<https://docs.microsoft.com/en-us/learn/paths/azure-fundamentals/>

Table of Contents

[AZ 500 Notes 4](#_Toc103598792)

[Azure AD Group and membership types (manage identity and access) 4](#_Toc103598793)

[Azure AD groups 4](#_Toc103598794)

[Azure AD membership types 4](#_Toc103598795)

[dynamic membership rule (implement platform protection) 4](#_Toc103598796)

[Azure role definition (implement platform protection) 4](#_Toc103598797)

[Azure role example (secure data and apps) 4](#_Toc103598798)

[testing 5](#_Toc103598799)

[types of availability tests 5](#_Toc103598800)

[multi-step web test (manage security operations) 5](#_Toc103598801)

[monitoring 5](#_Toc103598802)

[monitor metrics of Linux VM Logs (manage security operations) 5](#_Toc103598803)

[targeting monitoring (manage security operations) 5](#_Toc103598804)

[Azure monitor alerts (manage security operations) 5](#_Toc103598805)

[Azure monitoring agent (manage security operations) 6](#_Toc103598806)

[LAWS Log Analytics workspace (implement platform protection) 6](#_Toc103598807)

[enable LAWS for SQLdb1 (manage security operations) 6](#_Toc103598808)

[LAWS ARM for VM (manage security operations) 7](#_Toc103598809)

[collect WIN event logs in LAWS (manage security operations) 7](#_Toc103598810)

[collect Security Log Failures on VM in LAWS (manage security operations) 7](#_Toc103598811)

[collect AzureBackupReport log in LAWS (manage security operations) 7](#_Toc103598812)

[Azure Sentinel to ASC (manage security operations) 7](#_Toc103598813)

[security playbook (manage security operations) 8](#_Toc103598814)

[target a solution (manage security operations) 8](#_Toc103598815)

[alerts 8](#_Toc103598816)

[alert state (manage security operations) 8](#_Toc103598817)

[email alert when CPU over 70% (manage security operations) 8](#_Toc103598818)

[email alert when resource lock is deleted (manage security operations) 8](#_Toc103598819)

[alert suppression (manage security operations) 9](#_Toc103598820)

[diagnostic logs 9](#_Toc103598821)

[activity logs (manage security operations) 9](#_Toc103598822)

[containers 9](#_Toc103598823)

[AKS cluster 9](#_Toc103598824)

[AKS deployment (implement platform protection) 10](#_Toc103598825)

[AKS ingress controller (implement platform protection) 10](#_Toc103598826)

[AKS service principal (implement platform protection) 10](#_Toc103598827)

[Azure Container Registry 11](#_Toc103598828)

[ACR content trust 11](#_Toc103598829)

[ACR permissions (manage identity access) 11](#_Toc103598830)

[container groups (implement platform protection) 11](#_Toc103598831)

[container groups example (implement platform protection) 12](#_Toc103598832)

[enable containers to use Azure Virtual Network capabilities (implement platform protection) 12](#_Toc103598833)

[container.yaml 12](#_Toc103598834)

[Azure Firewall 12](#_Toc103598835)

[AzureFirewallSubnet (implement platform protection) 12](#_Toc103598836)

[conflict ASC JIT feature (implement platform protection) 12](#_Toc103598837)

[RDP through firewall to VM with private (itexams Q11) 13](#_Toc103598838)

[steps to install firewall (implement platform protection) 13](#_Toc103598839)

[Configure network address translation NAT rule 13](#_Toc103598840)

[enable App firewall on App Gateway (secure data and apps) 14](#_Toc103598841)

[enable disk encryption access through AKV firewall (secure data and apps) 14](#_Toc103598842)

[JIT (manage identity access) 15](#_Toc103598843)

[request access 15](#_Toc103598844)

[JIT enabling (implement platform protection) 15](#_Toc103598845)

[JIT permissions for PowerShell on VM (manage security operations) 15](#_Toc103598846)

[authentication 15](#_Toc103598847)

[MFA Setup (manage identity access) 16](#_Toc103598848)

[SSO 16](#_Toc103598849)

[Azure AD: undelete (Manage identity and access) 16](#_Toc103598850)

[Azure AD Connect: Synchronization Rules Editor (Manage identity and access) 17](#_Toc103598851)

[Azure AD Connect: Accounts and permissions (Manage identity and access) 17](#_Toc103598852)

[Azure AD Identity Protection (Manage identity and access) 17](#_Toc103598853)

[Azure AD sensitivity label (Manage security operations) 18](#_Toc103598854)

[configure how end-user consents to applications (manage identity access) 18](#_Toc103598855)

[configure consent settings 18](#_Toc103598856)

[configure registration settings 19](#_Toc103598857)

[allow or block invitations to B2B users (manage identity access) 19](#_Toc103598858)

[app registration (manage identity access) 19](#_Toc103598859)

[storage 20](#_Toc103598860)

[(GUI) tools (manage security operations) 20](#_Toc103598861)

[Storage Encryption using key from AKV (secure data and apps) 21](#_Toc103598862)

[storage access policy: revoke (Manage identity and access) 21](#_Toc103598863)

[storage access policy lock (manage security operations) 21](#_Toc103598864)

[immutable Blob storage (manage security operations) 21](#_Toc103598865)

[storage security only from subnet (implement platform protection) 22](#_Toc103598866)

[storage security (implement platform protection) 22](#_Toc103598867)

[storage security config (implement platform protection) 22](#_Toc103598868)

[provision Azure AD Admin for SQL Server sql01 (implement platform protection) 23](#_Toc103598869)

[SQL server connection restriction (implement platform protection) 23](#_Toc103598870)

[ASC: Azure Security Center (implement platform protection) 23](#_Toc103598871)

[adaptive application control 23](#_Toc103598872)

[ASC recommendation 24](#_Toc103598873)

[ASC Auto Provisioning (manage security operations) 24](#_Toc103598874)

[Azure Container Registry vulnerability scanning of images 24](#_Toc103598875)

[PIM 24](#_Toc103598876)

[PIM (manage identity and access) 24](#_Toc103598877)

[need to elevate access to 24](#_Toc103598878)

[PIM create access review 24](#_Toc103598879)

[PIM two assignment types 25](#_Toc103598880)

[PIM example 25](#_Toc103598881)

[subscription 26](#_Toc103598882)

[transfer subscription billing ownership (manage identity access) 26](#_Toc103598883)

[Azure Blueprints (manage identity and access) 26](#_Toc103598884)

[management groups (implement platform protection) 26](#_Toc103598885)

[Lock App Service Plan (implement platform protection) 26](#_Toc103598886)

[virtual machines 26](#_Toc103598887)

[encryption tier (implement platform protection) 26](#_Toc103598888)

[VM disk encryption setup steps (secure data and apps) 27](#_Toc103598889)

[VM disk encryption steps (secure data and apps) 27](#_Toc103598890)

[VM disk encryption AKV requirement (secure data and apps) 27](#_Toc103598891)

[Microsoft enable Antimalware extension (implement platform protection) 27](#_Toc103598892)

[Microsoft Antimalware deploy extension (implement platform protection) 27](#_Toc103598893)

[Microsoft Antimalware scan schedule for VM1 (implement platform protection) 27](#_Toc103598894)

[compute permissions (manage identity access) 28](#_Toc103598895)

[permissions user can manage all VMs in RG (manage identity access) 28](#_Toc103598896)

[permissions user can manage AKV (implement platform protection) 29](#_Toc103598897)

[Locks (manage security operations) 29](#_Toc103598898)

[Lock VM (manage security operations) 29](#_Toc103598899)

[create policy to deploy (implement platform protection) 29](#_Toc103598900)

[create policy to deploy requires managed identity (secure data and apps) 30](#_Toc103598901)

[Azure automation state configuration 30](#_Toc103598902)

[ARM deploy Win VM (implement platform protection) 30](#_Toc103598903)

[Update Management (implement platform protection) 30](#_Toc103598904)

[Update Management example (implement platform protection) 31](#_Toc103598905)

[add network interface of VM1 to ASG (implement platform protection) 31](#_Toc103598906)

[steps to enable RDP on VM1 (implement platform protection) 31](#_Toc103598907)

[steps to set locks on VNet1 (implement platform protection) 31](#_Toc103598908)

[security baselines (implement platform protection) 31](#_Toc103598909)

[network (implement platform protection) 31](#_Toc103598910)

[HDInsight (manage identity and access) 31](#_Toc103598911)

[ASG 32](#_Toc103598912)

[NSG (implement platform protection) 32](#_Toc103598913)

[log network traffic basic steps 32](#_Toc103598914)

[log network traffic (manage security operations) 33](#_Toc103598915)

[log network traffic in storage account for 30 days (manage security operations) 33](#_Toc103598916)

[traffic rules 33](#_Toc103598917)

[route network traffic through VM1 (implement platform protection) 33](#_Toc103598918)

[VNet peering (implement platform protection) 33](#_Toc103598919)

[custom domain name (manage identity and access) 34](#_Toc103598920)

[Hybrid-networking hub and spoke (mjm) 34](#_Toc103598921)

[route table subnet map (implement platform protection) 35](#_Toc103598922)

[CIDR classless inter-domain routing 35](#_Toc103598923)

[BGP: Border Gateway Protocol (implement platform protection) 36](#_Toc103598924)

[NSG rule overview 37](#_Toc103598925)

[securing Apps 37](#_Toc103598926)

[enable SSL on website (secure data and apps) 37](#_Toc103598927)

[configure connection to contained SQL Db from SSMS (secure data and apps) 38](#_Toc103598928)

[connect VM to SQL contained Db user (secure data and apps) 38](#_Toc103598929)

[connect SSMS to SQL (secure data and apps) 38](#_Toc103598930)

[enable user to logon to contained dB with Azure AD account 38](#_Toc103598931)

[configure continuous deployment (secure data and apps) 38](#_Toc103598932)

[app registration to allow Microsoft Graph read directory access (secure data and apps) 38](#_Toc103598933)

[make SSL cert available in app code (secure data and apps) 39](#_Toc103598934)

[require storage account to use SSL (secure data and apps) 39](#_Toc103598935)

[ensure registered app can access AKV (secure data and apps) 39](#_Toc103598936)

[enable Advanced Data Security for SQL (secure data and apps) 39](#_Toc103598937)

[ATP for SQL (secure data and apps) 39](#_Toc103598938)

[enable Azure AD authentication for web app (secure data and apps) 39](#_Toc103598939)

[Azure Information Protection policy (secure data and apps) 40](#_Toc103598940)

[Azure Information Protection policy order (secure data and apps) 40](#_Toc103598941)

[Azure AKV restore (secure data and apps) 40](#_Toc103598942)

[Azure AKV restore New-AzureRmKeyVault (secure data and apps) 40](#_Toc103598943)

[Azure AKV enable ARM (secure data and apps) 41](#_Toc103598944)

[Azure AKV ensure user permissions (secure data and apps) 41](#_Toc103598945)

[Azure AKV enable runbook (secure data and apps) 41](#_Toc103598946)

[Azure AKV linked template (manage Identify and access) 42](#_Toc103598947)

[WAF (secure data and apps) 42](#_Toc103598948)

[configure SQL backup (secure data and apps) 42](#_Toc103598949)

[configure SQL always encrypted (secure data and apps) 42](#_Toc103598950)

[SQL contained database user (secure data and apps) 43](#_Toc103598951)

[Azure Front Door 43](#_Toc103598952)

[Cosmos DB 43](#_Toc103598953)

[Cosmos DB Add users and assign roles 43](#_Toc103598954)

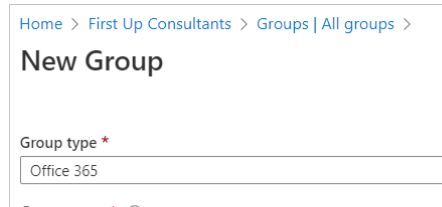
[miscellaneous 43](#_Toc103598955)

# AZ 500 Notes

## Azure AD Group and membership types (manage identity and access)

### Azure AD groups

1. two groups
   1. security
   2. Office 365



### Azure AD membership types

1. assigned
   1. can only add individual members
2. dynamic user
3. dynamic device

