNEXPECTED FAILURES

Transparent Application Continuity [1]
(Transaction Replay)



Level 1: Use Services, Connect String, Level 2: FAN, Level 3: TAC Configuring Continuous Availability for Applications (oracle.com)

MAA Validated Solutions

MAA Tier	BaseDB VM	ExaDB-D	ExaDB-C@C	ADB-S	ADB-D
	Base DB – Single Instance	NA	NA	NA	NA
	Base DB – Two RAC Node	ExaDB-D (Default)	ExaDB-CC (Default)	ADB-S (Default)	ADB-D (Default)
	Base DB – Two RAC Node w/ADG	ExaDB-D w/(A)DG	ExaDB-CC w/(A)DG	ADB-S w/AuDG (Cross-AD only)	ADB-D w/AuDG
	Base DB – Two RAC Node w/ADG & OGG	ExaDB-D w/ADG & OGG	ExaDB-CC w/ADG & OGG	Planned	Manual OGG deployment

Oracle Cloud Infrastructure Topology

Maximum Availability Architecture

MAA Best Practices

MAA Validations and Recommendations Everywhere

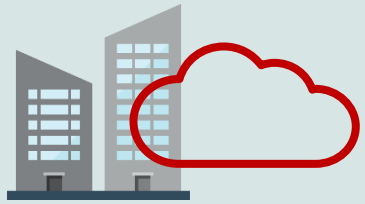
On-premises

[MAA Best Practices - Oracle Database]

Oracle Cloud

[MAA Best Practices for the Oracle Cloud]

Hybrid Cloud



[Hybrid Cloud and Multicloud Best Practices]

Multicloud

[MAA Best Practices for Oracle Database@Azure]

MAA Best Practices for Oracle Database@Google Cloud

Oracle Cloud Infrastructure global footprint

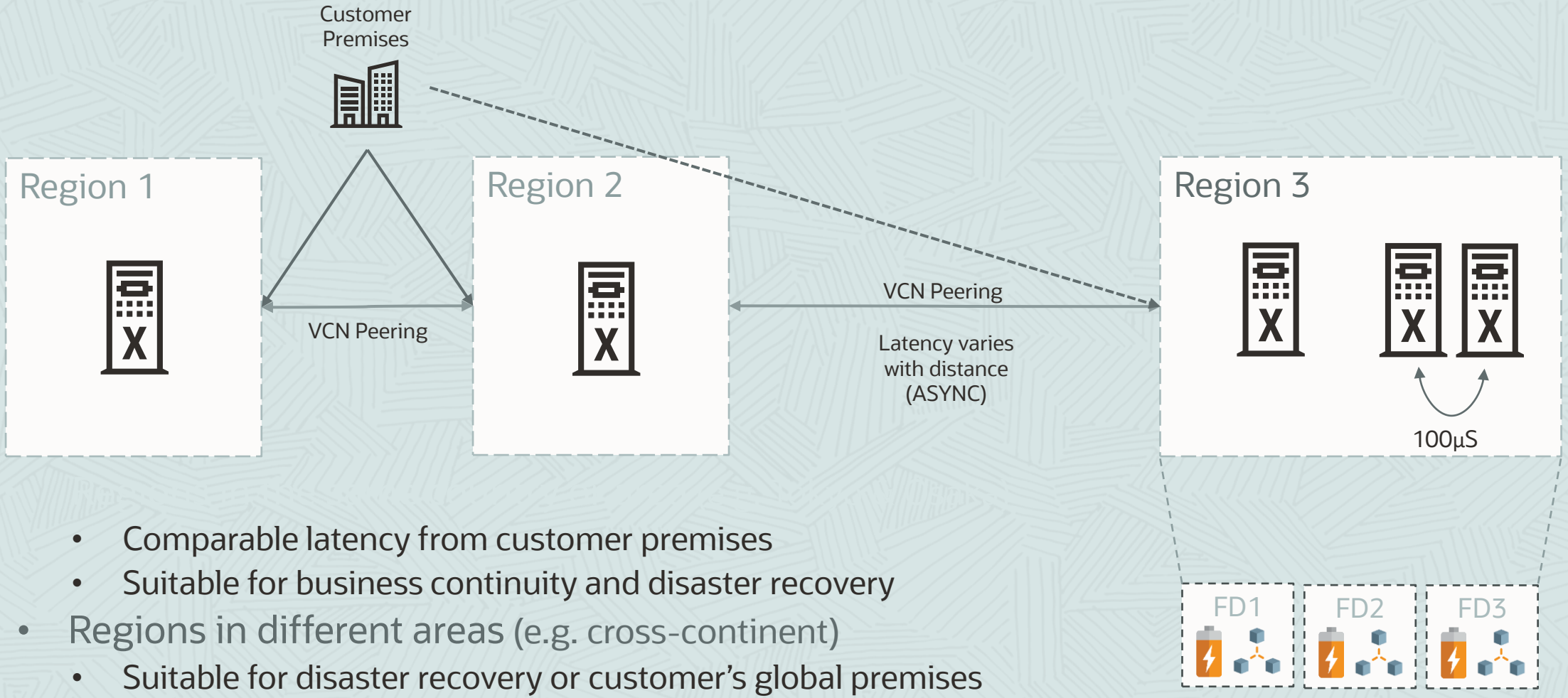
October 2024 – 165 live or planned regions[1]

100% renewable energy by 2025

	Available	Planned
Commercial	41	9
Government	8	
EU Sovereign	2	
Dedicated Region	16 D	D 15
Oracle Alloy	3 A	A 15
Oracle Database@Azure	7	24
Oracle Database@Google Cloud	4	14

[1] Not all regions listed on map

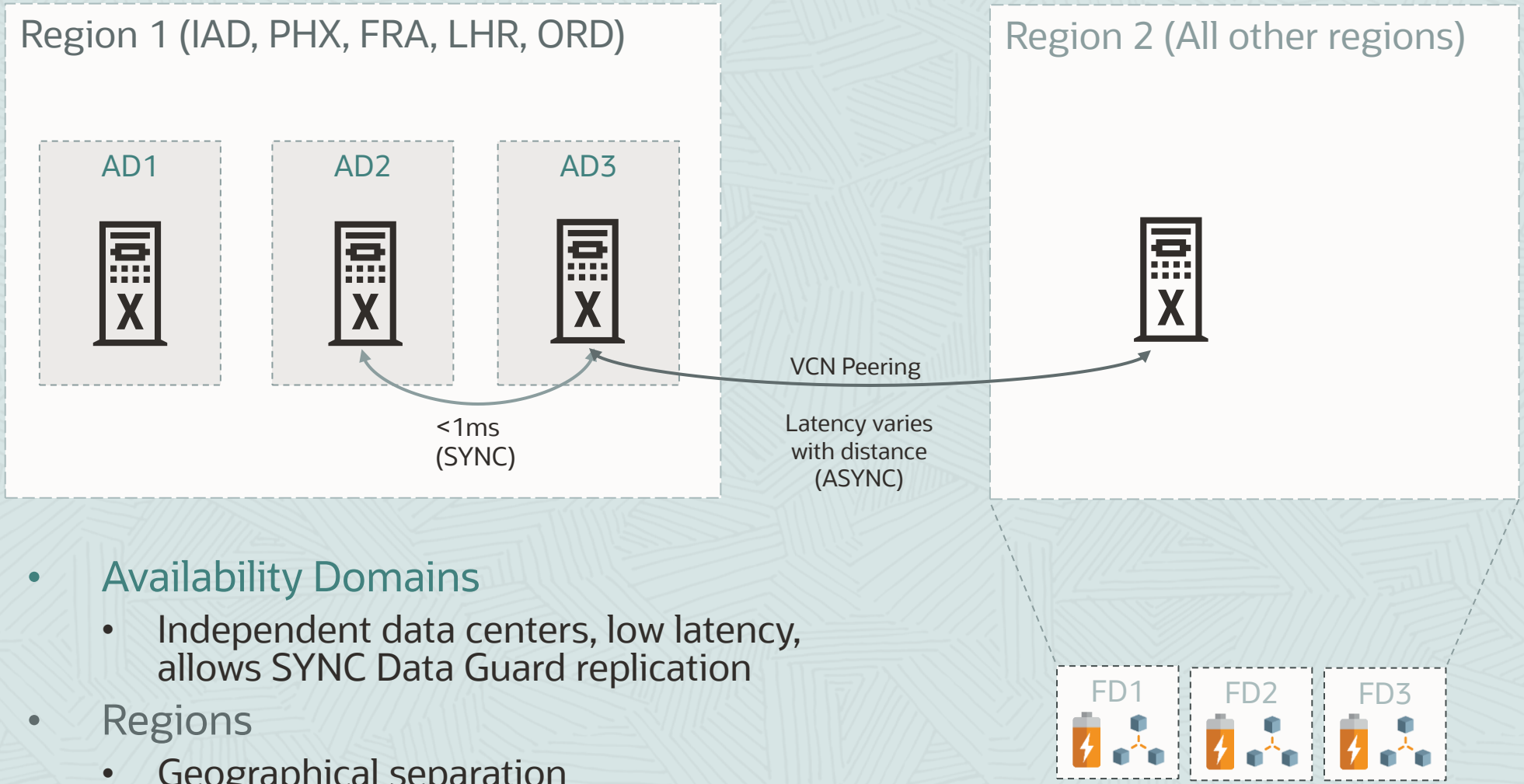
Oracle Cloud Infrastructure topology



- 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, London and Chicago



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

Oracle Cloud Infrastructure Dedicated Region

Data sovereignty

Regulation, and data privacy requirements

Sensitive/IP data can't leave premises

Security and control

Physical security of infrastructure and data

Single tenant, self-contained environment

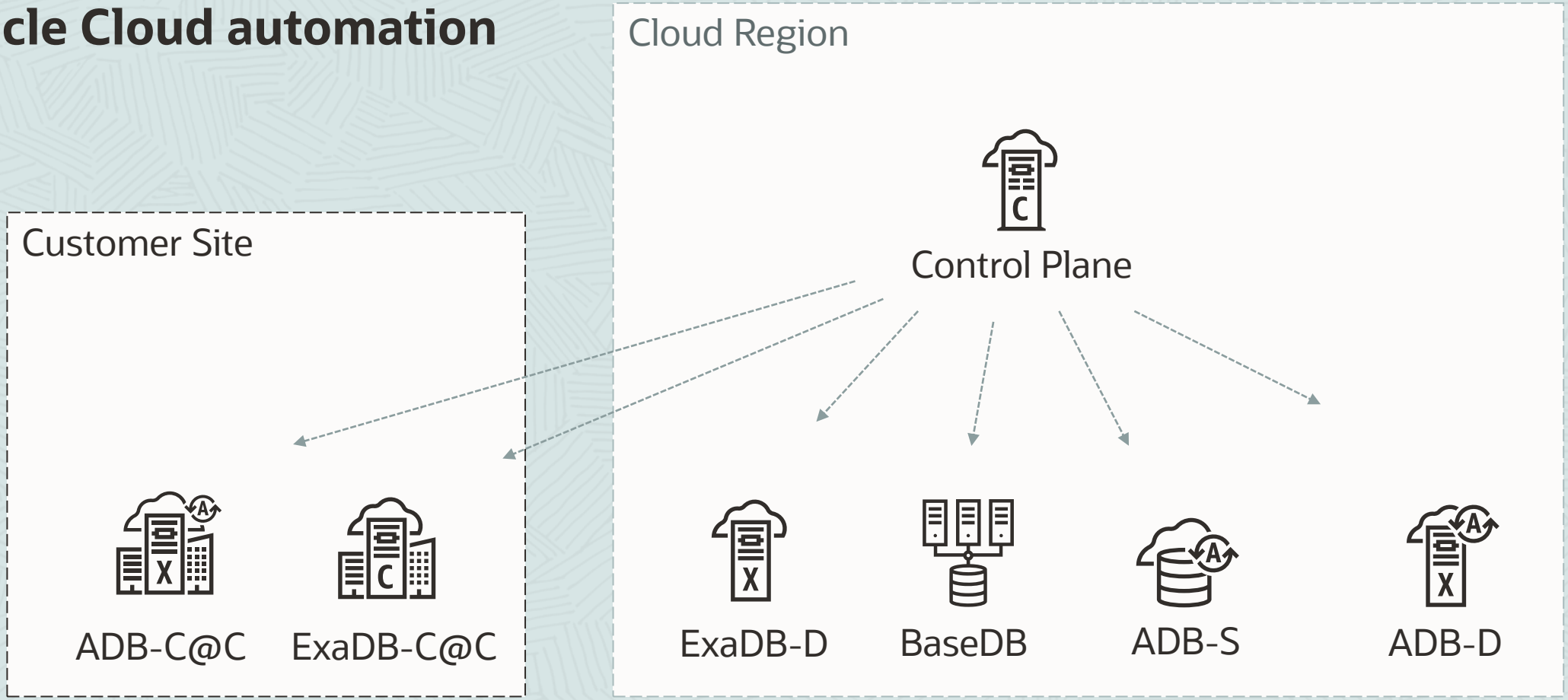
Latency

Stringent latency requirements for high volume applications

Legacy applications tied to on-premises operational systems

Same Architecture
Same Billings
Same Operations
Same Security
Same Cloud Services
Same SLAs

Oracle Cloud automation



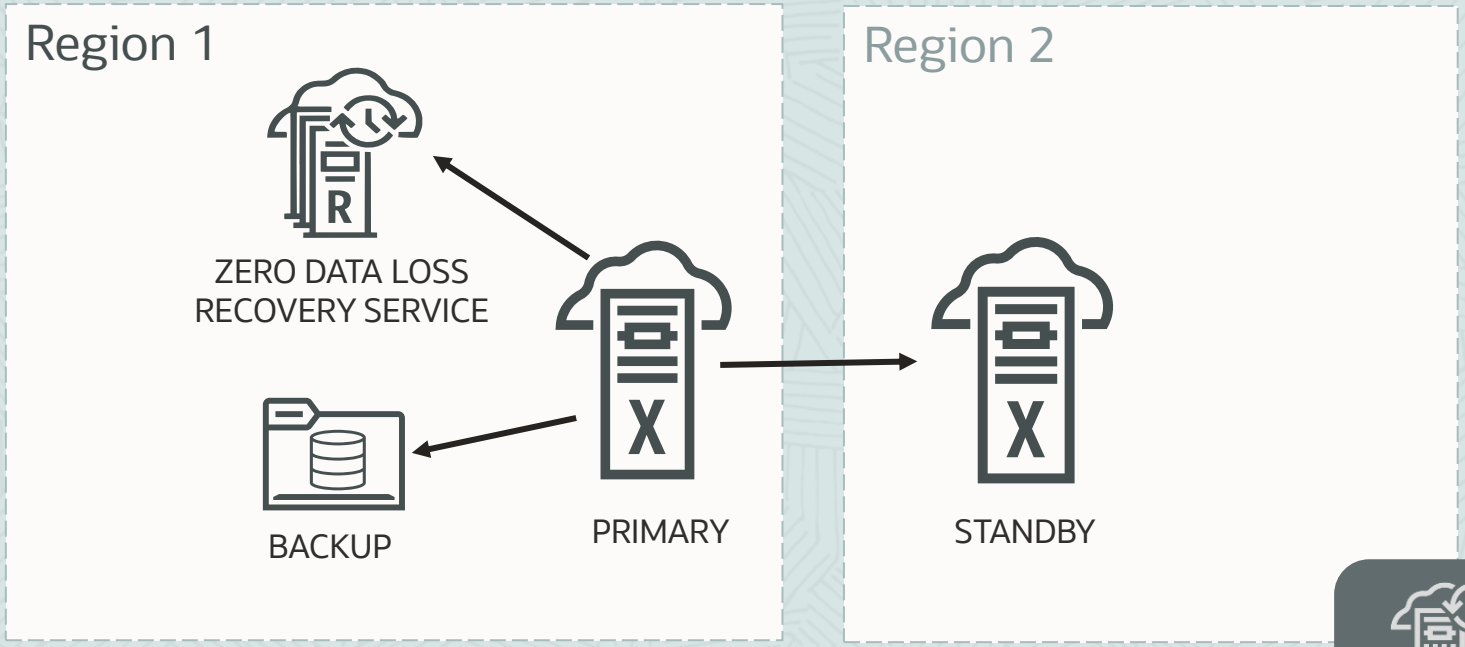
- Cloud automation can be either:
  - 100% managed by the service
  - Achieved with the OCI Tooling, through the Control Plane:
    OCI User Interface, OCI Rest API, SDK, OCI CLI, Terraform OCI Provider, etc.

