Business continuity and disaster recovery (BCDR) for Oracle Database@Azure

Article • 02/08/2024

This article builds on the considerations and recommendations that are defined in the Azure landing zone design area for BCDR. Following the guidance, this article provides you with design considerations and recommendations surrounding business continuity and disaster recovery (BCDR) options for Oracle Database@Azure.

The first step to building a resilient architecture for your workload environment is to determine availability requirements for your solution by the recovery time objective (RTO) and recovery point objective (RPO) for different levels of failure. RTO is the maximum time an application is unavailable after an incident and RPO is the maximum amount of data loss during a disaster. After you determine the requirements for your solution, the next step is to design your architecture to provide the established levels of resiliency and availability.

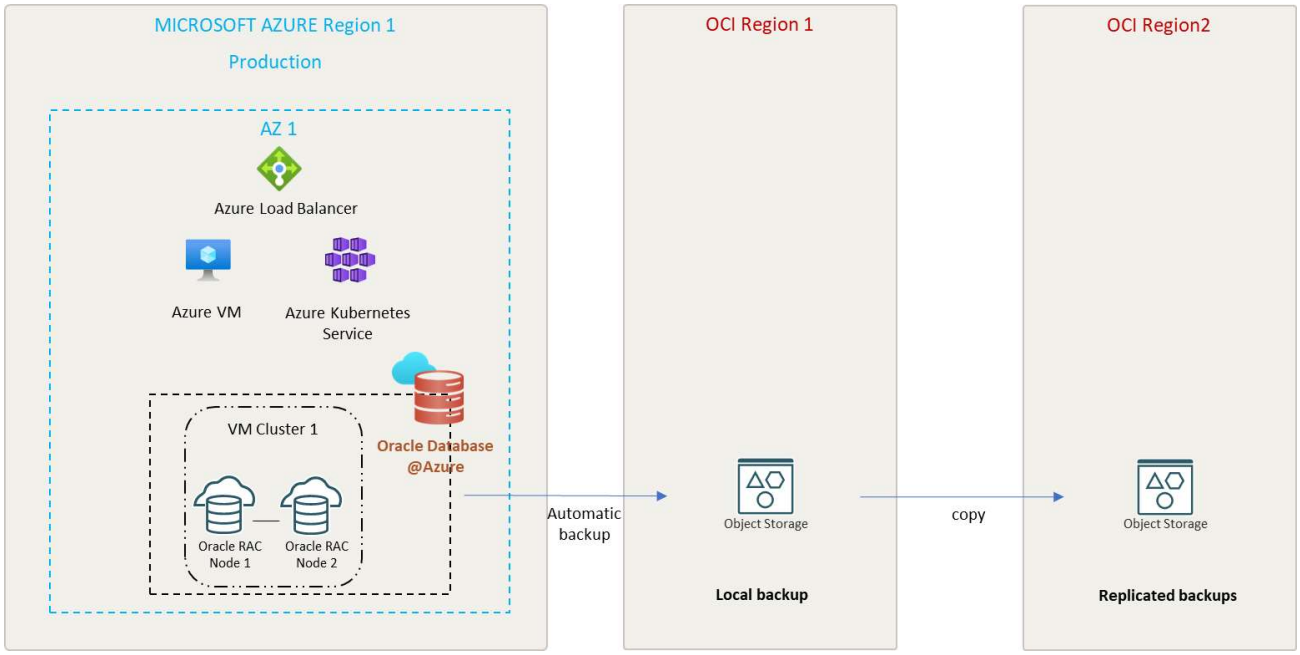
Design Considerations

- The Oracle Database@Azure appliance is placed in Azure Datacenters and can be placed in an Azure Availability Zone. In light of this it is important to remember that availability zones are specific to a subscription, i.e. availability zone 1 is not necessarily the same physical datacenter in one subscription as availability zone 1 in another subscription. This is described in more detail in What are availability zones
- The Oracle Database@Azure solution comes with connectivity to Oracle Cloud Infrastructure to be leveraged for RMAN backups (stored on OCI object storage) which are thus stored in a different cloud/data center entirely from the Azure Data Center where the Oracle Database@Azure appliance is situated.
- The Oracle Database@Azure solution, out-of-the-box, provides native Oracle technologies for high availability and disaster recovery, such as Real Application Cluster (RAC), Data Guard and Golden Gate. This is possible since the solution is in actuality Oracle Exadata CS, managed through Azure and OCI, but with the actual Exadata hardware placed in Azure Datacenters.
- The Oracle Database@Azure solution and core components are constrained to the subscription and region where the instance is created. The service is not multi-zonal and does not span multiple regions.