### dynamic membership rule (implement platform protection)

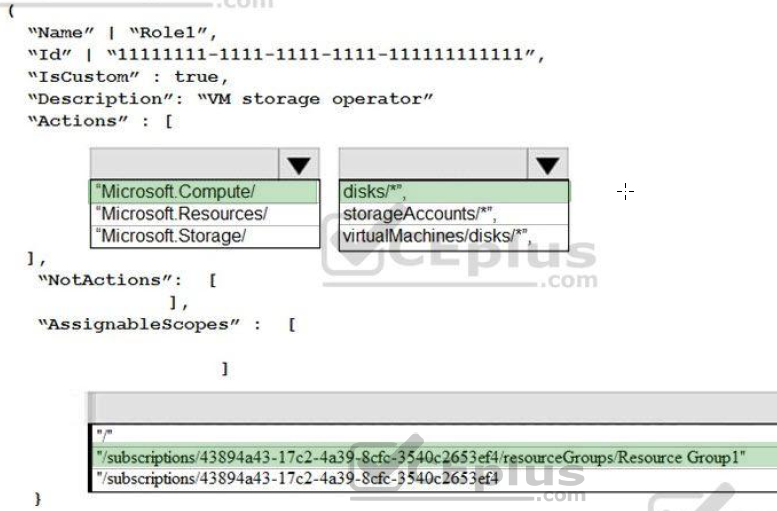
1. <https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership>
2. dynamic filter **not case sensitive**
   1. user.city -contains ”ON”
   2. user.city -match ”.\*on”

### Azure role definition (implement platform protection)

1. create new role definition
   1. steps to create
      1. create json file
      2. run cmdlet New-AzureRmRole**Definition**
      3. run cmdlet New-AzureRmRole**Assignment**

### Azure role example (secure data and apps)

1. create role permissions to allow
   1. admin of managed disks in RG1
   2. role must be available to RG1 only



#### dynamic user (manage identity access)

1. link
   1. <https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-create-rule>
2. can create a dynamic user membership type group
   1. for
      1. devices or
      2. for users
   2. but **can't create rule that contains both**
3. security groups can be used for either devices or users
   1. but Microsoft 365 Groups can be only user groups

## testing

### types of availability tests

1. three types of availability tests
   1. [URL ping test](https://docs.microsoft.com/en-us/azure/azure-monitor/app/monitor-web-app-availability#create-a-url-ping-test)
      1. simple test can create in Azure portal
   2. [Multi-step web test](https://docs.microsoft.com/en-us/azure/azure-monitor/app/availability-multistep)
      1. depend on Visual Studio webtest files
      2. sequence of web requests
         1. test more complex scenarios
         2. created in Visual Studio Enterprise
         3. uploaded to portal for execution
      3. **upload the web test**
         1. **in Application Insights portal**
            1. on Availability pane

select Create Test > Test type > Multi-step web test

* + - 1. set test
         1. locations
         2. frequency and
         3. alert parameters
  1. [Custom Track Availability Tests](https://docs.microsoft.com/en-us/dotnet/api/microsoft.applicationinsights.telemetryclient.trackavailability?view=azure-dotnet)
     1. the TelemetryClient.TrackAvailability() method
        1. to send results to Application Insights

1. **You can create up to 100 availability tests per Application Insights resource**

### multi-step web test (manage security operations)

1. ensure test can run unattended
   1. upload .webtest file to Application Insights

## monitoring

### monitor metrics of Linux VM Logs (manage security operations)

1. use Linux Diagnostic Extension (LAD)

### targeting monitoring (manage security operations)

1. three steps to targeting a solution
   1. **create** a **computer group**
   2. **create** as **scope** **configuration**
   3. **apply** the scope **configuration** to the solution

### Azure monitor alerts (manage security operations)

1. when create security alerts using Azure Monitor
   1. first create an Azure Log Analytics workspace

### Azure monitoring agent (manage security operations)

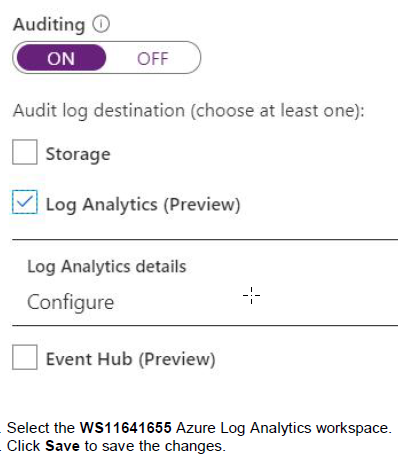
1. when turn on (enable) Auto provisioning
   1. from Azure Security Center
2. agent installed on
   1. all supported existing VMs
   2. any new supported
      1. Ubuntu 14.04 and up
3. connected to Log Analytics workspace

### LAWS Log Analytics workspace (implement platform protection)

1. VM **needs to be in same region and resource group?? NO**
   1. only in same subscription
   2. <https://docs.microsoft.com/en-us/azure/azure-monitor/insights/vminsights-configure-workspace?tabs=CLI#supported-regions>
2. SQL just needs to be in same subscription (manage security operations)
   1. <https://docs.microsoft.com/en-us/azure/azure-sql/database/audit-write-storage-account-behind-vnet-firewall#prerequisites>

### enable LAWS for SQLdb1 (manage security operations)

1. in portal type SQL in search box
2. select SQL databases then select SQLdb1
3. in **SQLdb1 properties**
   1. select **Auditing** in the security section
   2. **turn auditing** on if not already
      1. **check Log Analytics**
         1. then click Configure

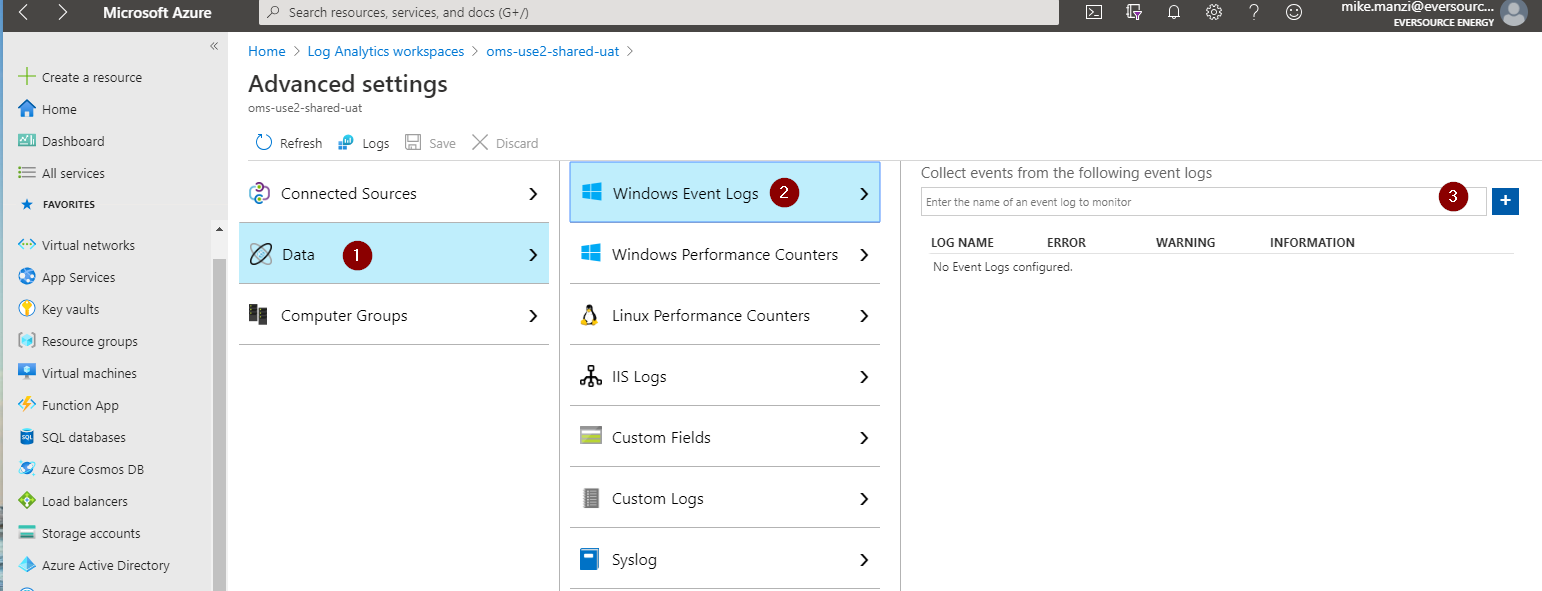


### LAWS ARM for VM (manage security operations)



### collect WIN event logs in LAWS (manage security operations)

1. locate desired Log Analytics Workspace
   1. click advanced
   2. select **data**
   3. select **windows Event Logs**
   4. add log
   5. check severities (error, warning, …)
   6. save



### collect Security Log Failures on VM in LAWS (manage security operations)

1. Step 1 create Log Analytics Workspace
2. Step 2 enable the logs analytics VM extension

### collect AzureBackupReport log in LAWS (manage security operations)

1. from Recovery Services Vaults
   1. select Vault1
   2. click **Add a diagnostic setting** link
   3. enter log name in Diagnostic Settings name box
   4. in Log section, select AzureBackupReport

### Azure Sentinel to ASC (manage security operations)

1. overview
   1. security playbook is collection of procedures
      1. can run from Azure Sentinel in response to alert
   2. can
      1. automate and orchestrate your response
         1. run manually
         2. run automatically when specific alerts are triggered
   3. security playbooks in Azure Sentinel are
      1. based on Azure Logic Apps
         1. get the
            1. power, customizability, and
            2. built-in templates of Logic Apps
   4. **each playbook is created for** 
      1. **specific subscription**
2. question
   1. how automate the migration of incidents in Azure Sentinel
3. options
   1. an alert rule
   2. a **playbook**
   3. a functional app
   4. a runbook

### security playbook (manage security operations)

1. configured to send email
2. to edit email
   1. use
      1. Azure Logical Apps Designer

### target a solution (manage security operations)

1. **create** a **computer** **group**
2. **create** a **scope** **configuration**
3. **apply** the scope **configuration** to a solution

## alerts

### alert state (manage security operations)

1. **alert state** can go from
   1. new to acknowledged
   2. acknowledged to closed
   3. **closed to new or acknowledged**

### email alert when CPU over 70% (manage security operations)

1. from selected resource
2. select **Alerts** **from monitoring section**
3. select **add metric alert**
   1. metric: CPU percentage
   2. condition: greater than
   3. period: last 15 min.
   4. notify via: email
   5. enter email

### email alert when resource lock is deleted (manage security operations)

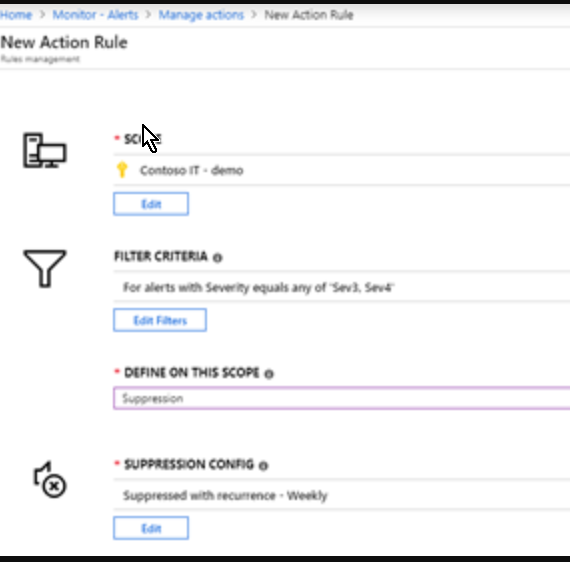
1. **from Monitor**
   1. **click Alerts**
      1. then +New Alert Rule
         1. set scope to
            1. resource type = locks
         2. select management locks
            1. in condition section
            2. select Delete management locks
            3. create action group

for notification type select Email…

….

