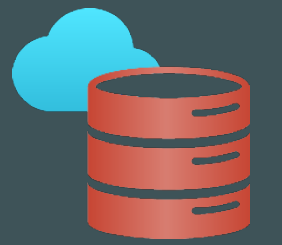
ORACLE

Oracle Database@Azure workshop

Focus area : Azure Design



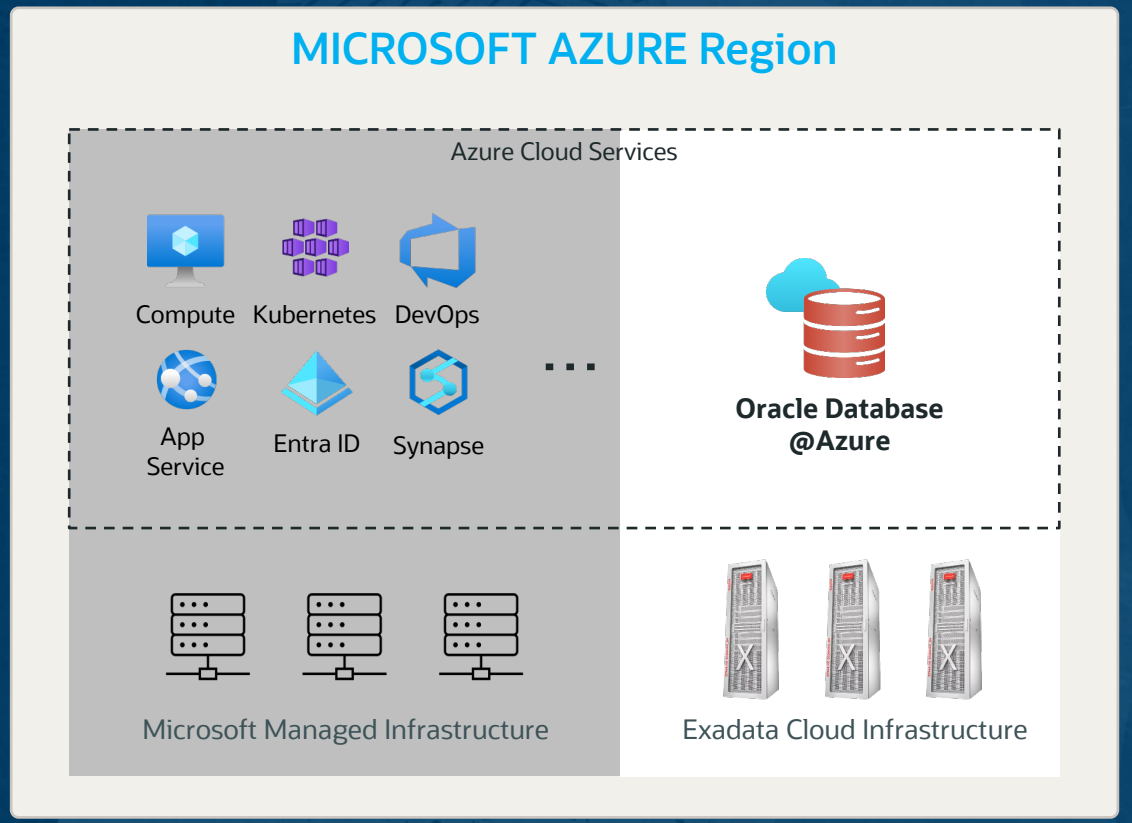
Multicloud Specialist Team
EMEA
April, 2024

Safe harbor statement

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

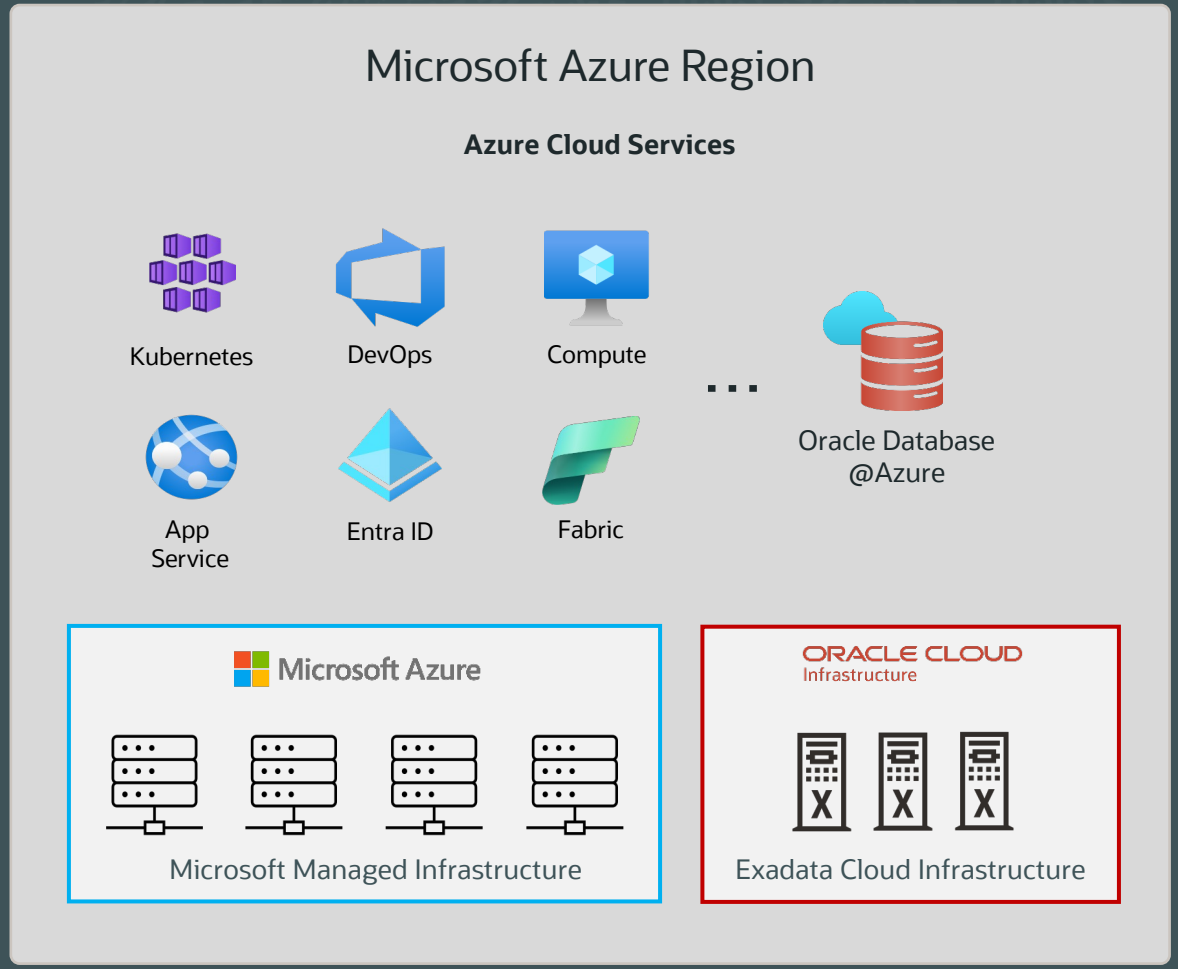
Oracle Database@Azure

Oracle and Microsoft deliver
Oracle database services
on OCI *in* Azure



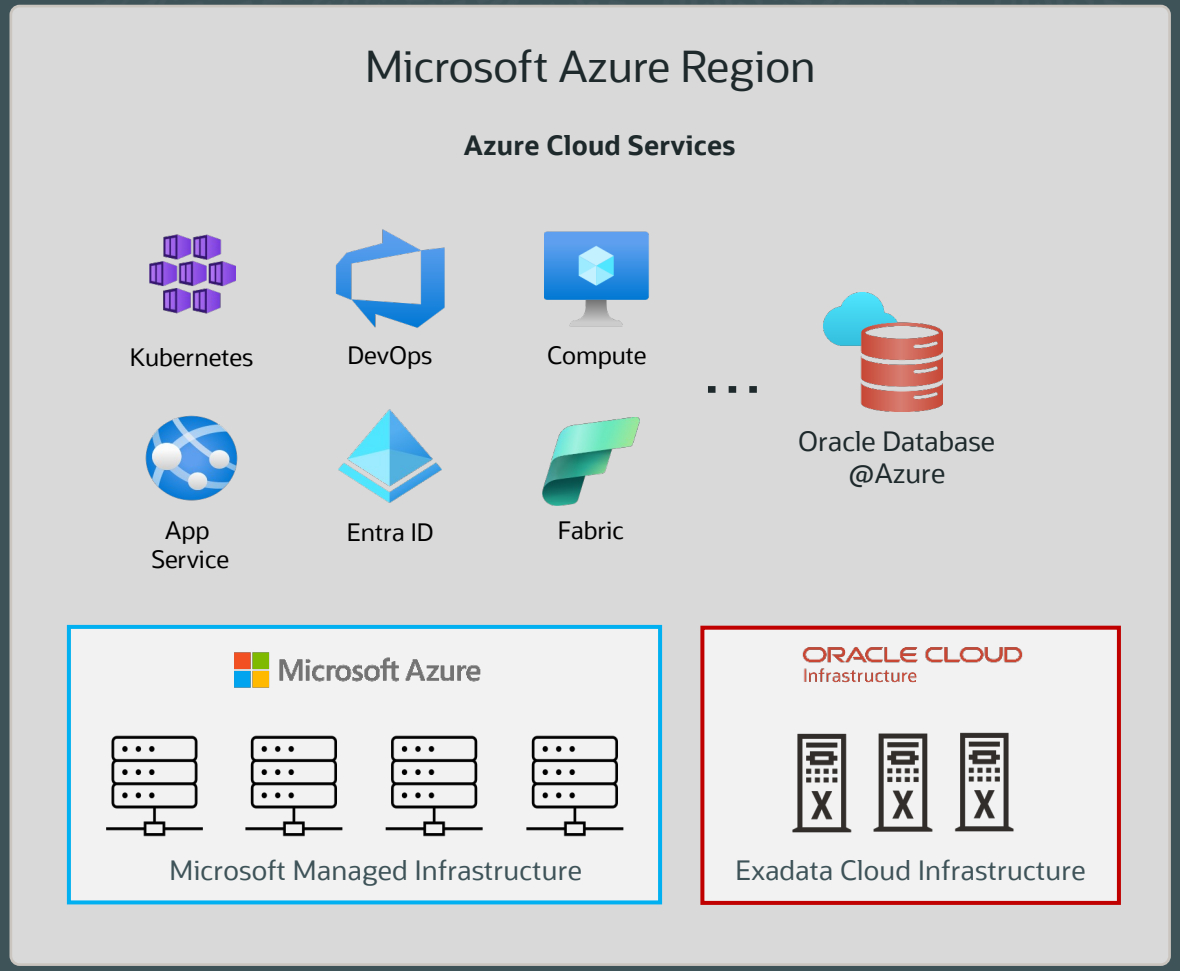
Introduction to Oracle Database@Azure

- The following material is inteded to give an overview of the different parts building up this solution, which could be of interest or is needed to discuss/decide if planning to deploy or having an interest in this solution
- There are more detailed material of sections described on the next page, which can be follow on workshops for respective interested roles



