**1.Providers:**

- Subscription'a ilgili providers (authorization, automation, storage, network) register edilir resource acmak icin.

**2.Azure Active Directory Tenant:**

**a.Genel:**

- Roller Azure AD tenant’lar arasinda otomatik gecmez.

- Global administrator-1’in kurdugu tenant’ta diger tenant veya subscription’daki Global administrator veya owner’in yetkisi yoktur.

**b.Global administrator:**

- tenant olusturabilir.

- Baska tenantta user olusturabilir. Yetki verilirse sanirim.

- Tenant root management group'ta policy olusturabilir. Access management for Azure resources da gerekli.

- Authentication icin SSPR’de set edilmis security questions’larini modifiye edebilir.

- Kendisinin kurmadigi Azure Active Directory tenant’ta user account kuramaz.

**c.Owner:**

- User olusturamaz resource olusturabilir.

- Resource uzerinde tum yetki vardir. Resource acip kapatabilir.

- Device'i Azure AD'ye join edebiliyorsa Owner'dir.

- Child management group'ta veya subscriptionlarda policy olusturabilir.

**d.User administrator:**

- Sadece user ve group olusturabilir, yonetir. User ve Device’leri group’lara add eder.

- Authentication icin SSPR’de set edilmis security questions’larini modifiye edemez.

- Can update password expiration policies.

- External User'i Azure AD tenant'e Davet Etme:

> User’s Settings > Manage external collaboration settings (External Users'in altinda) > Guest invite settings

**e.Authentication Administrator:**

- Authentication icin SSPR’de set edilmis security questions’larini modifiye edebilir.

**f.Local Administrator:**

- Device Owner (default olarak): can join devices to Azure AD.

- Global administrator (default olarak)

**g.Contributer/MG Contributer:**

- Her turlu resource'u create, rename, move, delete, read yapabilir.

- assign access, assign policy olusturamazlar. (Owner'dan farkli olarak baskasina access yetkisi veremez.)

**h.Resource Policy Contributer:**

- Yalniz assign policy yapabilirler.

**d.Network contributor (on RG1):**

- Internal Load balancer’e backend pool eklemek icin yeterli.

- Public Load balancere health probe eklemek icin yeterli.

- LB ile backend pool veya health probe'u birlestirmek icin ayni RG'da olusturulur. Hem LB hem backend pool'a ulasir.

- “Traffic Analytics”: Subscription icinde enable edebilir.

**g.Reader role:**

- “Traffic Analytics”: Subscription icinde enable edebilir.

- Owner, Contributer, Reader ve Network Contributer “Traffic Analytics”i enable edebilir.

**e.User administrator administrative role:**

- Bu rolu verebilmek icin; from Directory role blade modify directory role.

**f.User Access Administrator Role for Vnet1:**

- User’lara role atamaya yarar.

**g. Logic App Contributer:**

- Azure AD Tenant'ta bir developer group tanimli ve Subscription'da ugur RG var. Developer group, ugur'da Azure logic apps olusturabilmek icin ugur RG'da developer group'a Logic App Contributer rolu atanir

**h. Logic App Operator:**

- Azure AD Tenant'ta bir developer group tanimli ve Subscription'da ugur RG var. Developer group, ugur'da Azure logic apps olusturabilmek icin ugur RG'da developer group'a Logic App Contributer rolu yetersiz. Update, edit yapamaz.

**f.DevTest Labs User:**

- You can connect, start, restart, and shutdown your virtual machines in your Azure DevTest Labs.

**f.Storage File Data SMB Share Reader role:**

- User ve grouplara atanabilir. Cihazlara atanamaz.

**i. Cloud device administrator:**

- He has only read permission on groups. Baska gruba device add edemez.

**j.Traffic Manager Contributor:**

- Traffic analytics rolunu yeterli seviyede icra edemez.

**g.Role:**

- Users > User1 > Assigned roles > + Add assignments

\* Rolleri modify edebiliriz.

**h.UPN (User Principal Name):**

- Name of a system user in an email address format. (example: firstname.lastname@domain.com)

- It consists of the user name (logon name), separator (the @ symbol), and domain name (UPN suffix).

- UPN should not be confused with email addresses. A UPN is not the same as an email address. Sometimes, a UPN can match a user's email address, but this is not a general rule.

**i.IdFix tool:**

- UPNs, special character sebebiyle Azure AD desteklemeyebilir.

- When there is a mismatch in UPN then the IdFix tool should be run, should be updated to synchronize on-premise AD to Azure AD.

**j. Microsoft 365 tenant:**

- “expiration policy” can be set ONLY for “Office 365 groups”. Assigned membership veya Dynamic -user membership type olmasi farketmez.

**k. Azure AD Premium P2 license:**

- “Licenses blade of Azure AD, assign a license**”:** Tenant’a lisans alirsan user’larin premium features’leri kullanabilmesi icin lisanslari user’lara atarsin.

**l.Device Settings:**

> Device > Device Settings

- We can assign the local administrators to all the computers that have been joined to Azure AD domain.

- This service needs an Azure AD premium license.

**o.Group – Membership type: Dynamic Device / Assigned:**

- Dynamic olan gruplara yetkili user da olsa “add device to group” yapamaz.

**p. Hybrid Deployment of Azure AD:**

- Azure AD user1, Windows Server AD user2 ve Microsoft account user3 dahil hepsinde UserLocation bilgisini modify edebilir.

- Azure AD user1 ve Microsoft account user3 JobTitle bilgisini modify edebilir.

- Hybrid platformlarda Azure AD ve Windows Server AD ve Microsoft accounts sync oldugu icin tum userlar yapabilir.

**3.Subscription:**

- Mevcut Subscription’u tenant’lar arasinda move edebiliriz.

- Tenant’taki user’a Subscription’lari manage etme yetkisi verirsek tum subscriptionlar uzerinde yetkisi olur. Aksi halde subscription’dan yetkili bir user bizi yetkilendirmeli.

**a. Subscriptionlar arasi Resource Tasima:**

- Storage account, VM, Vnet, Managed disk, Recovery Service Vault… aktarilabilir.

- AD, App service gateway, Backup vault aktarilamaz.

**a.Izin:**

- "Set-AzMarketplaceTerms cmdlet" komutu PowerShell'de calistirilarak yeni User'a Marketplace'ten template deploy yetkisi verildi.

- User'a yetki verirken Subscription uzerinden IAM'e gidilerek istenen role tanimlanir.

**b.Tenant:**

- Global Access'i olan User'da olsa Subscriptionu goremez. Yetkilendirilmeli.

- Tenant'ta olusturulan group Subscription'daki RG'da Logic App Contributor rolu ile resource olusturabilir.