### alert suppression (manage security operations)

1. suppressed alert won’t fire for scope item
2. [administrative alerts](#AdministrativeAlerts)
   1. includes start and stop VM
   2. not adding tags



### diagnostic logs

1. enable for storage account
   1. following to retrieve diagnostics logs
      1. Azure Storage Explorer
      2. AZCopy

### activity logs (manage security operations)

1. report control-plane events in subscriptions
   1. aka
      1. audit logs
      2. operational logs

## containers

### AKS cluster

1. when create AKS cluster
   1. Azure creates service principal
   2. use principal for authentication with ACR registry
      1. also need to create an Azure AD role assignment
         1. that grants cluster's service principal access
            1. to container registry

### AKS deployment (implement platform protection)

1. steps to deploy
   1. **create server app**
      1. provides user authentication
   2. **create client app**
      1. uses server app for authentication of credentials provided by client
   3. **deploy an AKS cluster**
      1. use **az group create** command to create the resource group
      2. use **az aks create** command **to deploy** the AKS cluster
   4. **create an RBAC binding**
      1. must create role-binding or cluster role-binding
      2. roles define permissions to grant to users
         1. can be assigned to
            1. namespace or
            2. across entire cluster

### AKS ingress controller (implement platform protection)

1. scenario
   1. given
      1. have disabled HTTP app routing
      2. need to implement app routing
         1. to provide reverse proxy
         2. and TLS termination
      3. for AKS services
         1. by using a single IP address
   2. answer
      1. create an AKS ingress controller
2. **AKS ingress controller** for Kubernetes services
   1. provides
      1. **reverse proxy**
      2. **configurable traffic routing**
      3. **and TLS termination**
   2. **single IP address** 
      1. used to route traffic
         1. **to multiple services in Kubernetes cluster**

### AKS service principal (implement platform protection)

1. scenario
   1. AKS cluster that will connect to ACR
   2. need **to use auto generated service principal for AKS Cluster**
      1. to authenticate to the ACR
   3. create options
      1. create secret in AKV
      2. create Azure AD user
      3. create Azure AD group
   4. solution
      1. **create a role assignment**

### Azure Container Registry

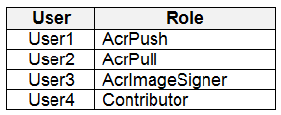
1. overview
   1. ACR is a managed, private Docker registry service
      1. stores and manages container images
      2. for Azure deployments in central registry

### ACR content trust

1. implements Docker's content trust model
   1. enabling pushing and pulling
      1. of signed images
2. to push trusted image to container registry
   1. enable content trust and
   2. push image with docker push
3. to work with trusted images
   1. both image
      1. publishers and
      2. consumers
   2. need to enable content trust
      1. for their Docker clients
   3. as publisher, can sign images
      1. pushed to content trust-enabled registry

### ACR permissions (manage identity access)

1. upload / down load image



* 1. can upload
     1. User 1 & 4
  2. can download
     1. User 1, 2 & 4

1. min two permissions needed to create trusted images in ContReg1
   1. AcrPush
   2. AcrImageSigner

### container groups (implement platform protection)

1. containers in container group share
   1. lifecycle
   2. resources
   3. local network and
   4. storage volumes
2. similar in concept to pod in Kubernetes
3. using container group
   1. Azure Container Instances support
      1. deployment of multiple containers onto single host
4. useful when building an
   1. application sidecar for
      1. logging
      2. monitoring
      3. where service needs second attached process
5. reference
   1. <https://docs.microsoft.com/en-us/azure/container-instances/container-instances-container-groups>

### container groups example (implement platform protection)

1. scenario
   1. application has two containers
      1. application container
      2. validation container
2. given
   1. need app and validation container
      1. scheduled to be deployed together
      2. containers must communicate with each other
         1. only on ports that are not externally exposed
3. options
   1. use ASG or NSG or management groups
4. solution
   1. use container group

### enable containers to use Azure Virtual Network capabilities (implement platform protection)

1. Azure **CNI** (container network interface)
   1. **plugin installs on VMs** (Linux and Win)
      1. assigns IP address from virtual network
         1. to containers in VM
   2. attaching to VNet and connecting directly
      1. to other containers and VNet resources does
         1. not rely on overlay networks or routes
            1. for connectivity and
            2. provides same performance as VM’s

### container.yaml

1. variables
   1. defined secretValue
      1. can only be accessed from inside container defined

## Azure Firewall

### AzureFirewallSubnet (implement platform protection)

1. Azure firewall needs dedicated subnet
   1. named AzureFirewallSubnet

### conflict ASC JIT feature (implement platform protection)

1. Azure Security Center and JIT conflict
   1. problem
      1. if VM is accessed using JIT
         1. and in same subnet with user-defined route
            1. that points to Azure Firewall as default gateway
      2. ASC JIT doesn’t work
         1. result of asymmetric routing
            1. packet comes on VM’s public IP (JIT opened the access)

but the return path is via firewall

drops packet because no established session on firewall

* 1. solution
     1. place the **JIT VMs on separate subnet**
        1. that **doesn’t have** **user-defined route to firewall** as default gateway
  2. <https://aviatrix.com/learn-center/cloud-security/azure-firewall/>

### RDP through firewall to VM with private (itexams Q11)

1. create new subnet
   1. name it AzureFirewallSubnet
2. deploy Azure Firewall
3. create NAT rule collection

### steps to install firewall (implement platform protection)

1. install on VNet3
   1. configure VNet3
      1. select virtual networks
         1. find VNet3
      2. in overview section
         1. **note** VNet
            1. **location - region**
            2. **resource group name**
      3. click Subnets
         1. **add new subnet**
            1. **name it AzureFirewallSubnet**
            2. enter ip range for subnet

in Address range box

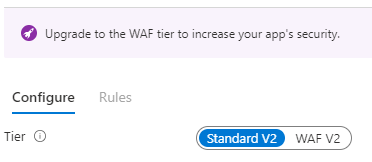
* + 1. click OK
  1. add **Azure Firewall**
     1. in VNet3 settings
        1. click Firewall
     2. select **Click here to add a new firewall**
     3. **resource group** will **default to that of VNet**3
     4. enter firewall name
     5. in **region select same as VNet**3
     6. in Public IP address
        1. select an available public IP address or add new
        2. click Review + create
        3. verify and click Create button

### Configure network address translation NAT rule

1. can create load balancer inbound NAT rule
   1. to forward traffic from specific port of front-end IP address
   2. to specific port of a back-end VM
2. allow RDP traffic to VM with no public IP
   1. open the **RG-DNAT-Test** and select the **FW-DNAT-test** firewall
   2. on the **FW-DNAT-test** page, under **Settings**, select **Rules**
   3. select **Add NAT rule collection**
   4. for **Name**, type **RC-DNAT-01**
   5. for **Priority**, type **200**.
   6. under **Rules**, for **Name**, type **RL-01**
   7. for **Protocol**, select **TCP**
   8. for **Source Addresses**, type \*.
   9. for **Destination Addresses** type the firewall's public IP address
   10. for **Destination ports**, type **3389**
   11. for **Translated Address** type private IP address for the VM
   12. for **Translated port**, type **3389**
   13. Select **Add**

### enable App firewall on App Gateway (secure data and apps)

1. to inspect for malicious requests
   1. from portal select App Gateway
   2. from properties
      1. click on **Web application firewall**
      2. for Tier setting select **WAF V2**



* + 1. in Firewall status, slide to Enabled
    2. in Firewall mode, slide to Prevention
    3. click save

### enable disk encryption access through AKV firewall (secure data and apps)

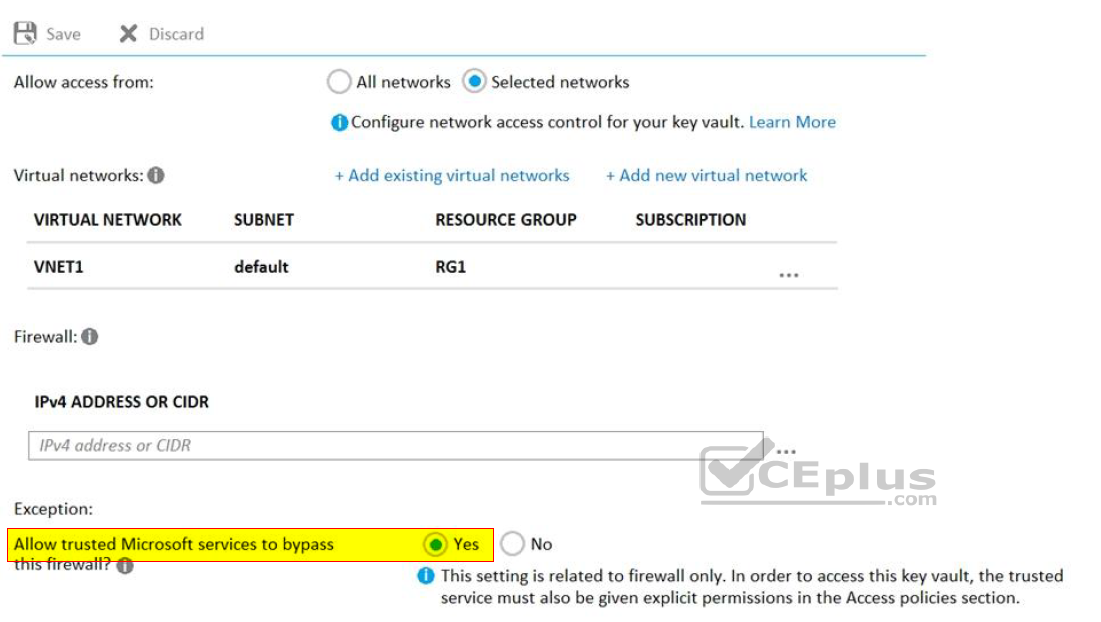
1. from portal, select vault, in networking section
   1. **allow trusted Microsoft services to bypass**
      1. includes
         1. Azure Disk Encryption volume encryption service
            1. allow access to

BitLocker Key (Windows VM) or

DM Passphrase (Linux VM)

and Key Encryption Key

* + - * 1. during VM deployment
      1. Azure Virtual Machines deployment service
         1. allow deploy certificates to VMs from customer-managed Key Vault
      2. Azure Storage Service
         1. encryption using customer-managed keys in AKV
      3. ARM template deployment service
      4. Azure Application Gateway v2 SKU
         1. TLS termination with AKV certificates
      5. APIM
         1. Deploy certs for Custom Domain from key vault using MSI
      6. …
         1. <https://docs.microsoft.com/en-us/azure/key-vault/general/overview-vnet-service-endpoints#trusted-services>
  1. **must give explicit permission in Access Policies Section**



## JIT (manage identity access)

### request access

1. in Azure portal
   1. open VMs pages
2. select VM to connect to
3. select connect
4. [request access](#RequestAccess)

### JIT enabling (implement platform protection)

1. to enable JIT
   1. **NSG needs to be enabled**
      1. either at VM level
      2. or subnet level
2. ports
   1. 20 - FTP - for data transport
   2. 21 - FTP - for command and control
   3. 22 - SSH
   4. 25 - SMTP
   5. 80 - HTTP
   6. 443 - HTTPS
   7. 3389 - RDP
   8. **5985** - **TCP** (HTTP) Transmission Control
   9. **5986** - **TCP** (HTTPS)
3. ranges
   1. well known ports: 0 through 1023
   2. registered ports: 1024 through 49151
   3. dynamic/private : 49152 through 65535

### JIT permissions for PowerShell on VM (manage security operations)

1. user needs write permissions
2. need to enable TCP port 5986

## authentication

### MFA Setup (manage identity access)

1. from portal
   1. select Active Directory
      1. select Security
         1. select MFA