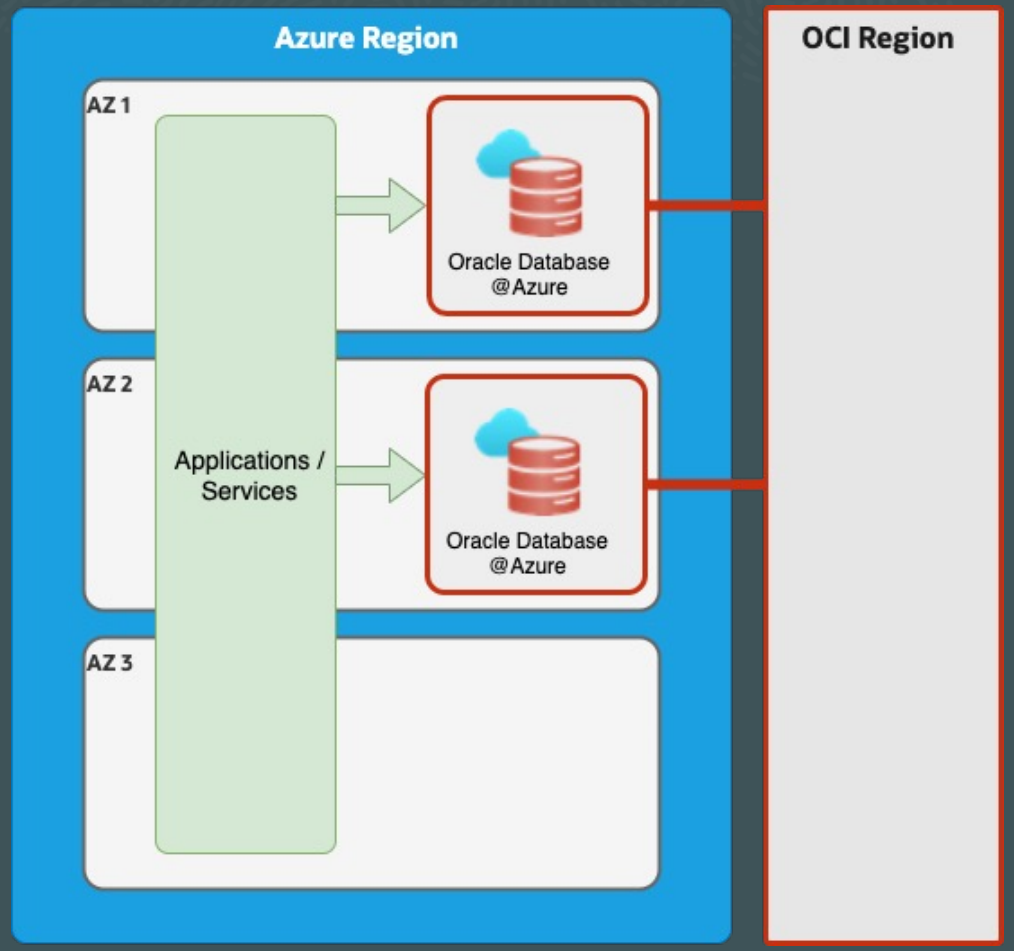
Section overview

1. Oracle Database@Azure overview
2. Oracle Database@Azure Database offerings
3. Database essentials
4. Azure Networking
5. Azure DNS
6. Backup/Restore
7. Database Key Management
8. Azure Identity
9. HA and D/R Architecture
10. Azure Automation & integration
11. *(Observability…wip)*
12. *(Security…wip)*
13. Azure Support & Compliance
14. Azure Database Migration
15. Requirements



1. Oracle Database@Azure – Overview

- This solution puts Oracle database services with it's infrastrucuture inside Microsoft Azure Availability zones in regions where offered
- Oracle DB infrastructure is placed inside Azure DC
- Databases are available in multiple availability zones in each region where this solution is offered
- Provides all the benefits of Exadata Database Service: direct accessable inside Microsoft Azure, including latency to Oracle databases as a native Azure resource
- Databases are accessable from within Azure or from on-premises through ExpressRoute/VPN



Conceptual view of Oracle Database@Azure solution

2. Database offerings for Oracle Database @ Azure

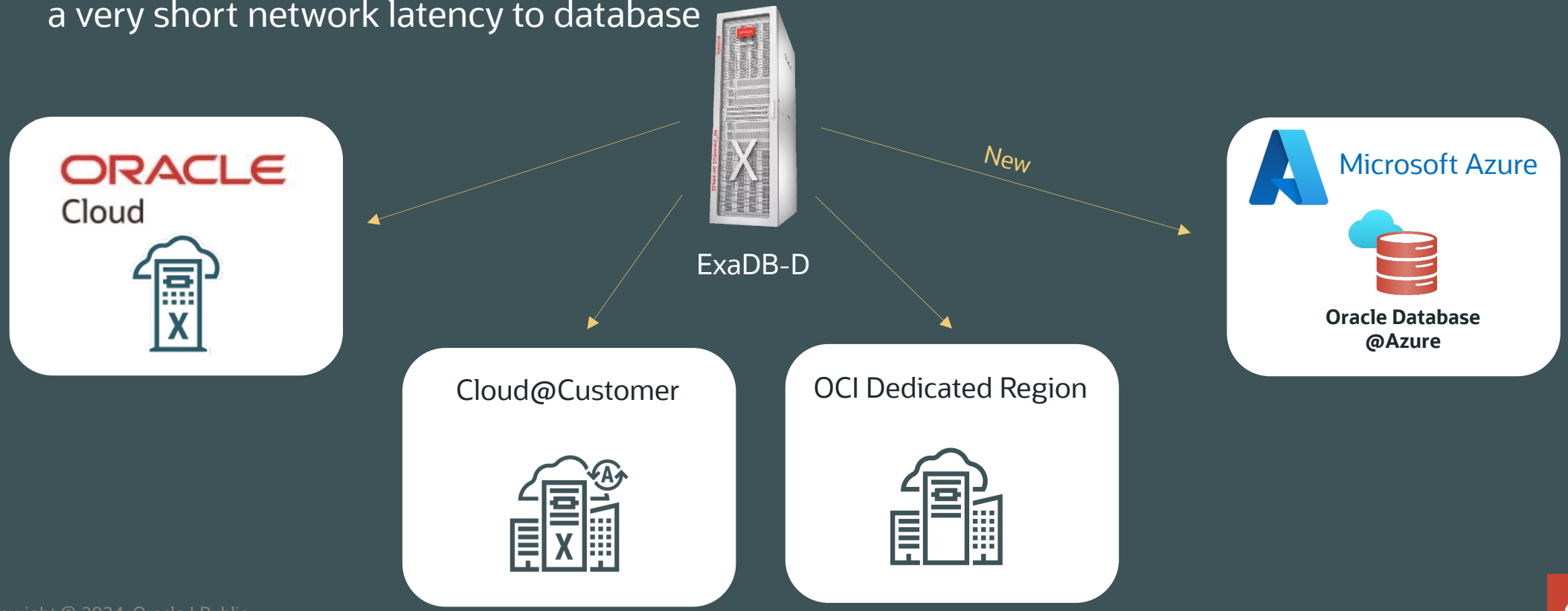
Released	Database offering
Currently available	Oracle Exadata Database Service on Dedicated infrastructure
Not released	Autonomous Database serverless – coming soon
Not released	Next offering – work in progress

Database essentials with Oracle Database@Azure

Oracle Database @Azure

3. Database essentials

- ExaDB-D that is available in Oracle Database@Azure is the same that is offered in other deployment models (OCI, Cloud@Customer and Dedicated Region)
- This new solution is optimized for those customer who need the performance, availability and resiliency of an ExaDB-D but want to continue with application tier in Azure and need a very short network latency to database



3. Database essentials

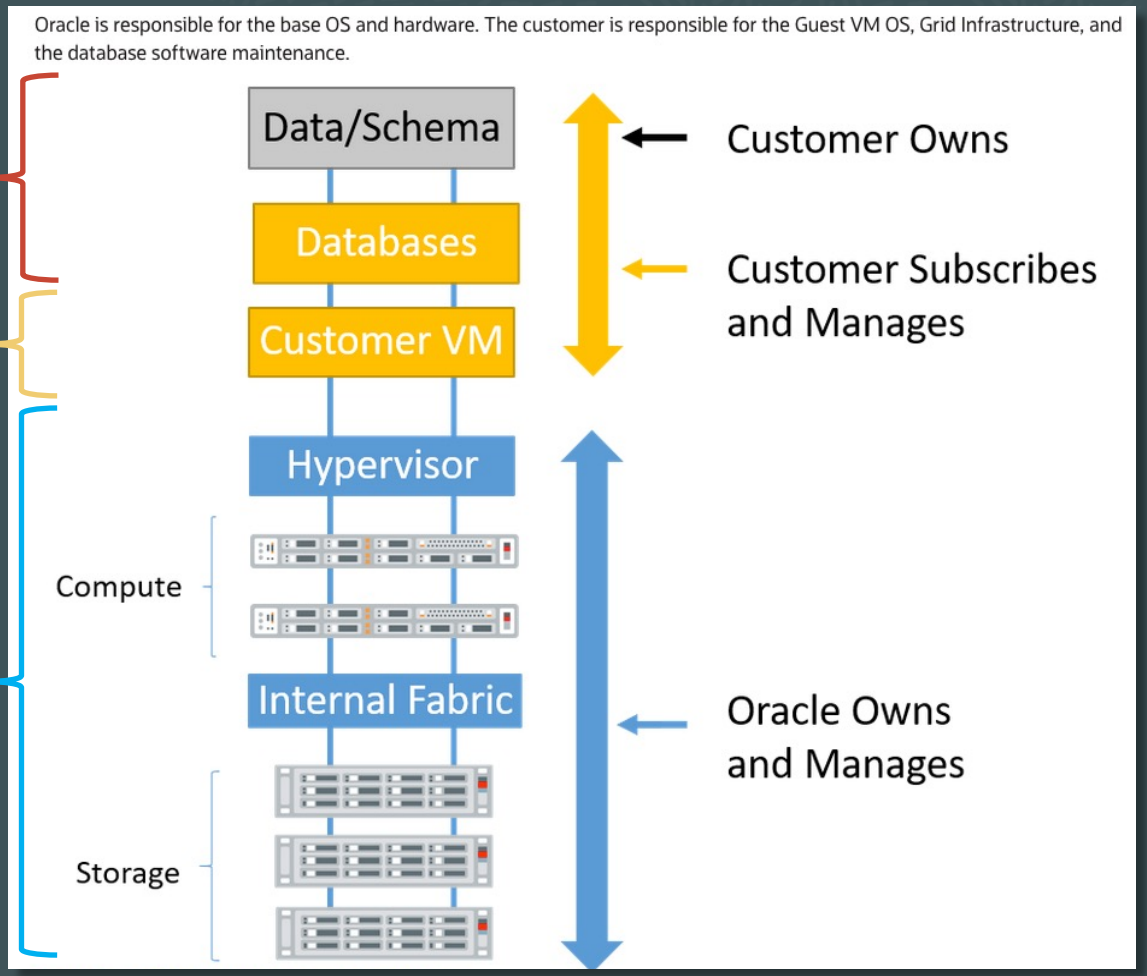
Different parts of ExaDB-D

Databases
Runs on top of VM clusters

VMs and cluster
Always runs Oracle Real Application Cluster (RAC) for high availability
Between 1-8 VM clusters*

