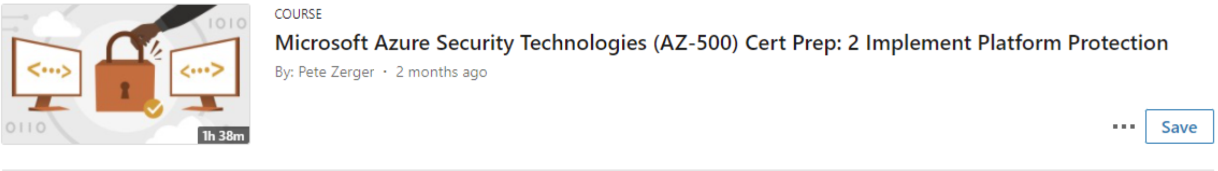
AZ-500 Cert Prep 2- Implement Platform Protection – Completed 2-2-22

Started: 1/22/2022 Updated: 2/2/2022 Completed: 2/2/2022


COURSE

Microsoft Azure Security Technologies (AZ-500) Cert Prep: 2 Implement Platform Protection

By: Pete Zerger · 2 months ago

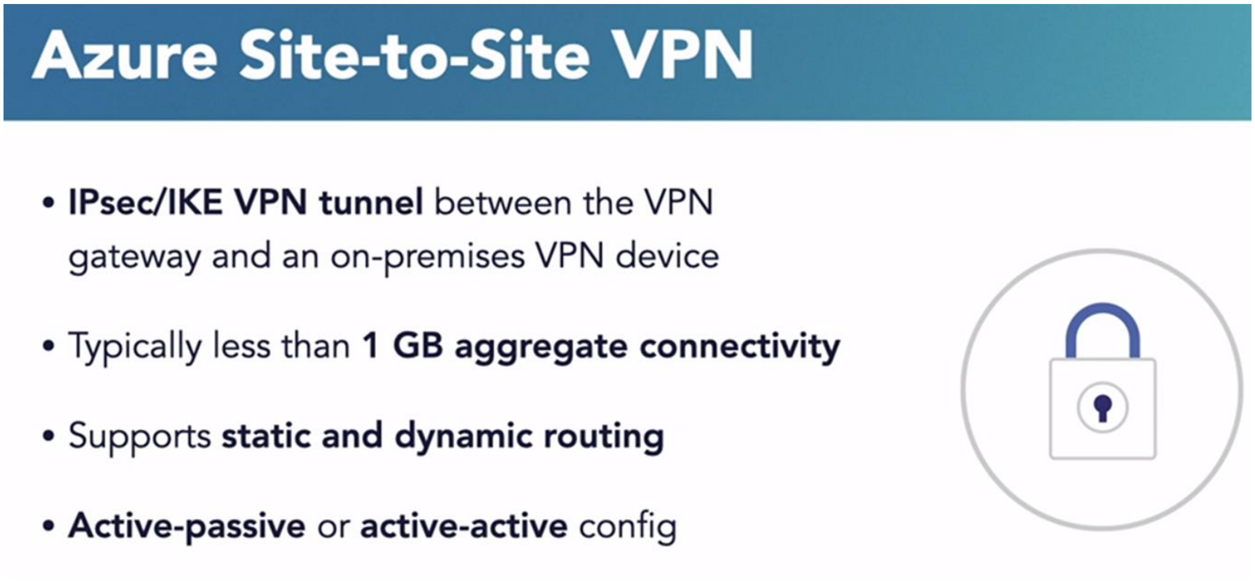
Table of Contents

0. Overview

With cyberattacks on the rise, professionals who can keep an organization's networks, applications, and data safe are in high demand. The Microsoft Azure Security Technologies (AZ-500) exam is the perfect opportunity for IT professionals to demonstrate their cybersecurity skills to current and future employers. In this course, Pete Zerger helps you deepen your knowledge of Azure security as you study for the "Implement Platform Protection" domain of the AZ-500 exam. Pete demonstrates how to implement advanced network security, including how to create and configure Microsoft Azure Firewall and implement service and private endpoints. Plus, he covers other important topics like hardening your IaaS, containerized, and serverless workloads in Azure, policy-based management of resource access and security, as well as data encryption in-transit and at rest.