### SSO

1. **password hash** synchronization
   1. requires least effort regarding
      1. deployment
      2. maintenance
      3. infrastructure
   2. applies to orgs that only need
      1. to sign in to Office 365
      2. SaaS apps
      3. Azure AD-based resources
   3. password hash synchronization
      1. part of the Azure AD Connect sync process
         1. runs every two minutes
   4. <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-password-hash-synchronization>
      1. two types of password policies affected
         1. by enabling password hash synchronization
            1. password complexity policy
            2. password expiration policy
2. **federated** authentication
   1. relies on an external trusted system to authenticate users
      1. some want to reuse existing federated system
      2. investment with their Azure AD hybrid identity solution
   2. maintenance and management
      1. falls outside control of Azure AD
      2. orgs responsibility to ensure
         1. deployed securely
         2. can handle authentication load
3. **pass-through** authentication
   1. need lightweight agents one or more (recommend three)
      1. installed on existing servers
         1. must have access to
            1. on-premises Active Directory Domain Services
            2. including on-premises AD domain controllers
            3. need outbound access to Internet and
            4. access to domain controllers
         2. for this reason
            1. not supported to deploy agents in perimeter network
   2. pass-through Authentication requires
      1. unconstrained network access to domain controllers
      2. all network traffic is encrypted and limited to authentication requests

### Azure AD: undelete (Manage identity and access)

1. restore deleted Microsoft 365 group in Azure AD
   1. restricted **exclusively to Microsoft 365 groups** in Azure AD
      1. not available for
         1. security groups
         2. distribution groups
   2. **30-day** group restoration period not customizable

### Azure AD Connect: Synchronization Rules Editor (Manage identity and access)

1. use **Synchronization Rules Editor to filter accounts**
   1. synced to Azure AD

### Azure AD Connect: Accounts and permissions (Manage identity and access)

1. synchronize info from Windows Server AD to Azure AD
   1. need three accounts
      1. **AD DS Connector** account
         1. to read/write info **to Windows Server Active Directory**
      2. **ADSync service** account
         1. to run synchronization service and access the SQL database
      3. **Azure AD Connector** account
         1. to write information **to Azure AD**
2. run Azure AD Connect
   1. four accounts used
      1. **Local Admin**istrator account
         1. admin installing Azure AD Connect and
            1. has local Administrator permissions on the machine
      2. **AD DS Enterprise Admin**istrator account
         1. optionally
            1. used to create the “AD DS Connector account” above.
      3. **Azure AD Global Admin**istrator account
         1. used to create the Azure AD Connector account and configure Azure AD.
      4. **SQL SA account**
         1. (optional)
            1. used to create the ADSync database when using full version of SQL
3. **express installation** Azure AD Connect (manage identity access)
   1. two accounts **need**ed
      1. **AD DS Enterprise Admin**istrator credentials
      2. **Azure AD Global Admin**istrator credentials

### Azure AD Identity Protection (Manage identity and access)

1. Azure AD Identity protection
   1. <https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa>
   2. detects six types of suspicious sign-in activities



1. **Azure IP three policies** are available
   1. **user risk policy**
      1. identifies and responds to user accounts with possible compromised credentials
      2. can prompt user to create new password
   2. **sign in risk policy**
      1. identifies and responds to suspicious sign-in attempts
      2. can prompt user to provide additional forms of verification
         1. using Azure MFA
   3. **MFA registration policy**
      1. makes sure users are registered for Azure MFA
      2. if sign-in risk policy prompts for MFA
         1. user must already be registered for Azure MFA

### Azure AD sensitivity label (Manage security operations)

1. need to create a custom sensitive information type
   1. customize a built-in sensitive info type
      1. <https://docs.microsoft.com/en-us/microsoft-365/compliance/customize-a-built-in-sensitive-information-type?view=o365-worldwide#modify-the-xml-and-create-a-new-sensitive-information-type>

### configure how end-user consents to applications (manage identity access)

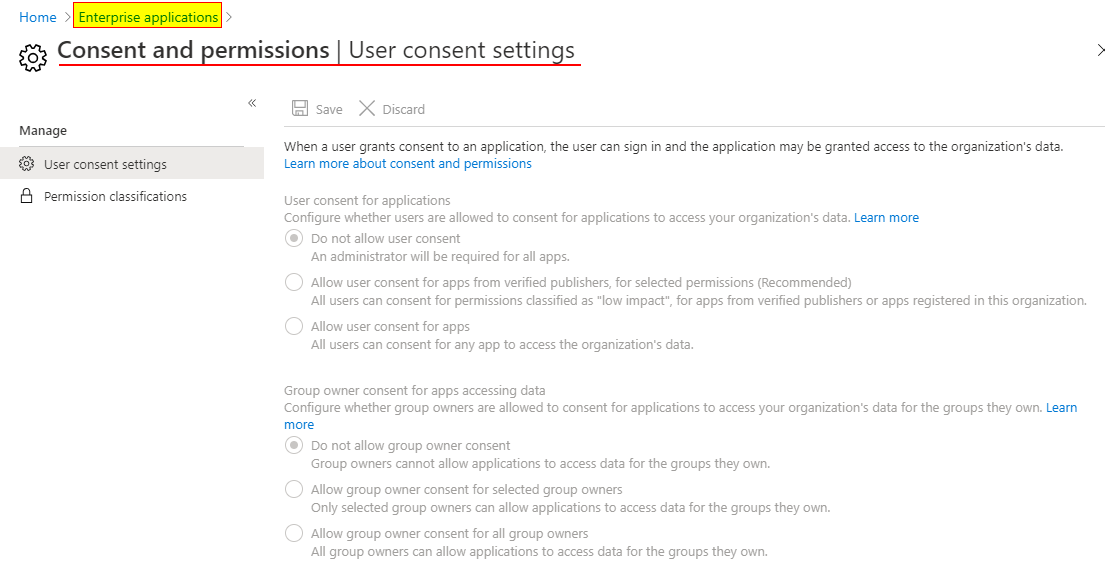
1. ref: <https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consent?tabs=azure-portal>
   1. configure user consent settings through Azure portal
      1. sign in as Global Admin
      2. select **Azure Active Directory** >
         1. **Enterprise applications** >
            1. **Consent and permissions** >

**User consent settings**

* + 1. under User consent for applications
       1. select which consent setting to configure for all users
    2. Select Save to save your settings.

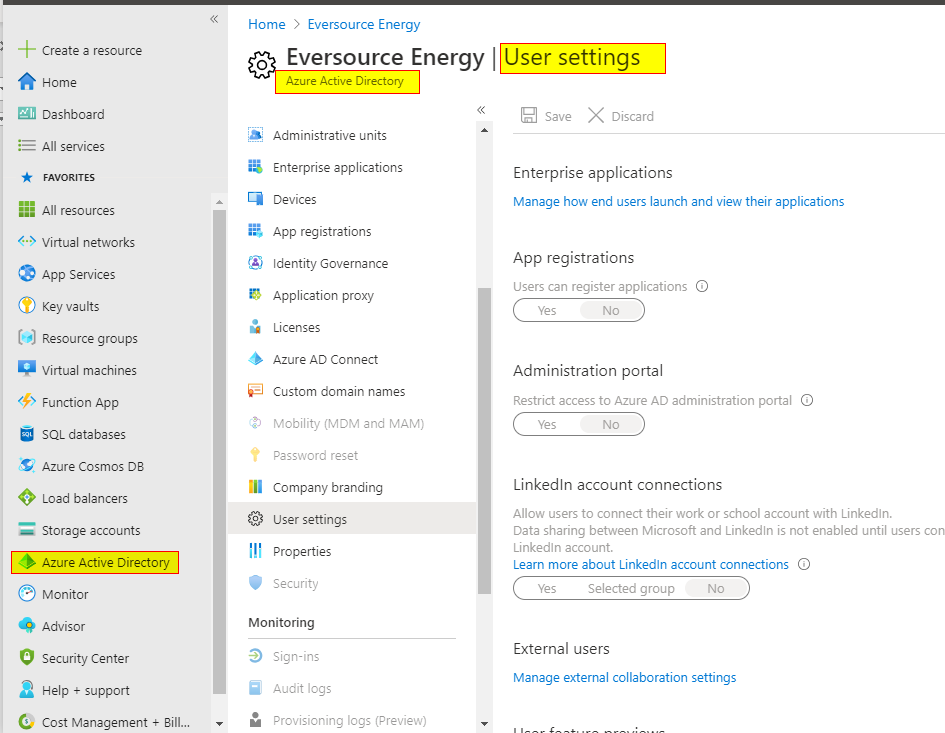
### configure consent settings

1. in Enterprise Applications



### configure registration settings

1. in Azure AD User settings



### allow or block invitations to B2B users (manage identity access)

1. select Azure Active Directory > **Users** > **User settings**
2. under External users
   1. select **External collaboration settings**

### app registration (manage identity access)

1. sign into Portal
2. select **Azure AD**
3. select **App Registrations**
4. select New Registration
5. name the App
   1. select supported account type
      1. determines who can use the app
6. under redirect URI
   1. select web
      1. for type of app
   2. enter a url
   3. click register

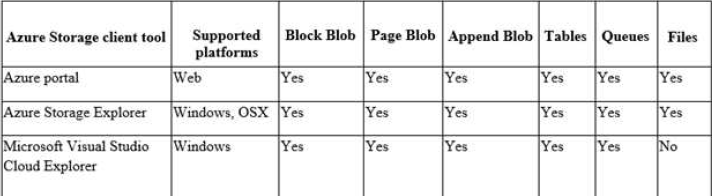


1. create a new app secret (if not creating a cert)
   1. select certificates & secrets
   2. select client secrets
      1. new client secret
   3. provide a description of the secret and duration
   4. select add
      1. be sure to copy key
         1. can’t retrieve later

## storage

### (GUI) tools (manage security operations)

1. tools for working with data in Azure Storage account
2. can use SAS with Azure Storage Explorer
   1. **S**hared **A**ccess **S**ignature
   2. to access contents in
      1. container blob file
      2. file share



### Storage Encryption using key from AKV (secure data and apps)

1. **from storage account**
   1. on settings blade, **click encryption**
      1. select **use your own key** option
   2. choose Select from Key vault option
      1. assumes already have AKV with desired key
   3. choose key vault123
      1. holding key
   4. choose key

### storage access policy: revoke (Manage identity and access)

1. to **revoke a stored access policy**
   1. can either
      1. **delete** policy **or**
      2. **rename** policy
   2. by changing signed identifier
      1. breaks associations
         1. between any existing signatures and
         2. stored access policy
   3. deleting or renaming stored access policy
      1. immediately affects all **s**hared **a**ccess **s**ignatures
2. don’t simply regenerate the access keys
3. don’t put a lock on storage access account

### storage access policy lock (manage security operations)

1. given
   1. to prevent blobs in container1 from being modified
2. options
   1. from container1 change access level
   2. from container1 modify Access Control (IAM) settings
   3. from storage1 enable soft delete
3. solution
   1. add an access policy

### immutable Blob storage (manage security operations)

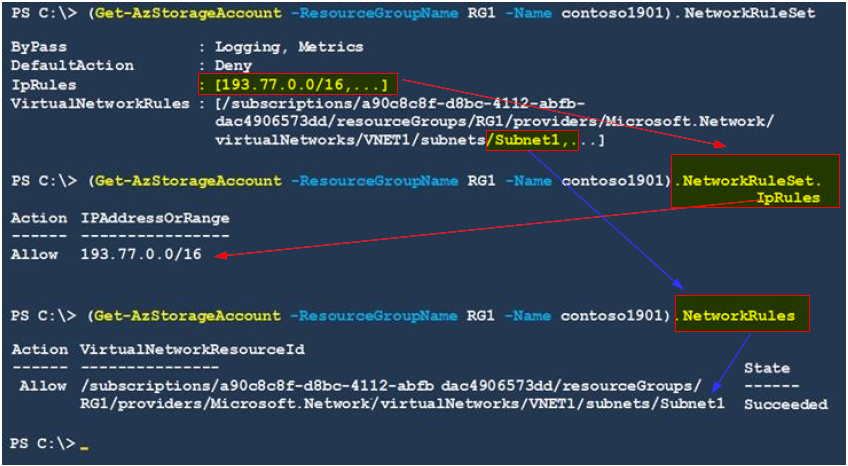
1. **blob two types of WORM policies** 
   1. **time-based retention**
   2. **and legal holds**
      1. all existing blobs move into an immutable WORM state in less than 30 seconds
      2. all new blobs uploaded to that policy protected container also move into an immutable state
      3. once all blobs in immutable state
         1. immutable policy is confirmed
         2. and any overwrite or delete operations in the immutable container are not allowed.
2. container and storage account **deletion**
   1. **not** **permitted** **if** any blobs in container protected by
      1. **legal** **hold** or
      2. **locked** **time-based** **policy**
3. only container with locked time-based policy
   1. will protect against storage account deletions
   2. **unlocked time-based policies**
      1. **not offer storage account deletion protection** nor compliance