* Up to 4 VM clusters with 2x Database nodes

Infrastructure
Always redundant hardware
Database servers = 2 - 32
Storage servers = 3 - 64



Exadata Cloud Infrastructure

3. Database essentials

Mapping of resources to Azure subscriptions and resource groups

Databases
Runs on top of VM clusters

- Databases belongs to a VM cluster and inherit its resource group and subscription

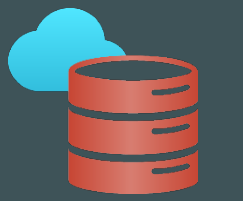
VMs and cluster
Always runs Oracle Real Application Cluster (RAC) for high availability
Between 1-8 VM clusters

- VM clusters will belong to same Subscription as infrastructure but can belong to different Resource groups

Infrastructure
Always redundant hardware
Database servers = 2 - 32
Storage servers = 3 - 64

- Each ExaDB-D/infrastructure can only belong to one Subscription and one Resource group

Azure Networking with Oracle Database@Azure



Oracle Database
@Azure

4. Azure Networking

Remember to plan for expansion

ExaDB-D – VM Cluster Networking in Azure

- Needs a VNet with 1x subnet (Client subnet) in Azure
  - Client subnet needs to be created and delegated to Oracle Database@Azure before ExaDB-D VM cluster deployment
- Need to provide Backup subnet CIDR block during VM cluster deployment
  - Backup subnet will be deployed in OCI, not in Azure
  - Should not overlap with network stack on Azure
- Non overlapping CIDR blocks are needed for each deployment in a DR scenario

The following table shows the minimum required subnet size depending on VM cluster configuration chosen.
Each VM cluster node require 4x IP addresses and in addition 3x addresses are reserved for Single Client Access Names (SCANs.)

Rack Size	Client Subnet # Required IP Addresses	Client Subnet : Minimum size *	Backup Subnet # (Not in Azure) Required IP Addresses	Backup Subnet : (Not in Azure) Minimum size **
Flexible infrastructure (X9M and higher)	4 addresses per VM cluster node + 3 for SCANs + 8 for ODBAA service	Minimum size determined by total number of IP addresses needed for VM cluster nodes	3 addresses per VM cluster node	Minimum size determined by total number of IP addresses needed for VM cluster nodes

*The Networking service in Azure reserves five (5) IP addresses in each subnet
**The Networking service in OCI reserves three (3) IP addresses in each subnet

4. Azure Networking for ExaDB-D – example

Size of subnet	Total number of IPs in subnet
/28	16
/27	32
/26	64
/25	128
/24	256
/23	512

ExaDB-D Network examples : 2x or 4x VM Cluster nodes

	Rack Size	Client Subnet # Required IP Addresses*	Client Subnet : Minimum size *	Backup Subnet size needed# (in OCI)**
Requirements	Flexible infrastructure (X9M and higher)	4 addresses per VM cluster node + 3 for SCANs + 8 for ODBAA service	Minimum size determined by total number of IP addresses needed for VM cluster nodes	3 addresses per VM cluster nodes Will be created automatically in OCI

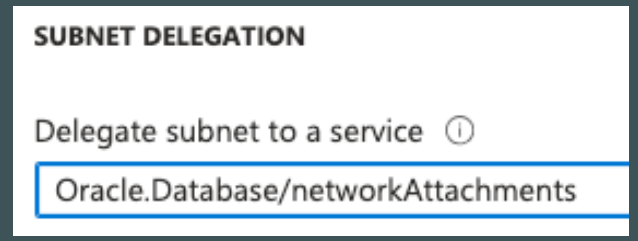
	Rack Size	Client Subnet # IP Addresses in this example*	Client Subnet : Minimum size in this example	Backup Subnet # (in OCI)**
Example 2x VM cluster nodes	X9M	4x2 VM cluster nodes + 3 = 11 IPs Azure reserves 5 IPs ODBAA reserves 8 IPs Total = 24	/27 minimum	/28 minimum (3x2 + 3 = 9)
Example 4x VM cluster nodes	X9M	4x4 VM cluster nodes + 3 = 19 IPs Azure reserves 5 IPs ODBAA reserves 8 IPs Total = 32	/27 minimum (recommend to to use larger for future expansions)	/28 minimum (3x4 +3 = 15)

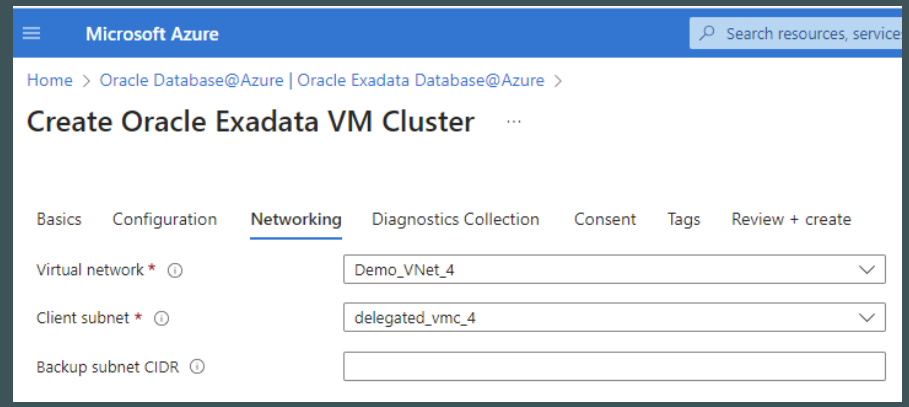
*The Networking service in Azure reserves five (5) IP addresses in each subnet
**The Networking service in OCI reserves three (3) IP addresses in each subnet

4. Azure Networking

VNet and subnets in Azure for this solution

- VM cluster from Exadata Cloud Infrastructure require a preconfigured VNet + 1x subnet in Azure, in the region where deployment will be
- Address space should be made up of one or more CIDR blocks specified in RFC 1918
- This subnet needs to be delegated to Oracle Database@Azure
- Nothing else can be installed in this subnet (only UDR)
- During VM cluster deployment: need to provide backup subnet CIDR block (this subnet will only be in OCI)



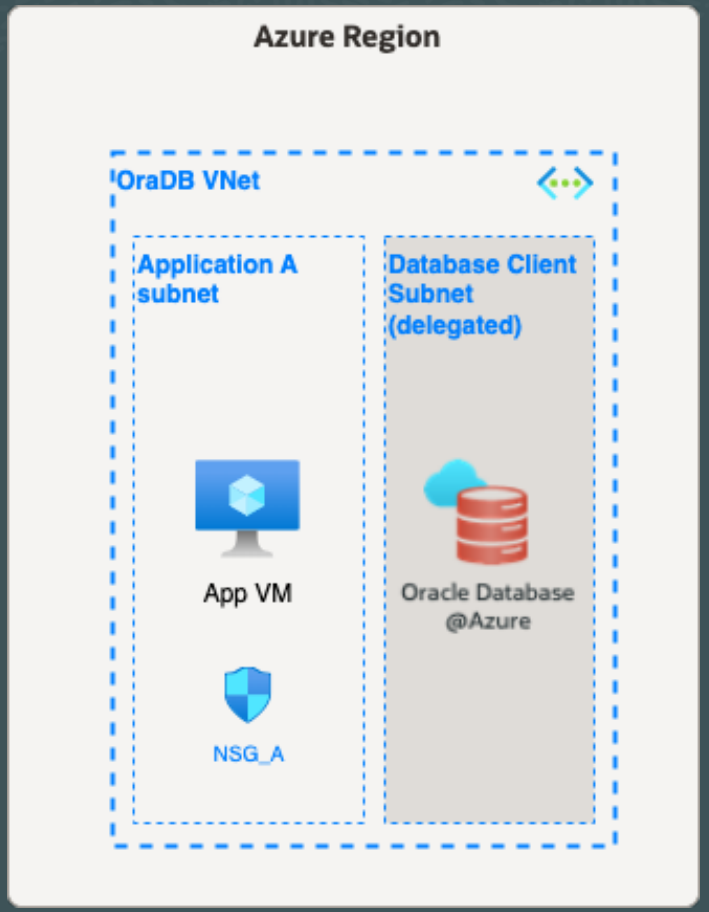


Network section, deployment of VM cluster

4. Azure Networking

VNet and subnets in Azure for this solution

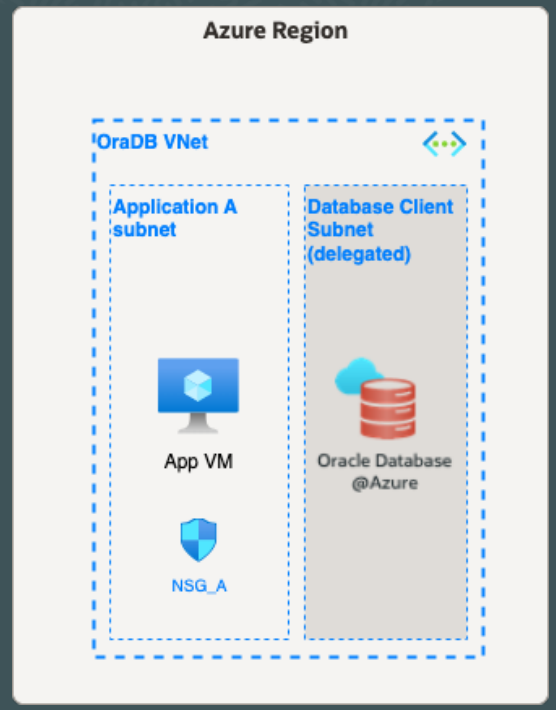
- VNet with delegated subnet and ExaDB-D VM cluster can be in separate resources groups
- It is not possible to assign a Network Security Group (NSG) to the delegated subnet
- Other subnets can be created in same VNet as delegate subnet if wanted, and resources can be placed there
  - This is the recommended approach for best network latency to database
- Maximum 1 delegated subnet per VNet



3. Azure Networking

VNet and subnets in Azure - Note !