Oracle Exadata Database Service on Dedicated Infrastructure (ExaDB-D)

Maximum Availability Architecture

Exadata Database Service: protection out of the box

AVAILABILITY / AUTOMATION *	
ZRCV	Recovery Service (default) or via automated OCI backups or Dbaascli
RAC	Exadata inherent HA, QoS, and Performance benefits plus *Exadata Fleet Update* for gold image patching
ACTIVE DATA GUARD	Via console or DBaaS API (Single Standby to ExaDB-D, cross-region possible, DBMS_ROLLING with cloud API)
GOLDENGATE	Manual (Capture & Delivery)
MAA LEVEL	SILVER Out of the Box / GOLD + Data Guard



EXADATA FLEET UPDATE

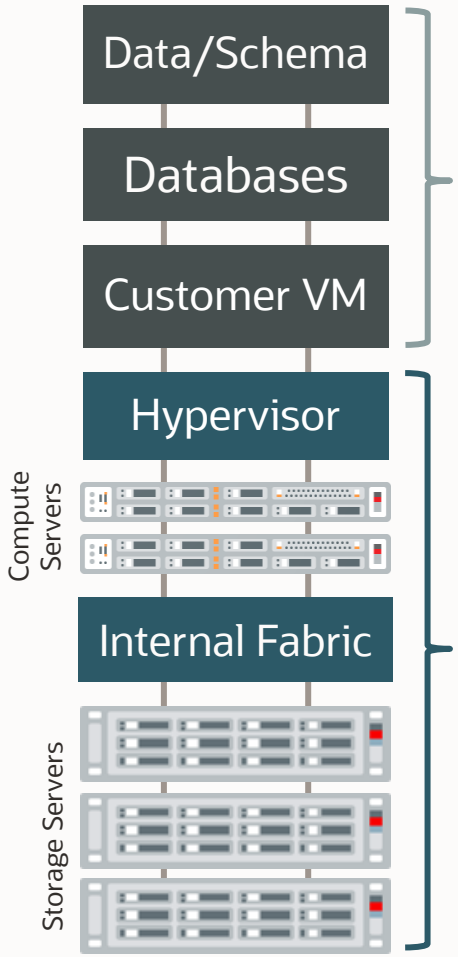
Outage Matrix

PLANNED MAINTENANCE	ZERO	ZERO
RECOVERABLE FAILURE	ZERO	SECONDS
UNRECOVERABLE FAILURE	SECONDS	MINUTES (1)
UPGRADE	ZERO	SECONDS

(1) No FSFO, based on time after custo

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

Exadata Database Service: 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 Database Service: Oracle Managed Backups

1-click configuration automatic simple backup (default/recommended)

SCHEDULING	• Done by control plane. Ability to change backup time for full and incremental backups, and the day for full backups • Automatic archivelog backup every 30 minutes, the frequency can be changed via dbaascli
DESTINATION	• Default is Database Autonomous Recovery Service with optional real time redo transport for near zero RPO • ExaDB-D managed backup storage, no direct control by the customer • Long term backup retention is available with alternative managed backup service: Object Storage Service (OSS)
REPLICAS	• Back-ups are highly redundant and can survive a complete storage outage
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
RESTORE	• Restore CDB and PDB capabilities. • Restore on the same host or different host within the same or cross region. • Restore the database using the same or different ORACLE_HOME, via control plane
FAILOVER	• Backup runs independently and can tolerate node or storage failures
STANDBY	• Backup and restore from the standby are possible using the object storage as destination

ZRCV

Exadata Database Service: User Configured Backups

RMAN backup via dbaascli

SCHEDULING	• No Control Plane (Cloud Console) backup scheduling • Scheduled by customer provided scheduler (DTRS) • Automatic archivelog backup every 30 minutes by default • Ability to change default backup time and L0 backup day
DESTINATION	• Customer-created bucket (fully controlled by the customer, including replication) • Autonomous Recovery Service is an option as well • No support for archive storage
REPLICAS	• Option to set up cross-region 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
FAILOVER	• Backup runs independently and can tolerate node or storage failures
STANDBY	• Backup and restore from the standby are possible using the object storage as destination

Not recommended

Exadata Database Service: manual RMAN backups

Direct RMAN backup with customer downloaded and configured backup module

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	• Restore CDB and PDB capabilities. From anywhere the backups are accessible (across ADs, across regions, on-premises)
FAILOVER	• Customer must configure where the backup executes
STANDBY	• Possible to backup standby databases or offload backups to the standby

Not recommended and incompatible with Oracle Managed and User Configured backup options.

Exadata Database Service: RMAN Best Practices

Use Control Plane Oracle Managed backups with OSS, ZRCV, or NFS (C@C) – highly recommended

- Use Database Autonomous Recovery Service (ZRCV)
  - DB19.16/21.7 without real-time transport or DB19.18/21.8 with real-time transport
- Ensure recovery window (backup retention period) settings meet SLAs
- If using OSS, the ability to offload backup to standby
- Increase RMAN parallelism for higher performance via dbaascli, trading off higher CPU processing

User-configured backup options via dbaascli - not recommended

- Use only when customer-created buckets or when backup replication is required
- Refer to Disaster Recovery Using Cross-Region Backups

Use manual RMAN backup solution for these exceptions - incompatible

- Not compatible with the above options, so no cloud automation
- Not cloud-supported

Exadata Database Service: Real Application Clusters

- Out-of-place update is built-in with control plane move command
- Software update orchestrates drain, service relocation and instance restart
  - For application drain attributes, refer to Achieving Continuous Availability For Your Applications https://docs.oracle.com/en/database/oracle/oracle-database/21/haovw/oracle-maximum-availability-architecture-exadata-cloud-database-systems.html#GUID-E9DF9482-A414-45E0-A5F4-29F6056E364F
- RAC uses 192.168.128.0/20 on IB and 100.64.0.0/10 on RoCE for interconnect
- Additional virtual IP addresses can be added via the Cloud console
  - Clusterware VIP still needs to be added manually via either srvctl, crsctl, or appvipcfg
- Change of SCAN listener port possible during VM creation (range 1024-8999)
- Changing local listener port is not supported, but additional ports can be added

Exadata Database Service: RAC best practices

- Create databases only through cloud control plane or dbaascli 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 Achieving Continuous Availability For Your Applications
  https://docs.oracle.com/en/database/oracle/oracle-database/21/haovw/oracle-maximum-availability-architecture-exadata-cloud-database-systems.html#GUID-E9DF9482-A414-45E0-A5F4-29F6056E364F
- Run exachk monthly and address alerts
- For “Single Instance”, consider PDB singletons or use a single VM cluster node
- Adjust hugepages as you add or resize databases (set `use_large_pages=ONLY`)
- Avoid DB and system customizations

Exadata Database Service: Multitenant via Control Plane

MULTITENANT

SETUP	• PDB creation or deletion from the cloud console • List PDBs by database • Retrieve PDB connection strings
CLONING	• Create clones or refreshable clones within the same CDB or across CDBs • Data Guard supported for PDB cloning operations
PROTECTION	• PDB creation synced to Data Guard Standby • PDB backup/restore from same CDB. PDB restore to another CDB for BaseDB and ExaDB-D (C@C later)
ADMINISTRATION	• Start and Stop the PDBs from the console on Primary or Standby (ADG)
CONTROL PLANE SYNC	• The PDBs created or dropped out-of-band via dbaascli or SQL are synched periodically

Exadata Database Service: Multitenant Best Practices

MULTITENANT

- Create pluggable databases only through cloud control plane or cloud APIs
  - MAA best practices incorporated
  - PDBs created via cloud APIs/SQL will sync with control plane shortly after creation completes
  - PDBs created with deferred recovery will not appear in the console on the standby
- For Data Guard-enabled CDBs, add temporary files to the standby PDB when creating new PDBs
- Do not use PDB save state or triggers to manage services or PDB startup. It may lead to service downtime during Data Guard role transitions.
- Manual PDB switchover and failover functionality in 19c:
  - PDB Switchover and Failover in a Multitenant Configuration (oracle.com)

Exadata Database Service: Data Guard via Control Plane

ACTIVE DATA GUARD

SETUP	• 1-click setup from control plane • Uses Data Guard broker and MAA best practices • Uses optimized Data Guard instantiation with retries and resume capabilities
TOPOLOGY	• Supports Data Guard in same rack for testing, same region, across ADs or across regions • Supports ExaDB-D to ExaDB-D or BaseDB to BaseDB or ExaDB-C@C to ExaDB-C@C
PROTECTION	• Asynchronous configuration by default (protection level MAX PERFORMANCE) • Synchronous configuration (protection level MAX AVAILABILITY) • OCI Vault, File-based TDE wallet, or Oracle key vault managed keys are supported. Data Guard fast-start failover (FSFO) and Far Sync require manual setup • Multiple standby is manual setup
ROLE CHANGES	• Supports failover and switchover operations • Out-of-band role transition is not recommended except for FSFO or multiple standby. DB role status will be resynchronized in minutes
OPEN MODE	• Choose Active Data Guard (open read-only) for additional data protection and read-only benefits. Alternatively, choose Data Guard (mounted standby); Snapshot Standby requires manual command
PATCHING & UPGRADE	• Control plane patching and offline database upgrade is available. Standby-first patching is available • Exadata Cloud Database 19c Rolling Upgrade With DBMS_ROLLING (Doc ID 2832235.1)

Exadata Database Service: 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 best 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. Redo Apply must be stopped manually. • Customers can manually use standby-first update strategy and DBMS_ROLLING for rolling upgrades

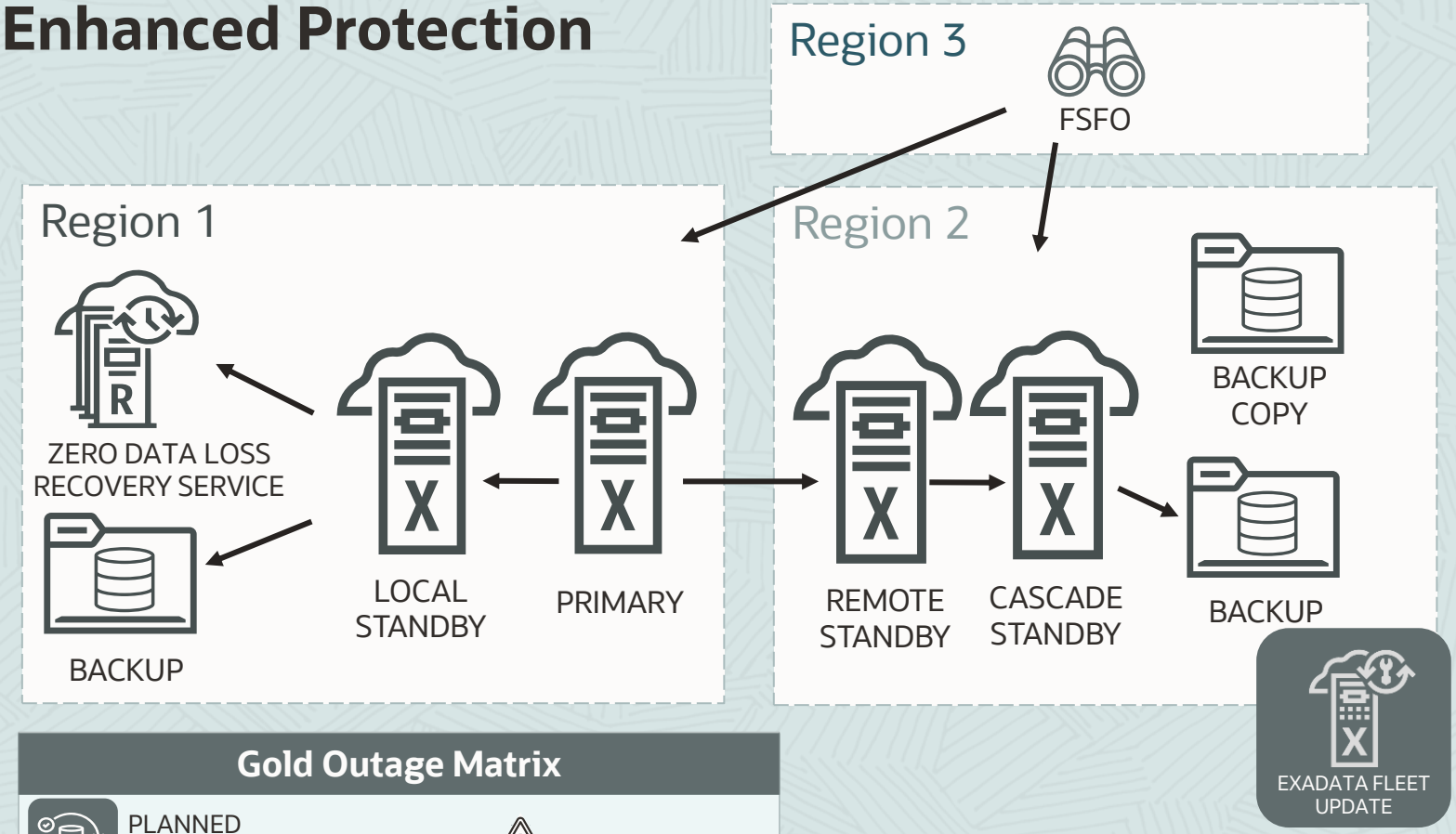
Not recommended unless for multiple standby or hybrid Data Guard use cases

Exadata Database Service: Data Guard Best Practices

- 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 a Data Guard association through the 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 best practices incorporated
  - Keep the primary and standby Oracle Home software the same as much as possible
  - Periodically test and validate end-to-end DR
  - Issue DG Broker VALIDATE commands at least monthly

Exadata Database Service: Enhanced Protection

AVAILABILITY / AUTOMATION *	
RMAN	Multiple backup copies Backup from the standby
RAC	Exadata inherent HA, QoS, and Performance benefits plus *Exadata Fleet Update* for gold image patching
ACTIVE DATA GUARD	Multiple standbys Fast-start failover
GOLDENGATE	MAA GoldenGate Hub (capture & delivery) Global Data Service
MAA LEVEL	SILVER ExaDB-D GOLD + Data Guard PLATINUM + GoldenGate



Gold Outage Matrix

PLANNED MAINTENANCE	ZERO	ZERO
RECOVERABLE FAILURE	ZERO	SECONDS
UNRECOVERABLE FAILURE	ZERO	SECONDS
UPGRADE	ZERO	SECONDS

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

Exadata Database Service: Read more

- Oracle Maximum Availability Architecture in Exadata Cloud Database Systems
  - Oracle Maximum Availability Architecture Benefits
  - Expected Impact with Unplanned Outages
  - Expected Impact with Planned Maintenance
  - Achieving Continuous Availability For Your Applications
  - Oracle Maximum Availability Architecture Reference Architectures in the Exadata Cloud https://docs.oracle.com/en/database/oracle/oracle-database/19/haovw/oracle-maximum-availability-architecture-oracle-exadata-cloud-systems.html
- ExaDB-D 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
- GoldenGate and Platinum MAA for Cloud
- MAA Platinum and Oracle GoldenGate Best Practices

Exadata Database Service: Read more

•(ODyS) Oracle Dynamic Scaling engine - Scale-up and Scale-down automation utility for OCI DB System (ExaCS/ExaC@C) (Doc ID 2719916.1)
https://support.oracle.com/epmos/faces/DocumentDisplay?id=2719916.1