**4.OAuth 2.0 endpoint:**

- consonto.com (tenant)'a OAuth 2.0 authorization endpoint kurarak AKS ile tenanttaki user'larin grant access olur kubectl’de.

- kubectl uses the Azure AD client application to sign the users with OAuth 2.0 device authorization.

**5.SSPR (self-service password reset)**

- SSPR is enabled for all users (non-enterprise admins). Ornegin BillAdmin, SecAdmin'i kapsamaz.

- SSPR policy does not apply for Administrator roles in Azure AD.

- Sifre resetleme, degtistirme gibi islemler icin kullanilir.

- Authentication Administrator ve Global Admin (not User admin) have permission to modify security questions.

**6.Storage:**

- Hepsi icin oncelikle Storage account acmak gerekli.

- Storage account upgrade edilerek gpv1’den gpv2’ye gecilebilinir.

- Azure Files: Sadece Files can give a persistent storage for containers. Image depolanabilir.

**a.Storage account kind/type:**

- General-purpose V2:

\* Blob

\* Table

\* Files

\* Queues

>> Standard/Premium

- General-purpose V1:

\* Blob

\* Table

\* Files

\* Queues

>> Standard/Premium

- BlockBlobStorage:

\* Blob

\* Storage > Performance: Premium > Account kind: BlockBlobStorage

- FileStorage:

\* Files

\* Only FileStorage type of storage account supports Premium file share.

\* Yalnizca share, sync durumlari icin kullanilir.

\* Storage > Performance: Premium > Account kind: FileStorage

- BlobStorage: Account altinda Containerler (pictures vb dosya). Container icinde de Blob (img001.jpg vb file)'lar olusturulur.

\* Container

> Blob

>> Standard

**b.Object Type:**

- Container: image store edip replica edebiliriz.

- File Share

- Table

- Queue

**c.Azure File Share:**

- Sadece file depolar.

- Only FileStorage type of storage account supports Premium file share.

- Storage, StorageV2 veya BlobStorage'de file share kurulamaz.

- Containerler icin persistent storage imkani saglar.

**d.Azure File Sync:**

- Bir azure file sync group'a yalniz bir cloud endpoint baglanabilirken; birden fazla server endpoint baglanabilir.

- Register edilen server basina yalniz bir server endpoint tanimlanabilir. (D:\Folder1) yanina (E:\Folder2) olmaz.

- Server register edilmeden server endpoint gruba eklenemez.

- Iki Server endpoint arasi dosyalar da paylasilir.

- Server ve Cloud endpoint’te ayni file varsa ikisini de copyalar, owerwrite yapmaz.

> Azure file share ile on-premise server arasinda "azure file sync" kurabilmek icin Subscription'da "Storage Sync Service" olusturulur.

> Subscription'da "sync group" olusturulur. Sync group'ta cloud endpoint olusur.

> Daha sonra on-prem server'a agent download edilir. Server endpoint olusur agentla.

> On-prem server (VM), storage sync service'e register edilir. Boylece arasinda bir link olusur.

> Server endpoint’ler gruba eklenir.

**c.Endpoints:**

- Cloud endpoint:

\* Olusturulan dosya yaklasik 24 saat icinde Server endpoint’lere aktarilir.

- Server Endpoint:

\* Her server’da bir adet olur.

\* Sync job ile 5 dk arayla tum endpointlerle senkronize olur.

**d.Archive access tiering:**

- Sadece StorageV2 ve BlobStorage’da archiving olur.

- Storage, FileStorage ... olmaz.

- Archive minimum 180 gun. Cool ise minimum 30 gun.

**e.GPV2:**

- Image depolayabilir.

- Live-migration: Standard (LRS, GRS) destekler. Premium desteklemez.

**e.Blob Storage:**

- Serving Image ve documents'leri directly to a browser.

- File'lar burada saklar ve distributed access.

- Streaming video/audio.

- Writing the log files.

- Storing backup and restore, disaster recovery, archiving.

- Storing data for analysis bu an on-perm or Az service.

- image'ler icin uygun.

- LRS destekler.

**f.Table Storage:**

- File'lar saklanamaz.

- NoSQL icin kullanilir.

**g.Azure Queue Storage:**

- Stores large numbers of messages. HTTP, HTTPS ile her yerden ulasilabilir.

- Asynronized ve 64 kb max calisir.

**h.General-purpose v1 Azure Storage account:**

- locally-redundant storage (LRS): tek storage.

**i.General-purpose v2 Azure Storage account:**

- ZRS redundancy model: farkli AZ'lerde replica imkani. Zone faillerine karsi iyi. Yalnizca standard GPV2 destekler.

- image'ler icin uygun. Blob'u destekler.

- LRS destekler.

- RA-GRS destekler.

**j.AzCopy:**

- Yalnizca blob ve file service'lerde kullanilir. Table ve queues de kullanilmaz.

- Tum OS’leri destekler.

- Blob Storage’a Azure AD veya SAS ile transfer yapilabilir.

- File Storage ile yalniz SAS ile transfer yapilabilir.

**k.Replication:**

- Storage account ayni anda en fazla 2 adet destinationa replication yapabilir.

- Ayri ayri en fazla 2 containerden baska storage'deki 2 containere yapabilir.

- Bir containere yalniz bir replication rule (destination veya source) tanimlanabilir.

- Storage accounta 1000 replication tanimlanabilirken, containere tek rule tanimlanabilir.

- GPV2 onerilir.

**l.UNC Path:**

- Storage account name.file\shared name: contostorage.file.core.windows.net\data

\* Storage account name: contostorage

\* file: file.core.windows.net

\* file share: data

**m.Lifecycle Management Rule:**

- General-purpose v1

- General-purpose v2

- BlockBlobStorage

- BlobStorage

- premium block blobs storage accounts

- Data Lake Storage Gen2 accounts ile calisir.

- Yalniz FileStorage ile calismaz.

**n.GRS, LRS, RA-GRS:**

- LRS:

\* Live migration'u destekler.

- GRS:

\* Live migration'u destekler.

- RA-GRS:

\* Live migration'u desteklemez.

**o.RG/Region Degisimi:**

- Storage account’lar mevcut RG’de private link baglantisi olmadigi surece farkli regionlardaki RG’lere tasinabilirler.

**p.Azure Storage Explorer:**

- Blueprint files’i on-prem’den Azure tasiriz.

- Import/export service daha cok buyuk veri aktariminda kullanilir.

- SAS ile de aktarilabilir ama ugras gerektirir.

**r.On-prem’den Storage Account’a Transfer:**

- On-premdeki disk file’leri storage’a gonderip VM olusturmak gaye.

> Storage account

> Firewalls and Virtual Networks

> Selected Networks

> Add on-premises network’s IP address

**7.Storage Account Tipleri:**

**a.LRS:**

- Tek Zone'da 3 syncronously replica yapar. AZ cokerse data gider.

