# Vnet, VMs

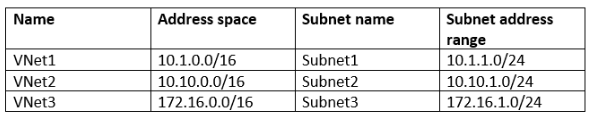
“Resource group 1” contains “Virtual Network 1”  
“Resource group 2” contains “Virtual Network 2” (no connectivity for vnet1)

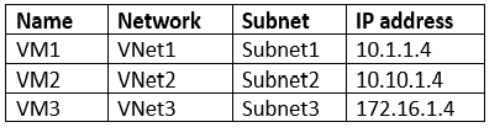
A VM gets created with a disk in vnet1 🡪 we want to move it to vnet2  
**We can’t move about VMs between networks 🡪 we have to identify the disk the VM uses, delete the VM and recreate it in vnet2 and attach the original disk.**

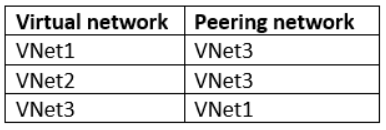
We have two subscriptions in two AD tenants.  
Subscription1 has vnet1, VM1, IP space 10.0.0.0/16  
Subscription2 has vnet2, VM2, IP space 10.10.0.0/24  
Let’s connect vnet1 to vnet2: **First, provision virtual network gateways***(we don’t need to modify address spaces, if we do it after connected, it’ll be updated automatically in the gateway)*

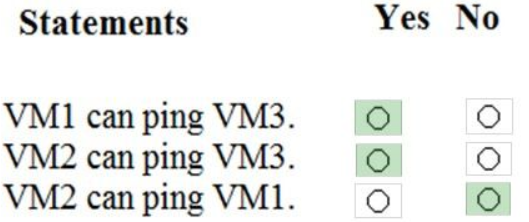
We plan to deploy 5 VMs to a subnet, each VM has public and private IP addresses, they require the same in-, and outbound security rules: how many network interfaces and network security groups we need? **5 VMs require 5 network interfaces. But 1 security rule is enough cause they share the inbound and outbound rules.**

VM1 in RG1, it runs services that deploy resources to RG1. Ensure that these apps in VM1 can manage resources in RG1 by using VM1’s identity: **Modify the value of the Managed Identity Service option for VM1**



  
VM firewalls configure to enable ICMP traffic (Internet Control Message Protocol)  
We have to create this:





**VM2 can’t ping VM1, because even though Vnet2 can peer Vnet3 and Vnet3 can peer Vnet1, it doesn’t work like that – it must be direct peering between networks.**

We have a subscription with 100 VMs. We regularly create and destroy VMs. We need to identify unattached disks which we can delete: **Azure Cost Management: Optimizer tab, create report**

We have a 10 VMs, we want to be notified via email whenever any of them are powered off, restarted or deallocated – how many rules and action groups do we need? **1 action group, 3 rules***3 separate rule for each condition, 1 action group for what to do (send email)*

We want to automate the deployment of VM Scale Set that uses Windows Server 2016 Datacenter image – when the scale set is provisioned, we need to ensure they have the web server components installed  
**1. Create a new VM Scale Set in the portal  
2. Modify the “extensionProfile” section of the ARM template**

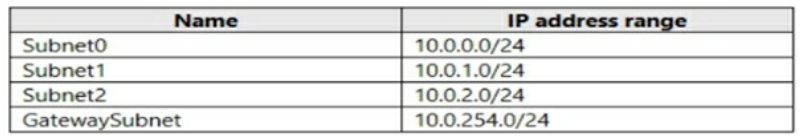
We have a lot of VMs, we want to know which is underutilized so we can scale it back down.  
**Use the “Advisor” tab from Cost**