• How to configure OCI-CLI with Instance/Resource Principals (Doc ID 2763990.1)
https://support.oracle.com/epmos/faces/DocumentDisplay?id=2763990.1

•Use Oracle Data Guard with Exadata Cloud Infrastructure
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 Database Service or Gen 2 Exadata Database Service Cloud@Customer)
https://docs.oracle.com/en/database/oracle/oracle-database/19/haovw/oracle-data-guard-hybrid-cloud-configuration1.html

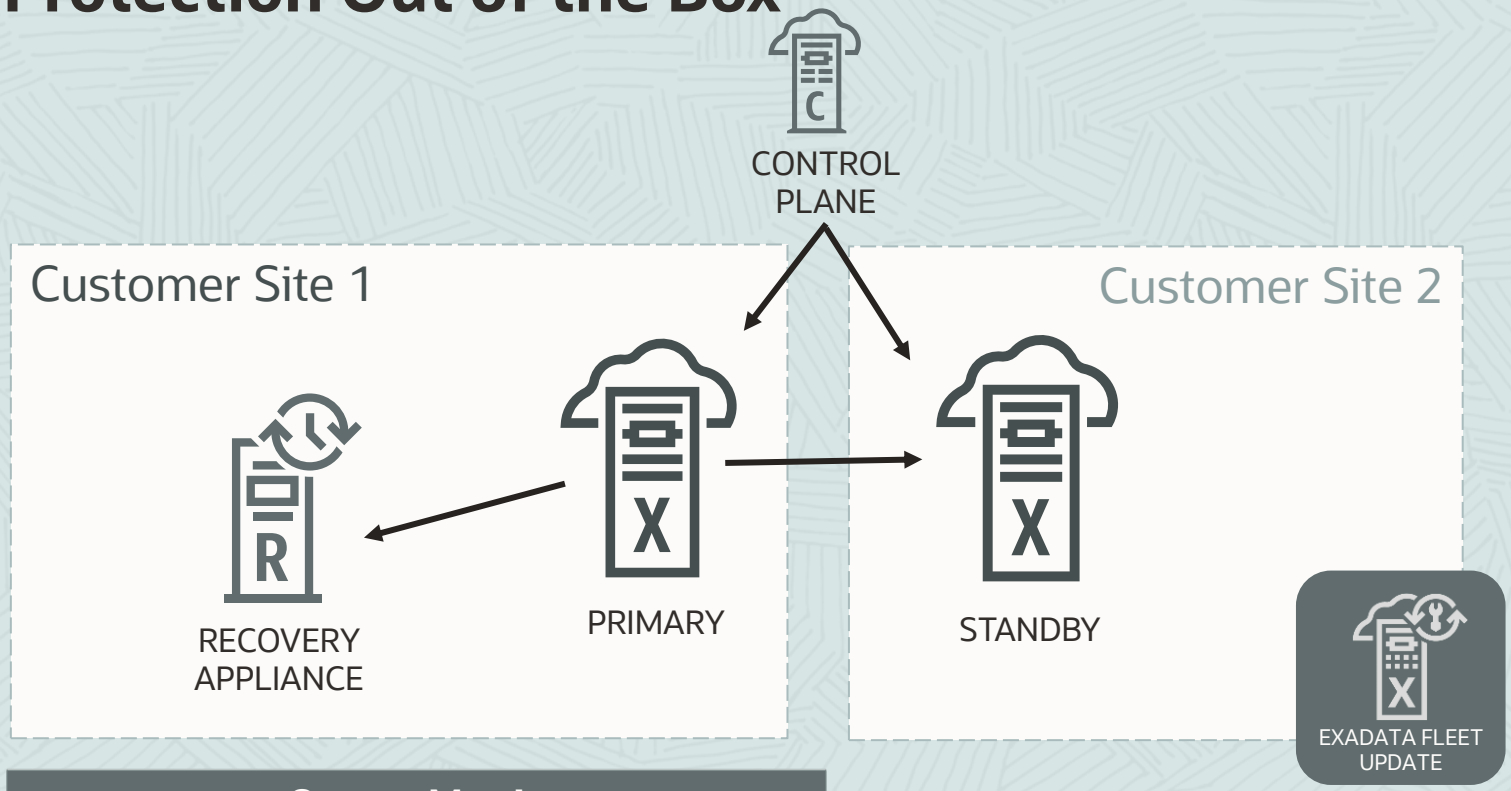
•(OCI) mv2bucket - Oracle Managed Bucket Content Manager (Doc ID 2723911.1)
https://support.oracle.com/epmos/faces/DocumentDisplay?id=2723911.1

Oracle Exadata Database Service on Cloud@Customer (ExaDB-C@C)

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 plus *Exadata Fleet Update* for gold image patching
ACTIVE DATA GUARD	Via console or DBaaS API (single standby, DBMS_ROLLING with cloud APIs only)
GOLDENGATE	Manual (Capture & Delivery)
MAA LEVEL	SILVER Out of the Box / GOLD + Data Guard



Outage Matrix

PLANNED MAINTENANCE	ZERO	ZERO
RECOVERABLE FAILURE	ZERO	SECONDS
UNRECOVERABLE FAILURE [1]	SECONDS	MINUTES (1)
UPGRADE	ZERO	SECONDS

(1) RPO can be seconds with ZDLRA

(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: Oracle Managed Backup

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 Oracle-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 • Restore PDB capabilities via dbaascli commands
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

Direct RMAN backup with customer configured backup module

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	• Restore CDB and PDB capabilities. From anywhere the backups are accessible (across ADs, across regions, on-premises)
FAILOVER	• Customer must configure where the backup executes
STANDBY	• Possible to backup standby databases

Not recommended and incompatible to Oracle Managed backup.

Exadata Cloud@Customer: RMAN best practices

- Use control plane automatic backup for database backup/restore in ExaDB-C@C
- Use ZDLRA for lowest RPO, incremental forever and additional backup/restore benefits
- If NFS is used as 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. Standalone backups for longer retention
  - 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

- Create databases only through cloud control plane or dbaascli 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: Achieving Continuous Availability For Your Applications https://docs.oracle.com/en/database/oracle/oracle-database/21/haovw/oracle-maximum-availability-architecture-exadata-cloud-database-systems.html#GUID-E9DF9482-A414-45E0-A5F4-29F6056E364F
- Avoid DB and system customizations
- Run exachk monthly and address alerts
- Adjust hugepages as you add or resize databases (set use_large_pages=ONLY)
- Change of SCAN listener port possible during creation (range 1024-8999)

Exadata Cloud@Customer: Multitenant via control plane

SETUP	• PDB creation or deletion from the cloud console • List PDBs by database • Retrieve PDB connection strings
CLONING	• Create clones within the same CDB or across CDBs within same AD
PROTECTION	• PDB creation synced to Data Guard Standby • Starting with 19c, PDB relocate and relocate + upgrade
ADMINISTRATION	• Start and Stop the PDBs from the console on Primary or Standby (ADG)
CONTROL PLANE SYNC	• The PDBs created or dropped out-of-band via dbaascli or SQL are synched periodically

Exadata Cloud@Customer: Multitenant best practices

- Create pluggable databases only through cloud control plane or cloud APIs to include configuration best practices
  - PDBs created via cloud APIs/SQL will sync with the control plane shortly after creation completes
  - PDBs created with deferred recovery will not appear in the console on the standby
- Always use either the connection strings provided by the console or custom application services to connect to a PDB
- For Data Guard-enabled CDBs, add temporary files to the standby PDB when creating new PDBs
- Perform per PDB backup/restore via dbaascli utility
  Exadata Cloud Service: Pluggable Database Backup and Restore (Doc ID 2809448.1)

Exadata Cloud@Customer: Data Guard via control plane

ACTIVE DATA GUARD

SETUP	• 1-click setup from control plane • Uses Data Guard broker and MAA best practices • Uses optimized Data Guard instantiation
TOPOLOGY	• Supports Data Guard in the same rack for testing, same region, across ADs or across regions • Supports ExaDB-C@C to ExaDB-C@C
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 except for FSFO or multiple standby. DB role status will be resynchronized in minutes
OPEN MODE	• Choose Active Data Guard (open read-only) for additional data protection and read-only benefits. Alternatively choose Data Guard (mounted standby)
PATCHING & UPGRADE	• Control plane patching and offline database upgrade is available • Exadata Cloud Database 19c Rolling Upgrade With DBMS_ROLLING (Doc ID 2832235.1)

Exadata Cloud@Customer: manual Data Guard setup

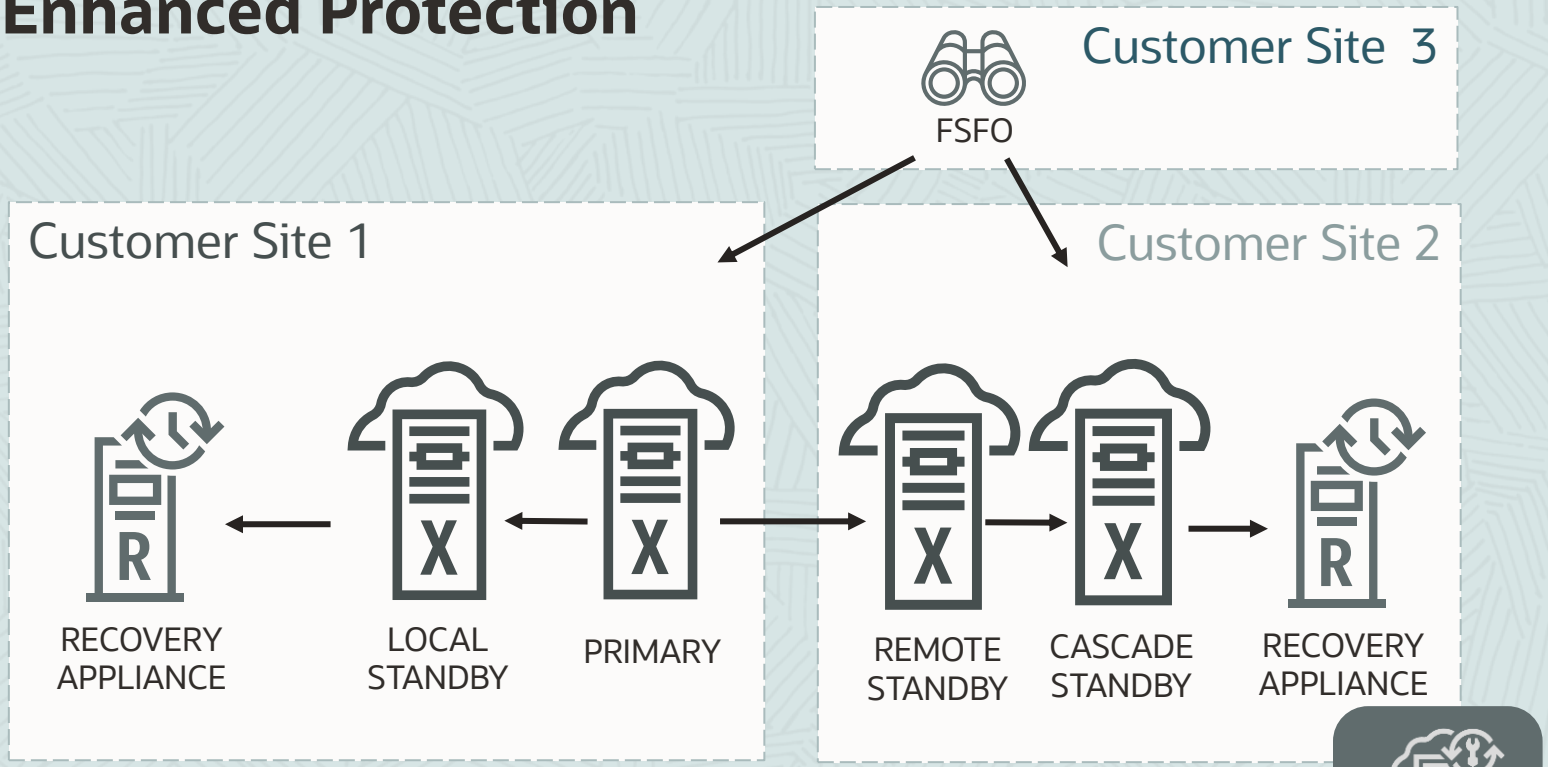
ACTIVE DATA GUARD

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 • 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 best 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. Redo Apply must be stopped manually. • Customers can manually use standby-first update strategy and DBMS_ROLLING for rolling upgrades

Not recommended unless for multiple standby or hybrid Data Guard use cases

Exadata Cloud@Customer: Enhanced Protection

AVAILABILITY / AUTOMATION *	
RMAN	Backup from the primary or/and standby. Offload backups to the standby.
RAC	Exadata inherent HA, QoS, and Performance benefits plus *Exadata Fleet Update* for gold image patching
ACTIVE DATA GUARD	Multiple standbys Fast-start failover
GOLDENGATE	Manual (capture & delivery) Global Data Service
MAA LEVEL	SILVER — ExaDB-C@C GOLD — + Data Guard PLATINUM — + GoldenGate



EXADATA FLEET UPDATE

Gold Outage Matrix

PLANNED MAINTENANCE	ZERO	ZERO
RECOVERABLE FAILURE	ZERO	SECONDS
UNRECOVERABLE FAILURE	ZERO	SECONDS
UPGRADE	ZERO	SECONDS

*
- 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 Cloud Database Systems
  - https://docs.oracle.com/en/database/oracle/oracle-database/19/haovw/oracle-maximum-availability-architecture-oracle-exadata-cloud-systems.html
- Using Oracle Data Guard with Exadata Cloud at Customer
  - https://docs.oracle.com/en-us/iaas/exadata/doc/eccusingdataguard.html
- GoldenGate and Platinum MAA for Cloud
  - MAA Platinum and Oracle GoldenGate Best Practices
- Guidelines When Using ZFS Storage in an Exadata Environment (2087231.1)
  - https://support.oracle.com/epmos/faces/DocumentDisplay?id=2087231.1
- Migration of file-based TDE to OKV for Exadata Database Service on Cloud at Customer Gen2 (Doc ID 2823650.1)
  - https://support.oracle.com/epmos/faces/DocumentDisplay?id=2823650.1