**b.ZRS:**

- Regiondaki 3 AZ'de de syncronously replica yapar. Bir AZ cokse de data kaybi olmaz.

- StorageV2(General purpose v2)

**c.GRS:**

- Cross-Regional Redundancy for regional outages.

- Ayni regionda 3 syncronously replica yapar.

- Farkli regionda asyncronously replica yapar.

- Ikinci regiondakine read access icin Read Access Geo Redundant Storage (RA-GRS) enable edilir.

**d.GZRS:**

- Geo Zone Redundant Storage high availibility ve max durability icindir.

- Ayni regionda 3 syncronously replica yapar.

- Farkli regionda asyncronously replica yapar.

- Ikinci regiondakine read access icin Read Access Geo Redundant Storage (RA-GZRS) enable edilir.

**8.Azure Import/Export Service:**

- Azure blob storage and Azure File storage ile import calisir. Azure Data Factory, Azure SQL database, A virtual machine, Azure File Sync service, Azure Data Lake store, Azure Cosmos DB database ile calismaz.

**a.Import:**

- Yuksek verinin Azure'a fiziki transferi.

- Azure Blob Storage

\* Container

- Azure File Storage

\* Files

> Attach an external disk to on-prem Server and then run waimportexport.exe (datayi disk drive'a kopyalar.). (BitLocker ile disk drives encrypted edilir.)

> From the Azure portal, create an import job. (Gonderilecek storage'da import edilir.)

> Detach the external disks from Server and ship the disks to an Azure data centre.

> From the Azure portal, update the import job.

**b.Export:**

- Azure Blob Storage

\* Container

**c.Import Hazirlik:**

- Import oncesi the DATASET.CSV and the DRIVESET.CSV files are the two files that are needed when we want to import a file or a folder using the Azure Import/Export service.

- Kendi disk drives'lariniz veya Azure'un gonderebilecegi disk drives'lar ile transfer yapilabilir. USB 3.0 ve uzeri connection olmali.

- Herbir order ile max 5 adet SSD ile toplam 40TB transfer yapilabilir.

**d.Azure Data Box Disk:**

- Azure'un diskleri transfer icin talep edilecekse istenir.

**9.Recovery Service Vault:**

**a.Tanim:**

- All the backups configured using azure native backup service are stored in Recovery service vaults.

- Backup'lar burada saklanir.

- Recovery point'leri store eder.

- Resource ile Vault ayni regionda olmali. RG ve Vnet onemli degil.

- Blob haric her turlu data source'unu depolayabilir: Share, VM, disk, SQL...

- Once Recovery service vault sonra VM’ler register edilir.

- On-prem’in backup’i icin Agent for Windows Server or Windows Client (MARSAgentinstaller.exe) yuklenir.

**b.Vault Baglama:**

- VM1’in backup’ini VM2'e restore backup yapmak icin VM2'ye Microsoft Azure Recovery Agent yuklenir.

- Storage account'taki containere de backup set up edilebilir.

- Bir VM’ye ayni anda yalniz bir RSV baglanilabilir. baska RSV'ye backup aktarilacaksa once backup aktarilan mevcut RSV'den ayrilinir.

**c.Storage ile Baglama:**

- Vault ile Storage ayni region'da olmali.

- Farkli RG'da olabilirler.

- Daha sonra Diagnostic settings for the AzureBackupReports log configure edilebilir.

- Storage ve blob backed up to Vault yapilamaz, sadece Share yapilabilir.

**10.Backup:**

**a.Genel:**

- Azure VM Agent (WaAppAgent.exe): Backup alinacak VM’ye latest version yuklenir.

**b.Backup policy:**

- Azure backup uses a policy to define the frequency and the type of the backup for the virtual machines.

- VM'in kapali olmasi ve Windows/Linux olmasi backup'i etkilemez. Planli zamaninda backup alinir.

- Backup policy’de uzun donem ile kisa donem cakisirsa uzun esastir. Aylik ve gunluk cakisirsa aylik’in retention of monthly esastir.

**b.Agentsiz olarak Windows VM'den olusan backup:**

- File recovery: Interneti olan herhangi Windows makineye restore pointi connect eden bir script download ederek yapilabilir.

- Restore backup: Backup'i alinan VM veya yeni bir VM'ye restore yapilabilir.

**11.Recovery plan:**

- It is used to define the parameters while performing the disaster recovery of your infrastructure.

**a.Azure Site Recovery:**

- Region'un cokmesi durumuna karsin failover senaryosunda Disaster recovery icin kullanilir.

- Sistem hata verince recovery site olarak yedeklenmis sistem marifetiyle baska bir regiona sistemi tasiyarak 10-15 dk'da acar.

- Site-Recovery tum sistemi ec2'lar, storage'lar, public ip'ler, load balancer'lari...vb baska yerde syncronized olarak hazir bulundurur.

**b.VM’deki Bozulan/Eksik Dosyanin On-Prem’e Indirilmesi:**

> In the Backup dashboard menu, click File Recovery.

> From the Select recovery point drop-down menu, select the recovery point that holds the files you want.

> To download the software used to copy files from the recovery point, click Download Executable (for Windows Azure VM) or Download Script (for Linux Azure VM, a python script is generated).

> Copy the files by using AzCopy

**12.SMB Protocol:**

- "net use" uses SMB protocol which supports Account key only for authentication against storage accounts.

- SAS key ile girilemez.

**13.DNS:**

**a.NS record:**

- To delegate a subdomain named research.adatum.com to a different DNS server in Azure, adatum.com zone'da record isimli NS record olusturulur.

- Azure DNS kullanilarak mevcut DNS recordlarinin internette resovable olmasi icin Domain register Records’taki NS record'lar modify edilmeli. NS records otomatik olusur. Biz sadece domain’deki named serverslari degistiririz.

**b.SOA record:**

-  We cannot create a new SOA record separately. There is one SOA record created automatically with each DNS zone.

**b.TXT or MX records:**

- They are used to verify the ownership of a domain, which is required while adding a custom domain in Azure AD tenant.

- Custom domain aldin ve Azure’un verify edebilmesini istersen kullanilir.

**c.Private DNS Zone:**

- Bir Vnet'e register edilir ve Vnet'in Subnetlerindeki VM'ler can register the hostname records in example.local zone.

- Private zone'a register edilmemis diger Vnetteki VM'ler local hostname'leri register edemez.

- Automatically register ozelligi varsa private zone'lar farkli region ve Vnetlerde kullanilabilir.

- Vnet’e birden fazla private DNS zone register edilebilir.

- Auto registration enable ise register edilmis baska Vnetteki VM’ler dahil private IP addressleri ile otomatik register edilir. Public DNS, Vnet’e link edilemez, yalniz Private olup auto regidtration acik olanlar.