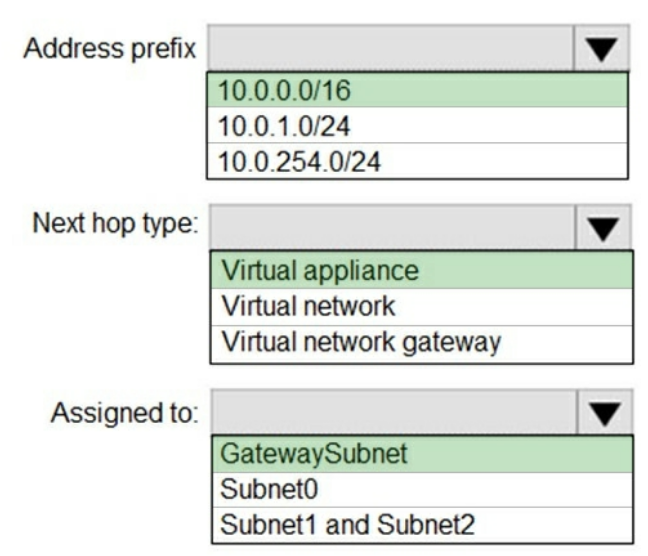
We have an app that uses a VNet with 2 subnets  
- One subnet is for app server  
- One subnet is for DB server  
Network Virtual Appliance is used as a firewall  
Traffic for one of the addresses is prefixed and routed to the NVA, then to on prem DB server  
Border Gateway Protocol (BGP) route is used for on prem DB server  
We need to create user defined route  
**- For the virtual network configuration, use a VPN  
- For the next hop type, use a Virtual Network Gateway***These user defined routes override Azure’s default system routes, or add additional routes to the subnet’s route table.  
Virtual Appliance: just a VM that typically runs a network app, like a firewall.  
Virtual Network Gateway: Specify when you want traffic destined for specific address prefixes routed to a virtual network gateway –* ***this must be used with a VPN. Cannot be ExpressRoute in user defined route, cause ExpressRoute must be Border Gateway Protocol.***

**We cannot specify VNet peering or Virtual Network Service Endpoint as the next hop type in user defined routes – these are only created by Azure.**

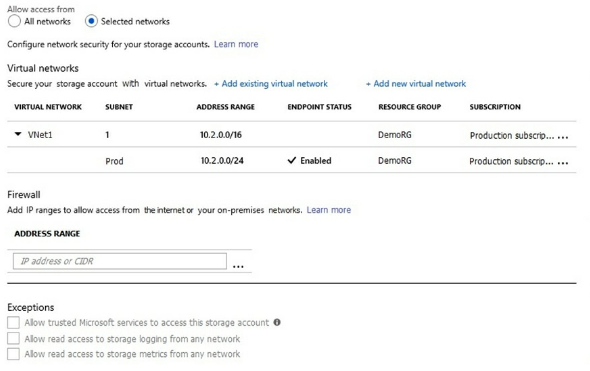
**We cannot specify a Virtual Network Gateway created as ExpressRoute, cause if user defined, it must use BGP.**

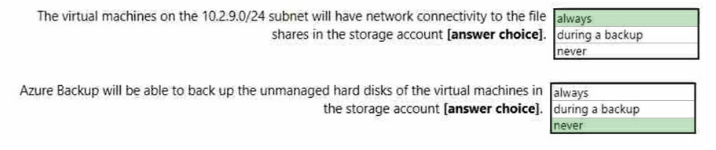
We have 1 single VM, but the traffic to it increased a lot. We need to scale without downtime, scale rules dynamic.  
**Create VM scale set  
Deploy application automatic horizontal scaling  
Deploy custom auto-scale implementation**

We have a single vnet, IP: 10.0.0.0./16, with subnets:  


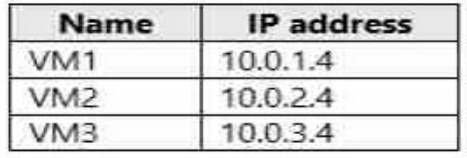
Subnet1 has a Virtual Appliance (VM1, it operates as a router)  
We create a routing table RT1  
We need to route all inbound traffic to VNet1 through VM1  
**How do we configure RT1?**

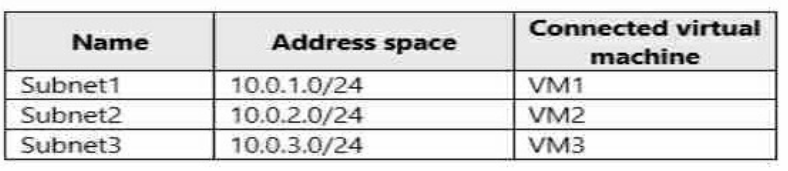
We have 10 vnets in one subscription, but in different resource groups.  
An admin plans to create several network sec. groups (NSGs)  
We want these to automatically block TCP port 8080 between vnets.  
**A resource lock, which we assign to lock the subscription is not sufficient 🡪 that just makes sure resources are not accidentally deleted**

We have a few VMs on vnet1.  
We configure a Storage Account  


 **(1st, because its enabled. 2nd because the checkbox is unticked: Allow trusted Microsoft services to access this storage account)**

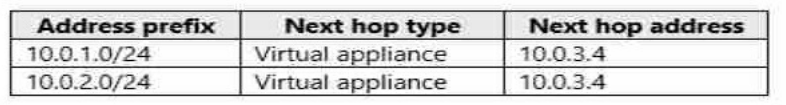
We have a subscription with these VMs and subnets:





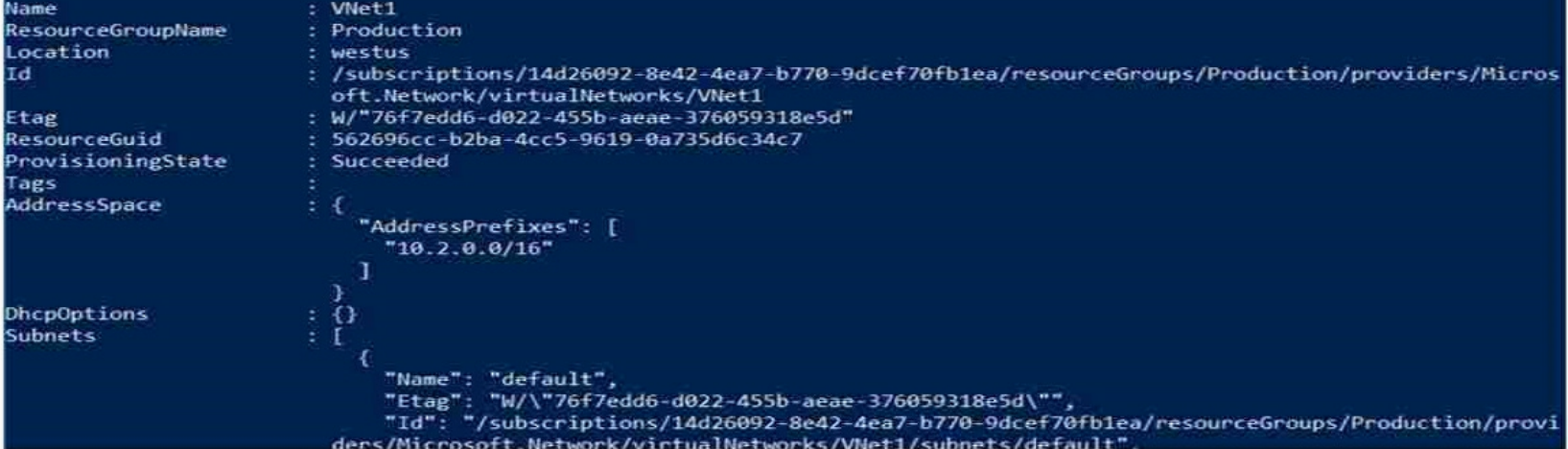
VM3 has multiple network adapter, including NIC3, which IP forwards, and routing is enabled in VM3 as well.

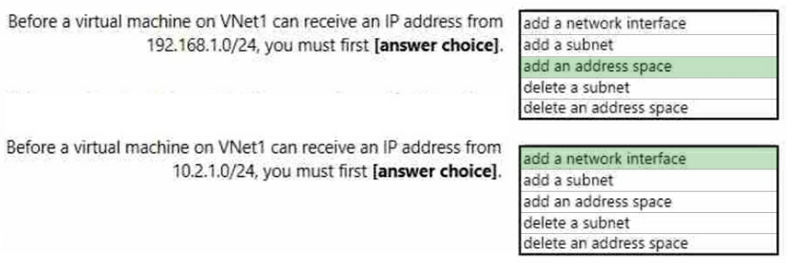
We have this routing table, applied to Subnet1, Subnet2:

****

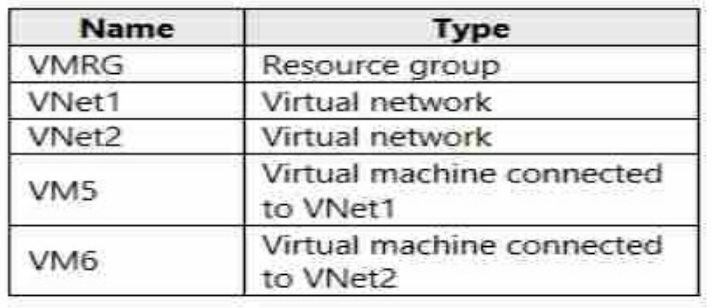
**Can VM3 establish network connection to VM1? Yes** (VM3 can connect to both VM1 and VM2) **If VM3 is turned off, can VM2 establish connection to VM1? No** (VM3 does IP forwarding, but only when turned on) **Can VM1 establish network connection to VM2? Yes** (Table allows from VM1 and VM2 to VM3, and IP forwarding allows VM1 to connect to VM2 via VM3)

