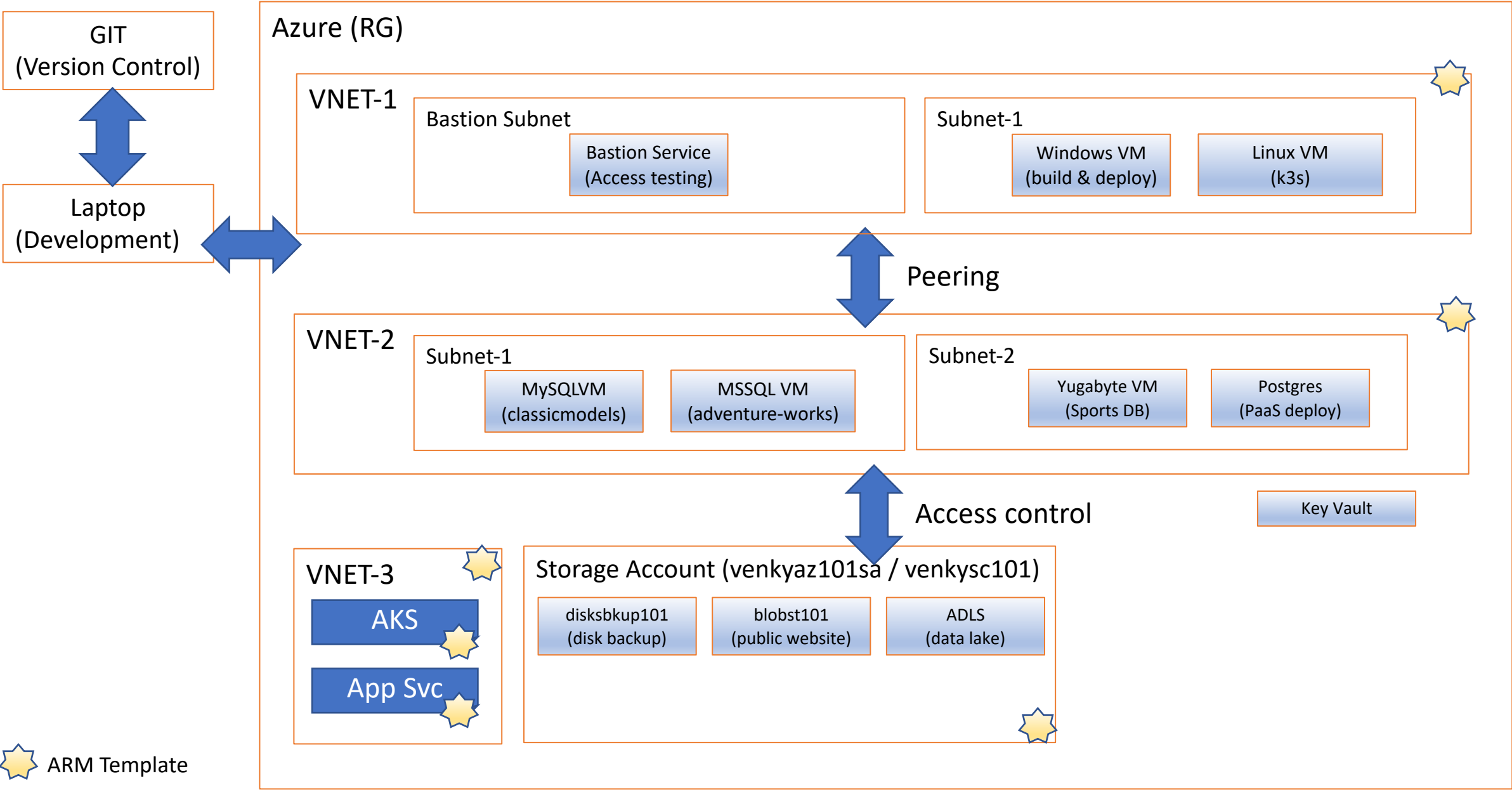


AZ-104 Notes

Sample Project Architecture



Implement and manage storage (15–20%)

Secure storage

- configure network access to storage accounts
- create and configure storage accounts
- generate shared access signature (SAS) tokens
- manage access keys
- configure Azure AD authentication for a storage account
- configure access to Azure Files

Manage storage

- export from Azure job
- import into Azure job
- install and use Azure Storage Explorer
- copy data by using AZCopy
- implement Azure Storage replication
- configure blob object replication

Configure Azure files and Azure Blob Storage

- create an Azure file share
- create and configure Azure File Sync service
- configure Azure Blob Storage
- configure storage tiers
- configure blob lifecycle management

Deploy and manage Azure compute resources (20–25%)

Automate deployment of virtual machines (VMs) by using Azure Resource Manager templates

- modify an Azure Resource Manager template
- configure a virtual hard disk (VHD) template
- deploy from a template
- save a deployment as an Azure Resource Manager template
- deploy virtual machine extensions

Configure VMs

- configure Azure Disk Encryption
- move VMs from one resource group to another
- manage VM sizes
- add data disks
- configure networking
- redeploy VMs
- configure high availability
- deploy and configure virtual machine scale sets

Create and configure containers

- configure sizing and scaling for Azure Container Instances
- configure container groups for Azure Container Instances
- configure storage for Azure Kubernetes Service (AKS)
- configure scaling for AKS
- configure network connections for AKS
- upgrade an AKS cluster