- Bir Vnet’e birden fazla Private DNS zone associate edilebilir ama bir tane Private DNS zone auto register edilir.

- 1 zone birden fazla Vnet’e associate edilebilir, auto register edilebilir.

- Peering olan Vnet’ler DNS name’i resolve edebilir.

**c.On-prem’deki Private Zone’un Azure (Subscription)’a Tasinmasi:**

- Azure CLI: support importing/exporting zone files from on-prem to Azure.

- PowerShell ve Azure portal desteklemiyor.

**d.DNS Server:**

-  The domain naming service (DNS) in Azure 53 portunu kullanir.

- TCP 53: Zone transfers ve UDP 53: Lookups

- Diger Vnet’ler de DNS Server’a (VM’da kurulu) register edildiyse peering ile diger Vnet’lerdeki VM’ler de kullanabilir.

**e.Virtual Network Link:**

- DNS Private zone’u bir VM’e kursak bile tum Vnet’i kapsar.

- Baglanan link’in auto registration enable edilmisse baska region’daki VM’ler dahil Private DNS zone’a eklenir.

- VM’ler private zone’a eklenir ama public zone’a eklenmez.

**f.Reverse DNS Lookup:**

- VM1’e VM2’den DNS lookup yapilirsa: vm1.internal.cloudapp.net (FQDN doner)

**g.Custom Domain name ile User Olusturma:**

- Custom olarak third-party registardan alinmis contoso.com adresi ile [ugur@contoso.com](mailto:ugur@contoso.com) seklinde user olusturabilme:

> Add a custom name to Azure AD tenant.

> Add a TXT or MX record to the public contoso.com DNS zone in order to prove ownership of domain.

> Verify the domain

**14.Monitor:**

> VM'lerin monite etmek icin Log Analytics workspace configure edilip, source olarak kullanilir.

> Microsoft Monitoring Agent, VM'e yuklenir.

> Create an alert in Azure Monitor and specify the Log Analytics workspace as the source.

- All system event logs are stored in the log analytics workspace and we can create a query to fetch those logs and then set up an alert using that query.

**a.Azure Network Watcher:**

**- IP flow verify:**

\*  Test the communication between VMs and informs if the connection succeeds or fails.

\* If the connection fails, IP flow verify informs which security rule allowed or denied the communication, so that we can resolve the problem.a

\* Identify a security rule that prevents a network packet from reaching an Azure virtual machine icin kullanilabilir.

\* Specify a source and destination IPv4 address, port, protocol (TCP or UDP), and traffic direction (inbound or outbound).

\* IP flow verify then tests the communication and informs you if the connection succeeds or fails.

\* NIC’e apply edilmis NSGs’lerin veya Subnete apply edilmis NSGs’lerin rulelarini control eder.

**- Connection troubleshoot:**

\* Validate outbound connectivity from an Azure virtual machine to an external host icin kullanilabilir.

\* It enables you to test a connection between a VM and another VM, an FQDN, a URI, or an IPv4 address.

**- Connection Monitor:**

\* Reachability, latency, and network topology changes between the virtual machines and endpoints.

\* It also gives the average round trip of packets (measured in milliseconds) between the different virtual machines in a virtual network.

\* It enables the user to monitor the communication (network traffic) between two virtual machines within a virtual network.

\* We can inspect all the network traffic from VM1 to VM2 for a specified period.

\* VMs arasindaki iletisimi izler ve Connection monitor metric'te tanimli alertleri gonderir.

\* Communication problemlerini (VMs arasindaki) diagnose eder.

**- To Record VM's successful and failed connection attempts:**

\* Enable Azure Network Watcher in the VM’s region,

\* Register the Microsoft.Insights resource provider

\* Enable Azure Network Watcher flow logs,

- NSG flow log data is written to an Azure Storage account therefore we need to create an Azure Storage account first.

**b.Azure Monitor:**

- Network In/Network Out: metrics'leri sadece VM'lerden gelen bytes sayisini verir. Inspect etmeye yaramaz.

**c.Performance Monitor:**

- (Data Collector Set):

\* Performance monitor belirli zaman araliklarindaki network performansini verir.

\* It detects network issues like traffic blackholing, routing errors, and issues etc.

\* It does NOT help to inspect network traffic between virtual machines (VMs).

**15.NSG flow logs:**

- NSG’den gecen network trafigini (ingress-egress) Network Watcher’in NGS flow logs ozelligi ile takip edebiliriz.

- It allows viewing information about ingress and egress IP traffic through a Network security group.

- Through this the IP addresses that connect to the ILB can be monitored when the diagnostics are enabled on a Network Security Group.

**a.VM'nin connection log kayitlarinin alinmasi:**

> Bir VM olusturulur.

> NSG: ile inbound ve outbound trafik belirlenir.

> Azure Storage account: NSG flow log data is written to an Azure Storage account and therefore we need to create an Azure Storage account first.

> Azure Network Watcher: NSG flow log ile VM'nin log kayitlari alinirken VM ile ayni region'da enable the Azure Network Watcher edilir.

> Microsoft.Insights: Sonra “Microsoft.Insights” provider register edilir.

> NSG flow log: Enable a traffic flow log for an NSG, using Network Watcher's NSG flow log capability.

> Download the logged data

(NSG flow log: We can log network traffic that flows through an NSG with Network Watcher's NSG flow log capability.)

**16.Site-To-Site Connection:**

- Gateway (gateway subnet de) kurulur her iki Vnete. Bu kapsamda bosta Vnetin IP addresi olmali Site to Site con icin.

- 2 Vnet arasinda da kurulabilir ama her iki Vnet’te Gateway subnet icin bosta IP araligi olmali.

- Vnet ile On-prem network IP address'ler cakismamali.

- Azure Virtual Network (VNET) Gateway: On-premde SMB share mevcut, Azure'da VNET ve webapp varsa S2S baglantisi icin kullanilir. VPN gateway kurulumu icin gereklidir.

- IPSec VPN connections encrypt data in transit.

- Bulutta LB gerekirse Internal LB kurulur. Private IP’ler ile baglanilir. Bir de Application Gateway kurulur web app icin.

**a.On-prem ile Vnet arasinda Site-to Site VPN:**

1. Create a gateway subnet: The gateway subnet is part of the virtual network (Kurulu degilse Vnet kur) IP address range that you specify when configuring your virtual network. It contains the IP addresses that the virtual network gateway resources and services use.

2. Create a VPN gateway: The virtual network (Vnet) gateway uses the gateway subnet.

3. Create a local network gateway: It represents your on-premises location (the site) for routing purposes. You give the site a name by which Azure can refer to it, then specify the IP address of the on-premises VPN device to which you will create a connection.