### storage security only from subnet (implement platform protection)

1. from storage account stg1
   1. click **Firewalls and virtual networks**
      1. choose **allow access from selected networks**
      2. click save
2. in storage account
   1. click **Firewalls and virtual networks**
   2. to **grant access to VNet**
      1. click Add existing VNet
      2. select **Virtual Networks and Subnets** option
         1. enter IP of subnet
3. note
   1. can limit access to storage
      1. to request originating from
         1. specific IP addresses
         2. IP range or
         3. list of subnets

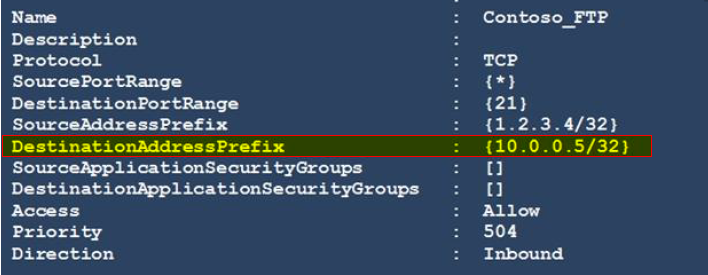
### storage security (implement platform protection)

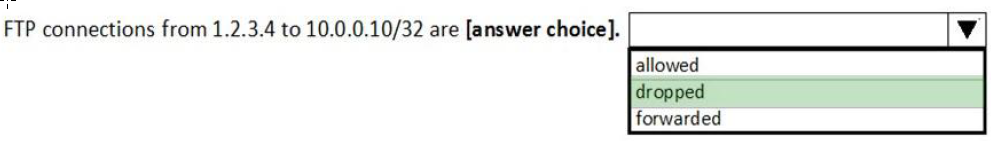
1. result is only IP and Subnet1 have access



### storage security config (implement platform protection)

1. Port 21 is FTP
2. Protocol is good
3. IP Address **.10** not match **.5** mask





### provision Azure AD Admin for SQL Server sql01 (implement platform protection)

1. in portal search box
   1. type SQL Server
2. in **SQL Server properties** page
   1. click on **Active Directory Admin**
      1. click the **Set Admin** button
   2. in **Add Admin window**
      1. **search** for SQL server **sql01**
      2. click **Select** button to add
      3. click **save**

### SQL server connection restriction (implement platform protection)

1. in portal search box
   1. type SQL Server
2. in **SQL Server properties** page
   1. click on **Firewalls and virtual networks**
      1. click **Add existing** button
   2. in **Create/Update virtual network rule** window
      1. in **Virtual Network box**, select VNet01
      2. in **Subnet name** box, select Subnet0
      3. click **OK** to save rule
      4. back on Firewalls and virtual networks window
         1. set **Allow access to Azure services** to **On**

## ASC: Azure Security Center (implement platform protection)

### adaptive application control

1. in Azure Security Center
   1. **adaptive application control**
      1. is **intelligent automated end-to-end a whitelisting solution**
      2. helps control which apps can run
         1. on Azure and non-azure VMs
         2. Win and Linux
      3. helps harden against malware

### ASC recommendation

1. install endpoint protection solution
   1. means add Microsoft Antimalware extension to VM

### ASC Auto Provisioning (manage security operations)

1. off by default
2. when on
   1. Security Center deploys the Log Analytics agent
      1. on all supported Azure VMs
      2. and any new ones that are created

### Azure Container Registry vulnerability scanning of images

1. enable in Registry1
   1. **only Linux scanned**
      1. Windows not scanned
2. if enable Image scanning after pushed images
   1. must push again to start scanning
   2. <https://medium.com/faun/azure-container-registry-image-scanning-aaeae84d1c0c>

## PIM

### PIM (manage identity and access)

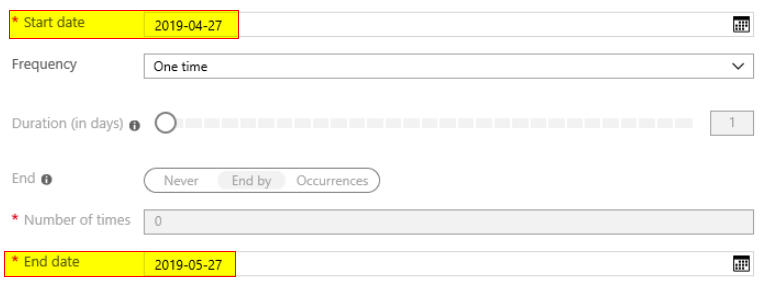
1. steps to turn on
   1. **must be Global Admin**
      1. not Security Admin
   2. **consent to PIM**
   3. **verify identify via MFA**
   4. **sign up PIM for Azure AD roles**

### need to elevate access to

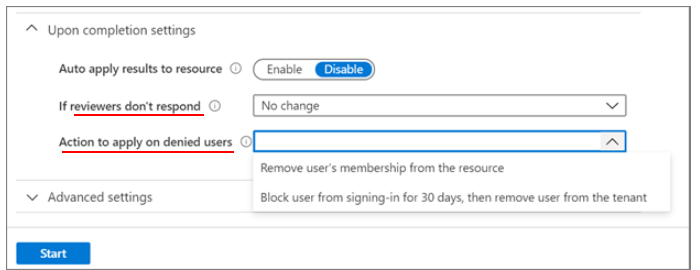
1. Global Administrator in Azure AD
   1. might not have access to all subscriptions
      1. and management groups in your directory
2. can elevate access to
   1. see all subscriptions and management groups
   2. regain access to Azure subscription
      1. or management group
      2. when user has lost access
   3. grant another user or yourself access
      1. to Azure subscription or management group
   4. allow an automation app
      1. such as an invoicing or auditing app
      2. to access all Azure subscriptions
         1. or management groups

### PIM create access review

1. steps
   1. **create** an access **review program**
   2. **create** an access **review control**
   3. **set** reviewers to **group owners**
2. link
   1. <https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>
      1. prerequisites
         1. Azure AD Premium P2
         2. Global or User admin
   2. <https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review>
      1. start date
         1. default
            1. review occurs once
            2. starts same time it's created
            3. ends in one month



* + 1. if reviewers don't respond
       1. no change - leave user's access unchanged
       2. remove access - remove user's access
       3. approve access - approve user's access
       4. take recommendations - take the system's



### PIM two assignment types

1. **eligible** 
   1. requires role member to perform an action
      1. before can use role
         1. MFA check
         2. providing a business justification
         3. or requesting approval from designated approvers
2. **active** 
   1. not require member to perform action
      1. to use the role
      2. assigned as active have privileges assigned
         1. to role always

### PIM example

1. given
   1. user marked eligible
   2. requires MFA for activation = true
   3. user has MFA disabled
2. result
   1. user can’t request role activation

## subscription

### transfer subscription billing ownership (manage identity access)

1. sign in to portal as administrator of billing account
   1. **Billing Administrator**
2. all user groups or service principals who had role base access
   1. lose their access
      1. to manage subscriptions and its resources
   2. only user in new account who accepts transfer
      1. will have access to manage resources
3. can only transfer subscription to email part Azure AD Tenants

### Azure Blueprints (manage identity and access)

1. enables cloud architects
   1. to define repeatable set of Azure resources
      1. that adheres to org's standards, patterns, and requirements
2. declarative way to orchestrate deployment
   1. of various resource templates
   2. and other artifacts
      1. Role Assignments
      2. Policy Assignments
      3. Azure Resource Manager templates
      4. Resource Groups

### management groups (implement platform protection)

1. are container objects that encompass
   1. one or more Azure subscriptions
   2. subscriptions in group receive entries by simple inheritance
      1. Azure Policy or
      2. RBAC
2. solves problem of needing to impose governance policy
   1. on more than one Azure subscription simultaneously
3. however, need to use an initiative, not a resource graph
   1. to bundle policy definitions into a group
      1. that can be applied to the management group
4. can create a policy initiative and assignments scoped to management group
   1. not a resource group

### Lock App Service Plan (implement platform protection)

1. from Azure portal
   1. App Service Plans from search
   2. select Homepage
   3. in properties click Locks
   4. click Add
   5. enter name
   6. select Lock type of Read-Only

## virtual machines

### encryption tier (implement platform protection)

1. VM’s minimum
   1. tier
      1. at least Standard
         1. not basic
   2. type
      1. L4s not supported
   3. OS
      1. Ubunto 16.04 and up supported

### VM disk encryption setup steps (secure data and apps)

1. create an Azure key vault
2. configure access policies for AKV
3. run Set-AzureRmVmDiskEncryptionExtension

### VM disk encryption steps (secure data and apps)

1. <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-portal-quickstart>
2. select **VM**
3. on left-hand sidebar, select **Disks**
4. on top bar, select **Additional Settings**
5. under **Encryption settings** > **Disks to encrypt**, select **OS and data disks**
   1. choose **Select a key vault and key for encryption**
      1. select **Create New**
6. on the **Access Policies** tab
   1. check the **Azure Disk Encryption for volume encryption** box

### VM disk encryption AKV requirement (secure data and apps)

1. **VM and AKV must be in same subscription and geography**
   1. **can restore to any region in geography**
   2. data sovereignty

### Microsoft enable Antimalware extension (implement platform protection)

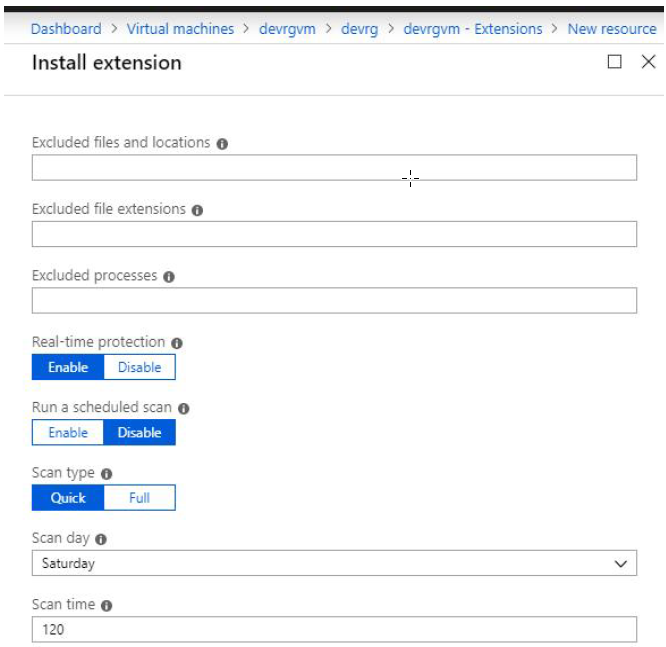
1. ways to enable
   1. VMs
      1. in Azure **portal**
         1. under security extensions
      2. using **Visual Studio virtual machines configuration in Server Explorer**
         1. under security extensions
   2. VMs and Cloud Services
      1. using Antimalware **classic deployment** model
      2. using Antimalware **PowerShell** cmdlets

### Microsoft Antimalware deploy extension (implement platform protection)

1. deployed as an extension
   1. not windows feature
2. create custom policy definition set to
   1. depolyIfNotExists
      1. Append: used to add fields to resource during creation or update
         1. i.e. cost center
3. create a policy assignment and modify
   1. the create managed identifier setting
      1. Azure policy runs depolyIfNotExists policy using a managed identity