Subnet	Restrictions
Client subnet	Do not use a CIDR block that overlaps with 192.168.16.16/28
	Do not use a CIDR block that overlaps with 100.106.0.0/16 or 100.107.0.0/16
Backup subnet	Do not use a CIDR block that overlaps with 192.168.128.0/20

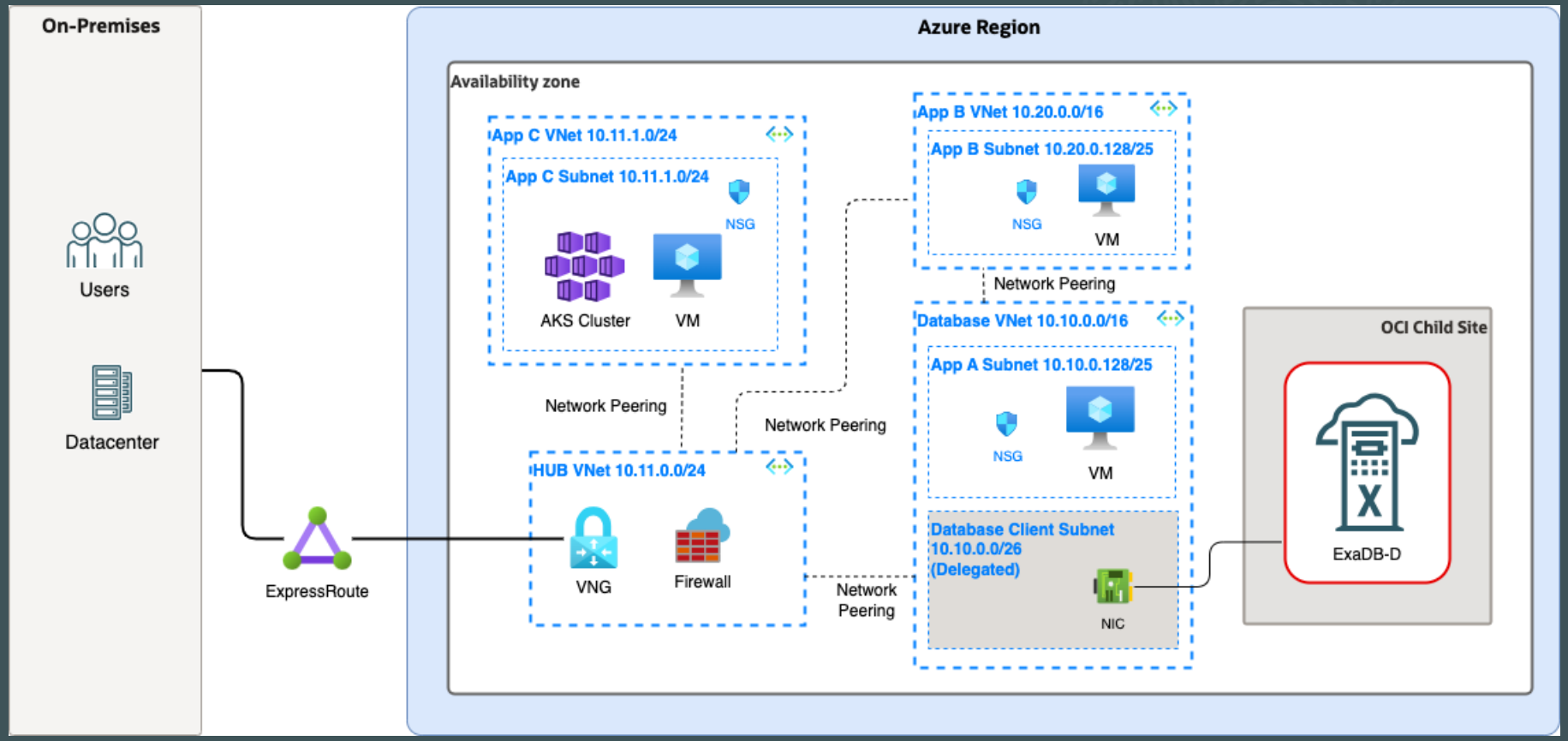


- If using Data Guard : client and backup subnet cannot overlap between Primary and Standby networks

4. Azure Networking

From where can I connect to this database and how might it affect performance

From	Comment
App A subnet	Best network latency to DB
App B subnet	Similar network latency to DB as from App A subnet
App C subnet	Will add latency due to hop in HUB VNet and possible added firewall network latency
On-premises	Possible but network latency will impact performance



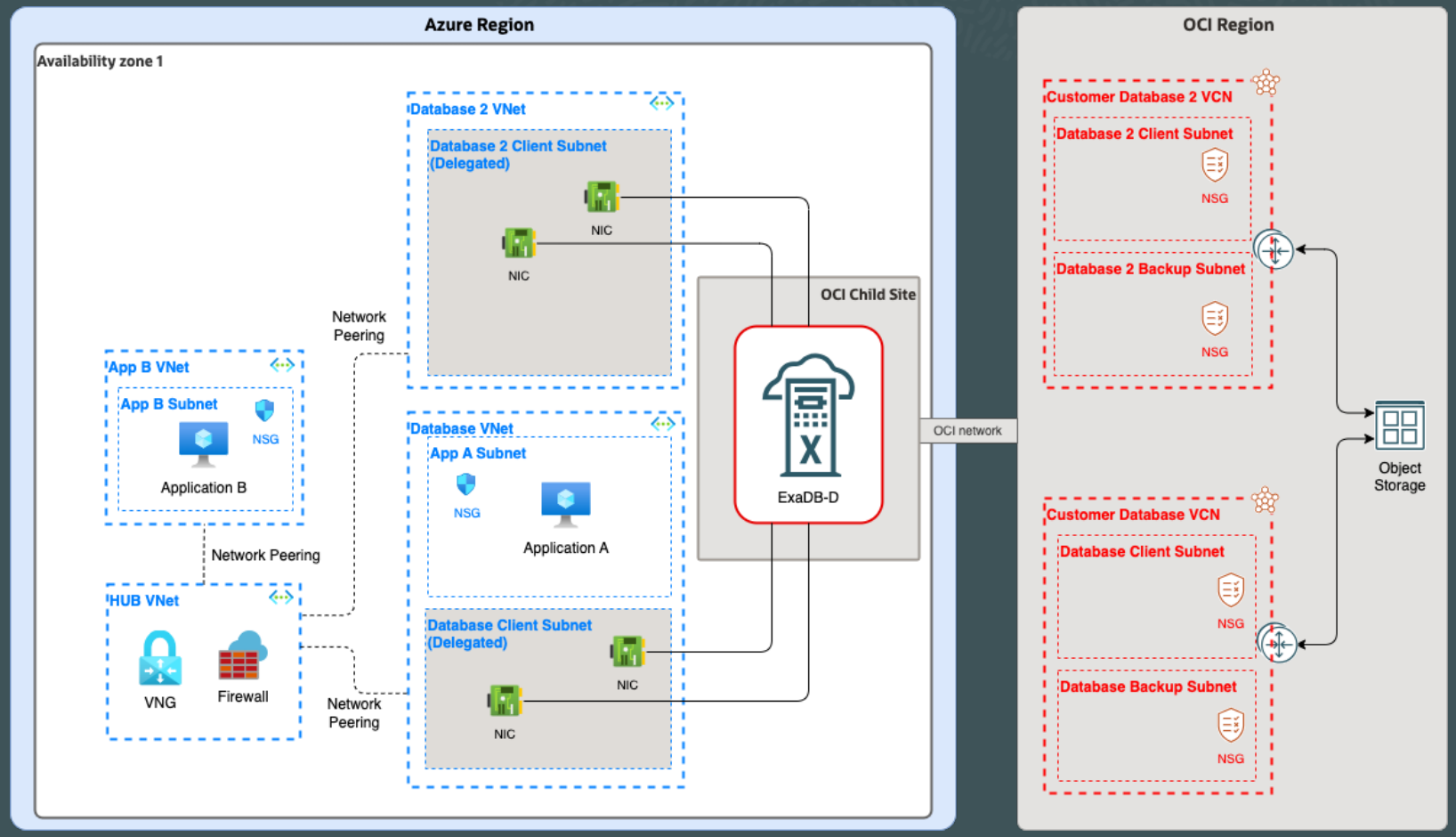
Example with one ExaDB-D Infrastructure and one VM Cluster

Some applications are more sensitive to network latency than others, so decision needs to be taken upon each customer requirements and applications

4. Azure Networking

- One or several VM clusters can be deployed in same VNet/delegated subnet if coming from same infrastructure
- Different ExaDB-D infrastructure cannot use same delegated subnet for their VM cluster nodes
- VM clusters from same infrastructure can be deployed in different VNet's/delegated subnets
- Applications can reach DB from DB VNet or other spoke VNet's through normal VNet peering

(normal Azure VNet peering charges applies)