4. Create a VPN connection: Create the Site-to-Site VPN connection between your virtual network gateway and your on-premises VPN device.

- Azure VPN Gateway sadece dynamic IP address assignment’i destekler. Bu yuzden basic sku ve dynamic IP addr olur.

**b.ExpressRoute’a Automatic Failover icin S2S:**

- Kurulu ExpressRoute duserse automatic failover kapsaminda on-prem baglantisinin S2S ile yapilabilmesi icin:

> Create a connection

> Create a local site VPN gateway

> Create a VPN gateway that uses VpnGw1 SKU (Vpn type: route based olmali)

**b.Minimumlar Yuksek Availibility:**

- 1 IP address

- 2 VPN network gateway: Ama 1’den fazla VM varsa 1 adet de yeter.

- 2 Local network gateway

**c. Application Gateway:**

- Web app’ler icin kurulur ve gerekli olursa internal LB kurulur.

**17.Point-To-Site Connection:**

**a.Kurulum:**

> Vnet1’de VPN gateway kurulur. Static routing yapiyor.

> On-prem Client’e VPN client configuration package download edilir.

**b.Self-signed certificate:**

- Computer1’de Self-signed certificate olusturup Vnet baglantisina eklenir.

- Sonradan baska bir on-prem cihaza P2S yapilirsa C1’deki certificate C2’ye export edilir veya self-signed certificate regenerate edilip Vnet connection’a eklenir.

- Self-signed connection kurulmus P2S’e Azure AD authentication policy ile baglanilamaz.

**c.Genel:**

- Route-based virtual network gateway ile kurulur.

- Policy-based virtual network gateway varsa silinir.

- Connection topology’sinde degisiklik yapilirsa Client’e VPN client configuration package reinstall edilir.

- Vnet1 ile Vnet2 peering varsa Client Vnet2’ye de baglanabilir.

**18.VPN:**

- Max 30 tunnels.

**19.Virtual WAN Hub:**

- Her regionda en fazla bir Virtual WAN olur.

- Virtual WAN’i Vnet’e baglamak icinde Vnet Connection gerekir.

- Officelere Virtual Hub kurup, Vnet’e Virtual WAN uzerinden baglanabilir.

- 3 farkli bolgedeki office’in her birine 1’er Virtual Hub (toplam 3 Hub) kurup, Vnet’e 1 Virtual WAN kurarak baglanabilir.

- Large scale VPN icin kullanilir. Region basina 1000 branch baglanabilir.

**20.Basic SKU Load Balanser:**

- VM'ler icin yalniz bir Availibility Set olusturulabilir. Tum VM'ler tek availibility sette olur veya VMSS’de olmali.

- VPN can connect only with Dynamic IPs and Basic SKUs.

- Single availibility set ile calisir. Dogrudan VM'e balance yapmaz.

**21.Standard Load Balancer (internet facing):**

**a.Backend Pool:**

- LB'nin Backend pool'una VM'i tanitmak icin LB'de static IP of Standard SKU attached olmali veya no IP.

- Backend VM'lerin ya "no Public IP" veya "Standard Public IP" (static IP address) olmali.

- Backend VM'lerin "Basic SKU Public IP" olmamali. Dynamic public IP olmamali varsa silinir.

- Backend poola VM baglarken acik, stop olmasi farketmez. Backend poola baglarken VM’de dynamic IP varsa silinir.

- Herbir service icin bir pool olusturulur.

- Tum VM’ler ayni Vnet’te olmali.

**b.NSG:**

- VM'yi LB'ye baglarken olusturmaliyiz.

- Static IP'ler olursa tek bir nsg ile tum Vnet'in nsg'si olusturulabilir.

- Sadece bir VM’e LB ile gonderim yapilacaksa inbound NAT rule belirlenir.

**c.Health probe:**

- (HTTP:80/Probe1.htm) VM'lerde yuklu ise saglikli gorur ve yuku 80 portundan VM'lere balance eder.

- Health probe yuklu olmayan/hata veren VM’ye LB gonderim yapmaz.

**d.Rule:** Silinirse (frontend IP addresini, backend pool ve Health probu gosteren) LB calismaz.

**e.Frontend IP Address**: VM'lere disardan ulasmak maksadiyla inbound NAT rule'lar tanimlanmadan once tanimlanmali.

**g.** **Floating IP**: active-active state de failing senaryosu icin kullanilir. Standard LB ile calisir.

**h.active-standby state:** 2 dk’dan kisa surede kalkar. Bir IP addres’i yeter. Bir aktif bir standby cihaz kuruludur.

**h. Session persistence to Client IP:** Session persistance’dan client IP secilirse her defasinda ayni client ayni VM’a yonlendirilir.

**22.Internal (Private) Load Balancer:**

- Frontends ve backend pool (VMs) ve LB ayni Vnet'te olmali. Peering’le de olsa baska Vnet’teki VM’leri gormez.

**a.Standard SKU LB:**

- VM’lerin ya Standard SKU public IP addressi veya no Public IP address olmali.

- LB kurulu oldugu Vnet'in disinda calismaz peering olsa da.

- Standard LB’ler, Basic SKU Public IP Address’i desteklemez.

- VM’de mevcut Basic SKU nic ise Standard Nic ile degistirilir.

**23.NIC (netwok adapters):**

- Vnet ile ayni region'da olusturulur.

- Baska regiondaki RG’lara aktarilabilirler VM ve Vnet’e bagli olsalar bile. Neticede region degismiyor.

- VM'nin kendi nic seviyesinde DNS (settings) tanimli degilse Vnet'in nic'ine tanimli DNS settings'i kullanir.

- VM’in kendi NIC’ine tanimli custom DNS varsa Vnet’e tanimli DNS’i kullanmaz. Kendininkini kullanir.

- VM’ye birden fazla nic baglanabilir.

**a.IP Forwarding:**

- IP forwarding VM1’in NIC’inde enable edilir.

- Virtual appliance yuklu VM1 kapanirsa IP forwarding son bulur.

- Farkli NIC’ler ile VM1 farkli Subnet’leri connect ederse buradaki VM’ler kendi arasinda da connect olur.

**b.Routes:**

- Route table ile olusturulur.

- VM1’e virtual appliance yuklenir.

- Address prefix: Hedef (nihai) Vnet/Subnet IP address. IP forwarding yapilacak adrestir. Yani VM1 buradaki VM’lerle connect olur.

- Next hop type: Virtual appliance

- Next hop address: VM1 IP address

- Assigned to: Gateway Subnet (Route Table’a gelen adres )

**24.Azure CLI:**

- az aks Install-cli: kubectl clienti install eder. This command requires AZ Cli pre-installed on the system to work.