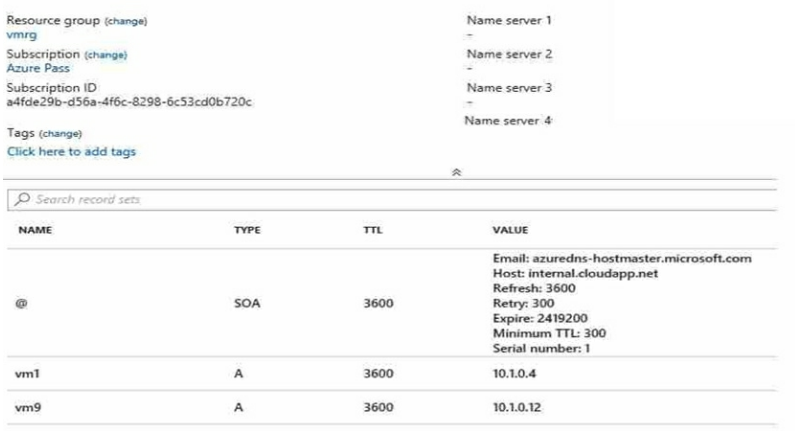
We have Vnet1:

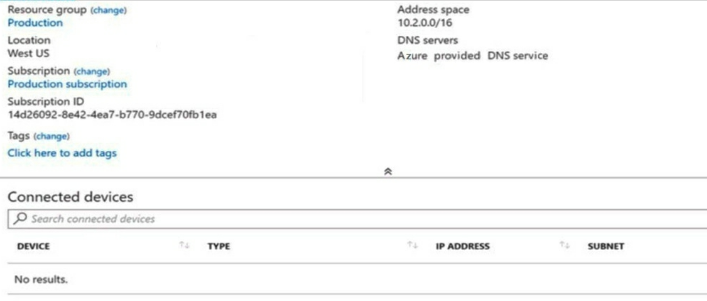




**Address space:** IaaS and PaaS stuff in vnet automatically has private IP addresses which we specify, based on the address space of the subnet they are connected to. We need to add this public IP to the address space.  
**Network interface:** The IP here already exists in the subnet, so we need just a network interface.

We have this:  
  
In Azure, we create a DNS zone called adatum.com  
Registration vnet is Vnet2.


We have a vnet:  


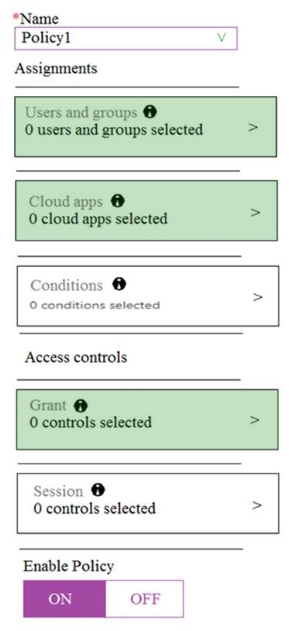
We have vnet2 in the same region (10.2.0.0/16), we want to peer vnet1 with this.  
**First we need to modify vnet1’s address space: it’s the same as vnet2 (they must not overlap)**

We want to backup all VMs at 2 AM, we need to prepare the environment to ensure that new VMs can be configured quickly for backup. 2 AM daily backups should be retained for 90 days.  
**Create a Recovery Services Vault  
Add -> Backup -> Backup Global -> Where’s the workload running? Azure -> What to backup? VMs  
To create the schedule, Microsoft Azure Backup agent (in VM) -> Schedule backup**

# Azure AD

We have a resource group in which someone creates some resources with ARM templates.  
We need to view the ARM templates that was used 🡪 **Azure Portal’s resource group blade**

AD tenant has conditional access policy Policy1 (enforces use of AD joined devices when members of Global Admin group authenticate to Azure AD from untrusted locations). We need to enforce MFA from untrusted locations: **Modify grant control of Policy1 (but its now possible to explicitly apply “require MFA for admins” rule)**