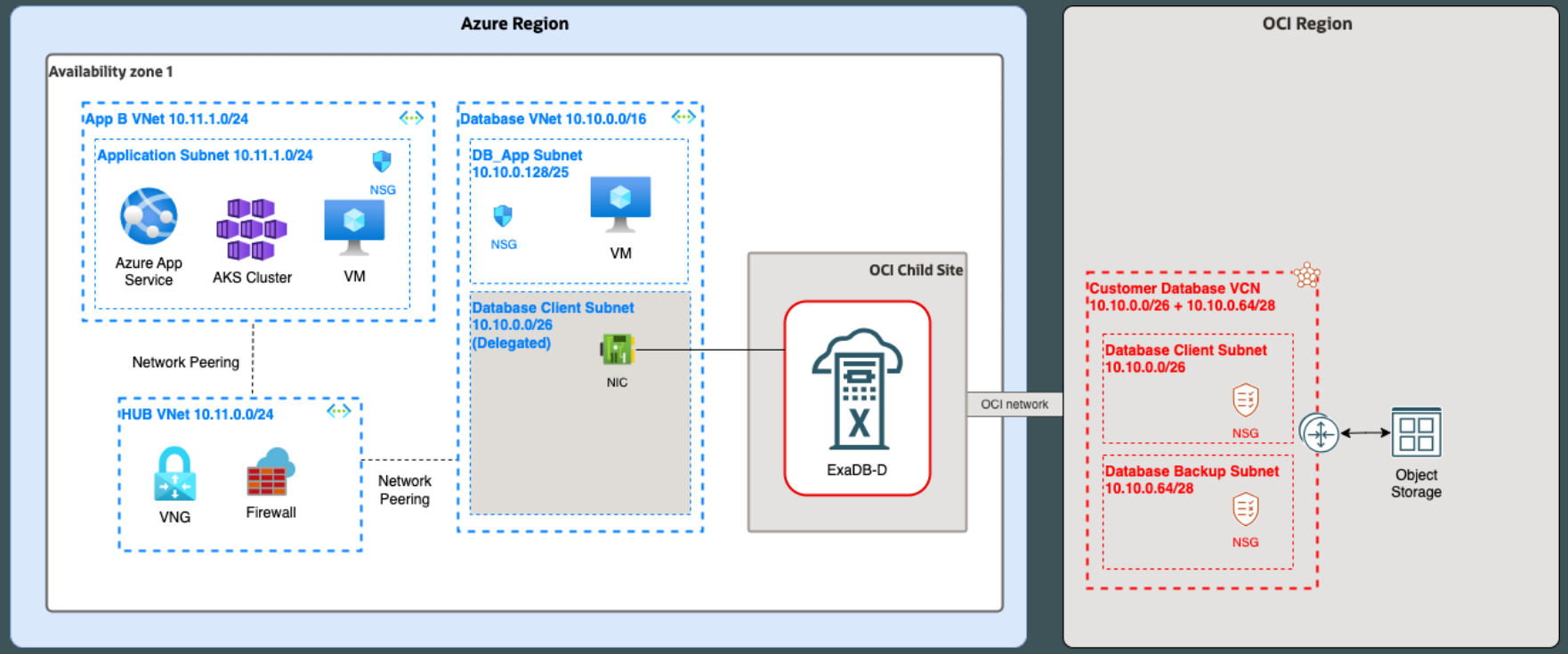


Example : 2x VM clusters on same Exadata Cloud Infrastructure

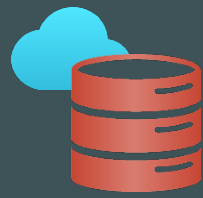
4. Azure Networking

NSG's (Network Security Groups)

- No NSG will be allowed to be associated with Azure delegated subnet used for Oracle Database@Azure
- Delegated subnet can be referenced by NSGs applied elsewhere in Azure
- Firewall in Hub VNet can be used to apply security rules from other spoke VNet's
- NSG in OCI can be used to limit access to DB client subnet



DNS with Oracle Database@Azure



Oracle Database
@Azure

5. Azure DNS

- There are different options for integration of DNS between Oracle Database@Azure and customer DNS solution

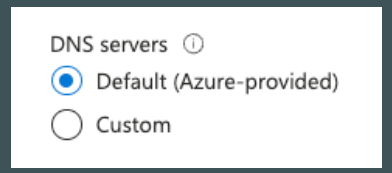
Use case	DNS in Azure	VM Cluster Networking	Fully Qualified Domain Name (FQDN)	Azure Subscription	Steps
Fully Managed	DNS Servers Default (Azure provided)	Uncheck private DNS Service	`*.oraclevcn.com`	Same as ExaDB-D	• Fully managed in Azure and OCI
Custom FQDN	DNS Service Default (Azure provided)	Check Private DNS Service	`*.yourdomain.com`	Any subscription	• Managed in OCI DNS Private View and Private zone • Add records in custom DNS zone • If needed, link private DNS zone to VNET
Custom FQDN	DNS Servers Custom (can be on-prem or in Azure)	Check Private DNS Service	`*.yourdomain.com`	N/A	• Managed in OCI DNS Private View and Private zone • Add records in custom DNS zone • If needed, link private DNS zone to VNET

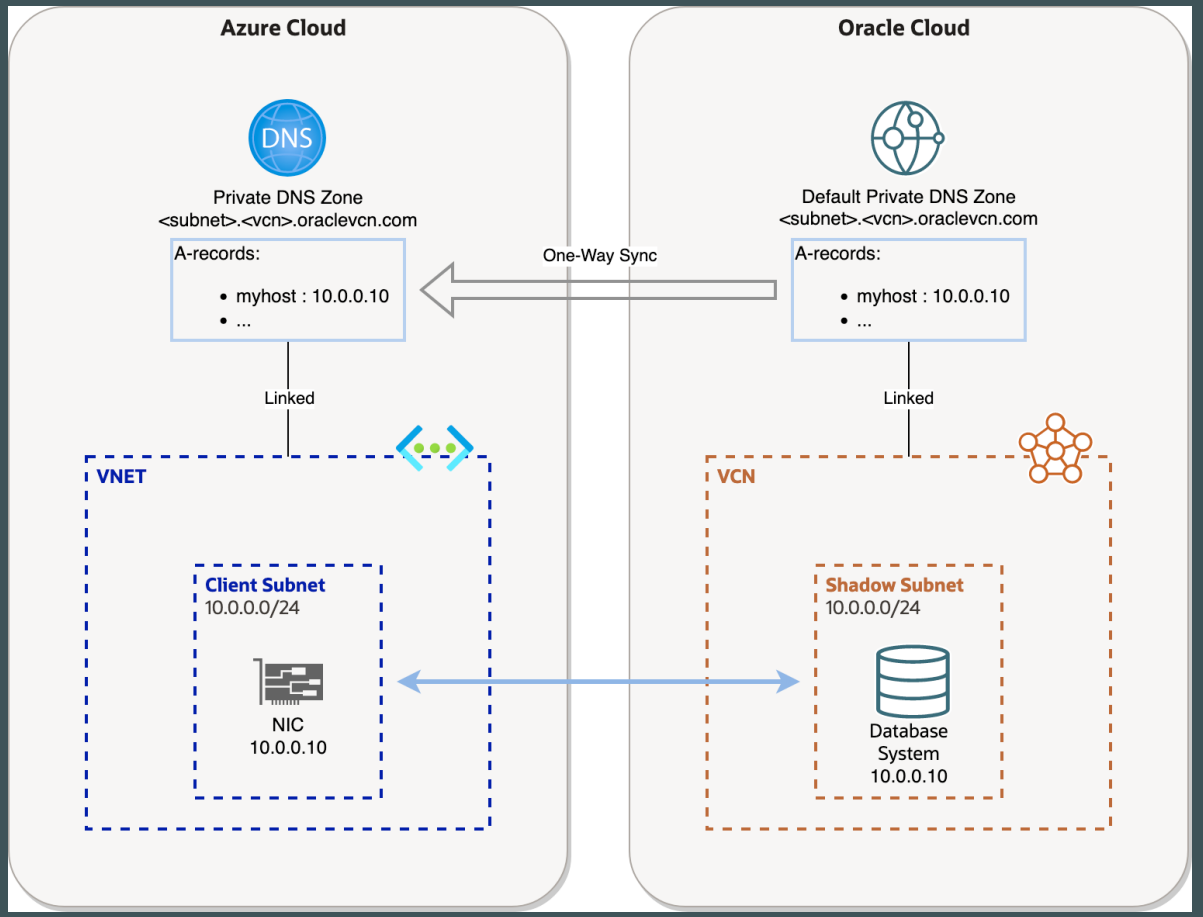
5. Azure DNS – Fully managed

Fully managed DNS resolution : FQDN will be `*.oraclevcn.com`

- don't check the checkbox called "Use private DNS service"

- Private DNS zone will be in same Azure subscription as ExaDB-D subscription
- Prereq : Using Azure DNS service