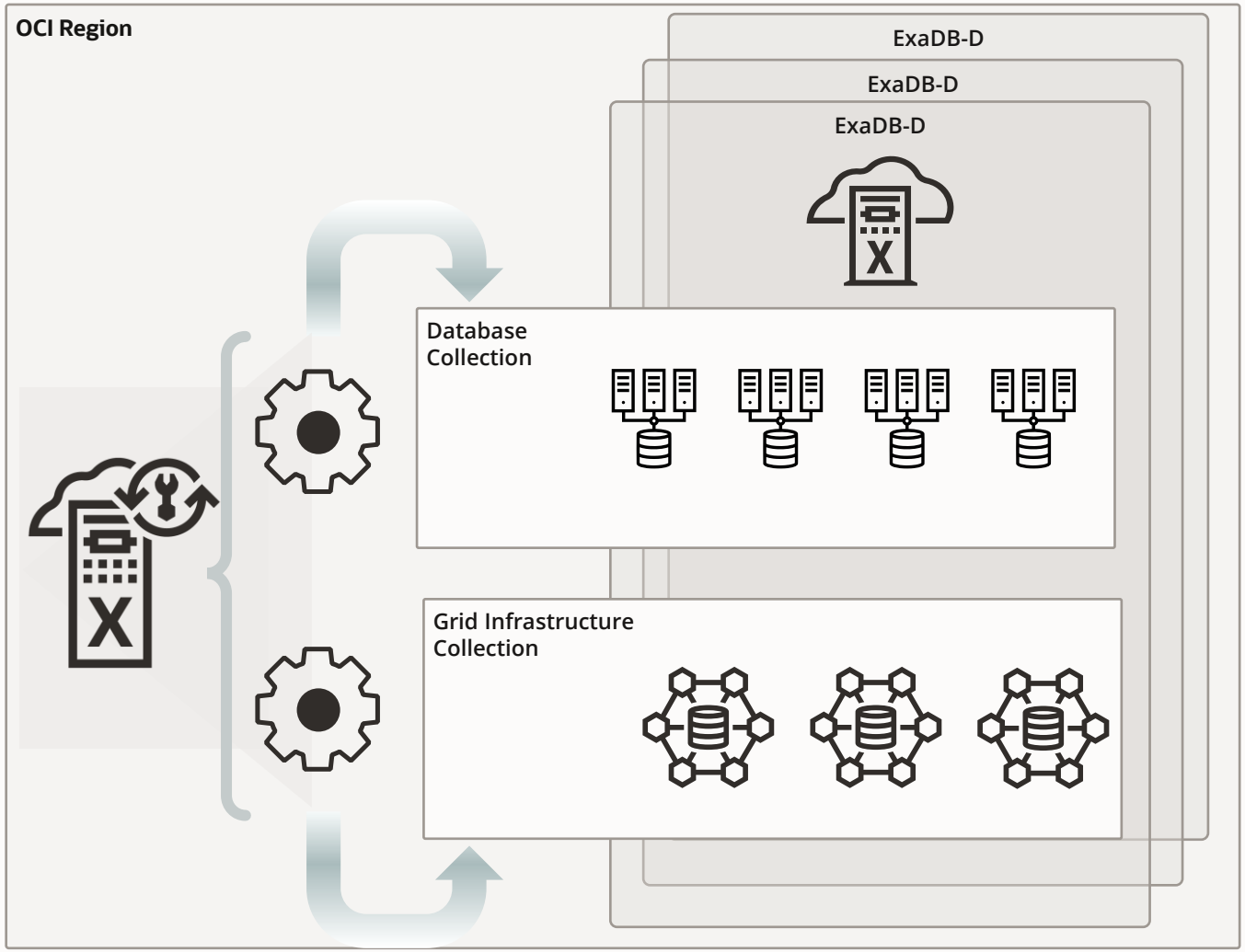
Exadata Fleet Update

Maximum Availability Architecture

Exadata Fleet Update

Streamlines Database and Grid Infrastructure updates for large-scale deployments

- Group multiple Oracle Databases and Oracle Grid Infrastructures into collections to allow patching in a single operation and maintenance schedule
- Offers various capabilities such as rolling and non-rolling, session draining, scheduling of pre-check, staging, and patch operations
- Automates fleet-wide patching, gold image standardization, reduces manual intervention
- Reduces patching time and complexity using standard out-of-place patching mechanism and Oracle-provided or customized database software images
- Available for ExaDB-D and ExaDB-C@C deployments



Ref. https://blogs.oracle.com/maa/post/announcing-exadata-fleet-update

Oracle Base Database Service – Virtual Machines (BaseDB)

Maximum Availability Architecture

Base Database Service VM: basic information

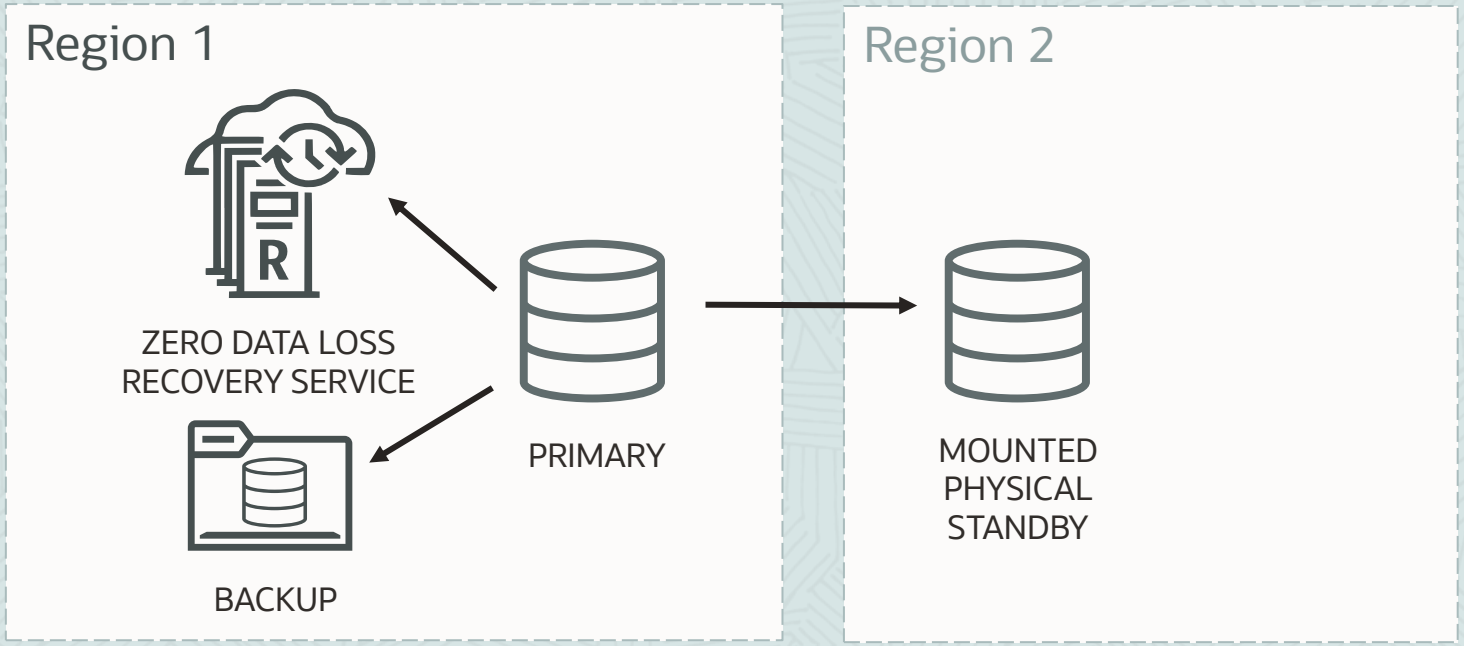
- BaseDB uses standard Intel or AMD Compute with block storage
  - Block storage is triple-mirrored automatically
  - Either on LVM or ASM (Grid Infrastructure)
    - ASM uses external redundancy
- VMs are automatically restarted on failure
- VMs are automatically relocated to a different hypervisor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

Base Database Service 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	✗	✗	✗	✓	✓

Base Database Service VM 1-Node: Protection Out of the Box

AVAILABILITY / AUTOMATION *	
ZRCV	Recovery Service or via 1 copy to 3-way mirrored object storage via automated OCI backups
RAC	It requires 2 nodes EE Extreme Performance
ACTIVE DATA GUARD	Via console or DBaaS API (one standby to BaseDB)
GOLDENGATE	Manual (Capture & Delivery)
MAA LEVEL	BRONZE Out of the Box



Outage Matrix

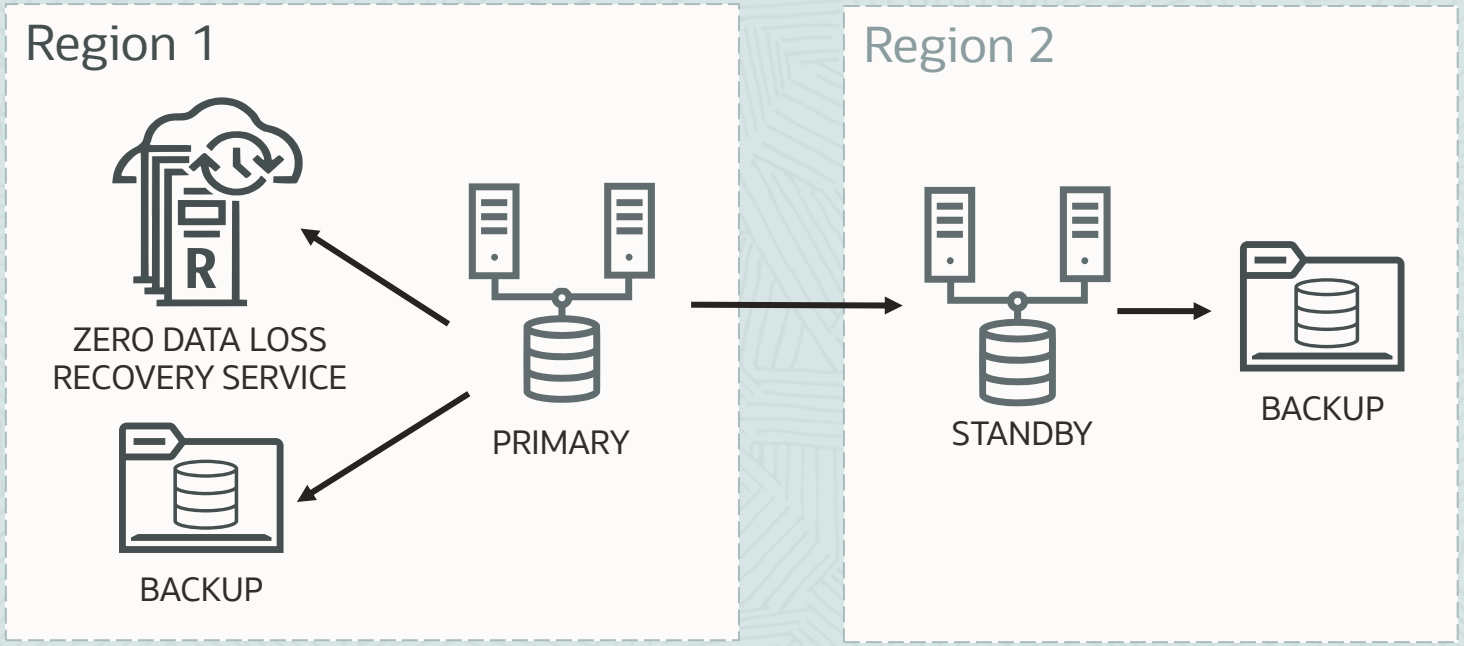
PLANNED MAINTENANCE	ZERO	MINS/HOURS
RECOVERABLE FAILURE[1]	SECONDS	MINUTES
UNRECOVERABLE FAILURE[1]	SECONDS	MINS/HOURS
UPGRADE	ZERO	MINS/HOURS

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

(1) RPO can be seconds with Autonomous Recovery Service (ZRCV)

Base Database Service VM RAC: Protection Out of the Box

AVAILABILITY / AUTOMATION *	
ZRCV	Recovery Service or via 1 copy to 3-way mirrored object storage through automated OCI backups
RAC	It requires 2 nodes EE Extreme Performance
ACTIVE DATA GUARD	Via console or DBaaS API (one standby to BaseDB)
GOLDENGATE	Manual (Capture & Delivery)
MAA LEVEL	SILVER Out of the Box / GOLD + Data Guard



Outage Matrix

PLANNED MAINTENANCE	ZERO	ZERO
RECOVERABLE FAILURE[1]	ZERO	SECONDS
UNRECOVERABLE FAILURE[1]	SECONDS	MINUTES (1)
UPGRADE	ZERO	MINS/HOURS

(1) No FSFO, based on time after customer action

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

(1) RPO can be seconds with Autonomous Recovery Service (ZRCV)

Base Database Service VM: Oracle Managed Backup

1-click configuration automatic RMAN backup

ZRCV

SCHEDULING	• Done by control plane. Ability to change backup time for full and incremental backups, and the day for full backups • Automatic hourly archivelog backup via BaseDB agent
DESTINATION	• Default is Database Autonomous Recovery Service with optional real time redo transport for near zero RPO • Long term backup retention is available with alternative managed backup service: Object Storage Service (OSS)
REPLICAS	• Back-ups are highly redundant and can survive a complete storage outage • No support for archive storage
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	• Restore on same host or different host within same region or across region. • No duplicate on the same host (only 1 CDB supported per DB system)
FAILOVER	• Backup runs independently and can tolerate node or storage failures
STANDBY	• Backup of standby database with Object Storage Service

Base Database Service VM: User Configured Backup

RMAN backup via dbcli

SCHEDULING	• Scheduled by BaseDB 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	• Standby backup is also an option using DBCLI

Base Database Service VM: manual RMAN backups

Direct RMAN backup with customer downloaded and configured backup module

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	• From anywhere the backups are accessible (across ADs, across regions, on-premises)
FAILOVER	• Customer must configure where the backup executes
STANDBY	• Possible to backup standby databases or offload backups to the standby

Not recommended and incompatible to Oracle Managed and User Configured backup options.

Base Database Service VM: RMAN best practices

- Use Control Plane **Oracle Managed** backups with OSS or ZRCV– highly recommended
  - Use Database Autonomous Recovery Service (ZRCV)
    - DB19.16/21.7 without real-time transport or DB19.18/21.8 with real-time transport
- The performance of the RMAN backup is defined by the network.
  - Depending on VM shape (network bandwidth is correlated to the number of CPUs)
- The number of backup channels depends on the VM shape and should be adapted manually
- Additional separated manual backup of TDE wallet recommended
- Backup retention can be set to 7, 15, 30, or 60 days
- Use standalone backups (full) through the control plane for long-term backups with longer retention requirements
  - Automatic backups are deleted by default 72 hours after the instance is terminated
  - Standalone backups will stay until deleted manually

Base Database Service 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

Base Database Service 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 an 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.
- Avoid DB and system customizations

ACTIVE DATA GUARD

Base Database Service VM: Data Guard via control plane

SETUP	• 1-click setup from control plane • Uses Data Guard broker • Only via DUPLICATE FROM ACTIVE DATABASE
TOPOLOGY	• Possible only between BaseDB • Not supported between RAC and single instance • Data Guard Far sync, cascade redo transport or multiple standby databases are manual setups
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
OPEN MODE	• It depends on Database software edition. On EE-EP, change is possible between Data Guard (mounted) or Active Data Guard (open read-only)
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

Base Database Service VM : 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 Data Guard 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 when 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