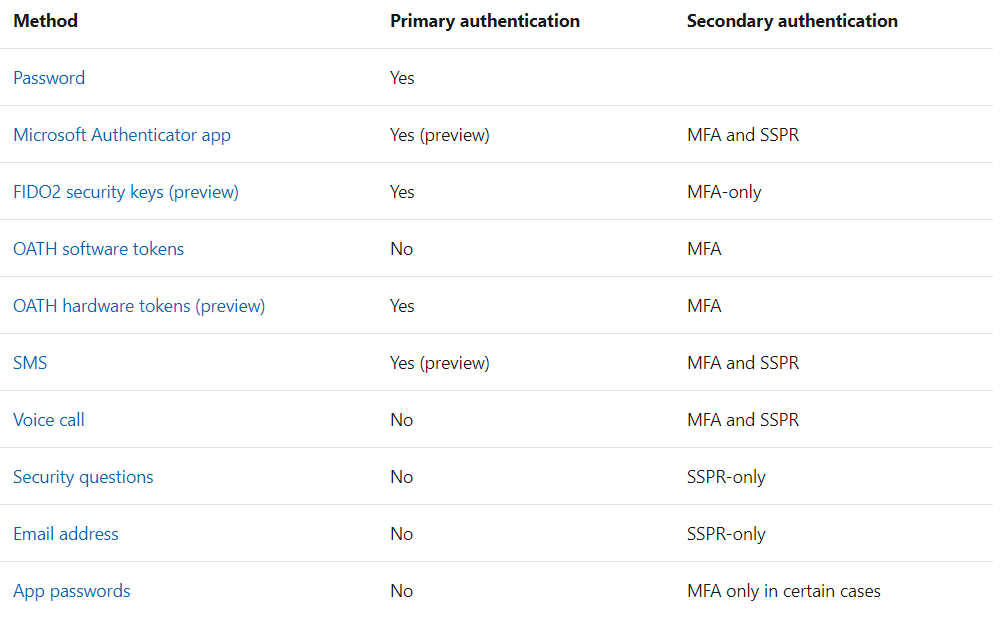
In Azure AD we want a policy to require MFA when accessing the Azure Portal – what three to specify?  


Azure AD Connect for AAD Seamless SSO: but users prompted multiple times to sign in with onmicrosoft.com account: **there’s an UPN mismatch between Azure AD and on prem AD**  
**In Azure AD, we gotta add and verify a custom domain name**

OnPrem system, we install Azure AD Connect to use password hash synchronization and SSO (staging mode is enabled)  
But oops, Synchronization Service Manager does not display any sync jobs: **run Azure AD Connect and disable staging mode***Because in staging mode, the server is active for import and synchronization, but not exports.  
It does not do password sync or writeback, even if the features are selected.*

We have an AAD tenant with the initial domain name.  
We also have contoso.com registered at a third party  
We need to ensure we can create AAD users that have @contoso.com accounts  
**1. Add custom domain name to Azure AD  
2. Add DNS information to the domain registrar  
3. Verify custom domain name in AAD**

We are implementing authentication for apps.  
We plan to have Self Service Password Reset (SSPR) + MFA in AAD  
What can support both?  
**- Short Message Service (SMS) messages  
- Microsoft Authentication App  
- Voice call**



We have onprem file server running Windows Server 2016, we want to sync it to Azure  
We have a subscription containing Azure file share  
We deploy Azure File Sync Storage Sync Service, create a sync group

**Install Azure File Sync Agent  
Register Server1** (establishtrust) **Add a server endpoint**sync group gets created, which defines topology for a set of files (must contain 1 endpoint)  
cloud endpoint within a sync group are kept in sync with each other

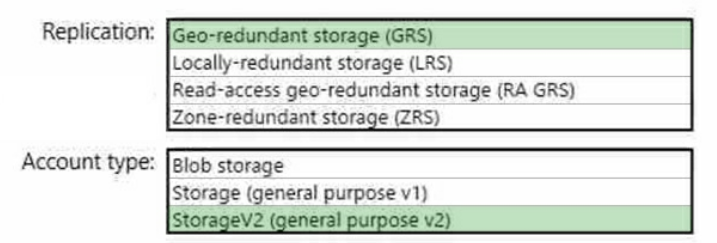
We plant to use Azure Import/Export service to copy files to **storage account/ Azure Files**  
What two files to create before we prepare the drives for the import job?  
**1) Dataset CSV file** (in the root folder where the tool resides: add entries what to import) **2) Driveset CSV file** (the driveset file has the list of disks and corresponding drive letters so that the tool can correctly pick the list of disks to be prepared)

# App Service

We have an App Service running D1 plan.  
Now traffic is increased: ensure when CPU load is above 85% it scaled out, but cost is minimized.  
**1. Upgrade to Standard Tier  
2. Enable autoscaling  
3. Add Scale Rule  
4. Configure a Scale condition**

# Storage Account

Create Storage acc in East US 2, which:  
- replicates synchronously  
- remains available if a single data center in the region fails



LRS:   
GRS:   
RA GRS: this is async  
ZRS: three clusters in single region 🡪 **only supports StorageV2**  
LRS:

We create a Storage Account, and want to create a file share, to which users from home PCs running Windows 10 could connect. Which port to open? **445**