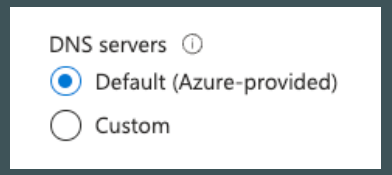


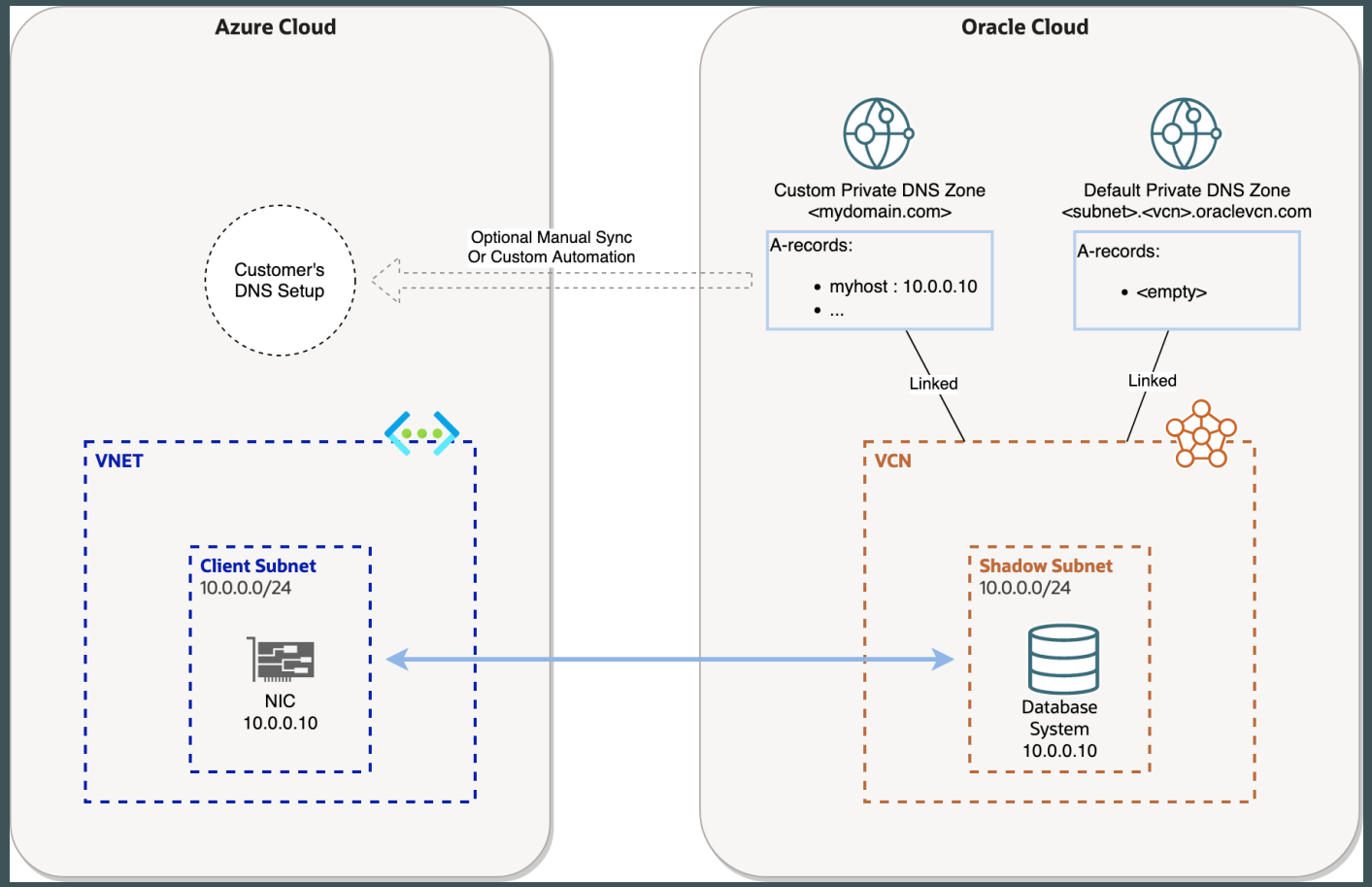


5. Azure DNS – Custom FQDN

FQDN will be of your choice: `*.yourdomain.com`

- Check the checkbox called “Use private DNS service”
- Private DNS zone can be in any Azure subscription
- Option : Using Azure DNS service or Custom DNS server



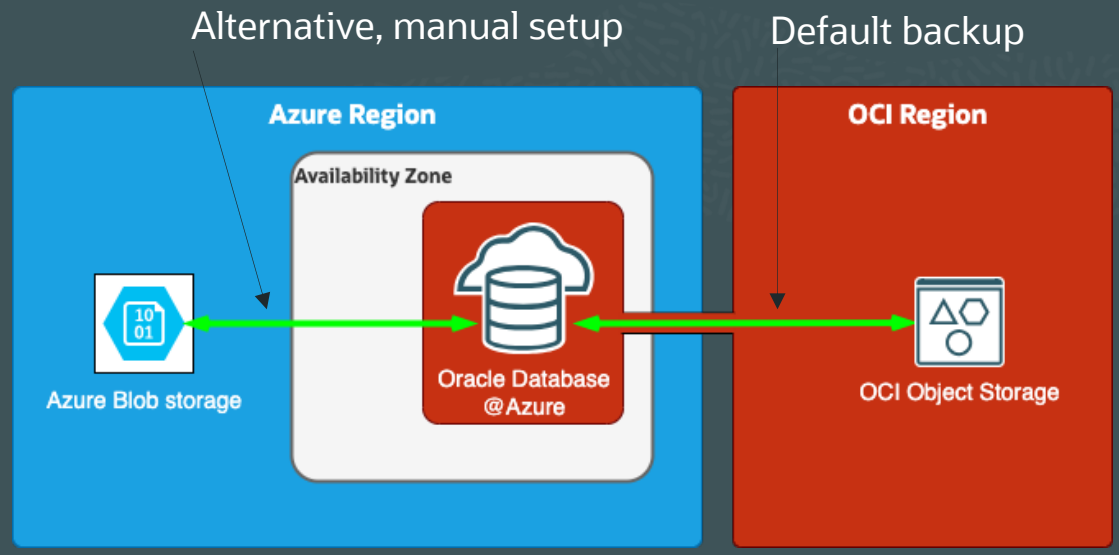


Backup options with Oracle Database@Azure

Oracle Database
@Azure

6. Backup/Restore

- Below table shows default backup for this solution and some of the other options



Backup Option	Info	Retention period	Backup Destination
Oracle managed backup	Default and recommended From OCI cloud tooling	Automatic backup Max 60 days retention Standalone backup = until deleted	OCI Object storage (Oracle Managed) Charged from Azure credits
User configured backup	Configure backups from the host using the `dbaascli database backup` and `dbaascli` database recover commands.	Defined by customer	OCI Object storage (Customer managed) Charged from OCI credits
Manual setup	RMAN (Recovery Manager) or other backup tools can be configured to do backup to Azure Blob Storage or OCI Object storage	Defined by customer	To Azure Blob storage or OCI Object storage Charged from Azure or OCI credits

Database Key managment options with Oracle Database@Azure

Oracle Database
@Azure

7. Database Key management

Key management options for Oracle Database@Azure

Option	Service	Info	
Oracle Managed keys	Wallet based	Default in Exadata Cloud Infrastructure	
Customer managed keys	OCI Vault (service in OCI, UCM credits needed)	Virtual Vault Multitenant partition	HSM Keys - A master encryption key protected by an HSM is stored on an HSM and cannot be exported from the HSM. All cryptographic operations involving the key also happen on the HSM. These keys are FIPS Level 3 compliant.
			Software Keys - A master encryption key protected by software is stored on a server and can be exported from the server to perform cryptographic operations on the client instead of on the server. While at rest, the software-protected key is encrypted by a root key on the HSM. These keys are FIPS Level 1 compliant.
		Private Vault** Own partition in HSM Better and consistent transactions per second for cryptographic operations Cross Region Replication Cross Region Back/Restore of Keys	HSM Keys - A master encryption key protected by an HSM is stored on an HSM and cannot be exported from the HSM. All cryptographic operations involving the key also happen on the HSM. These keys are FIPS Level 3 compliant.
			Software Keys - A master encryption key protected by software is stored on a server and can be exported from the server to perform cryptographic operations on the client instead of on the server. While at rest, the software-protected key is encrypted by a root key on the HSM. These keys are FIPS Level 1 compliant.
Customer managed keys	Oracle Key Vault* (license needed)	Software on VM, manual installation	

* Certification in progress

** Need for Data Guard setup

Identity and Access management with Oracle Database@Azure

Oracle Database
@Azure

8. Azure Identity - access to Oracle Cloud

- Database management (Oracle Home, CDB, PDB) are done through Oracle Cloud
- With Identity Federation from Microsoft Azure, user administration is simplifyied for those users
- Azure Identity federation is optional but recommended

Identity to use	Info
Normal Oracle cloud identity domain users i.e. create users in OCI console	No identity integration
OCI Federation with Microsoft Entra ID Recommended	Users who needs to access OCI uses their Microsoft Azure credentials Identity Federation with Microsoft Entra ID
OCI Federation with Microsoft Active Directory Federation Services	Users who needs to access OCI uses their Microsoft Active Directory credentials Identity Federation with Microsoft Federation Service

8. Azure Identity – Roles and Groups

Groups and roles in Azure created for this solution – for Infrastructure and VM cluster management

Group name	Role Assigned	Description
odbaa-exa-infra-administrators	odbaa-exa-infra-administrator	User of this group will be able to administrate ExaDB-D resources in Azure
odbaa-vm-cluster-administrators	odbaa-vm-cluster-administrator	User of this group will be able to administrate VM Cluster resources in Azure
odbaa-db-family-administrators	N/A	This group is replicate in OCI as part of the federation process, OCI policies will be attached to it.
odbaa-db-family-readers	N/A	This group is replicate in OCI as part of the federation process, OCI policies will be attached to it.
odbaa-exa-cdb-administrators	N/A	This group is replicate in OCI as part of the federation process, OCI policies will be attached to it.
odbaa-exa-pdb-administrators	N/A	This group is replicate in OCI as part of the federation process, OCI policies will be attached to it.

Groups and policies in OCI created for this solution – for database management

Group name	Policy	Description
odbaa-db-family-administrators	manage database-family	Group to manage DB family actions.
odbaa-db-family-readers	read database-family	Group to read DB family actions.
odbaa-exa-cdb-administrators	manage db-homes manage databases manage db-backups	Group to manage CDB actions.
odbaa-exa-pdb-administrators	manage pluggable-databases	Group to manage PDB actions.

HA and Disaster/Recovery options with Oracle Database@Azure

9. Disaster-Recovery and High-Availability – Basic info

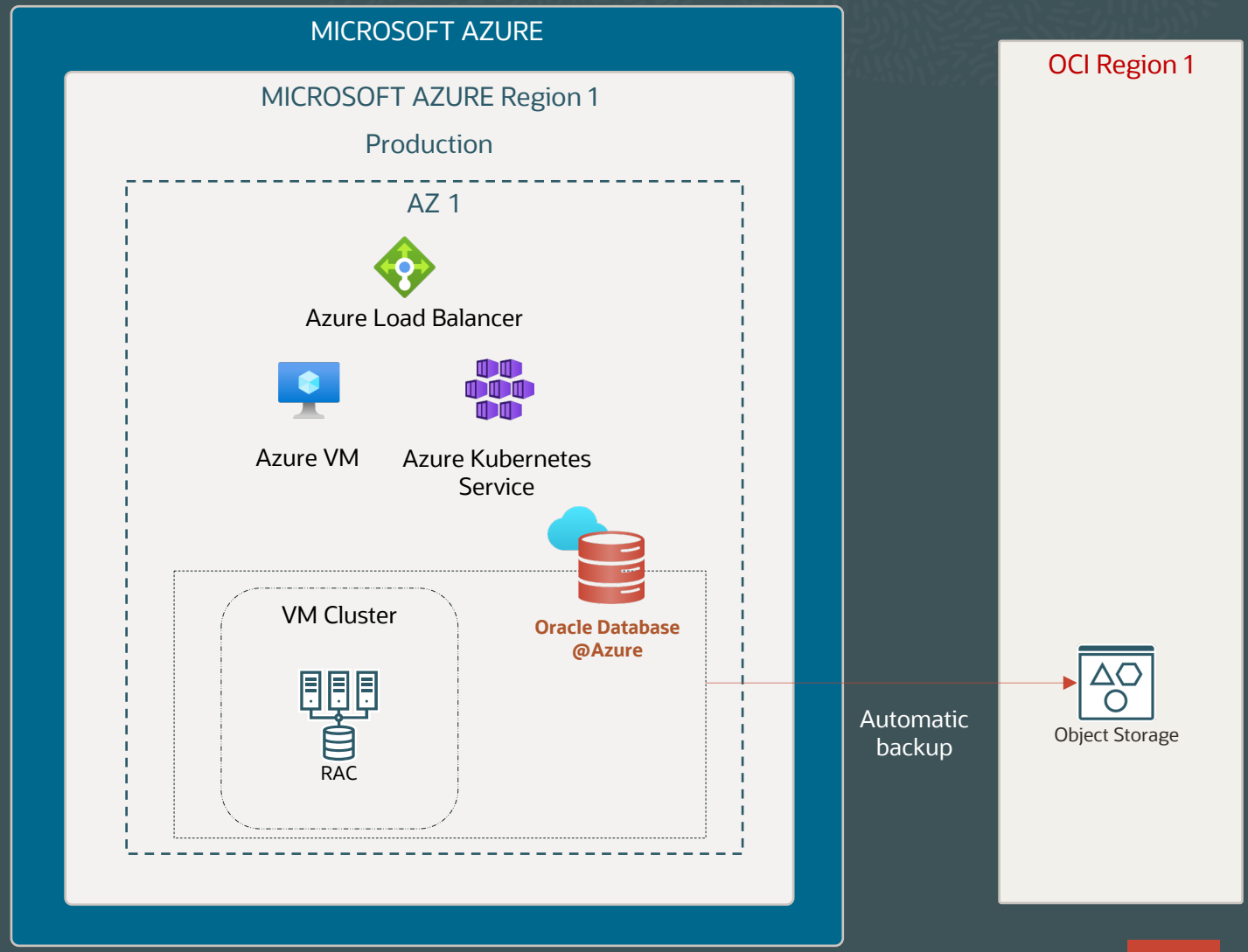
What is Oracle Maximum Availability Architecture (MAA)?