- az storage account create -g RG1 -n storageaccount1 --kind StorageV2 --sku Standard\_GRS

\* StorageV2: Hot, Archive and Cold blob tiers'i support eder.

\* Standard\_GRS: Birden fazla regionda replica olusturarak disaster'a karsi fault tolerance saglar.

- azcopy copy D:\folder1 https://contosodata.blob.core.windows.net/public --recursive

\* localdeki folderi contosodata isimli storage accounta blob'a kopyalar.

- azcopy *make* ‘https://mystorageacount.*blob*.core.windows.net/imagedosyam’

\* “make”: create, “blob”: container, “imagedosyam”: containere verilen isim

-"Set-AzMarketplaceTerms cmdlet" komutu PowerShell'de calistirilarak yeni User'a Marketplace'ten template deploy yetkisi verildi.

- az aks create: AKS olusturur.

- az acr build: Azure Container Registry (cluster ile entegre edilmis), AKS Cluster ve image varsa ilgili image'i build edip Cluster'a deploy eder.

- Get-AzureRmRoleDefinition - Name “Reader” | ConvertTo-Json : Role create edilmeden once role define edilir.

**25.AKS:**

- Pod CIDR: container'lerin IP address'leri buradan atanir.

- Service CIDR: Service'lerin IP address'leri buradan atanir.

- az aks: ile cluster autoscaler ... ayarlanir.

- kubectl: ile cluster autoscaler ... ayarlanir.

- node pools: Node'lari scale etmek icin kullanilir esas olarak. Node sayisini degistirebiliriz.

**a.Azure CNI (Container Networking Interface):**

- Tum pode’lar Subnetten public IP address’i alir. Boylece pode’lara netten dogrudan baglanilabilir.

- Bu IP adress’leri unik olmali.

**26.VM'de yapilabilecek degisikliklerin etkisi:**

- Change the size to D8s v3: downtime yapar, VM'nin stop etmesi gerek.

- Add a 500-GB managed disk: downtime yapmaz.

- Add the Puppet Agent extension: downtime yapmaz.

- Enable Desired State Configuration Management: downtime yapmaz.

**27.Azure Cost Management:**

**a.Azure Cost Management > Advisor Recommendations:**

- Microsoft Ai-based recommendation engine.

- It gives recommendations based on different pillars like operational efficiency, performance, cost, security etc.

- Identify unattached disks that can be deleted.

**28.Azure Key Vault:**

**a.Tanim:**

- Password'leri sifreli olarak saklar. The ARM template would use the password that is stored in vault to deploy VMs.

**b.Sifreli ARM Template ile multiple VM acma:**

- Once template'e “access policy” tanimlanir. Boylece Vault'a ulasabilir.

- ARM template would use the password that is stored in this vault to deploy VMs.

**29.Azure Resource Manager library:**

- Template'ler burada saklanir.

- Calisan VM'nin template'i alinabilir.

- Template ile VM acilirken RG konfigure edilebilir.

- Template ile VM acilirken OS, administrator user ve VM size konfigure edilemez.

- Template uzerinde ornegin location degisikligi yapilirken resource section’da yapilir.

**30.Templates:**

> RG > Deployments: templates ile olusturulan resources'larin olusturulma date and time 'ini gosterir.

> RG > Automation script: RG’deki resourcelarin json filelarini gosterir.

**31.Deployment template:**

- A deployment template can be used to deploy multiple Azure web apps.

**32.App Service Plan:**

- App Service ile App Service Plan ayni regionda olmali.

- Web app baska region’a tasinsa da, App Service plan ayni regionda kalir.

- Herbir OS basina bir App Service Plan olusturulur. “Hosting platform: Linux/Windows” secilir.

- Ayni anda multi app ve multi VM’ye yukleme yapabilir.

- Ruby, Java yalniz linuxta calisiyor.

- app service plan: We can define the configurational parameters of the compute and storage resources required for the web apps.

- Multiple web apps can share a common app service plan.

- Premium tier’da App service plan region’da siniri yoktur; RG basina 100 App service plan deploy edilebilir. Free tier’de region basina 10 App service plan deploy edilebilir.

**a.Scale up App Service Plan:**

- Staging Slot:  Standard, Premium and Isolated tiers only support staging slot.

**b. Scale out the App Service plan:**

- Yeni VM ekler.

**33.Web App Service:**

a.Vnet’e Baglama:

- Web app kurulurken Vnet integration feature’u ile; Ilgili Vnet’te bir subnet olusturup web app’i Vnet’e baglariz. Boylece Vnet’teki resource’larla connect olur.

b.Web Server Logging:

> web application > Application service logs > Web server logging

- Connection hatasi (HTTP 500 error) applicationda degil web server’da olur. Real time olarak takip edilebilir.

- Ayrica “Log stream” ile de error’lar takip edilebilir.

a.Premium tier: Region bazinda limit olmayip RG bazinda 100 App service plan deploy edilebilir.

b.Free tier: Region bazinda 10 App service plan deploy edilebilir.

c..Net Core 3.0, PHP 7.3: Windows/Linux'a deploy edilebilir. App Service Plan ayni regionda olmali.

d.ASP.NET 4.7: Yalniz Windows ile calisir. App Service Plan ayni regionda olmali.

e.Ruby 2.6: Yalniz Linux ile calisir.

**34.Web App Move:**

- RG1'den RG2'ye web app move edebilmek icin R2’nin lock (read only vb) olmamali.

- Onceden kurulu web app olmamali.

- Farkli Subscriptionlar ve regionlar arasi da web app gonderilebilir.

- Baska regiona web app tasinirsa gittigi region’daki RG’un policy’sine tabi olur.

- Web app baska regiona tasinsa da App Service plan ayni regionda kalir.

**35.Resource Group:**

**a.Silmek:**

- Remove resource lock from Vnet (varsa)

- Vault'a backup varsa once durdurulur/deregister edilir. Daha sonra Vault'un icindeki backup data silinir.

- Protected ise resource kaldirilir.

**36.Budget:**

- Sadece monite eder ve Action group'ta belirtilen sekilde bildirimde bulunur.

- Maximum limite ulasilinca VM veya web-app'i kapatmaz.

**37.Log Analytics workspace:**

> Bunun icin install the Microsoft Monitoring Agent on VM.

> Create an alert in Azure Monitor.

> VM'den system event logs monite edilecekse Log Analytics workspace source olarak kullanilir.

- Log Analytics workspaces for Azure Backup reports of Vault: Subscription ve regiondan bagimsizdir. Vault baska log analytics workspace baska regionda olabilir.

- search in (Event) “error” : Workspace'te error events'leri Event isimli tablodan gormeyi saglar.

- search in (Event, SecurityEvent) “error” : Multiple table'da arama yapar.

- Tum Windows events logs buraya kaydedilir.