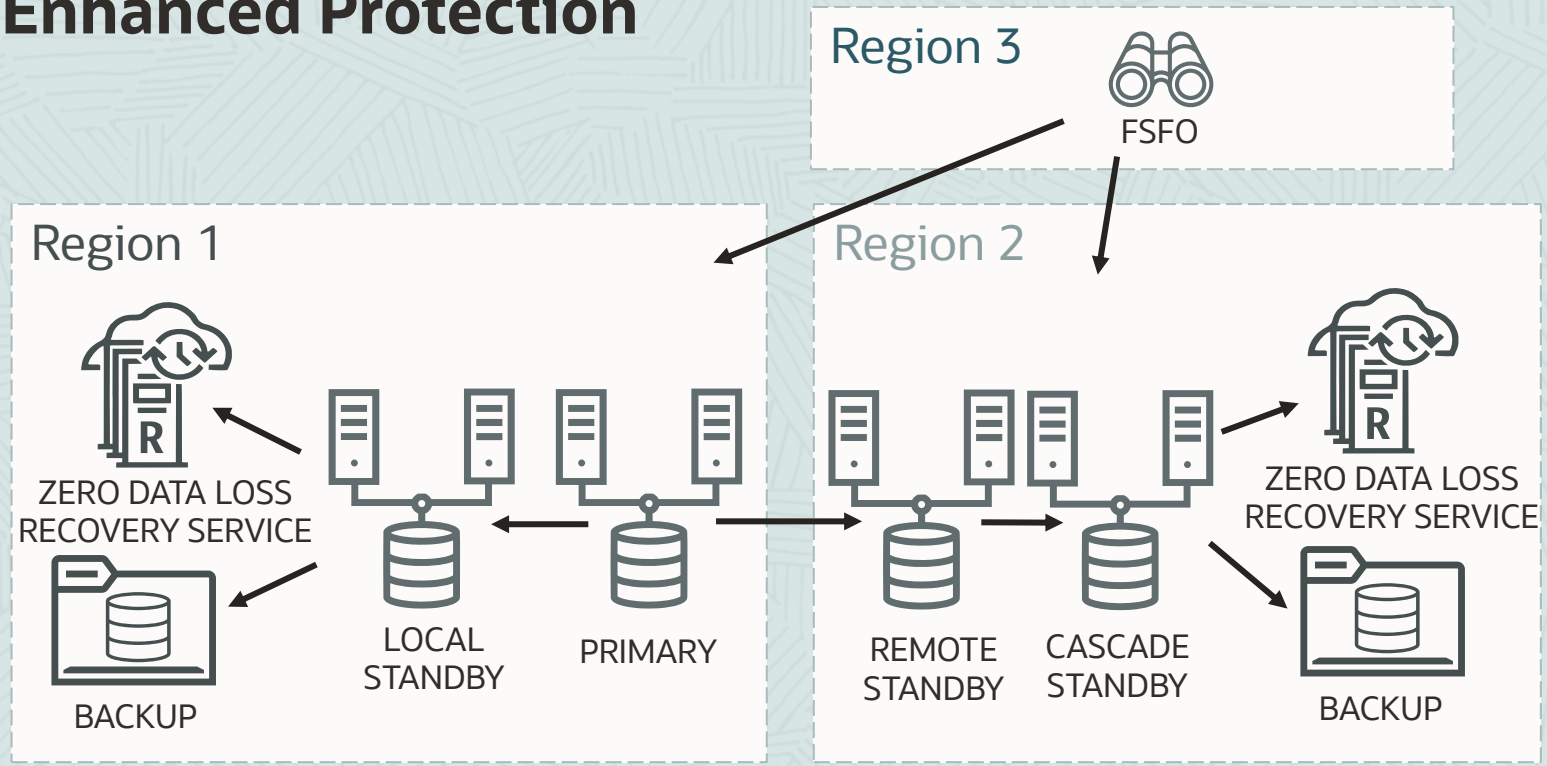
Not recommended unless for multiple standby or hybrid Data Guard use cases

Base Database Service 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)
- `Verify that db_block_checking` is set to TYPICAL (this may vary depending on version and shape)
- 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

Base Database Service VM: Enhanced Protection

AVAILABILITY / AUTOMATION *	
ZRCV	Recovery Service or via multiple backup copies with optional backup from the standby
RAC	Custom application services
ACTIVE DATA GUARD	Multiple standbys Fast-start failover
GOLDENGATE	Manual (capture & delivery) Global Data Service
MAA LEVEL	SILVER BaseDB · GOLD + Data Guard · PLATINUM + GoldenGate



Gold Outage Matrix

PLANNED MAINTENANCE	ZERO	ZERO
RECOVERABLE FAILURE	ZERO	SECONDS
UNRECOVERABLE FAILURE[1]	ZERO	SECONDS
UPGRADE	ZERO	SECONDS

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

(1) RPO can be seconds with Autonomous Recovery Service (ZRCV)

Base Database Service VM: read more

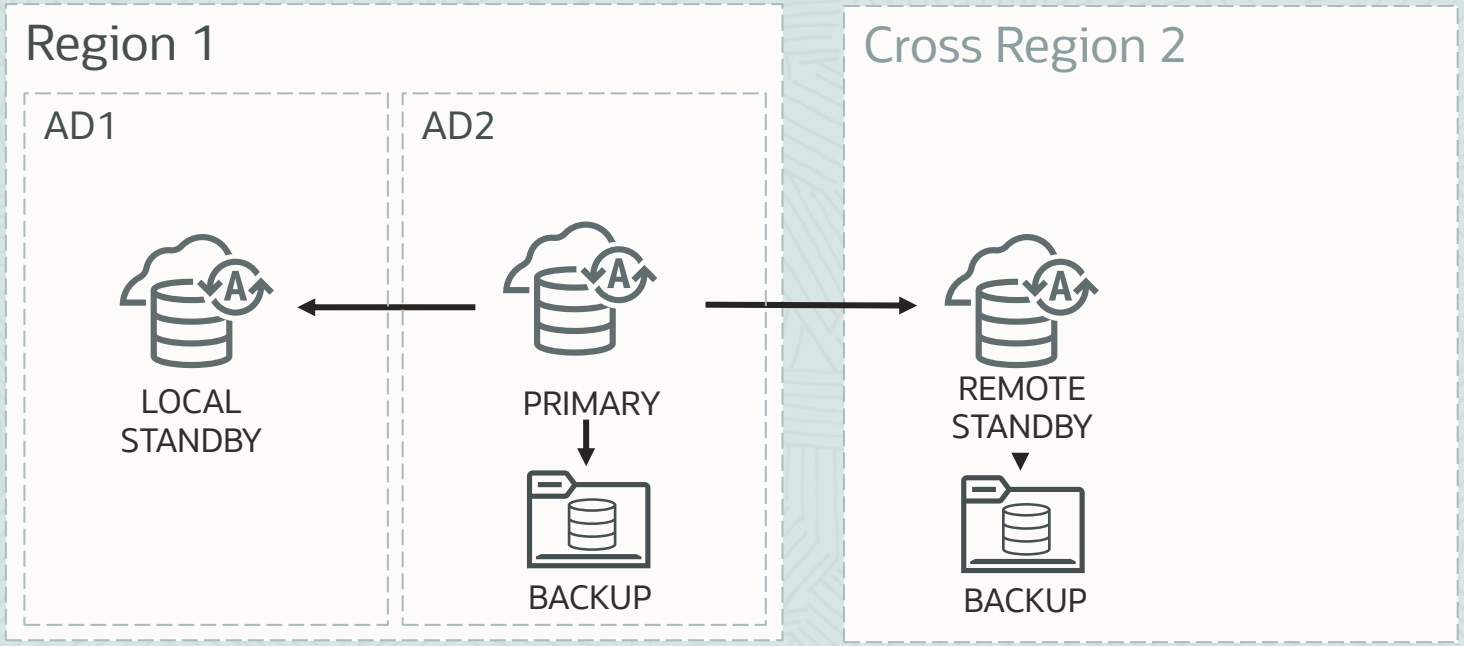
- Backing Up a Database to Oracle Cloud Infrastructure Object Storage
  - https://docs.oracle.com/en-us/iaas/Content/Database/Tasks/backingupOS.htm
- Using Oracle Data Guard
  - https://docs.oracle.com/en-us/iaas/Content/Database/Tasks/usingdataguard.htm
- How to configure oci-cli with Instance/Resource Principals (Doc ID 2763990.1)
  - https://support.oracle.com/epmos/faces/DocumentDisplay?id=2763990.1
- (OCI) mv2bucket - Oracle Managed Bucket Content Manager (Doc ID 2723911.1)
  - https://support.oracle.com/epmos/faces/DocumentDisplay?id=2723711.1

Oracle Autonomous Database Serverless

Maximum Availability Architecture

Autonomous Database Serverless: Protection Out-of-the-box

AVAILABILITY / AUTOMATION *	
RMAN	Backup from primary only Backups are redundant Retention is 60 days Long term backup retention available
RAC	Exadata inherent HA, QoS and Performance benefits Services out of the box
ACTIVE DATA GUARD	Max 2 Standbys: 1 local and 1 remote Bounded minimal data loss possible Manual AuDG role transitions or automatic failover with bounded data loss option
GOLDENGATE	• Using OGG Hub or OCI OGG • Flexible configurations
MAA LEVEL	SILVER: Out of the Box GOLD: + Autonomous Data Guard (within same region)



Gold Outage Matrix

PLANNED MAINTENANCE	ZERO ZERO
RECOVERABLE FAILURE	ZERO SECONDS
UNRECOVERABLE FAILURE	SECONDS MINUTES
UPGRADE	ZERO MINUTES

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

Autonomous Database Serverless: Automatic backup

SCHEDULING	• Automatically done by the service (60-day full, daily incremental, 5 mins archivelog, some optional retention control)
DESTINATION	• Service-managed bucket, no direct customer access
REPLICAS	• Mirrored and replicated.
CREDENTIALS	• Managed internally • Automatic password rotation
WALLET	• TDE wallet managed and backed up by Oracle
RESTORE	• Restore backup within the retention window
RETENTION	• 60 days of retention and long-term backups are available
STANDBY	• No backup on the standby database

Autonomous Database Serverless: Real Application Clusters

- Services are automatically created
  - ATP and ADW: _high, _medium, _low
  - ATP only: _tp, _tpurgent
- Client access only via TLS or mTLS
- Application Continuity can be enabled and configured via DBMS_CLOUD_ADMIN package
- No configuration requirement for Fast Application Notification
  - FAN events are handled by the Connection Manager (CMAN)
- Patching is rolling and announced in the user interface (No database downtime . Zero application downtime for short transactions, long transactions might have an impact)

Autonomous Database Serverless: Autonomous Data Guard

ACTIVE DATA GUARD

SETUP	• 1-click setup from control plane • Via PDB hot clone
TOPOLOGY	• Option to configure 1 or 2 standby databases within the same region as the primary or cross-region • Remote region destinations predefined based on lowest latency • From ADB-S to ADB-S
PROTECTION	• Same region standby configuration (MAA validated with local standby: local RPO < 10 seconds, local standby RTO < 131 secs) • Automatic failover available with bounded RPO in the same region • RTO does not include detection time
ROLE CHANGES	• Switchover and failover available through control plane • Connection string only contains regional information. Cross-region needs manual connection string configuration.
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 Serverless: read more

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

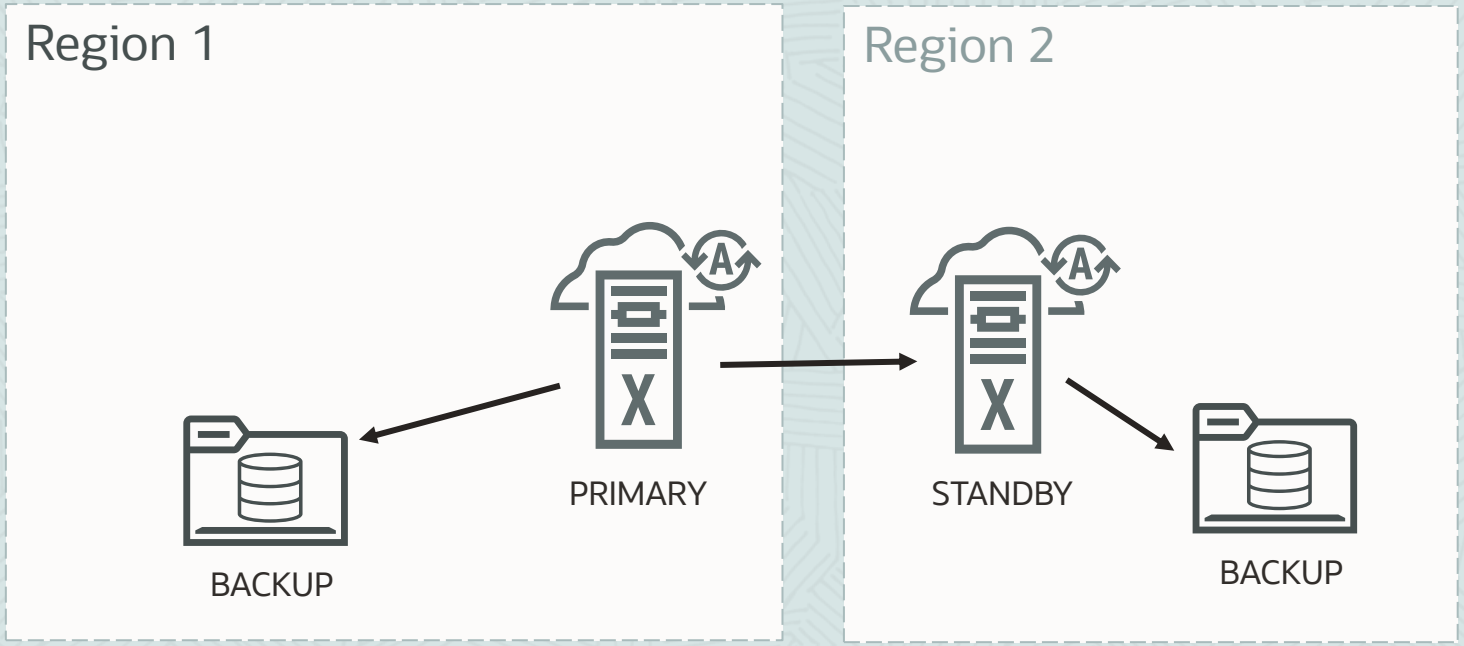
- Continuous Availability - Application Continuous Service for MAA Solutions
  - https://docs.oracle.com/en/database/oracle/oracle-database/19/haovw/configuring-continuous-availability-applicationsconfiguring-continuous-availability-applicati.html

Oracle Autonomous Database on Dedicated Exadata Infrastructure (ADB-D and ADB-C@C)

Maximum Availability Architecture

Autonomous Database - Dedicated: Protection Out-of-the-box

AVAILABILITY / AUTOMATION *	
RMAN	• Manage or Cancel Backups • Primary/Standby backup/restore available and long-term retention • CDB or PDB backup/restore
RAC	Exadata inherent HA, QoS, and Performance benefits, Agility, and Expansion (CPU, memory, disk storage, DB node, Storage Cell, DB Node (or new Clusters)
ACTIVE DATA GUARD	• 1 standby, local or remote • Automatic failover option (FSFO) • Max Availability or Max Performance
GOLDENGATE	• Using OGG Hub or OCI OGG • Flexible configurations
MAA LEVEL	SILVER ADB-D; GOLD + Data Guard; PLATINUM (with OGG)



Gold Outage Matrix

PLANNED MAINTENANCE	ZERO ZERO
RECOVERABLE FAILURE	ZERO SECONDS
UNRECOVERABLE FAILURE	SECONDS SECONDS
UPGRADE	ZERO MINUTES

*
- 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	• ADB-D: Service-managed bucket, no direct customer access • ADB-C@C: NFS, ZDLRA (recovery appliance) or local (for • For ZDLRA, real-time redo transport is not available yet
REPLICAS	• Object storage, Mirrored backup • ADB-C@C: 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-D: Oracle Vault (KMS) supported for customer-managed keys • ADB-C@C: Oracle Key Vault supported for customer-managed keys
RESTORE	• Create new ADB from backup is possible. • Duplicate (clone) is supported
RETENTION	• Short-term retention is enabled and configurable • Long-term retention is available
STANDBY	• Automatic backup of standby database

Autonomous Database - Dedicated: automatic backup best practices

- Backup retention
  - Object storage or NFS up to 95 days
  - Long-term backup: between 90 days and 10 years (ADB-C@C: NFS only)
  - ZDLRA: controlled by the recovery appliance protection policy
  - Local: 7 days (ADB-C@C Only)
- On-demand PDB backup:
  - Used for fast PITR only
  - Follows backup retention
  - Can be used to create a new database

Autonomous Database - Dedicated: Real Application Clusters

- 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 ECPU count (<=16) by default only opened on a single node
- Databases with higher ECPU count (>16) by default opened on two or more nodes
- Container Database has RAC split control, open at OCPU count different than default 16
- Container Database has RAC affinity control, opening one node only until all resources used
- Patching is rolling and scheduled by the customer
- Fast Application Notification must be configured

Autonomous Database – Dedicated: RAC services

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

ACTIVE DATA GUARD

SETUP	• Setup from control plane on CDB creation or add standby post-CDB creation • A protected CDB can be chosen at ADB creation
TOPOLOGY	• Single primary-standby can be configured within the same region, across ADs, or cross-region • Only possible between same ADB-D type (On-premises to On-premises/OCI to OCI) • MAA practices integrated
PROTECTION	• Max Availability or Max Performance possible at CDB level • Automatic failover (Fast-Start Failover) is available
ROLE CHANGES	• Switchover, Failover and Snapshot Standby at CDB level available through control plane • Connection string is aware of Autonomous Data Guard
OPEN MODE	• Standby database is open read-only (DML redirection not supported) • Standby role listener services available
PATCHING & UPGRADE	• Customer controls when primary and standby are patched • Standby first patching best practices applied automatically • Zero database downtime with RAC rolling for any software or hardware updates