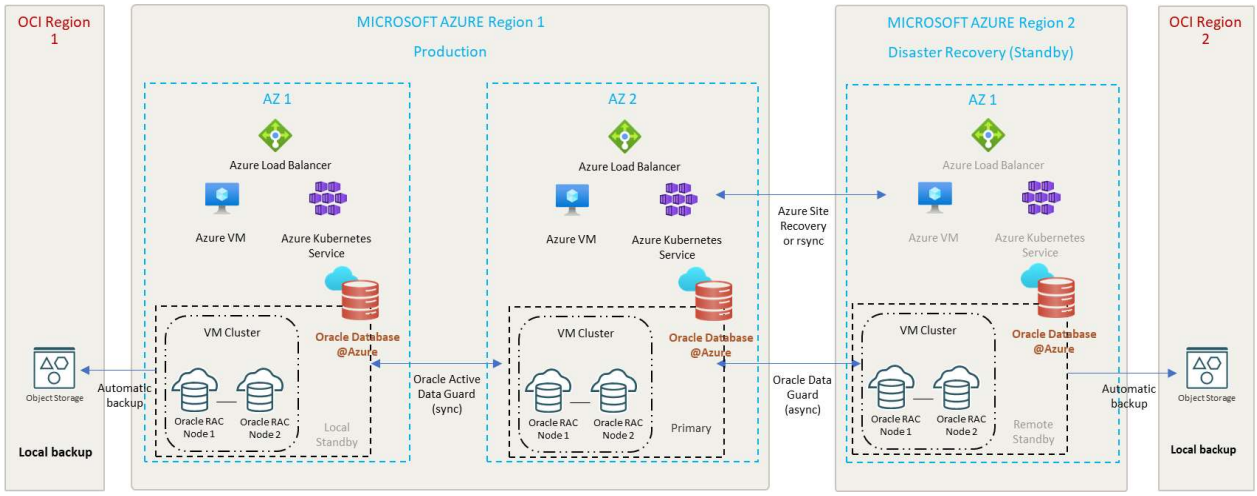
- High availability and disaster recovery for Oracle Database@Azure follows Oracle Maximum Availability Architecture (MAA) guidelines. See Oracle MAA Reference Architectures for more details. Note that the "Bronze" level of the Oracle MAA Reference Architectures is not covered in this article.
- The Oracle Database@Azure solution comes with built-in backup mechanisms (Oracle RMAN) that can be used to backup to OCI Object Storage. There is no integration to Azure Backup or Azure Recovery Vault.
- The Oracle Database@Azure solution can be accessed on the dataplane from Azure, access from e.g. VM clusters to Azure storage is pending further testing.
- The Oracle Database@Azure solution is available only in a limited set of regions, meaning that latency between regional failover options should be considered.