### Microsoft Antimalware scan schedule for VM1 (implement platform protection)

1. from portal
   1. go to Azure VM1’s blade
      1. in settings **click on Extensions**
      2. press Add
   2. scroll down select the ‘Microsoft Antimalware’ extension
   3. click Create
   4. complete the ‘install extension’ form as desired press OK
      1. scan day field
      2. scan time field



### compute permissions (manage identity access)

1. does not include attaching network interface to VM to VNet

### permissions user can manage all VMs in RG (manage identity access)

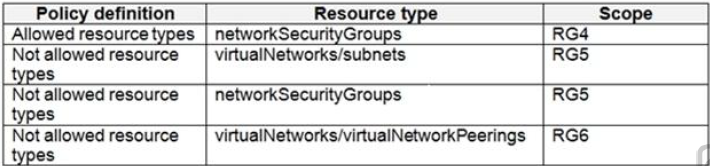
1. in portal select RG
   1. click **Access control (IAM)**
   2. click **Role assignment** tab
      1. to view all role assignments
         1. at this scope
   3. click **Add** then
      1. click **Add role assignment**
         1. opens **role assignment** pane
   4. in **Role drop-down**
      1. **select** role **Virtual Machine Contributor**
         1. **can manage VM**
         2. **but can’t**
            1. access them
            2. their virtual network
            3. storage account
      2. click Save to assign role
2. Resource Group roles permissions
   1. owner role
      1. only owner can change permissions
   2. contributor role
      1. can create, modify, delete anything
      2. but can’t change permissions

### permissions user can manage AKV (implement platform protection)

1. use key vault access policy
   1. can grant permissions separately to
      1. keys
      2. secrets
      3. certifications
2. use RBAC
   1. for finer grained control

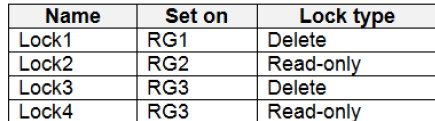
### Locks (manage security operations)

1. what resource groups can VNet be created given



* 1. can create VNET only in RG6
     1. RG4 allowed means everything else is denied
     2. RG5 implied can’t create a VNET because need Subnet and is not allowed

1. which VNets can owner delete (VNet 1 through 4)



* 1. only Vnet4 in RG4
     1. only RG4 does not have a lock
     2. **can’t delete if Read-only lock or Delete lock** is active

### Lock VM (manage security operations)

1. <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources#considerations-before-applying-locks>
2. read-only lock on resource group
   1. that contains VM
      1. prevents starting or restarting VM
         1. requires POST request

### create policy to deploy (implement platform protection)

1. when use DeployIfNotExists
   1. then need to use a template
   2. not a resource or existenceCondition
2. built-in policies
   1. Allowed Storage Account SKUs (deny)
      1. effect denies all storage accounts that don't adhere to set of defined SKU sizes
   2. Allowed Resource Type (deny)
      1. effect denies all resources that aren't part of defined list
   3. Allowed Locations (deny)
      1. effect used to enforce your geo-compliance requirements
   4. Allowed Virtual Machine SKUs (deny)
      1. specifies a set of virtual machine SKUs you can deploy
   5. Add a tag to resources (modify)
      1. applies required tag and default value
         1. if not specified by deploy request
   6. Not allowed resource types (deny)
      1. prevents list of resource types from being deployed

### create policy to deploy requires managed identity (secure data and apps)

1. requires managed identity
   1. DeployIfNotExists
2. following policies do not
   1. AuditIfNotExist
   2. Append
   3. Deny

### Azure automation state configuration

1. use to manage Azure VM’s
   1. classic and resource manager
   2. Win / Linux
      1. on-premises / cloud
   3. AWS & VMs
2. provides a DSC pull server
   1. like Windows Feature DSC-service
      1. so, target nodes automatically receive configurations
         1. eliminates need to setup and maintain
      2. conform to desired state
      3. report back compliance

### ARM deploy Win VM (implement platform protection)

1. to deploy with disabled **Windows feature**
   1. use Azure DSC virtual machine extension
      1. DCS: **desired state configuration**
2. works across subscriptions

### Update Management (implement platform protection)

1. link
   1. <https://docs.microsoft.com/en-us/azure/automation/update-management/update-mgmt-overview?toc=%2Fazure%2Fautomation%2Ftoc.json>
2. enable for VMs following ways
   1. from Azure automation account
      1. for one or more azure and non-azure machines
   2. manually for non-azure machines
      1. including machines or servers registered with Azure ARC enabled servers (preview)
   3. from VM page in Azure portal
      1. for single Azure VM
         1. for Linux and Windows VMs
3. Update Management
   1. requires linking Log Analytics workspace
      1. to Automation account
      2. for supported regions
         1. see [**Azure Workspace mappings**](https://docs.microsoft.com/en-us/azure/automation/how-to/region-mappings).
         2. region mappings not affect ability to manage VMs
            1. in separate region from Automation account
   2. can't use machine configured
      1. with Update Management
         1. to run custom scripts from Azure Automation
      2. this machine can only run
         1. Microsoft-signed update script

### Update Management example (implement platform protection)

1. update will run for all OS version for VM’s across resource groups
2. Linux machines must have access to update repository

### add network interface of VM1 to ASG (implement platform protection)

1. select desired VM
2. under Settings
   1. select Network
      1. select configure app security groups
         1. select application security groups want to
         2. add or remove from network interface

### steps to enable RDP on VM1 (implement platform protection)

1. select VM1
2. in Settings, select networking
3. in inbound port rules
   1. ensure the following
      1. priority: 300
      2. name: port3389
      3. protocol: tcp
      4. source: any
      5. destinations: any
      6. action: allow

### steps to set locks on VNet1 (implement platform protection)

1. select Virtual Networks
2. select VNet1
3. from settings blade
   1. select Locks
   2. select Add
   3. select Lock type of Delete Lock
   4. select OK

### security baselines (implement platform protection)

* 1. use **MDM security baselines in Intune**
     1. to **configure Windows 10 devices**
  2. applies to
     1. Windows 10 version 1809 and later

## network (implement platform protection)

### HDInsight (manage identity and access)

1. <https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network>
2. connect HDInsight to on-prem using
   1. create site-to-site VPN between VNet and on-prem
      1. create an Azure VNet
      2. create custom DNS server in the VNet
      3. configure vnet to use custom DNS
         1. instead of default Azure Recursive Resolver
      4. configure forwarding between
         1. custom DNS server
         2. and on-prem DNS server
3. don’t
   1. deploy on-premises data gateway to on-premises network

### ASG

1. all network **interfaces assigned to ASG**
   1. **must exist in same VNET** as first assigned

### NSG (implement platform protection)

1. allow traffic from internet to VNet1\subnet0 only over TCP port 7777
   1. in portal type **Virtual Networks** in search
      1. select Virtual Networks
      2. then select VNet1
      3. in VNet1 properties
         1. click Subnets
            1. note NSG name of Subnet0
   2. in portal type **Network Security Groups** in search
      1. select the NSG of Subnet0
         1. click Inbound Security Rules
         2. click Add to add new rule
            1. in Source field

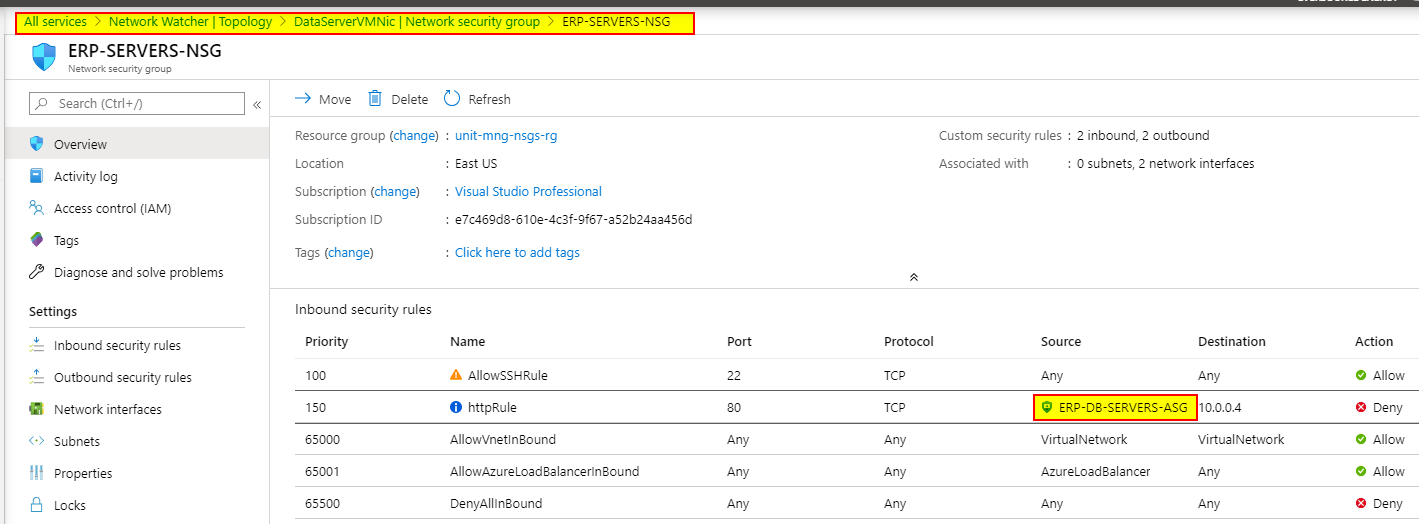
select Service Tag

* + - * 1. **in Source Service Tag**

**select internet**

* + - * 1. leave source port range at \* and destination at all
        2. in Destination port range enter 7777
        3. change Protocol to TCP
        4. Leave action at Allow
        5. Priority at 100
        6. Name and save

1. sample



### log network traffic basic steps

1. ensure network watcher is configured.
2. Azure subscription with Insights provider installed
3. existing Network Security Group
4. storage account
   1. must be in same region as NSG

### log network traffic (manage security operations)

1. create VM that uses an NSG
2. enable **Network Watcher**
3. **register Microsoft Insights** provider
4. **enable** a traffic flow log for an NSG
   1. using network watcher’s **NSG flow log** capability

### log network traffic in storage account for 30 days (manage security operations)

1. **select NSG**
   1. select **Diagnostic Settings**
   2. click **Add diagnostic settings link**
   3. provide name
      1. in Log section, select log
      2. in Destination details select **archive to a storage account**
      3. in storage account field select storage account
      4. in retention enter 30
      5. save

### traffic rules

1. general
   1. ping is ICMP not TCP traffic
   2. HTTP/s traffic is on port 80 or 443
   3. all traffic out to internet is allowed
   4. VM in different VNet can’t communicate by default
2. Internet Control Message Protocol (ICMP)
   1. network layer protocol
   2. used to diagnose network communication issues

### route network traffic through VM1 (implement platform protection)

1. two types of routes
   1. user defined route
   2. system defined route
      1. most environments only need system routes already defined by Azure
2. user defined routes
   1. may need to create route table
      1. and add one or more routes
         1. for specific cases, such as
            1. force tunneling to Internet via on-premises network
            2. use of virtual appliances in your Azure environment
            3. want to route network traffic through a VM

### VNet peering (implement platform protection)

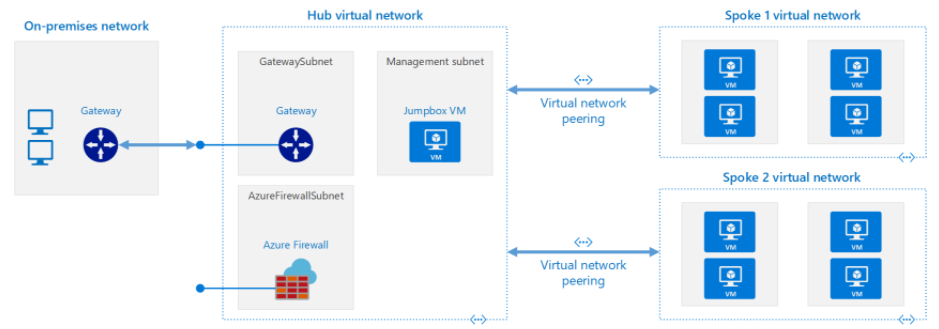
1. given
   1. configure network connectivity between VNet 1 & 2
   2. ensure VMs on VNet1 can communicate with VM’s on VNet2
   3. assuming one-way communication
2. solution is VNet peering
   1. in portal type Virtual Networks in search
      1. select Virtual Networks
         1. then **select VNet1**
      2. **in VNet1 click on Peering**
      3. in Peering blade
         1. click Add
         2. in **Name of the peering from Vnet1 to remote virtual network** box
            1. enter name like: VNet1-2
         3. in Virtual Network box select VNet2
         4. in **Name of the peering from remote virtual network to VNet1** box
            1. enter name like: VNet2-1
         5. option **Allow virtual network access from VNET to remote virtual network**
            1. should remain enabled
         6. option **Allow virtual network access from remote virtual network to VNET1**
            1. should disable
      4. click OK