- A set of best practices developed by Oracle engineers over many years for the integrated use of Oracle High Availability, data protection, and disaster recovery technologies.
- The key goal of Oracle MAA is to meet the most demanding Recovery Objectives (RTO) and Recovery Point Objectives (RPO) requirements.
- Oracle Databases hosted on OCI enjoy built-in resiliency and availability benefits. Administrators can easily employ MAA when required.
- See High Availability Overview and Best Practices for detailed information about the validated Oracle MAA benefits.

7. Disaster-Recovery and High-Availability

MAA: Silver in default

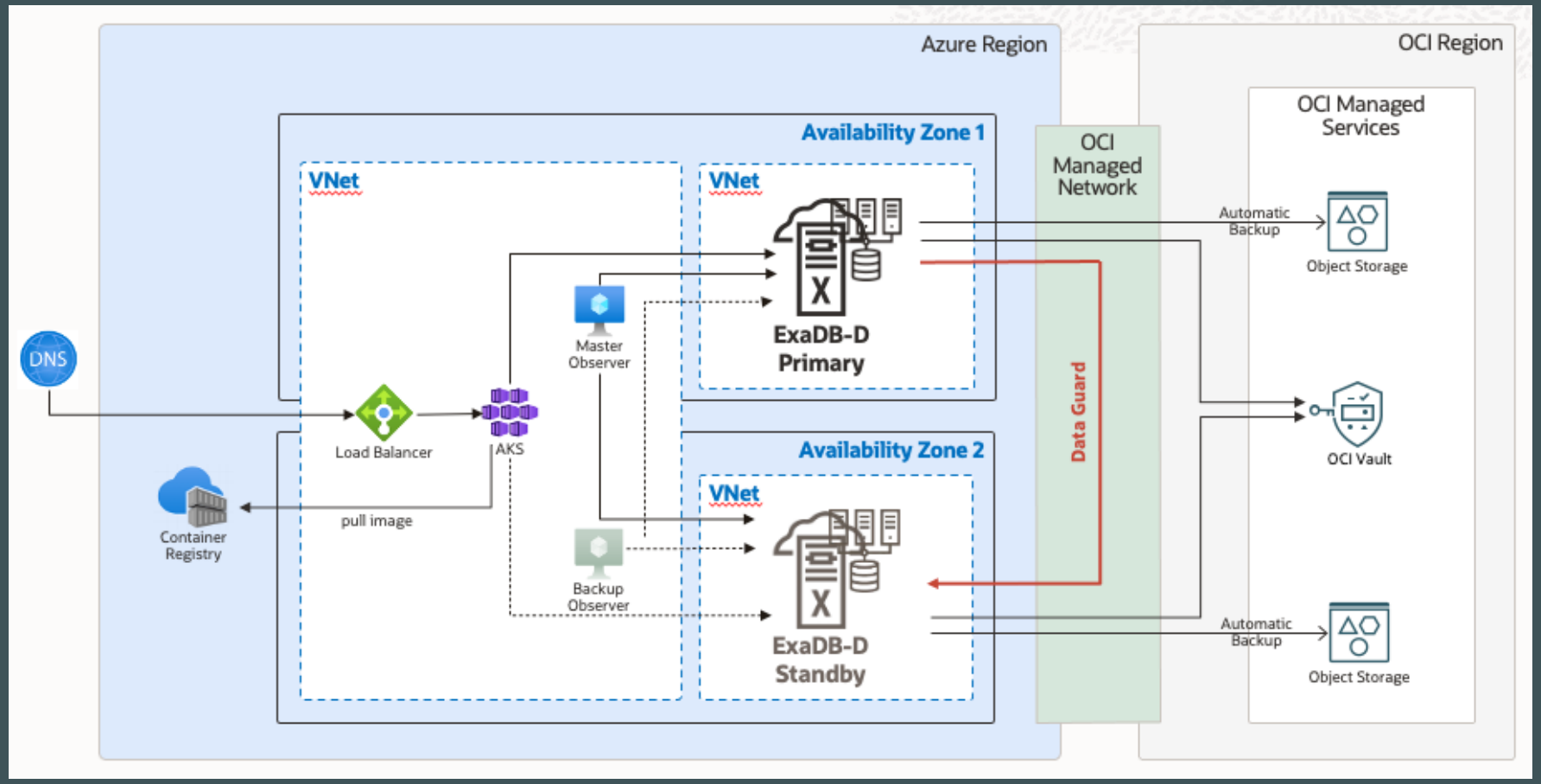
- Out of the box, 2x DB server and 3x storage nodes
- Residing within the same Azure Availability Zone
- SLO 99.9%, or max 22 minutes downtime per month by default.
- Backup to OCI Object Storage by default, which is automatically replicated to all AD's



9. Disaster-Recovery and High-Availability - Cross-AZ replication

MAA: Gold

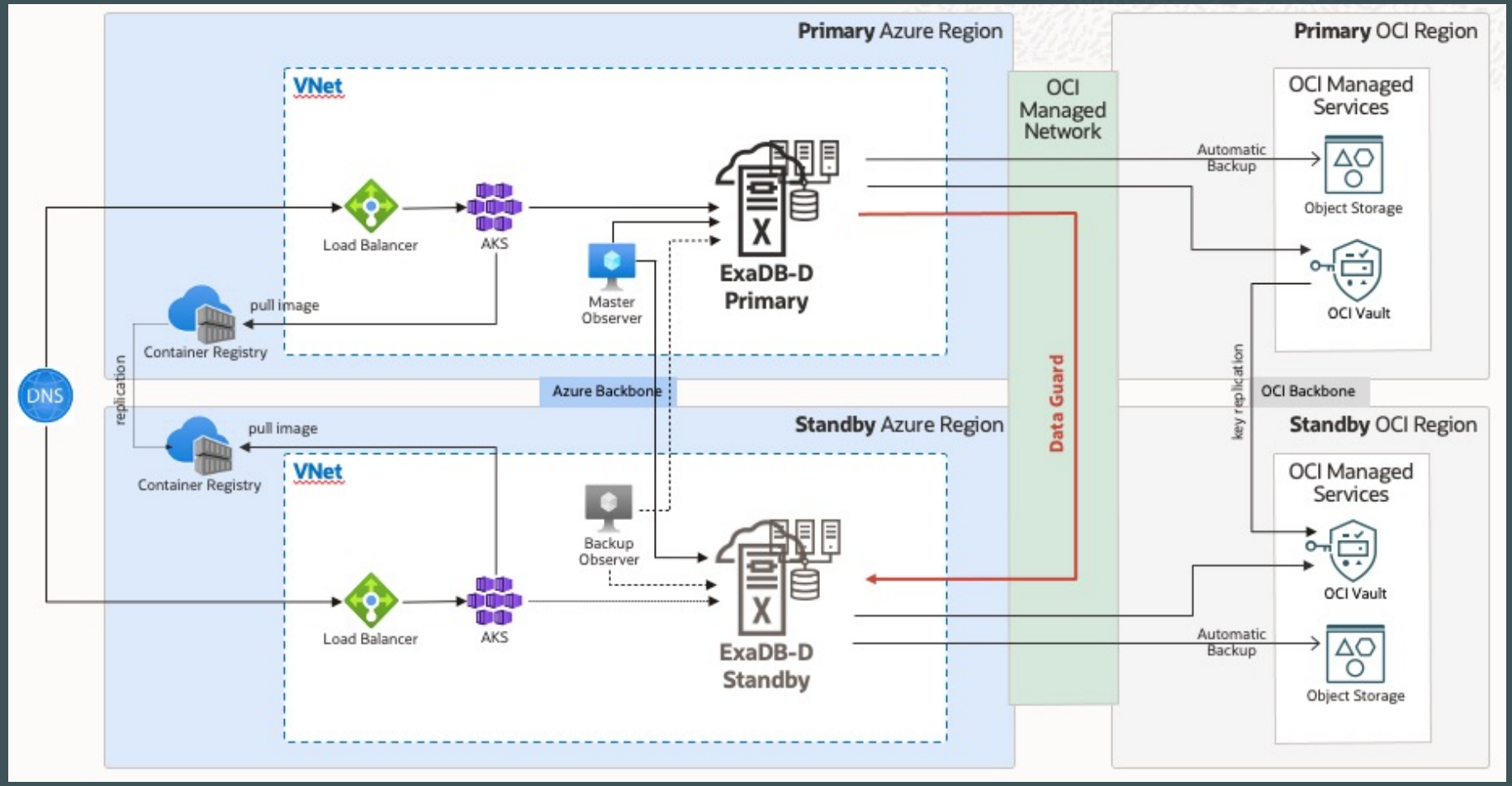
- The main system, with built in nodes as previously described, resides in AZ1
- A secondary system, with its own nodes, is deployed in another AZ.
- The two systems are paired with Data Guard for maximum resiliency.
- Fast-Start Failover to automate the database failover and reduce the recovery time without performing any manual steps.
- RPO within seconds



