Network topology and connectivity for Oracle Databases@Azure landing zone accelerator

Article • 02/08/2024

This article builds on several considerations and recommendations defined in Azure landing zone design area for network topology and connectivity. It offers key design considerations and recommendation for Oracle Databases@Azure networking and connectivity.

Design considerations

Consider the following when designing your network topology for Oracle Databases@Azure:

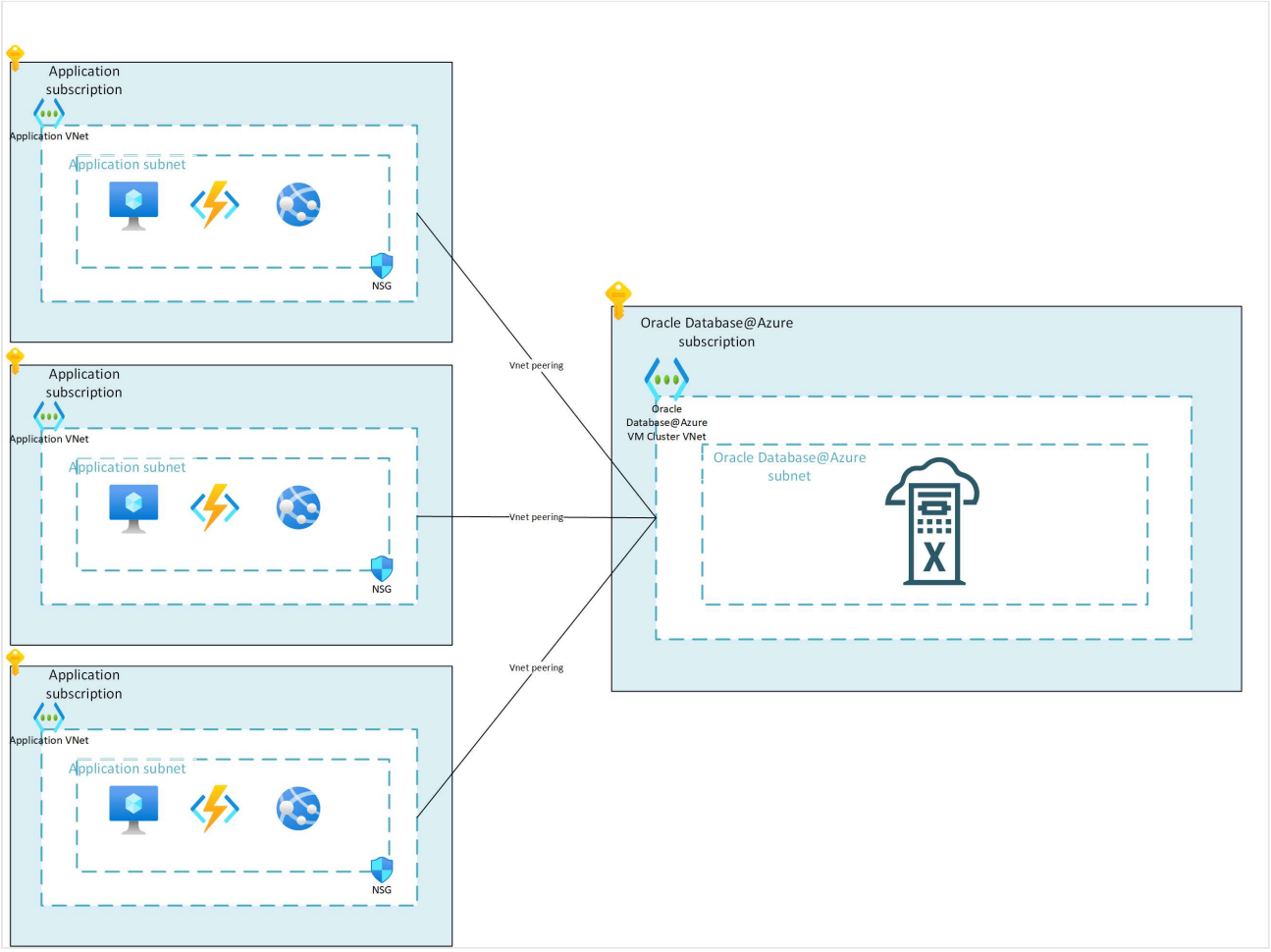
- The Oracle Database@Azure appliance is placed in Azure Datacenters and can be placed in an Azure Availability Zone. In light of this it is important to remember that availability zones are specific to a subscription, i.e. availability zone 1 is not necessarily the same physical datacenter in one subscription as availability zone 1 in another subscription. This is described in more detail in What are availability zones
- The scope for an Oracle Databases@Azure solution is constrained to the Azure subscription where it is deployed. This means that all VM Clusters and networking resources are deployed in the same subscription.
- Regardless of the Oracle Databases@Azure SKU deployed, you can deploy up to 8 VM clusters. Each VM cluster can be connected to a VNet which needs to exist prior to creating the VM Cluster. VM clusters can be connected to the same or different VNets.
- The Oracle Databases@Azure service is deployed in private subnets in Azure only. The service is not immediately accessible from the Internet.
- Minimum size of Oracle Database@Azure subnet depends on the SKU. See Fixme to be Azure product documentation for details.
- Network Security Groups and User Defined Routes are not supported on the Oracle Database@Azure subnet.
- As the Oracle Databases@Azure is deployed in private subnets only, there is no default name registration or resolution for database nodes.

Design recommendations

- Do not route traffic between application and database subnets through network appliances or firewalls of any kind, including Azure Firewall, as this will introduce latency. Instead leverage either direct subnet to subnet communication inside the same VNet or use VNet peering to connect the application and database subnets if they are in different VNets.
- If you have implemented Virtual WAN, and application and database subnets are in different VNets, use VNet peering to connect the application and database subnets. Do not use Virtual WAN to connect the application and database VNets as this will introduce latency due to the traffic being routed through the Virtual WAN hub.
- If you have one or a limited number of databases servicing a limited application portfolio managed by a single team, you should consider co-locating the application portfolio and database services in the same VNet. This will reduce latency and simplify the network design as well as meet Azure landing zone recommended practices for subscription democratization.
- If you have multiple databases servicing different applications manaaged by different teams, you should consider treating the Oracle Databases@Azure solution as a dedicated service. This means that you should deploy the Oracle Databases@Azure solution in one or more dedicated subscriptions, with application solutions in separate subscriptions, using VNet peering to connect the application and database subnets. This will allow you to manage the application and database subnets independently and meet Azure landing zone recommended practices for subscription democratization.
- To minimize latency between application and database, ensure that the application and database components are in the same region and availability zone. Specifically if you have application components in different subscriptions than the database components, 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.
- Since NSGs and UDRs are not supported on the Oracle Databases@Azure subnet, ensure that the following measures are taken:
  - Leverage NSGs on the application subnets to control traffic to and from the application subnets.
  - Leverage on-platform firewall products on the Oracle Databases@Azure VM clusters such as SELinux and cellwall to control traffic to the service.
  - Consider isolating the Oracle Databases@Azure VNET so that it is only peered to application VNETs and not to a HUB VNET.

- Leverage Azure Private DNS for name resolution between application and database subnets. See Azure Private DNS for details.

See below for potential network topologies for Oracle Databases@Azure.



See also

Manage and monitor Oracle Database@Azure landing zone accelerator fixme links to next subjects in the series fixme other relevant links to product documentation