### custom domain name (manage identity and access)

1. create **custom domain name**
   1. need to create three records
      1. **root "A" record** pointing to contoso.com
      2. **root "TXT" record** for verification
      3. **"CNAME" record** for the www name that points to the A record
2. to **use https**
   1. upload a **PFX file** to Azure Web App
      1. PFX file will contain SSL certificate required for HTTPS

### Hybrid-networking hub and spoke (mjm)

1. source
   1. <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke>



1. architecture components
   1. on-premises network
   2. VPN device
   3. gateway
      1. VPN VNet gateway or
      2. ExpressRoute gateway
         1. enables VNet to connect to
            1. VPN device or
            2. ExpressRoute circuit

used for connectivity with on-premises network

* 1. hub virtual network - in hub-spoke topology
     1. VNet used as hub in hub-spoke topology
        1. central point of connectivity to on-premises network
        2. place to host services
           1. consumed by workloads in the spoke VNets
  2. gateway subnet
     1. create subnet named GatewaySubnet
        1. with an address range of /27
        2. VNet gateways are held in same subnet
  3. spoke virtual networks - in hub-spoke topology
     1. one or more VNets that are used as spokes
        1. used to isolate workloads in own VNets
        2. managed separately from other spokes
     2. if require connectivity between spokes
        1. consider
           1. deploying

Azure Firewall or

NVA for routing hub

* + - * 1. and using **UDRs in spoke**

to **forward traffic to hub**

* 1. virtual network peering
     1. Virtual network peering is non-transitive relationship
        1. between two virtual networks
        2. if require connectivity between spokes
           1. consider adding a separate peering connection between those spokes
           2. or consider **f) ii)** above

### route table subnet map (implement platform protection)

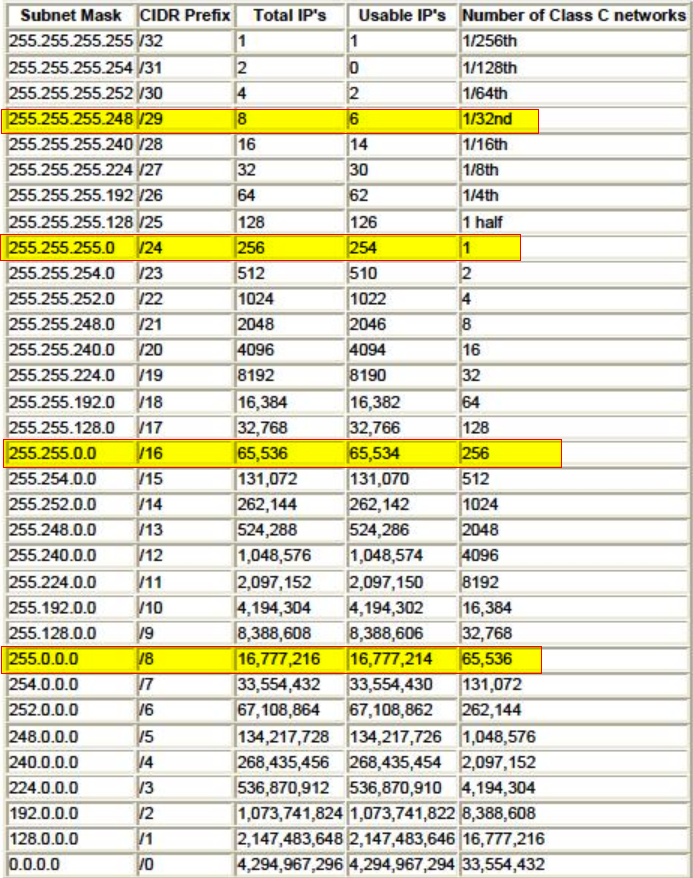
1. ensure traffic between a SpokeVNetSub0 and on prem flows through Azure firewall
   1. scenario
      1. RT1 includes user defined route points to private IP on firewall as next hop address
      2. RT2 disables BGP route propagation
         1. defines private IP of firewall as default gateway
      3. associate route table with proper subnet
   2. setting
      1. RT1 = SpokeVNetSub0
      2. RT2 = GatewaySubnet

### CIDR classless inter-domain routing

1. class masks



1. usable IPs
   1. 0 and 255 are always reserved
      1. usable = total -2

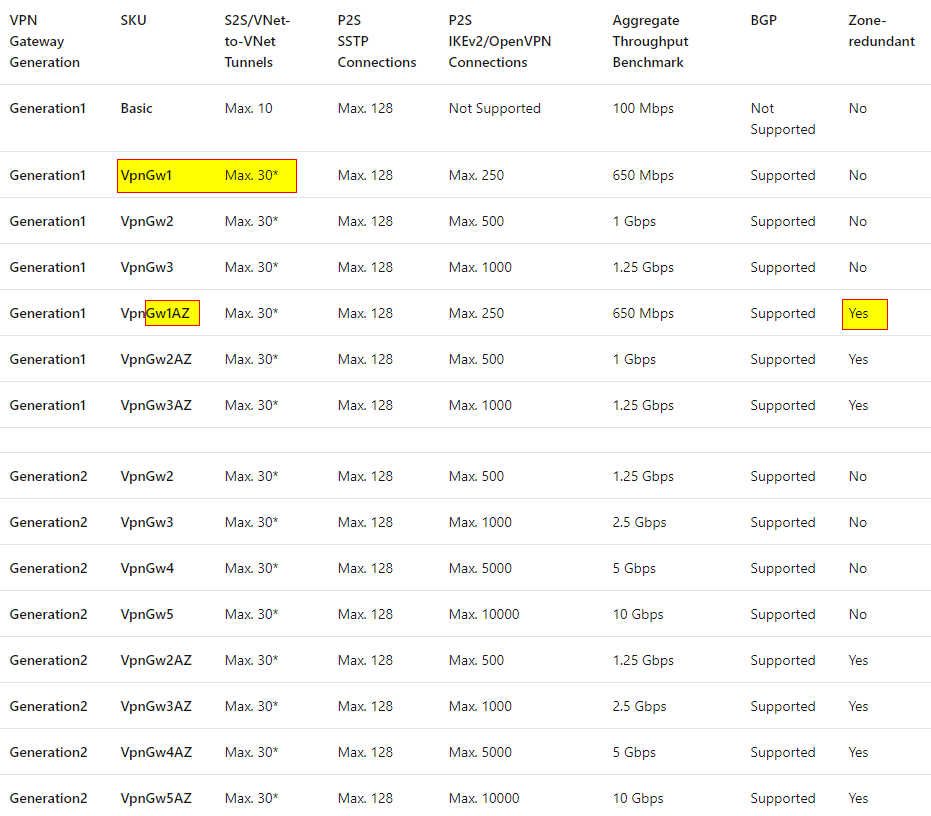


### BGP: Border Gateway Protocol (implement platform protection)

1. works with
   1. Azure VPN gateways or
   2. ExpressRoute
2. what is layer 3 connectivity?
   1. Microsoft uses an industry-standard dynamic-routing protocol
   2. BGP to exchange routes between
      1. on-premises network
      2. instances in Azure and
3. SKU’s
   1. <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways#gwsku>
   2. resizing of VpnGw SKUs is allowed
      1. within same generation
         1. except resizing Basic SKU
            1. is legacy SKU and has feature limitations

must delete the Basic SKU VPN gateway

and create a new gateway



### NSG rule overview

1. <https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview>
2. <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-vnet-plan-design-arm> log anal
   1. all traffic is allowed out to internet by default
   2. if no NSG rules then
      1. all traffic is allowed
         1. within and between subnets in VNet
      2. no traffic between networks is allowed by default
   3. web traffic is TCP on port 80
   4. ping is ICMP

## securing Apps

### enable SSL on website (secure data and apps)

1. steps to enable
   1. upload public cert
   2. set min TLS version to 1.2
   3. don’t turn on **HTTPS only** if need to support HTTP
2. notes
   1. TLS/SSL aka
      1. TLS mutual authentication
      2. client certificate authentication
   2. custom SSL is not supported in the F1 or D1 tier
      1. select any of non-free tiers
         1. B1, B2, B3
         2. or any Production tier
   3. <https://docs.microsoft.com/en-us/azure/app-service/app-service-web-configure-tls-mutual-auth>

### configure connection to contained SQL Db from SSMS (secure data and apps)

1. connect to the SQL Db using SSMS (mgt studio)
2. in SQL Db create contained dB users
3. in Azure AD, create a system-assigned managed identity
   1. system assigned identity for VM can access an SQL Server

### connect VM to SQL contained Db user (secure data and apps)

1. given no Azure AD
2. create a secrete in AKV

### connect SSMS to SQL (secure data and apps)

1. given Azure AD
2. if federated – using win 10 clients
   1. use Active Directory - integrated
3. if not federated
   1. use Active Directory - Password

### enable user to logon to contained dB with Azure AD account

1. **set Active Directory Admin**
   1. from portal in Azure SQL Server
      1. click Active Directory Admin
         1. select an Azure Global Admin
2. **log into SQL with SSMS** with that selected account
   * 1. authentication: to connect with Active Directory - password
     2. enter Global Admin user from above
     3. enter password
3. **create contained users**
   1. create a logon directly on dB not the server i.e contained
   2. run sql
      1. CREATE USER ([first.last@company.com](mailto:first.last@company.com)) FROM EXTERNAL PROVIDER;
      2. ALTER ROLE db\_owner ADD ([first.last@company.com](mailto:first.last@company.com))

### configure continuous deployment (secure data and apps)

1. to use Azure Repos
   1. **ensure Azure DevOps org is linked to Azure sub**scription
   2. **setup Azure DevOps Services account**
      1. so can deploy to a web app

### app registration to allow Microsoft Graph read directory access (secure data and apps)

1. three basic steps
   1. create app registration
   2. add application permissions
   3. grant permissions
      1. delegated permissions
         1. when signed-in user present
            1. acts on **behalf of a user**
         2. client apps access web API as signed-in user
            1. access restricted

to user’s permissions

* + 1. application permissions
       1. when on **behalf of service**- or daemon-type app
          1. that need to access web API as themselves
          2. without user interaction for sign-in or consent
       2. **unless defined app roles for web API**
          1. this option is disabled

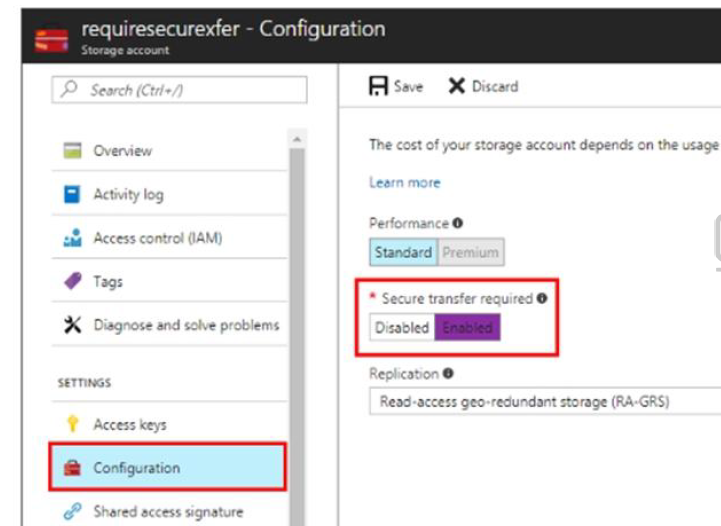
### make SSL cert available in app code (secure data and apps)