Autonomous Database - Dedicated: Read more

Oracle Maximum Availability Architecture and Autonomous Database Cloud

- Autonomous Database with Default High Availability Option
- Autonomous Database with Autonomous Data Guard Option
- Maintaining Application Uptime

https://docs.oracle.com/en/database/oracle/oracle-database/19/haovw/oracle-maximum-availability-architecture-and-oracle-autonomous-database.html

Multicloud

Maximum Availability Architecture

Oracle Database on Exadata in Multicloud

Deploy full-featured Oracle Databases on Exadata located within hyperscale cloud data centers

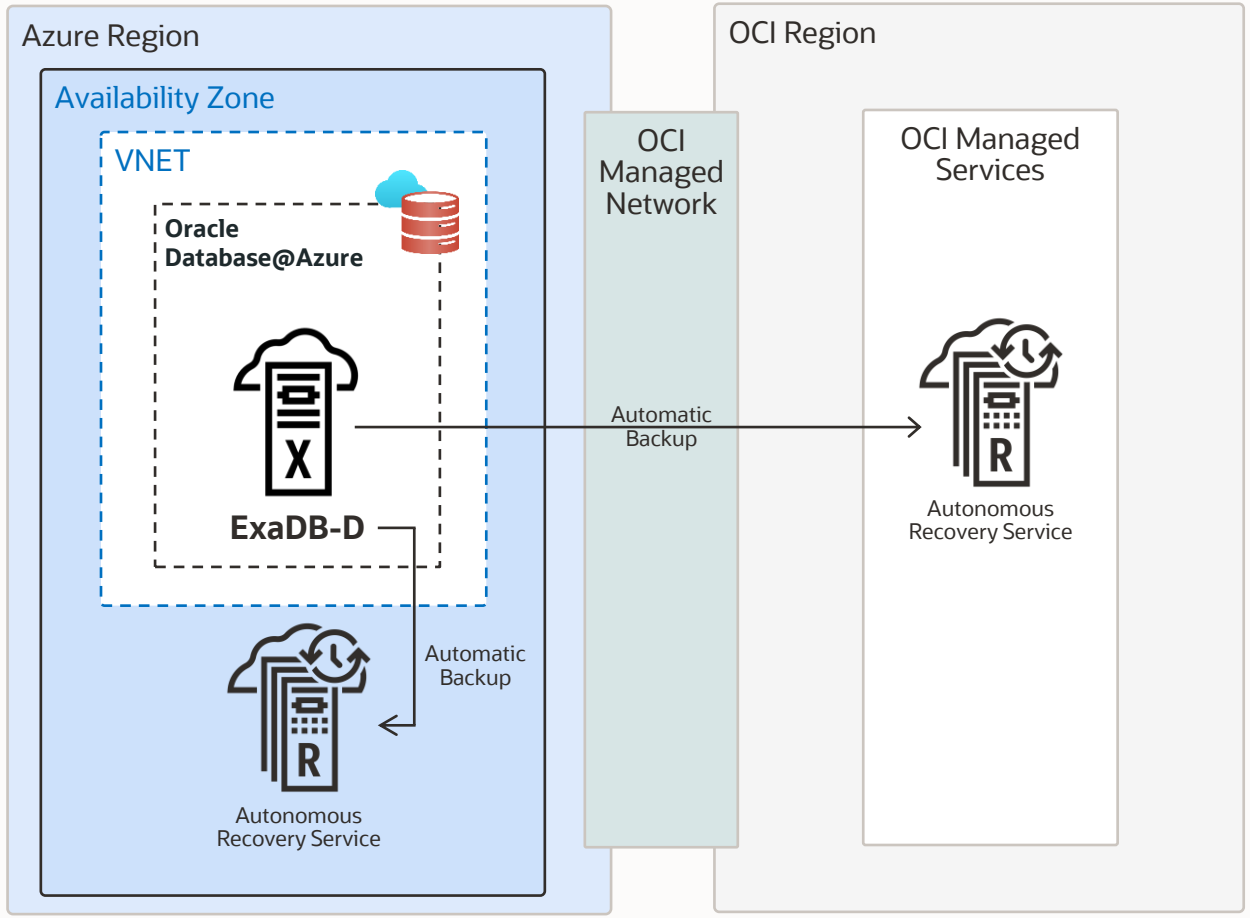
- Co-located apps and databases deliver superior performance
- Integrated cloud console, APIs, and monitoring with joint support enhances customer experience
- Full Oracle Database functionality and compatibility accelerates cloud migration and IT modernization

ORACLE CLOUD Infrastructure	Microsoft Azure	Google Cloud	aws
			
Oracle Database in OCI	Oracle Database@Azure	Oracle Database@GCP	Oracle Database@AWS

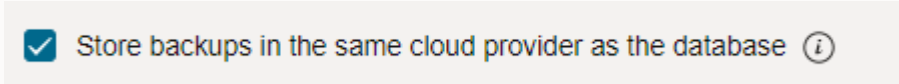
Oracle Database@Azure MAA Silver Level

High Availability and Data Protection Built-in by Default

SILVER



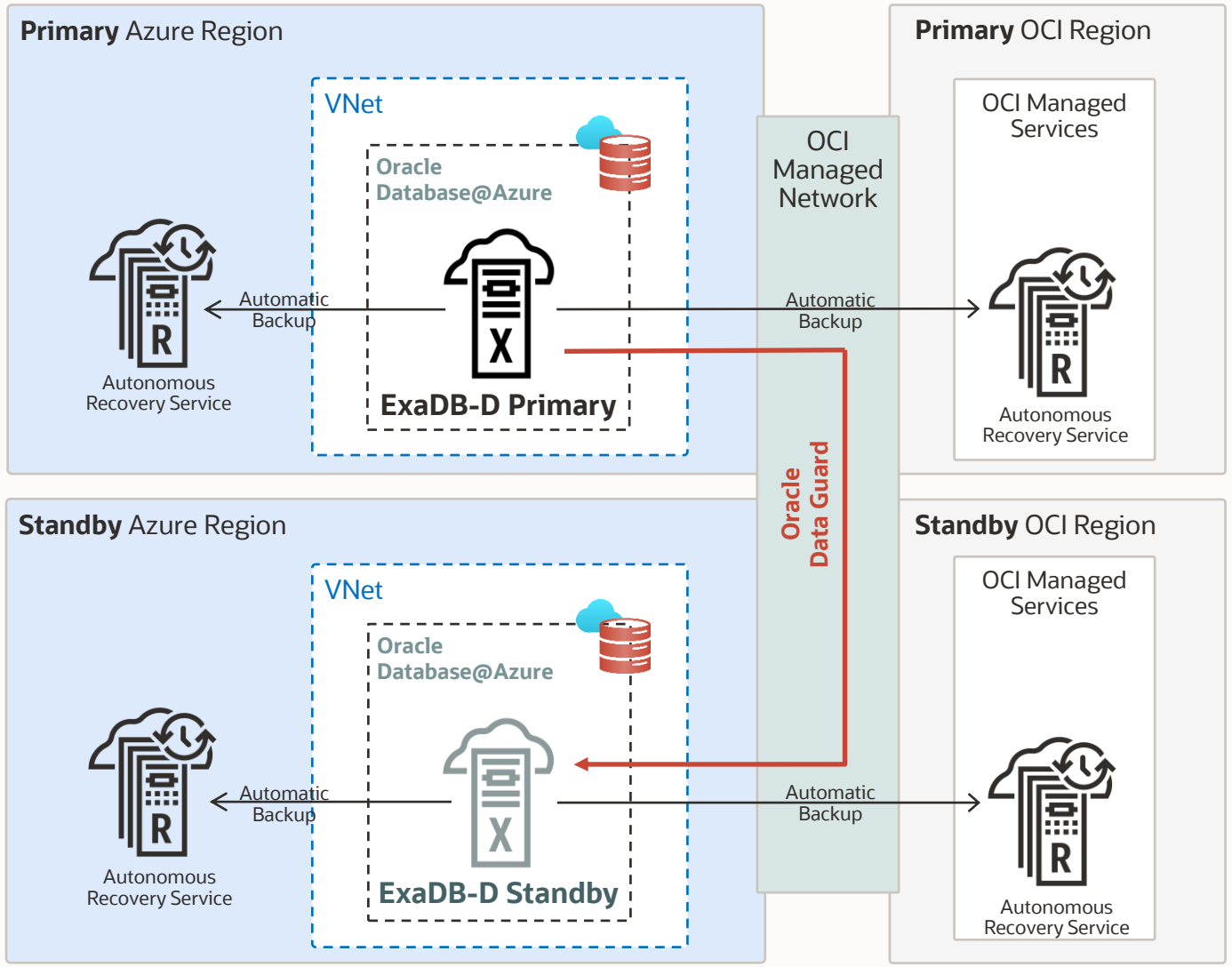
- ✓ Oracle Exadata and Oracle RAC
  - ✓ Agility to scale storage, compute, and memory without downtime
  - ✓ Node failure protection
  - ✓ Zero downtime software maintenance
- ✓ Zero Data Loss Autonomous Recovery Service
  - ✓ Available in OCI and in Azure
  - ✓ One click to choose backup destination



- ✓ Alternatively, backup to OCI Object Storage

Oracle Database@Azure MAA Gold Level | Cross-regions

Mission-Critical Deployments with Disaster Recovery



MAA Silver Level +

- ✓ Fully Automated Oracle (Active) Data Guard setup
  - ✓ **Regional disaster recovery protection**
  - ✓ Comprehensive data corruption prevention
  - ✓ Defense from ransomware attacks
  - ✓ Online upgrades and migrations
  - ✓ Offload backup and workload to standby with read-mostly scale-out

Oracle Data Guard for ExaDB-D on Oracle Database@Azure

Cross-region deployment options

Network Traffic through OCI (recommended)

- Automated setup via Cloud Tooling
  - VCN peering required
- Oracle controls the network and ensures reliability
- First 10TB/month cross-region traffic for free
- One standby database via Cloud Tooling
  - Multiple standbys via manual setup with optional Fast-Start Failover (FSFO)
- Can support the potential high redo throughput required for enterprise databases

Network Traffic through Azure

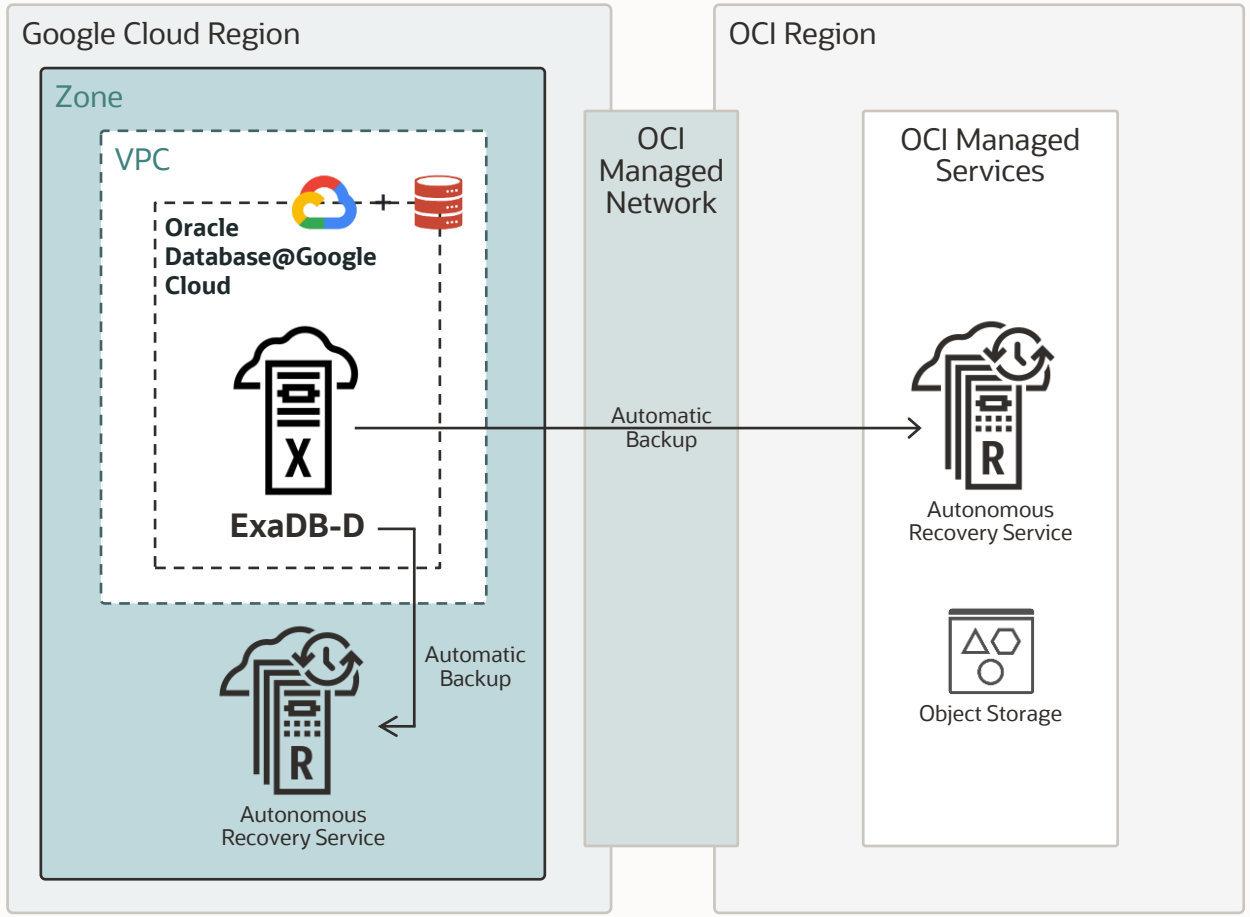
- Automated setup via Cloud Tooling
  - VNet peering required
- Microsoft controls the network and ensures reliability
- Chargeback for cross-region traffic
- One standby database via Cloud Tooling
  - Multiple standbys via manual setup with optional Fast-Start Failover (FSFO)

coming soon

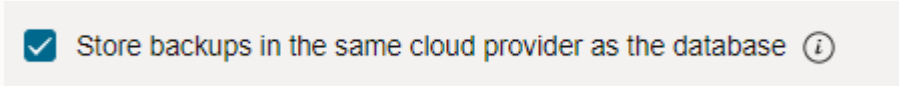
SILVER

Oracle Database@Google Cloud MAA Silver Level

High Availability and Data Protection Built-in by Default



- ✓ Oracle Exadata and Oracle RAC
  - ✓ Agility to scale storage, compute, and memory without downtime
  - ✓ Node failure protection
  - ✓ Zero downtime software maintenance
- ✓ Zero Data Loss Autonomous Recovery Service
  - ✓ Available in OCI and in GCP
  - ✓ One click to choose backup destination