- LB’den VM’lerin toplanan IP’leri analiz edilecekse resource olarak NSG secilir, yani diagnostics NSG’den enable edilir. NSG flow logs allow viewing info about ingress/egress IP traffic through NSG.

**38.Linux Diagnostic Extension (LAD) 3.0:**

- Monitor the metrics, health and the logs of linux VMs.

- Oncesinde VM'ye install edilir.

**39.Windows Azure Diagnostics Extension (WAD):**

- Monitor the metrics, health and the logs of Windows VMs.

- Oncesinde VM'ye install edilir.

**40.VMSS (VM Scale Set):**

- Autoscaling VM'lere ayarlaniyor.

- Arm templates ile veya automation script ile icra edilebilir.

- VMSS farkli bir region'da VM'ler farkli farkli regionlarda olabilir.

- VM'ler sonradan olusturularak eklenebilir.

**a.ScaleSetsVM orchestration mode:**

- VM’ler, VMSS’e configuration modeline gore eklenirler. Defaultu bu.

- VM’lerin lifecycle-creation, update, deletion is managed by scale set.

**b.VM orchestration mode:**

- Disarda olusturulan VM’ler olusum esnasinda VMSS’in ID’si tanimlanarak manual olarak VMSS’e eklenir.

- Bu modda VM olmayan bos bir VMSS olusturur.

- Region veya RG farkli olabilir VMSS ile VM’in. VM herhangi regionda olabilir.

**c.Scale Set'teki VM'lerin belli image ve User\_data ile Deploy Edilmis Olarak Olusturulmasi:**

- Azure Resource Monitor ile automate the deployment of VMSS.

> Upload a configuration script.

> Modify the extensionProfile section of the Azure Resource Manager template.

**d.NGINX available mi VMSS’deki VMs’lerde:**

- Azure Resource Manager Template ile olusturulan VMSS var.

- Desired State Configuration (DSC) extension.

- Azure Custom Script Extension.

**e. Planned Azure maintenance:**

- Availibility settler (10 VM secersek) default olarak  3 fault domains and 5 update domains olarak olusur.

- During maintenance, each update domain will have 2 machines, and one domain will be updated at a time.

- Bu yuzden maintenance durumunda surekli 8 VM isteniyorsa 10 VM secilmeli.

- %20 oraninda update eder ayni anda 5 update domain oldugu icin.

**41.Proximity Placement Group:**

- In a proximity placement group all the Azure resources are logically grouped.

- VMSS ile ayni regionda olmali.

- Sadece bir RG ile assign edilir. Proximity placement group ve VMSS farkli RG'da olabilir ama iki farkli RG'deki VMSS ile baglanamaz.

**42.Automation State Configuration:**

> Upload a configuration to Azure Automation State Configuration.

> Create a management group.

> Assign the node configuration

**43.Azure Availability Set:**

**a.update domain:**

- WebApp'in kurulu oldugu her bir VM ayri ayri planned maintenance'a uymasi gerektiginde kullanilir.

- Availibility setteki herbir VM, bir update domain ve fault domain'e atanir.

- 20 adet update domains olusturulabilir.

- Fiziksel olarak ayni anda baslatilabilirler. Bir grup VM'i ifade eder.

- 14 VM ve 10 update domain olursa: 4 update domainde 2, 6 update domain’de 1 VM olur. Maintenance kapsaminda update’ler esnasinda max 2 VM eksik olur.

**b.fault domain:**

- Availibility set, default olarak 3 fault domain'e bolunur.

- Ayni power source ve network switch'i kullanan VM grubunu ifade eder.

- 14 VM ve 3 fault domain olursa: 1 fault domainde 4, 2 fault domain’de 5 VM olur. Data center failure olursa max 5 VM eksik olur. Min 9 VM hep hazir olur.

**44.Resource'larin Baska Subscription'a Transferi:**

**a.Transfer edilebilir:**

- storage account,

- VM,

- Vnet,

- Managed Disk of VM,

- Recovery services vault

**b.Transfer edilemez:**

- Azure AD services,

- Azure Backup vaults,

- Azure App service gateways

**45.Microsoft System Center Service Manager:**

- On-premise'e deployment yapilir.

- alarm kurulabilir.

**a.IT Service Management Connector (ITSM):**

- Azure ile on-premise arasi iki tarafli connection saglar.

- On-prem'de threshold seviyesine cikilinca olusan alert, VM’ye deploy edilen “Microsoft System Center Service Manager” tarafindan gonderilebilir. Bunun icin Azure ve on-prem’i baglayan ITSM deploy edilir.

**46.Firewalls:**

**a.On-premise Disk > VM icin Storage account'a Transfer:**

> Storage account > Firewalls and virtual networks > Networking > Selected networks > Add on-premises network uses a public IP namely “131.107.1.0/24 “

\* On-prem'den Azure'a aktarilacak server/diskin IP adresi storage hesabina tanitilir.

**47.App in Vnet1 > App in Vnet2:**

**a.Vnet1'deki Applicationu'u Vnet2'ye en kolay aktarma:**

> VM stop edilip, deallocate edilir.

> VM delete edilir ama Disk muhafaza edilir.

> Vnet2'de yeni VM acilir ve Disk baglanir.

**48.Custom Policy to Subscription:**

- Subscription'a NSG'lerde 8080 portunun kapali olacagi custom policy olarak yazilirsa kurulan her NSG'yr otomatik etki eder.

- Policy'ler daha once olusturulan resource'lari etkilemez.

- Policy'lerde tanimli tag ... vb gecerlidir, isaret ettigi subs veya RG'un tagi degil.

- Global administrator ile policy tanimlariz.

- NSG, Custom policy ile tanimlanabilir. Built-in policy ile bulmak zor oldugu icin custom yapilir.

- Sonradan policy tanimlanirsa uymayan device’lar:

\* silinmez,

\* “non-complient” seklinde isaretlenir,

\* modify edilemez.

- Subscription ve Resource group bazinda uygulanabilir.

**a.Policy Tanimlama**:

> Azure Active Directory > Security > Conditional Access > + New Policy

> Name: MFA accesss

> Assignments – Users and groups: secilir

> Assignments - Cloud apps and actions > Select apps: Microsoft Azure Management

> Access control – grant > Radio (selected)

> Enable policy: On > create

- It creates a conditional access policy that requires all users to use MFA when they access the Azure portal.

- Assignments - Cloud apps and actions: because configuring “MFA” is part of “Microsoft Azure Management”.

- Sadece Conditional policies ile MFA access krulabilir.

**49.Azure Policy to RG:**

- tag name: Label, tag value: Value1 olarak policy'de belirtip ayrica RG'a baska bir tag atarsan yeni resource Label/Value1 degerlerini alir.