Implement and manage virtual networking

- create and configure virtual networks, including peering
- configure private and public IP addresses
- configure user-defined network routes
- implement subnets
- configure endpoints on subnets
- configure private endpoints
- configure Azure DNS, including custom DNS settings and private or public DNS zones

Secure access to virtual networks

- create security rules
- associate a network security group (NSG) to a subnet or network interface
- evaluate effective security rules
- implement Azure Firewall
- implement Azure Bastion

Configure load balancing

- configure Azure Application Gateway
- configure an internal or public load balancer
- troubleshoot load balancing

Monitor and troubleshoot virtual networking

- monitor on-premises connectivity
- configure and use Azure Monitor for Networks
- use Azure Network Watcher
- troubleshoot external networking
- troubleshoot virtual network connectivity

Integrate an on-premises network with an Azure virtual network

- create and configure Azure VPN Gateway
- create and configure Azure ExpressRoute
- configure Azure Virtual WAN

Create and configure Azure App Service

- create an App Service plan
- configure scaling settings in an App Service plan
- create an App Service
- secure an App Service
- configure custom domain names
- configure backup for an App Service
- configure networking settings
- configure deployment settings

Manage Azure identities and governance (15–20%)

Manage Azure Active Directory (Azure AD) objects

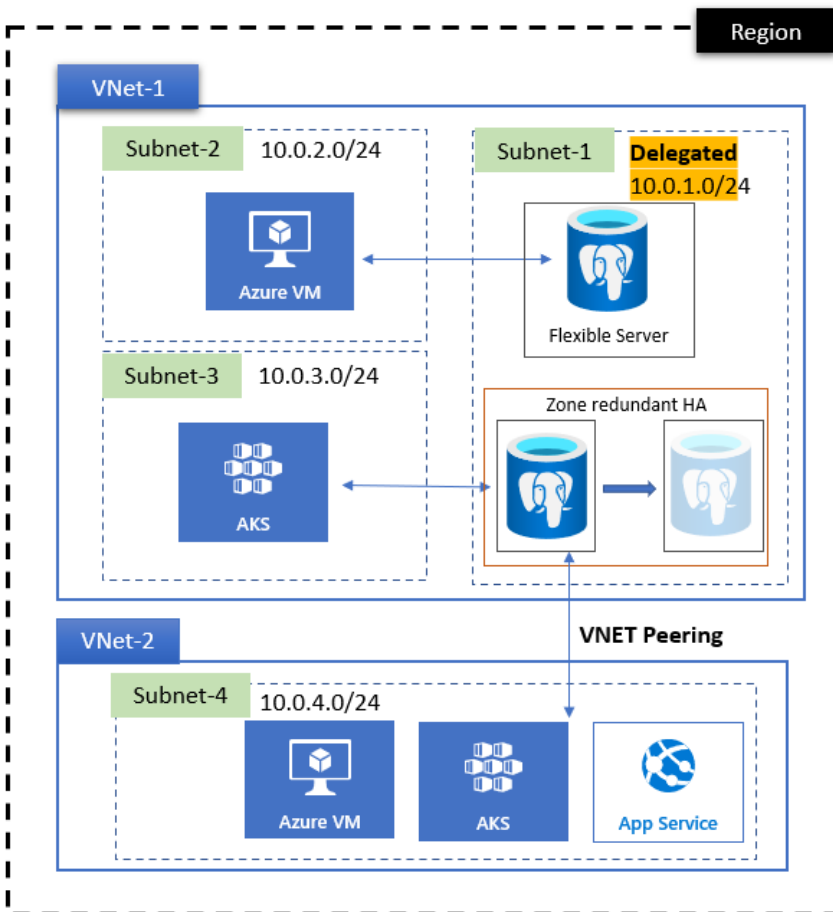
- create users and groups
- create administrative units
- manage user and group properties
- manage device settings
- perform bulk user updates
- manage guest accounts
- configure Azure AD join
- configure self-service password reset

Manage role-based access control (RBAC)

- create a custom role
- provide access to Azure resources by assigning roles at different scopes
- interpret access assignments

Manage subscriptions and governance

- configure Azure policies
- configure resource locks
- apply and manage tags on resources
- manage resource groups
- manage subscriptions
- manage costs
- configure management groups



Monitor and back up Azure resources (10–15%)

Monitor resources by using Azure Monitor

- configure and interpret metrics
- configure Azure Monitor logs

- query and analyze logs
- set up alerts and actions
- configure Application Insights

Implement backup and recovery

- create a Recovery Services vault
- create a Backup vault
- create and configure backup policy
- perform backup and restore operations by using Azure Backup
- perform site-to-site recovery by using Azure Site Recovery
- configure and review backup reports

- Build a windows VM and enable IIS
- Build a Linux VM and install nginx
- Add disk to VM
- Encrypt disk with key in key-vault + encryption set
- Configure Azure Disk Encryption (Note lock in windows for ADE disks)
- VM with Premium disks (Note not all VMs support it, specific VMs do)
- Take a snapshot of a disk
- Create un-managed disk and store into a storage account.
- Windows custom script extensions (from storage acct)
- Linux custom script extensions (from storage acct)
- Cloud-init scripts for Linux VM
- Serial Console and Boot Diagnostics
- Run Command to execute a power shell script on VM
- Bastion service
- Password reset for VM
- Redeploy VM to move it to a different host.
- Availability Set. (Fault & Update domain)

We have to ensure no virtual machine is associated with the availability set. So to delete the availability set, you can first delete the virtual machines linked to the availability set and then go ahead and delete the availability set.