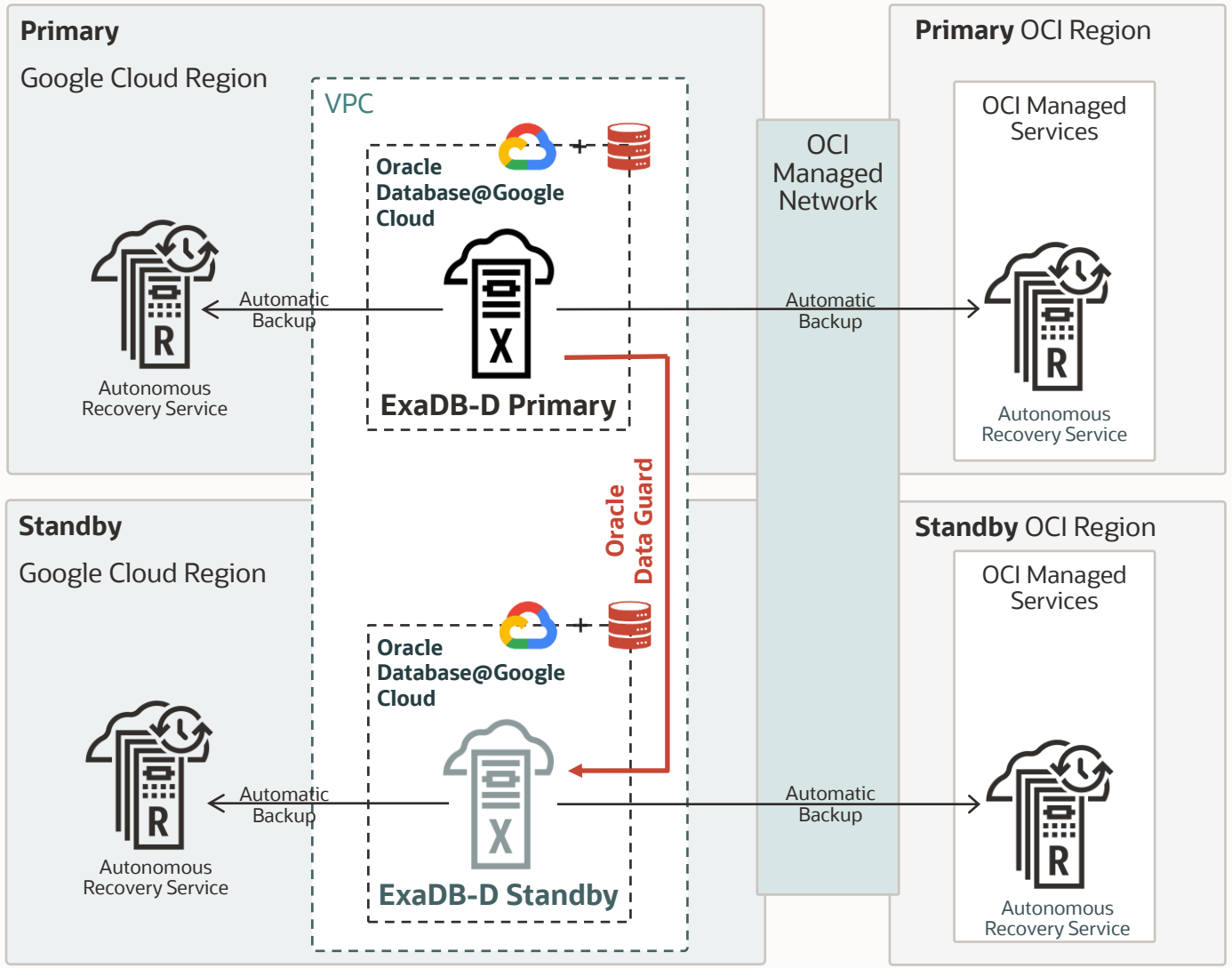
- ✓ Alternatively, backup to OCI Object Storage

coming soon

GOLD

Oracle Database@Google Cloud MAA Gold Level | Cross-regions

Mission-Critical Deployments with Disaster Recovery



MAA Silver Level +

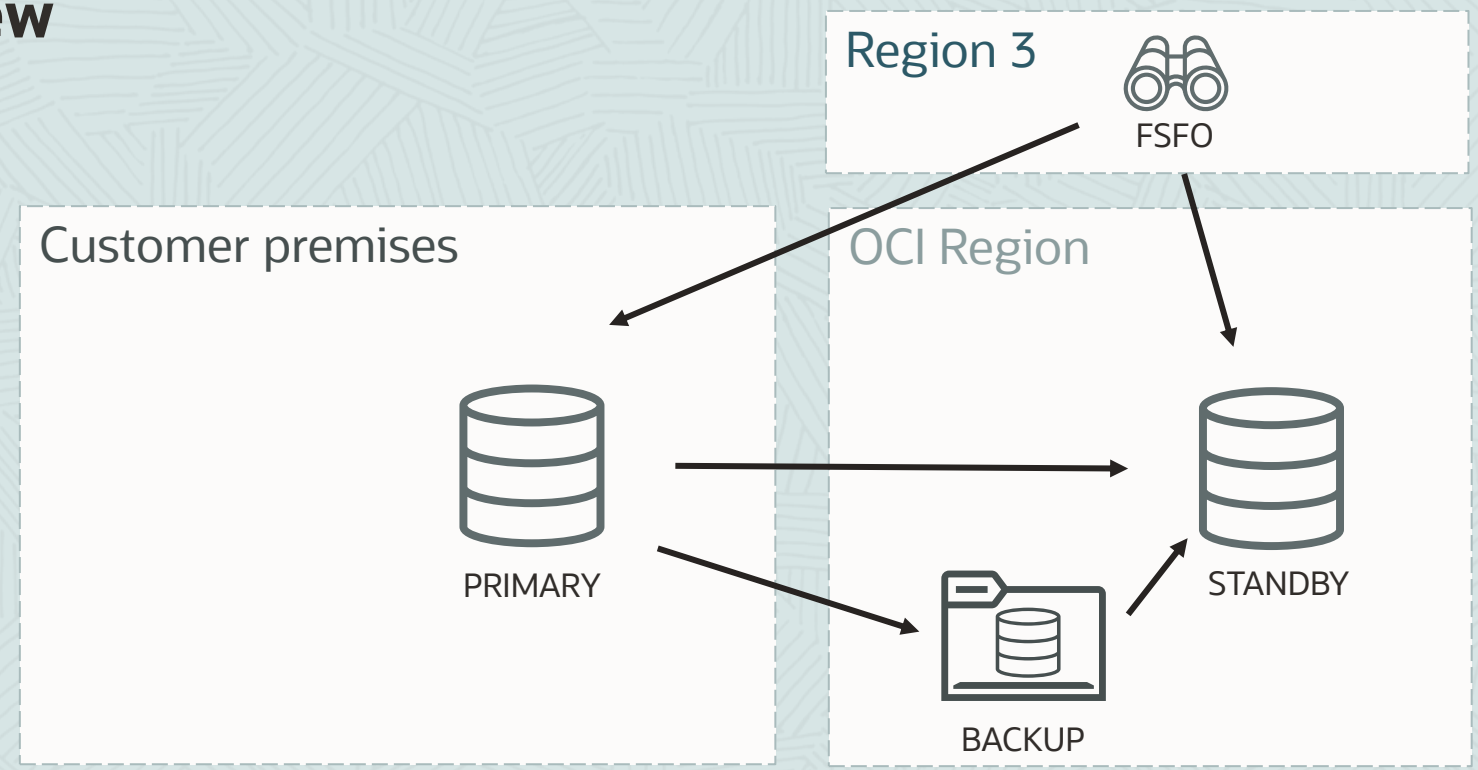
- ✓ Fully Automated Oracle (Active) Data Guard setup
  - ✓ **Regional disaster recovery protection**
  - ✓ Comprehensive data corruption prevention
  - ✓ Defense from ransomware attacks
  - ✓ Online upgrades and migrations
  - ✓ Offload backup and workload to standby with read-mostly scale-out

Hybrid Data Guard

Maximum Availability Architecture

Hybrid Data Guard: overview

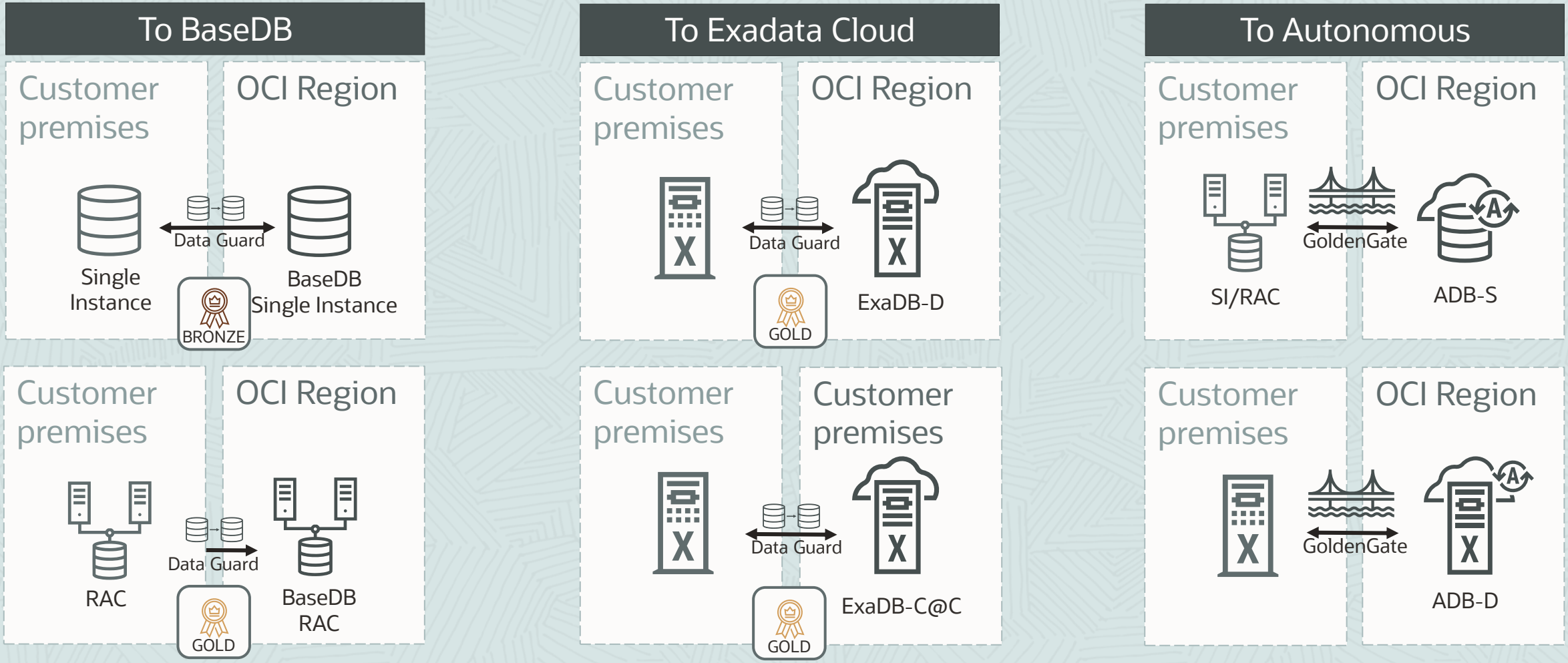
AVAILABILITY / AUTOMATION (1)	
RMAN	Backup to the cloud
RAC	Customer-specific
ACTIVE DATA GUARD	Instantiate & operate Data Guard configuration
GOLDENGATE	Manual (capture & delivery)
MAA LEVEL	SILVER, GOLD, PLATINUM Customer responsibility.



Gold Outage Matrix (2)		
PLANNED MAINTENANCE	ZERO	ZERO
RECOVERABLE FAILURE	ZERO	SECONDS
UNRECOVERABLE FAILURE	ZERO	SECONDS
UPGRADE	ZERO	SECONDS

(1) Customer responsibility
(2) Best case scenario (FSFO + SYNC or FAR SYNC)

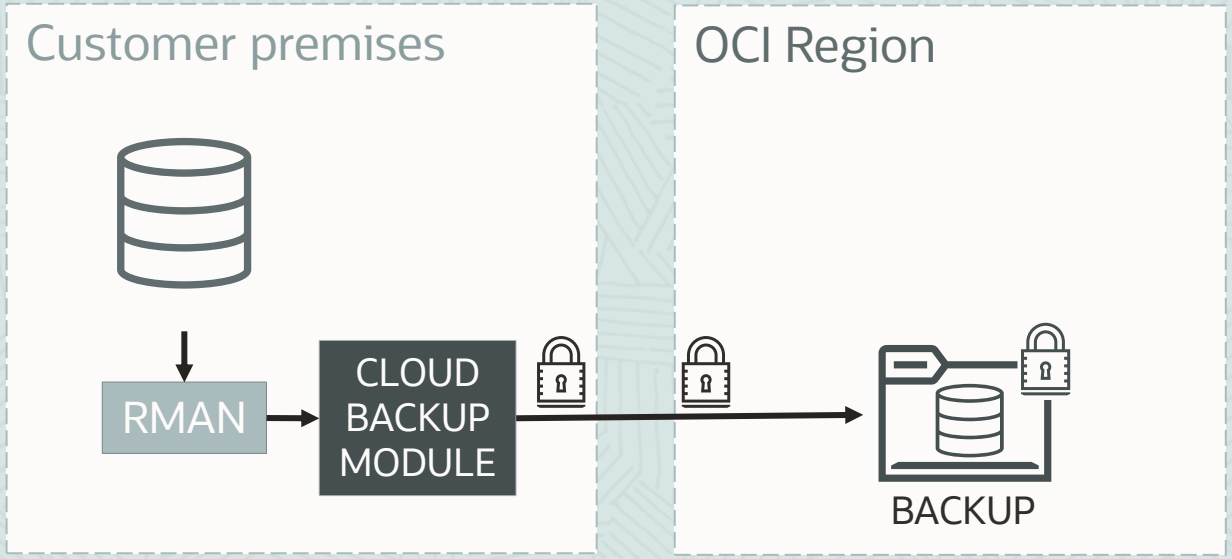
Hybrid Cloud: recommended hybrid sources/destinations



- All Hybrid configurations are achieved manually: no Control Plane automation
- On-premises non-Exadata to ExaDB-C@C/ExaDB-D 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
- Support for Immutable Backup



Hybrid Cloud: backup to Oracle Cloud Infrastructure

- 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

Hybrid Cloud: Data Guard destination matrix

ACTIVE DATA GUARD

		On-premises DB	BaseDB	BaseDB RAC	ExaDB-C@C	ExaDB-D
	OS	Linux Windows [1]	Linux	Linux	Linux	Linux
19c	VERSION	All supported versions	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
EE	EDITION	DG: EE	DG: EE, EE-HP	EE-EP	Included in ExaDB-C@C	Included in ExaDB-D
		ADG: +ADG option	ADG: EE-EP			

[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

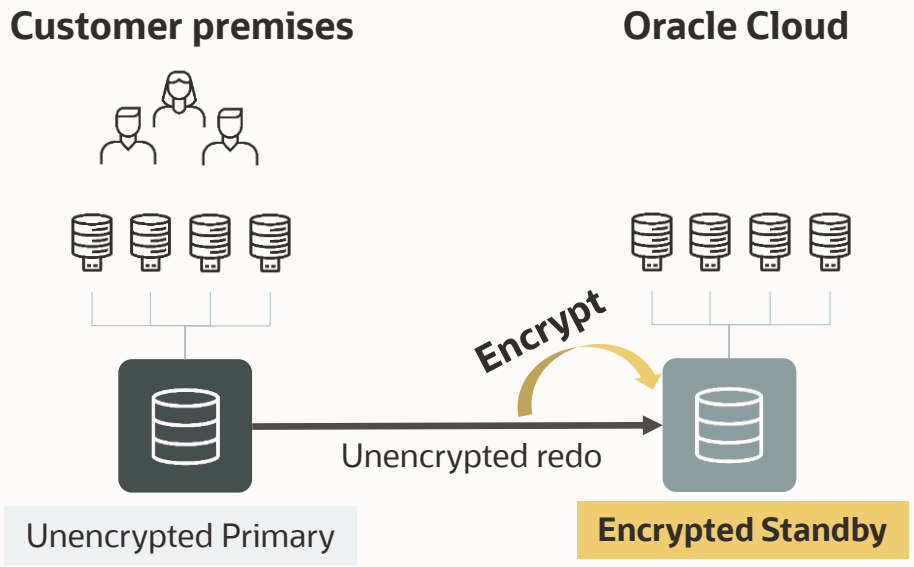
- Measure peak redo rates and ensure enough bandwidth
  - Assessing and Tuning Network Performance for Data Guard and RMAN (Doc ID 2064368.1)
    - Generally recommended:
      net.ipv4.tcp_rmem=4096 87380 134217728
      net.ipv4.tcp_wmem=4096 16384 134217728
- Communication must be bi-directional
- Use either IPSec VPN or FastConnect (recommended)
  - For FastConnect use private peering
  - If the internet is used, use SQL*Net encryption