**50.Resource Lock:**

- Resource locks are used to lock a Subscription or an Azure resource.

- Other users will not accidentally modify them or delete them.

**51. Network Interface:**

- Hem public hem de private IP addresses'i ayni anda destekler. Tek VM'e tek network interface yeter.

**a.ASG (Application Security Group):**

- Nic, ASG’ye associate edilir. Ayni Vnettekiler kullanilabilir.

- Nic’i silip yeni nic ekleyerek baska Vnet’e baglanilamaz. Ille de yeni VM acilir. Yeni nic ile ilave Subnet’e baglanilabilir.

> VM > Networking > Application Security Groups > Configure the application security groups

**52.Availibility Zones:**

- Use managed disk: AZ'ler sadece "managed disk"leri support ediyor. Managed disk secmeden AZ secilemez.

- Availibility options: Buradan istenen AZ secilir.

**53.Notifications, Alerts:**

**a.Alert Rule:**

- Mevcut notificationlar icin olusturulan signal miktarinca alert rule olusturulur.

- Rule tanimlanacak storage account vb secilir.

- Monite edip email notification alacak sekilde metric veya activity log secilir.

- Daha sonra rule'lara notify edilecek user'lar eklenir.

- 1 saat'te maksimum 100 email gonderilebilir.

- SMS ve Voice: max 5 dk'da 1 adet gonderilebilir.

**b.Action Group:**

- Alert Rule'larda customize edildiginde olusan herbir farkli grubun toplami. "user1 only", "user1 and user4", "user1, user2, user3 user4", "user1 and user4", "user1 only" tanimlandiysa 3 action group olusmustur.

**54.Peering:**

- Enabled ve Connected olmali yoksa calismaz.

- Disconnected: Disconnected olan bir peering’i connected yapabilmek icin silip address space’ini degistirirp re-establish etmeliyiz. Cunki kurulu peeringte address space degistirilemez veya eklenemez.

- Peering kurulu Vnet’te address space’te degisiklik yapabilmek mevcut peering’i silip address space’ini degistirirp re-establish peering etmeliyiz. Cunki kurulu peeringte address space degistirilemez veya eklenemez.

- Peering farkli region, subscription, RG arasinda olur. Overlapping olmamali yalnizca.

**55.Vnet:**

**a.Address Space:**

- Birden fazla private address space tanimlanabilir. 10.1.0.0/16, 192.2.0.0/16

- Region basina 250 adet olusturulabilir.

**56.RBAC:**

**a. AssignableScobes:**

- “/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e” : Subscription level de tanimlanir ve tum RG’lari etkiler.

**b.Permission elements:**

- “Microsoft.Authorization/\*” : Her turlu operasjon (create, delete, update, view …) yapabilir.

- “Microsoft.Authorization/roleDefinitions/write” : Write yetkisi verir.

**57.Cost Analysis:**

> Subscription blade > Ilgili Subscription > Cost analysis (under Cost Management) > Filter (with tag) : Tag ile resource bazinda aylik masraf cikarma.

**58.VM (Virtual Machine):**

**a.Redeploy blade:**

- Host’u yeni bir VM’e migrate eder.

- VM’i Subnet’ler arasinda move edebiliriz ama Vnet’ler arasinda move edemeyiz.

- Baska Vnet’e move etmenin tek yolu recreate VM baska Vnet’tir.

**b.Managed Identity Settings:**

-  VM’in identitys’si ile VM’deki service’ler, RG’deki resourcelari manage edebilir. Boylece VM’deki service’ler RG’deki resorce’lara deploy yapabilirler.

**59.Advisor:**

-  It recommends optimising opportunities in the categories of Cost, Performance, security, Operational Excellence and Reliability.

- Ucretsizdir. Az kullanilan VM’leri tespit edebiliriz.

**60.Metrics:**

**-** These are time-based performance indicators of Azure resources.

- Metrics are used to create alerts in Azure Monitor in order to automate tasks in case of an issue in any of the Azure resources.

**61.Customer Insights:**

**- It enables organizations of all sizes to bring together diverse data sets and generate knowledge and insights to build a holistic 360° view of their customers.**

**62.Router:**

**a. Mevcut Sistem:**

\* Subnet1 contains a virtual appliance named VM1 that operates as a router.

\* Route table var.

\* Vnet1: 10.0.0.0/16

\* Subnet1: 10.0.1.0/24

\* GatewaySubnet: 10.0.254.0/24

**b. To route all inbound traffic from VPN gateway to Vnet1 through VM1:**

\* Address prefix: Vnet (10.0.0.0/16) veya Route table’da birkac farkli Subnet olacak sekilde birkac route olabilir.

\* Next hop type: Virtual Appliance (gatewayden muteakip adres VM1, o da virtual appliance)

\* Next hop address: VM (routing’i yapan VM)

\* Assigned to: GatewaySubnet (rt’nin bulundugu subnet.)

- IP forwarding yapan VM kapatilirsa network kurulamaz.

- Farkli Subnetteki VM’ler de kendi arasinda IP forward yapan VM vasitasiyla gorusebilir.

**63.WAF tier:**

- SQL injections attaklarina ve other vulnerabilities’e karsi koruma saglar.

- application gateway that uses WAF tier LB olarak kullanilabilir.

**64.NSG:**

- Ayni region’daki Vnet’lere baglanabilir.

- Subnet veya VM’ye baglanir. Bulundugu Vnet’in RG onemsizdir.

- Vnet icinde default olarak tum portlar diger VM’lere aciktir. Disari ise nsg eklenirse default olarak kapalidir.

- NSG eklenmemis Vnet internete outbound olarak (cikis) aciktir.

- Vnet icinde default olarak inboundlar kapali, outboundlar aciktir. Subnet veya VM ile NSG eklenir.

- NSG olusturulmus olsa da baglanmadiktan sonra calismaz.

**65.Public IP:**

- Region’lari sabittir. Farkli region’daki RG’a aktarilabilse de region degismez.

**66.Azure Bastion:**

- Azure Resource Manager template to deploy a virtual network named VNET1 that will use Azure Bastion ise once AzureBastionSubnet olusturulur.

- You need to create a separate subnet for Bastion service with at least /27 as CIDR range. (/28, /29… ve /32 olmaz). Minimum 32 IP addresses available olmali.

**67.Azure CDN:**

- Static file'lara (media files) hizli ulasim saglar.

**68.Disk:**

- VM’e disk eklemek icin VM acik olmali. Disk boyutu VM’e gore degisir.

- Disc resize icin once detach edilir.

- App files OS diskine degil ek diske kaydedilmeli.

**69.VM Quota:**

- vCPU altinda yazan miktarlarin toplami Usage: Quota’yi gecmemeli. Stop (deallocated) olmasi farketmez.