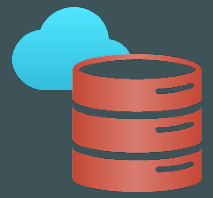
9. Disaster-Recovery and High-Availability - Cross-region replication

MAA: Gold

- The main system, with built in nodes as previously described, resides in Primary Region
- A secondary system, with its own nodes, is deployed in another Standby Region
- The two systems are paired with Data Guard for maximum resiliency.
- Fast-Start Failover to automate the database failover and reduce the recovery time without performing any manual steps.
- RPO within seconds



Automation & Integration with Oracle Database@Azure

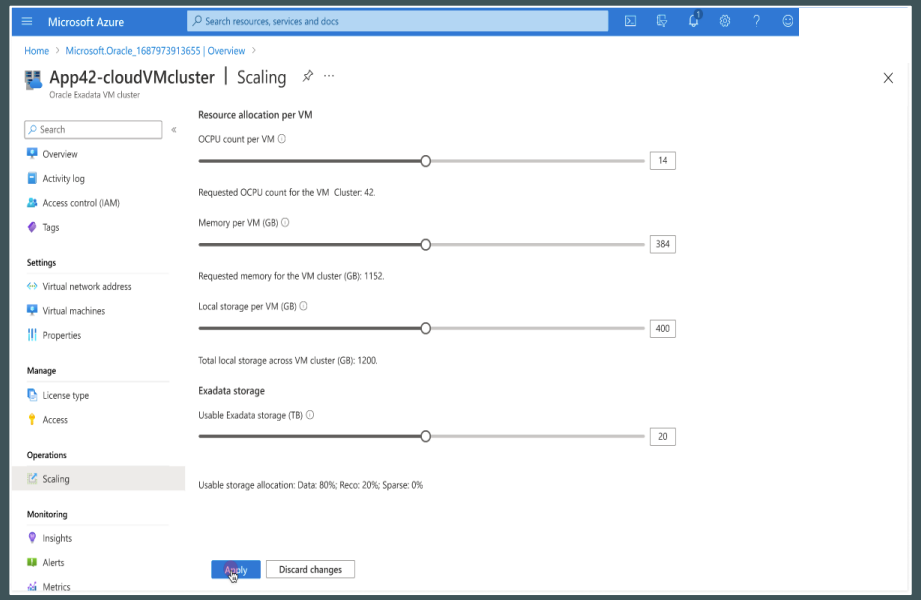


Oracle Database
@Azure

10. Automation & integration

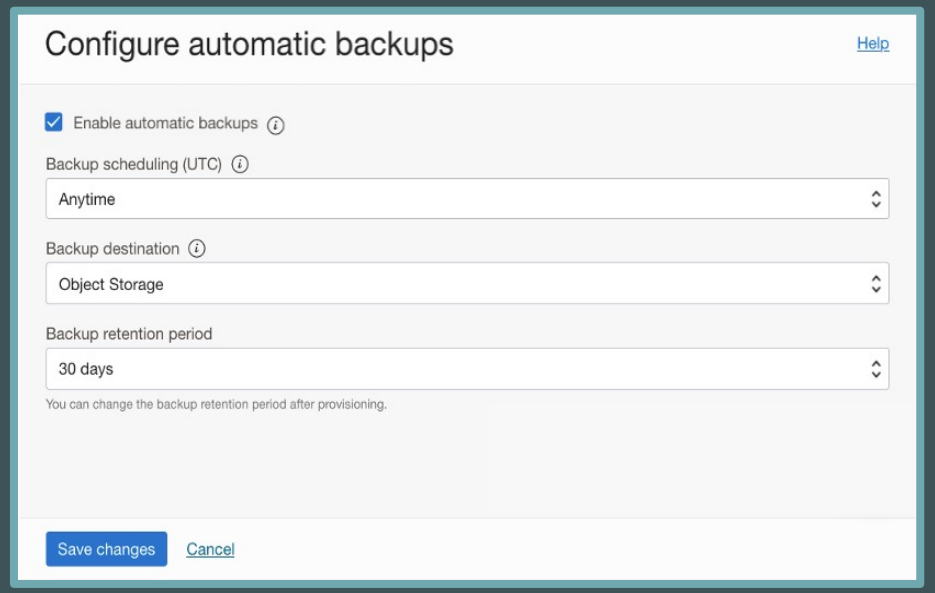
Microsoft Azure Portal UI REST APIs, SDK, CLI, Terraform

- Create Oracle Exadata Infrastructure and Exadata VM Clusters
- Schedule Infrastructure Maintenance
- Scale Servers and OCPUs (currently in OCI)

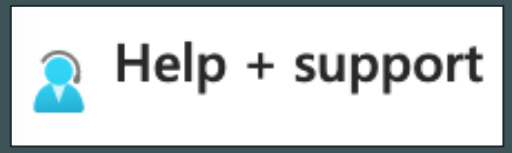


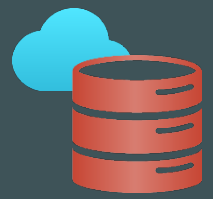
Oracle Cloud UI REST APIs, SDK, CLI, Terraform

- Create Database Homes and Databases
- Update Operating System, Grid Infrastructure, and Databases
- Backup and Recover Databases
- Enable Data Guard



Support & Compliance with Oracle Database@Azure





Oracle Database @Azure

13. Support and compliance

Oracle Database@Azure operates under a shared responsibility model:

- Oracle: security of the underlying cloud infrastructure and the connection between the Azure child site and the OCI parent site.
- Microsoft: physical security in Azure data centers and the logical connection security between the child site and the Azure substrate.
- Customers: securing their applications and workloads.

- Support Requests are raised with Oracle/Microsoft.
- Joint-effort support in collaboration between Oracle and Microsoft.
- SLA/SLO commitments are equivalent to those of Exadata on OCI and are guaranteed by Oracle.

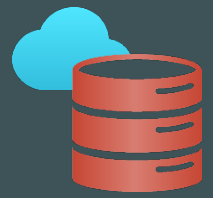
13. Support and compliance

The following compliance assessments are on the roadmap for H1 2024:

- SOC 1, 2 and 3.
- HIPAA.
- C5.
- CSA STAR.
- PCI DSS.
- ISO 9001, 20000-1, 27001, 27017, 27018, and 27701.
- HDS.

Note: while these compliance assessments are on the roadmap for H1 2024 – these are managed by third parties and as result, Oracle cannot guarantee outcome or timeframes for such.

Database Migrations with Oracle Database@Azure



Oracle Database @Azure

14. Database Migration
Migration methods

- The recommended migration method is Zero Downtime Migration (ZDM)
- It is a convenient approach with minimal downtime and seamless cutover
- ZDM is deployed on a VM, but its licensing is provided by Oracle free of charge

Other migration methods include:

Other options	Migration type	Downtime
Oracle Data Guard	Physical	Minimal / Seamless Cutover
Oracle GoldenGate	Logical	Minimal / Seamless Cutover
RMAN	Physical	Downtime Required
Oracle Data Pump (Conventional)	Logical	Downtime Required
Oracle Database Multitenant Operations	Physical	Downtime Required

14. Database Migration

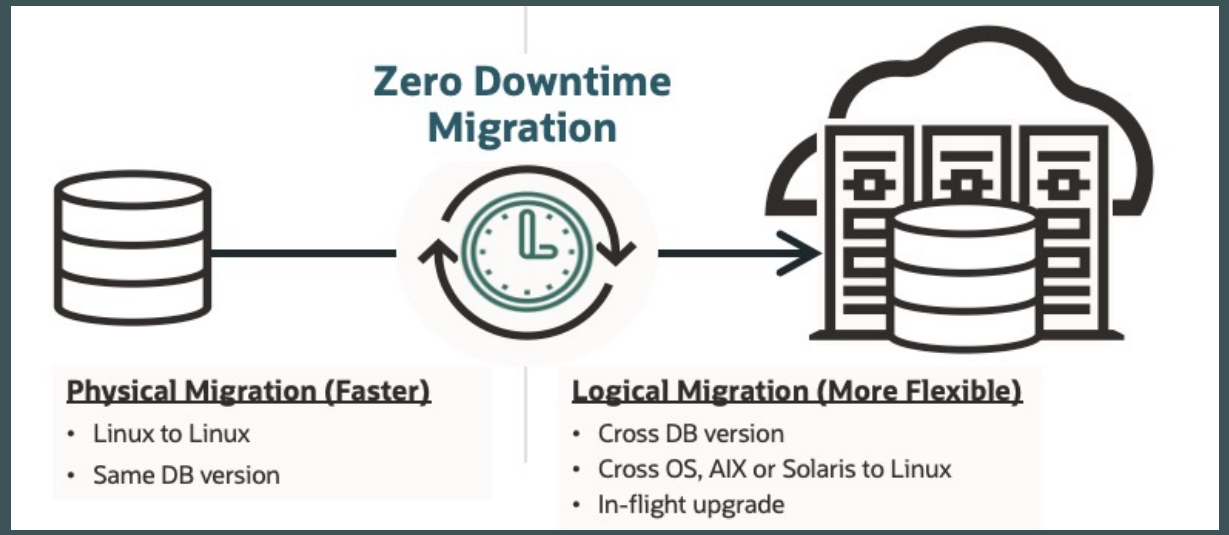
Oracle Zero Downtime Migration – Simple and Free!

Oracle Database Sources

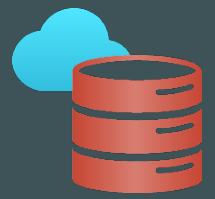
- On-premises deployments
- Cloud deployments
- Oracle Database Enterprise & Standard Editions
- Linux, AIX, Solaris
- RAC, RAC One Node, Single-Instance
- Non-CDB or CDB (Container Database)

Oracle Cloud Targets

- Oracle Exadata Database Service



Some requirements to discuss before Oracle Database@Azure deployments



Oracle Database
@Azure

15. Requirements

- Using a region where this solution is offered as of April 2024 :
  - Azure East US
  - West Germany Central
  - UK South
- Azure tenancy
  - Azure permissions (billing ID, roles, subscription needed)
- OCI tenancy to do account linking between Azure/OCI
  - Option 1 : Existing (IAM domain enabled)
  - Option 2 : New tenancy (no billing required)

Oracle Database
@Azure

15. Requirements

- The Azure user that creates the VM cluster should be part of less than 72 groups
- If OCI Vault or other services in OCI wanted, then UCM credits are needed

Oracle Database @Azure

Learn more about Oracle Database@Azure

Features, use cases, how it works, FAQs

Oracle.com/azure
Azure.com/oracle