Design Recommendations

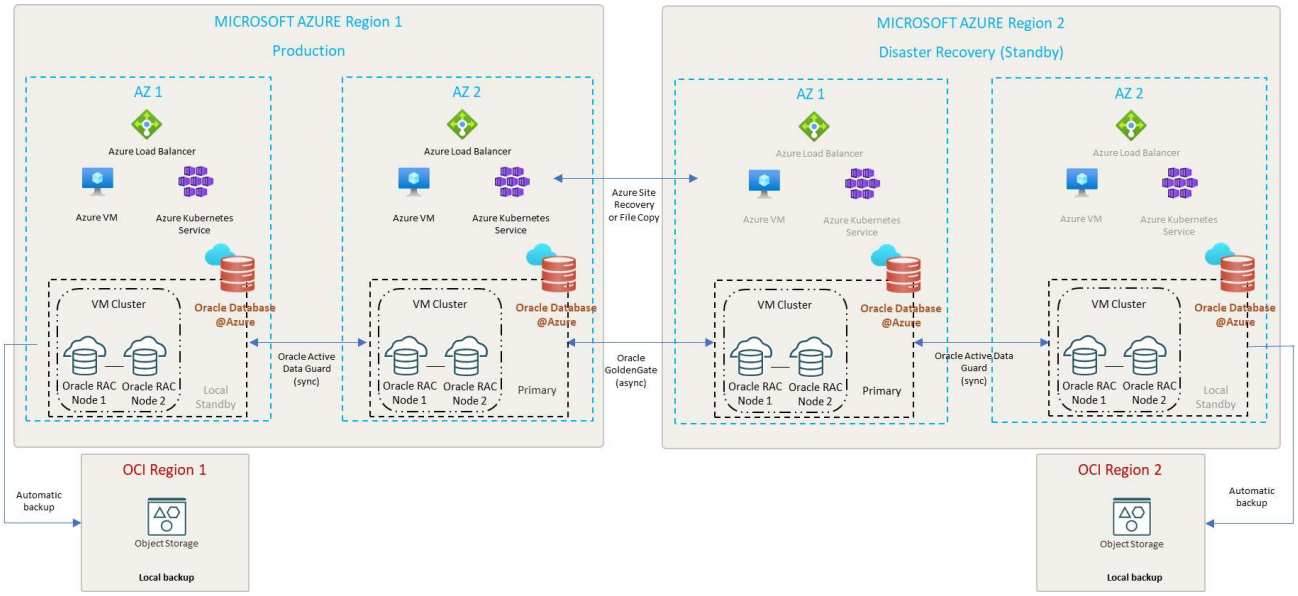
- For high availability leverage Oracle RAC and/or Data Guard in same availability zone depending on your requirements. This will enable you to achieve data center local resiliency for database services. For application services dependent on the database, be mindful that these should be in the same availability zone as the database services. This is particularly relevant if the application services are in a different subscription than the database services. If that is the case you should leverage the code found in What are availability zones and from the availabilityZoneMappings property determine the physical availability zone where the services should be co-located.
  - The above configurations would correspond to the "Silver" level of the Oracle MAA Reference Architectures if RAC is leveraged for HA and to the "Gold" level of the Oracle MAA Reference Architectures if Data Guard is leveraged for HA.
  - If you decide to use Data Guard for HA in the same availability zone, you are recommended to configure Data Guard in maximum availability mode since the proximity of the nodes should not necessitate the use of maximum performance mode. Maximum protection mode is not recommended for HA since that would require multiple nodes to avoid downtime in case of a failure on the secondary node.



- For disaster recovery leverage Data Guard in maximum performance mode with the secondary database in a different availability zone or in a different region depending on your requirements for disaster recovery. Depending on the specific requirements you may decide to have multiple secondaries in different availability zones and/or regions.
  - For availability zones the same considerations as for high availability applies, meaning that you should ensure that application services in other subscriptions than the database subscription are fault tolerant across the corresponding availability zones.
  - Resiliency for application services should be ensured through other means such as Virtual Machine Scale Sets, Azure Site Recovery, Azure Front Door or other features enabling application service availability across availability zones or regions.
  - For regional disaster recovery you are recommended to configure Data Guard with maximum performance mode as well, and depending on the network latency between regions you may decide to leverage Data Guard Far Sync to minimize the risk of data loss. For more details on network latency between regions see Azure Network Latency Test Results. For more details on Data Guard Far Sync see Oracle Data Guard Far Sync .
  - If you do decide on regional disaster recovery be mindful that you will need to instantiate an additional Oracle Database@Azure instance in the target region.
  - The above combination of configurations would correspond to the "Gold" level of the Oracle MAA Reference Architectures .



- For disaster recovery for globally distributed and partitioned databases where applications access and update a particular partition and data is eventually converged, but the constraints on data convergence are more relaxed, you are recommended to use Golden Gate replication in async mode between instances. This is only relevant for database instances that spans regions.
  - If multiple replicas are updated concurrently at any point, conflict detection and resolution must be configured.
  - Application switchover must be custom developed, it is not provided as rather than built in.
  - This particular architecture would correspond to the "Platinum" level of the Oracle MAA Reference Architectures .



- For backup of databases you are recommended to leverage managed backups, storing backup data to OCI Object Storage. As an extra precaution you could also mount Azure Storage (Azure Blob Storage, Azure Files or Azure NetApp Files) and stream backups to that.

fixme potential table for RTO/RPO

Additional Considerations

- Use Infrastructure-as-Code to deploy initial Oracle Database@Azure instance and VM Clusters. This will enable you to easily replicate the same deployment to a disaster recovery site and minimize the risk of human errors.
- Use Infrastructure-as-Code to deploy databases in Oracle Cloud Infrastructure. This will enable you to easily replicate the same deployment and will minimize the risk of human errors.
- Test failover and failback operations to ensure that you can execute them in a real disaster scenario. Automate failover and failback operations as much as possible to minimize the risk of human errors.

Next steps

fixme