1. add an app setting to the Web APP configuration

az webapp config **appsettings** set --name <app-name> --resource-group <resource-group-name> --settings WEBSITE\_LOAD\_CERTIFICATES=<comma-separated-certificate-thumbprints>

### require storage account to use SSL (secure data and apps)

1. from portal select storage account
2. select configuration
   1. enable **secure transfer required**



### ensure registered app can access AKV (secure data and apps)

1. in Azure AD, create a role
2. to call Azure Resource Manager
   1. use RBAC
   2. assign appropriate role to app
      1. so, can call key in AKV

### enable Advanced Data Security for SQL (secure data and apps)

1. also ensure Azure ATP alerts are sent to email
2. in portal, select dB
3. in security section select Advanced data security
   1. click Settings Icon
      1. tick checkbox: **Enable Advanced Data Security at the database level**
   2. click yes to confirm
   3. in storage account, select one if not by default
   4. under **Advanced Threat protection settings**
   5. in send alerts box
   6. enter email address
   7. click save

### ATP for SQL (secure data and apps)

1. can detect potential SQL injections
2. would flag select \* from table

### enable Azure AD authentication for web app (secure data and apps)

1. in settings, click Authentication / Authorization
   1. click App Service Authentication slider to On
   2. in Action to take when request is not authenticated box
      1. select log in with Azure Active Directory
   3. click save

### Azure Information Protection policy (secure data and apps)

1. two flavors
   1. Azure Information Protection
      1. classic client (old)
         1. downloads sensitivity labels and policy settings
            1. from Azure
            2. configure AIP policy from Azure portal
      2. unified labeling client (new)
         1. downloads sensitivity labels and policy settings
            1. from following admin centers

MS Office 365 security & compliance center

Microsoft 365 security center

Microsoft 365 compliance center

### Azure Information Protection policy order (secure data and apps)

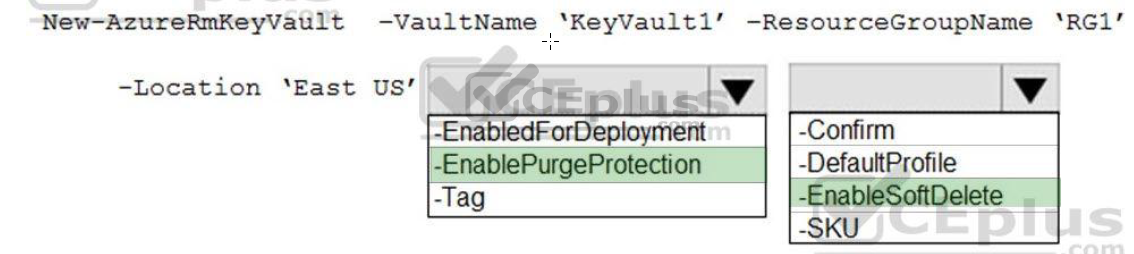
1. multiple conditions evaluated
   1. according to position in the policy
   2. first is lowest sensitivity
   3. highest position is most sensitive
      1. applied last
2. Automatic Classification
   1. applies to
      1. Word
      2. Excel
      3. PowerPoint
      4. Outlook email
   2. not
      1. Microsoft notepad

### Azure AKV restore (secure data and apps)

1. restore
   1. only specifically privileged user may restore
      1. key vault or
      2. key vault object
   2. by issuing recover command on the corresponding proxy resource
2. can restore secret or key
   1. to any vault in same
      1. subscription and
      2. region within same geography

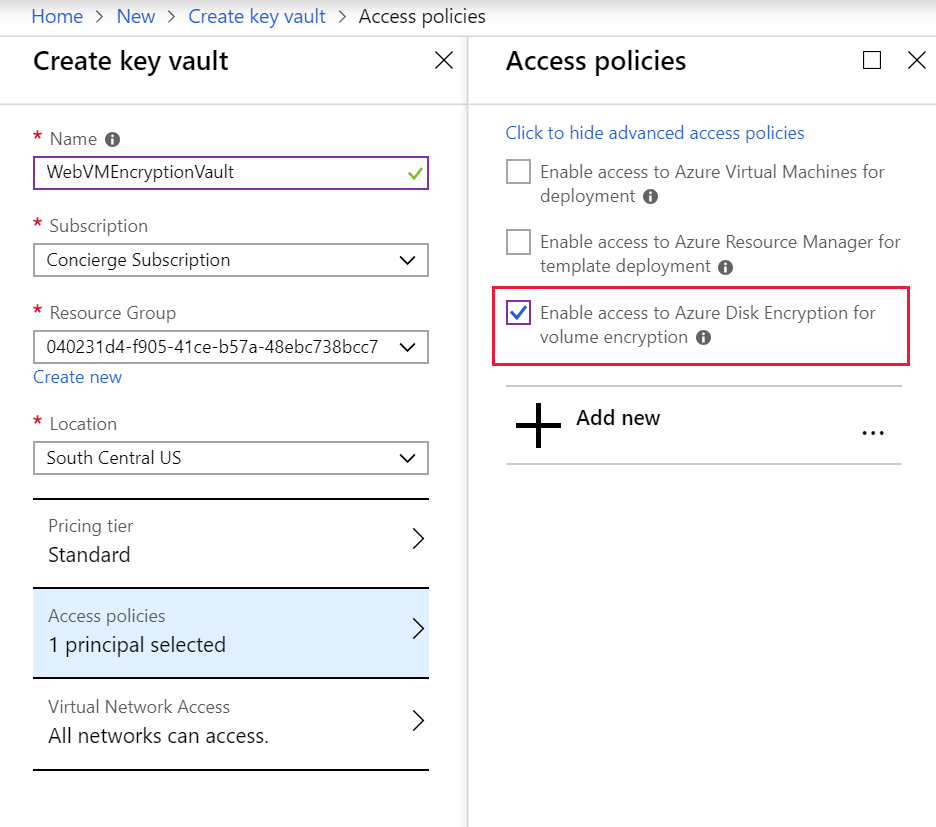
### Azure AKV restore New-AzureRmKeyVault (secure data and apps)

1. EnablePurgeProtection
   1. if enabled, protects against immediate deletion
      1. requires soft delete be enabled
2. EnableSoftDelete
   1. if enabled, for a grace period
      1. can recover key vault and its contents
         1. after being deleted



### Azure AKV enable ARM (secure data and apps)

1. ensure Azure disk encryption can retrieve secrets from AKV
2. in portal select AKV
   1. select the Advanced Access Policies blade
   2. check **Enable access to Azure Resource Manager for template deployment**

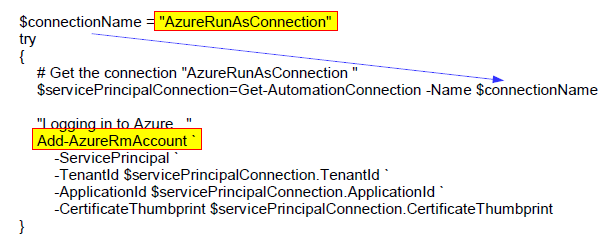


### Azure AKV ensure user permissions (secure data and apps)

1. assign user Key Vault Secrets Officer role
   1. in portal search Key Vaults
      1. **select desired KeyVaultName**
      2. in properties, select **Access control (IAM)**
      3. in **Add a role assignment** section, click Add
      4. in Role box, select the **Key Vault Secrets Officer** role
      5. in Select box, start typing users name, select user from results
      6. click Save
2. Key Vault Secrets Officer role
   1. has all key permissions
   2. can perform any action on the secrets of a key vault

### Azure AKV enable runbook (secure data and apps)

1. **create Automation account**
   1. **runbooks live within Azure automation account**
      1. can execute PowerShell scripts
2. **import PowerShell** modules
   1. to the Azure Automation account
   2. under ‘Assets’ from the Azure automation account Resources section
      1. select, add in Modules to the runbook
      2. **to execute Key vault cmdlets in runbook**
         1. **add AzureRM.profile and AzureRM.key**
3. **create a connection resource in Azure Automation Account**
   1. use **Run as account** to manage Resource Manager resource in runbooks



### Azure AKV linked template (manage Identify and access)

1. linked template
   1. to dynamically construct a resource ID
      1. that will designate the AKV
         1. containing the secret
            1. during each deployment
      2. the name of the AKV and
      3. secret will be provided as inline parameters

### WAF (secure data and apps)

1. WAF needs to be installed on
   1. Gateway
      1. Azure Application Gateway
      2. Azure Front door
   2. not a firewall
   3. or added as extension to web app

### configure SQL backup (secure data and apps)

1. in portal select
   1. Azure SQL Database
      1. select homepage
      2. select hosting Homepage
         1. click on Manage backups
      3. click on configure policies
      4. ensure Weekly backups
      5. configure how long would you like weekly backups to be retained
         1. to number of desired weeks
      6. click Apply

### configure SQL always encrypted (secure data and apps)

1. to ensure app developers can retrieve and decrypted data
   1. provide
      1. **column encryption key**
      2. **column master key**

### SQL contained database user (secure data and apps)

1. overview
   1. a contained dB is isolated from other databases
      1. and from instance of SQL Server that hosts database
   2. have no dependencies on server-level metadata and settings

### Azure Front Door

1. partly overlaps with Azure App Gateway
2. both services offer
   1. web app firewalling
   2. SSL offloading
   3. URL-based routing
3. main difference is
   1. Azure App Gateway
      1. inside virtual network
   2. Azure Front Door
      1. a global, decentralized service

### Cosmos DB

1. access must be granted to any collection
2. via SQL API access control model
   1. two types of access constructs
      1. master keys
         1. full admin access
            1. to all resources within Cosmos DB account
         2. created when Cosmos DB account is created
      2. resource tokens
         1. capture relationship between
            1. user of database and
            2. permission user has for a specific Cosmos DB resource

such as collection or document

### Cosmos DB Add users and assign roles

1. from portal select Azure Cosmos DB account
   1. click Access control (IAM) tab
      1. then click + Add role assignment
      2. in Add role assignment pane
         1. in Role box
            1. select Cosmos DB Account Reader Role
         2. in Assign access to box
            1. select

Azure AD user

group or

application

* + - * 1. can search directory by

display name

email address or

object identifiers

* + 1. selected item(s) appears in selected members list
    2. click Save.

## miscellaneous

down network the rat whole

<https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke>

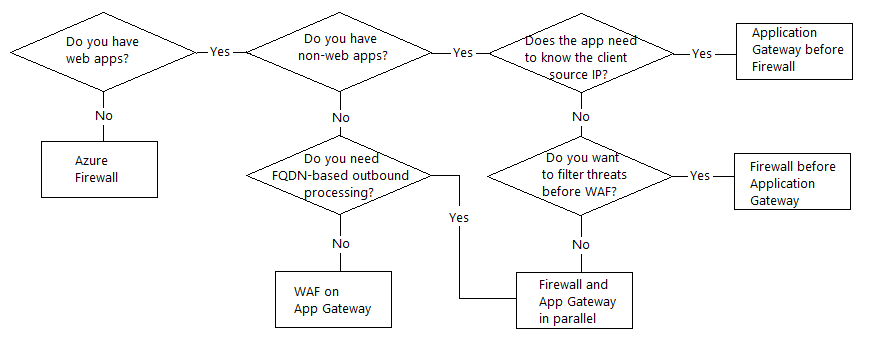
<https://docs.microsoft.com/en-us/azure/firewall/tutorial-hybrid-portal>

A route **from hub gateway subnet to spoke subnet** through the firewall IP address

A default route **from spoke subnet through firewall** IP address

<https://medium.com/@cohesivenet/4-things-you-should-know-about-transitive-routing-in-cloud-d534356a58f8>

<https://docs.microsoft.com/en-us/azure/architecture/example-scenario/gateway/firewall-application-gateway>



# 