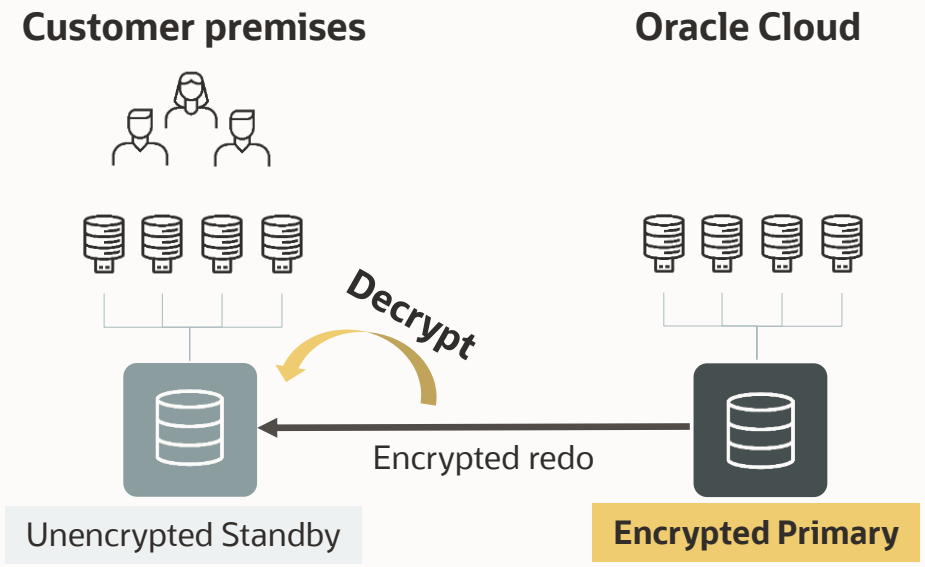
Transparent Data Encryption

- Recommended: 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)

Transparent Data Encryption in hybrid deployments

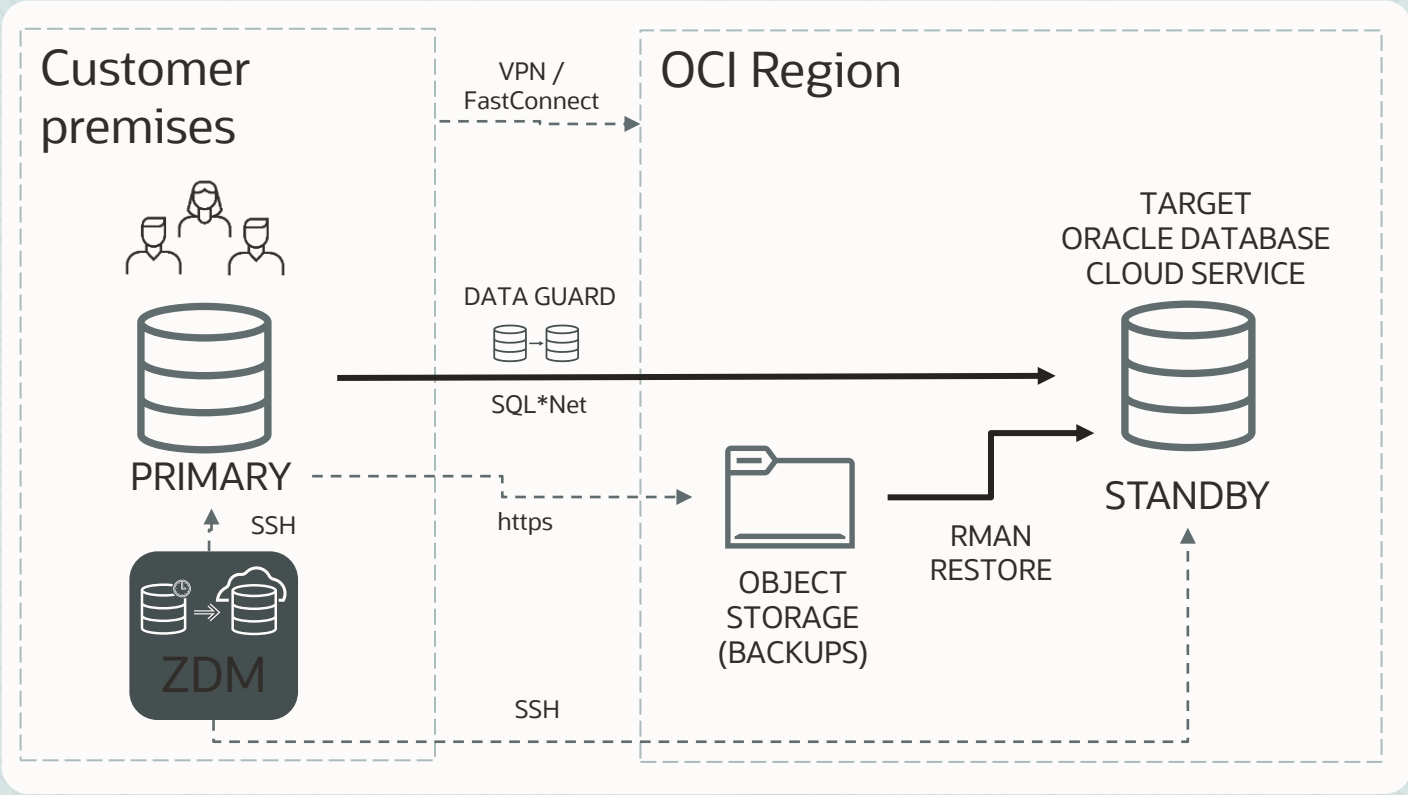
```
-- On-premises init.ora or spfile:
TABLESPACE_ENCRYPTION  = DECRYPT_ONLY;
-- OCI init.ora or spfile:
TABLESPACE_ENCRYPTION  = AUTO_ENABLE;
```





Hybrid Cloud: automatic setup with ZDM

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



https://oracle.com/goto/zdm

Hybrid Cloud: Data Guard high-level implementation steps

- Create a Database in the Cloud
  - Same patch level +one-offs as a 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 BaseDB, Exachk for ExaDB-D)
- Monitor DG health: **Monitoring a Data Guard Configuration (Doc ID 2064281.1)**

Patching for hybrid Data Guard in OCI

- The 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

- Hybrid Data Guard to Oracle Cloud Infrastructure Production Database on Premises and Disaster Recovery with BaseDB BM or VM shapes in Oracle Cloud Infrastructure
  https://www.oracle.com/docs/tech/database/hybrid-dg-to-oci.pdf
- Disaster Recovery using Exadata Cloud
  On-Premises Primary to Standby in Exadata Cloud Service or Gen 2 Exadata Cloud at Customer
  https://docs.oracle.com/en/database/oracle/oracle-database/19/haovw/oracle-data-guard-hybrid-cloud-configuration1.html
- 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

GoldenGate and Platinum MAA

Maximum Availability Architecture

MAA Platinum and Cloud GoldenGate Collateral

- MAA Platinum Reference Architecture Overview
- Overview of Oracle GoldenGate Best Practices
- Cloud-Specific GoldenGate Papers
  - Cloud: Configuring Oracle GoldenGate Hub for MAA Platinum
  - Cloud: Oracle GoldenGate Microservices Architecture on Oracle Exadata Database Service Configuration Best Practices
  - Cloud MAA Platinum: Oracle GoldenGate Microservices Architecture Integrated with Active Data Guard
- Managing Planned and Unplanned Outages for Oracle GoldenGate Hub
- Troubleshooting Oracle GoldenGate

Oracle Zero Data Loss Autonomous Recovery Service (ZRCV)

Maximum Availability Architecture

Zero Data Loss Autonomous Recovery Service

Gives the near zero RPO for ExaDB-D and BaseDB

Ransomware resiliency

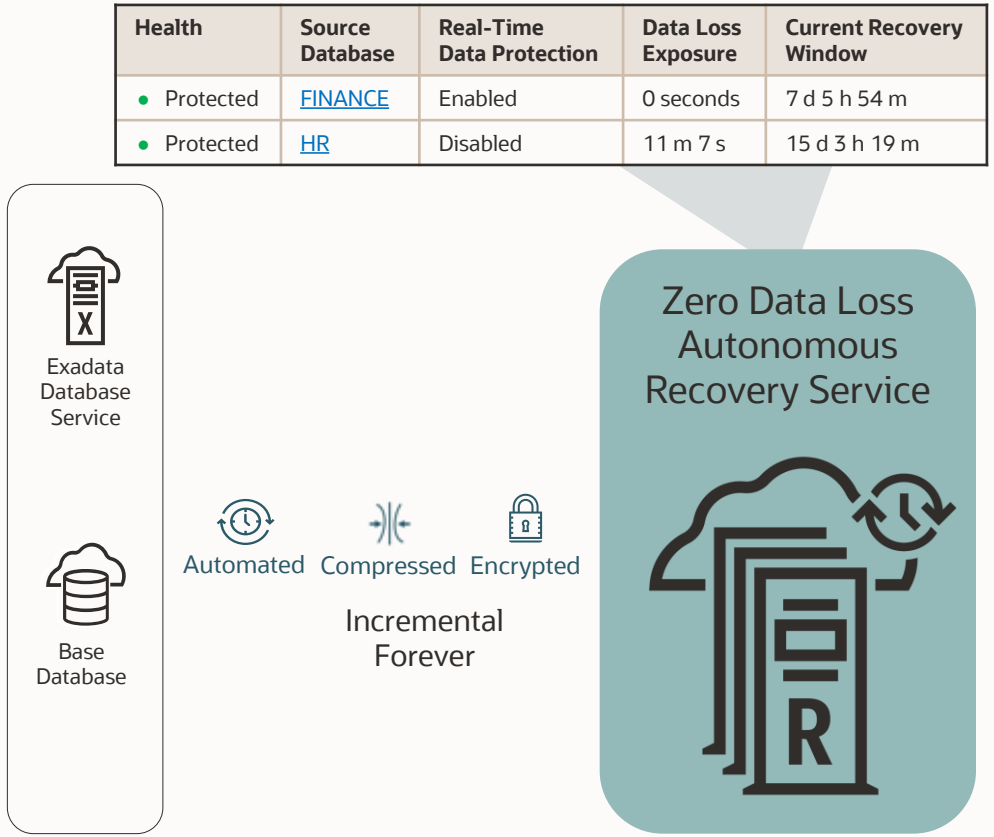
- Fast, zero data loss recovery with optimized backups
- Automated and mandatory encryption to help prevent data theft
- Safeguards backups with enforced policy-level database retention lock

Operational efficiency

- No more weekly full backups – eliminates production database overhead
- Shorter backup windows with incremental forever strategy
- Zero-impact database recovery validation for every backup

Cloud simplicity

- Quickly configure database protection at scale with zero data loss
- Control costs with database-specific backup consumption metrics
- Gain deep data protection insights with a granular recovery health dashboard



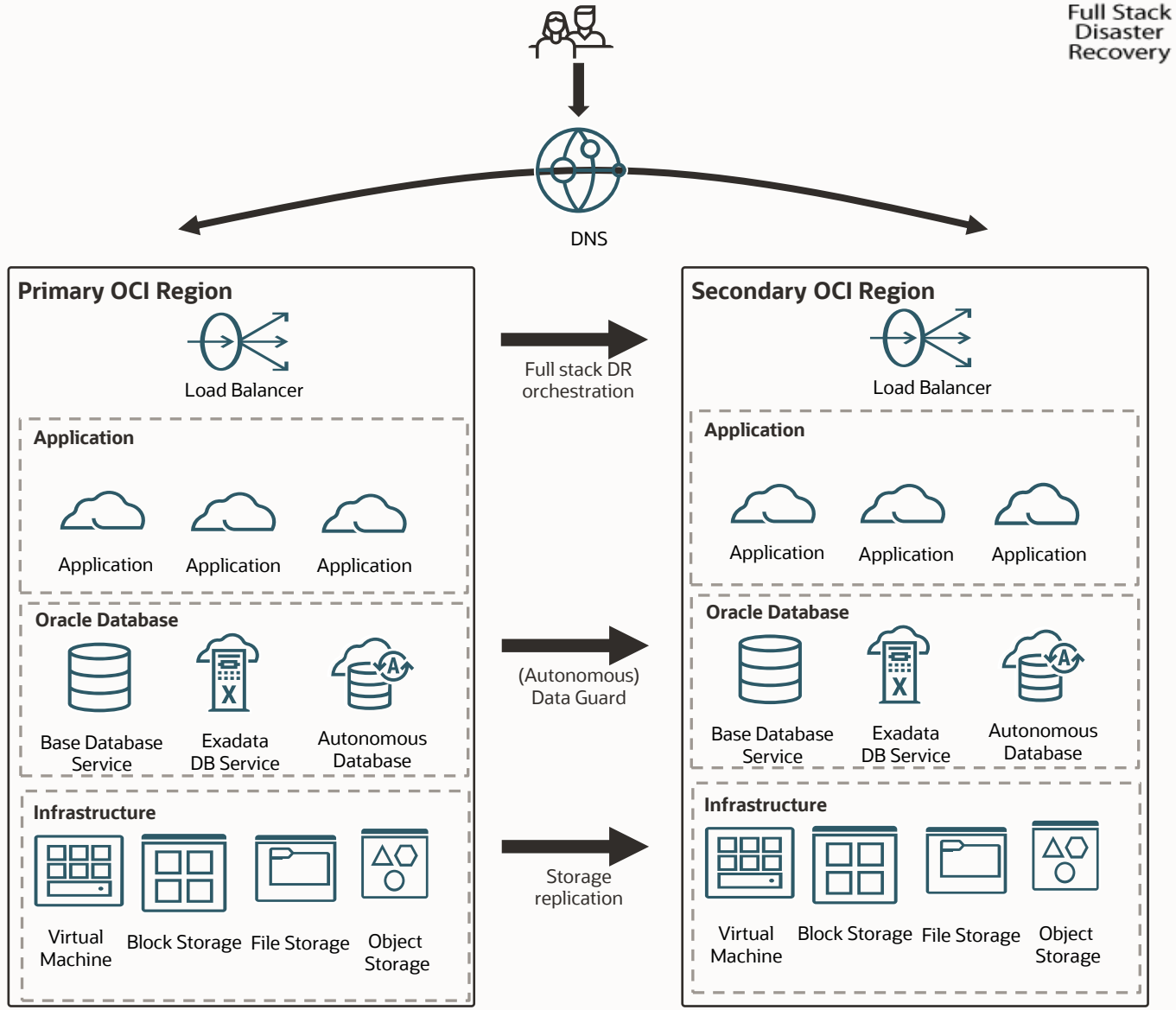
Encryption keys are owned by and managed with the database

OCI Full Stack Disaster Recovery (FSDR)

Maximum Availability Architecture

OCI Full Stack Disaster Recovery

- Fully managed disaster recovery (DR) service in Oracle Cloud
- DR for the entire application stack
  - Orchestrated single-click DR for infrastructure, applications & databases
- Automated discovery
  - Automates finding interdependent resources and creating and customizing DR plans
- Unified management
  - Validated and monitored execution of DR plans through an integrated UI / API



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
ExaDB-D	✓	✓	✓	✓	✓	✓	✓	✓
ExaDB-C@C	✓	✓	✓	✓	✓	✓	✓	✓
BaseDB RAC	✓	✓	✓	✓	✓	✓	✓	✓
ADB-S	✓	✓	✓	✓	✓	✓	✓	✓
ADB-D	✓	✓	✓	✓	✓	✓	✓	✓

✓ Out of the box

✓ Automated via control plane

✓ Manual setup

✗ Not yet available

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

- 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

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