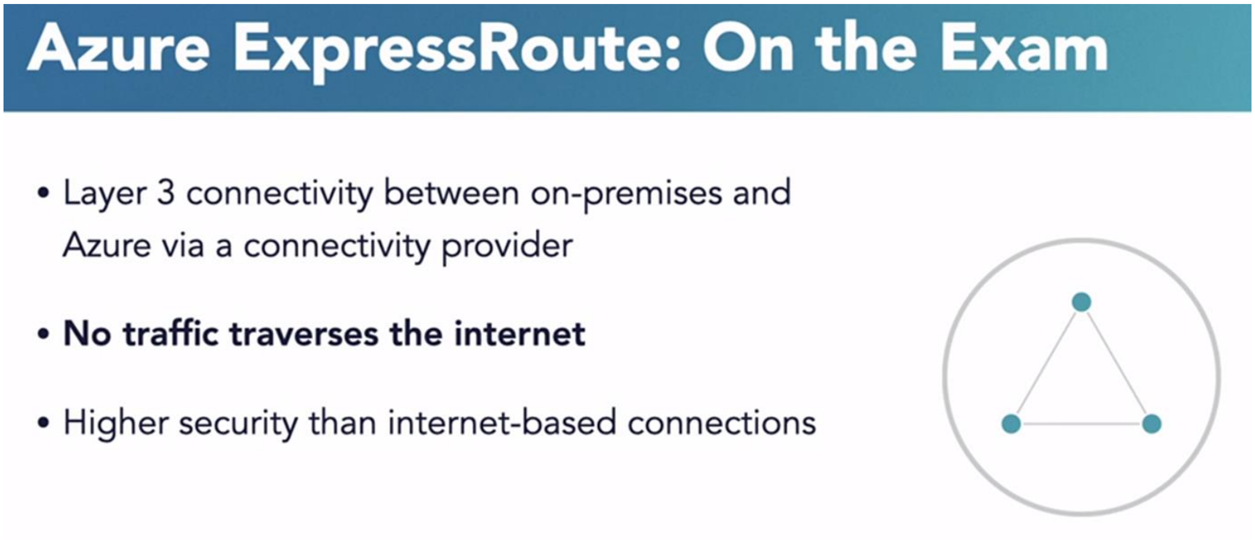
1. Implement Advanced Network Security

1.2 Secure the connectivity of hybrid networks



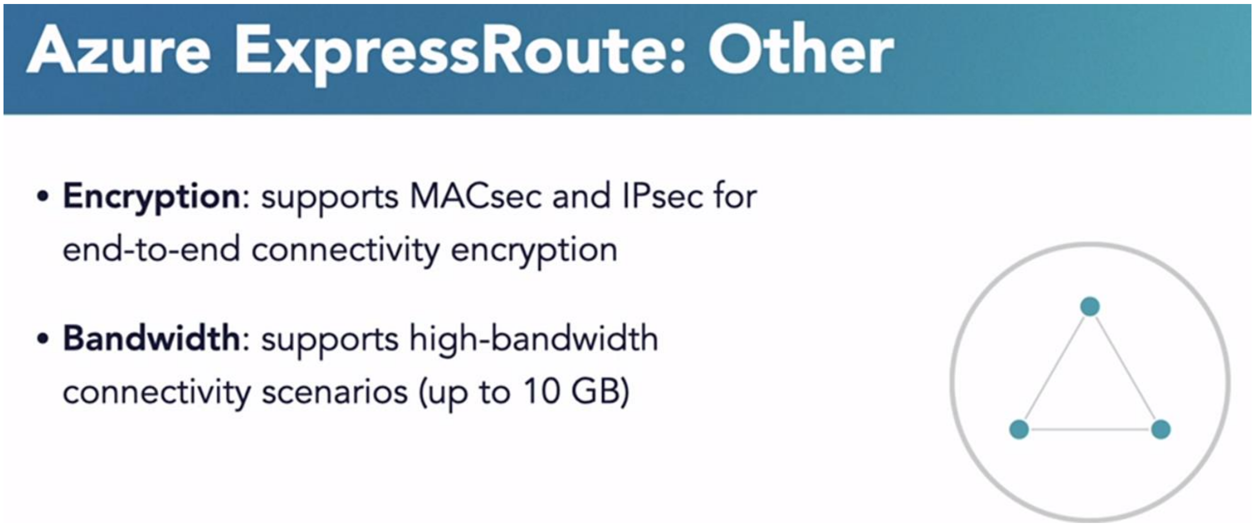
Azure Site-to-Site VPN

- **IPsec/IKE VPN tunnel** between the VPN gateway and an on-premises VPN device
- Typically less than **1 GB aggregate connectivity**
- Supports **static and dynamic routing**
- **Active-passive** or **active-active** config



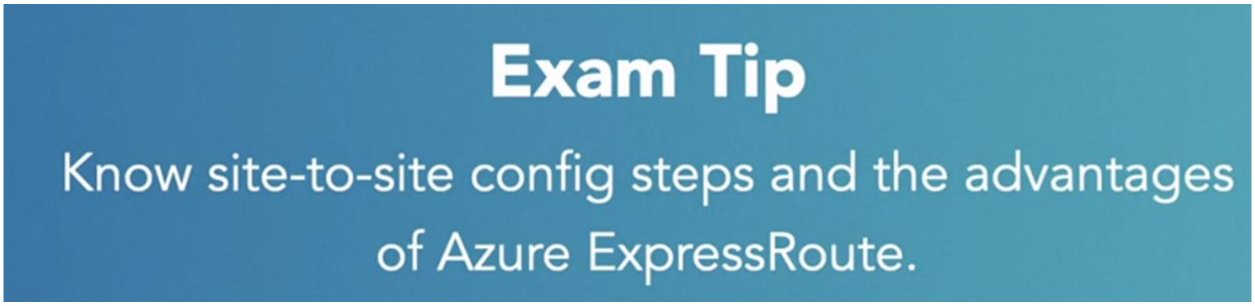
Azure ExpressRoute: On the Exam

- Layer 3 connectivity between on-premises and Azure via a connectivity provider
- **No traffic traverses the internet**
- Higher security than internet-based connections



Azure ExpressRoute: Other

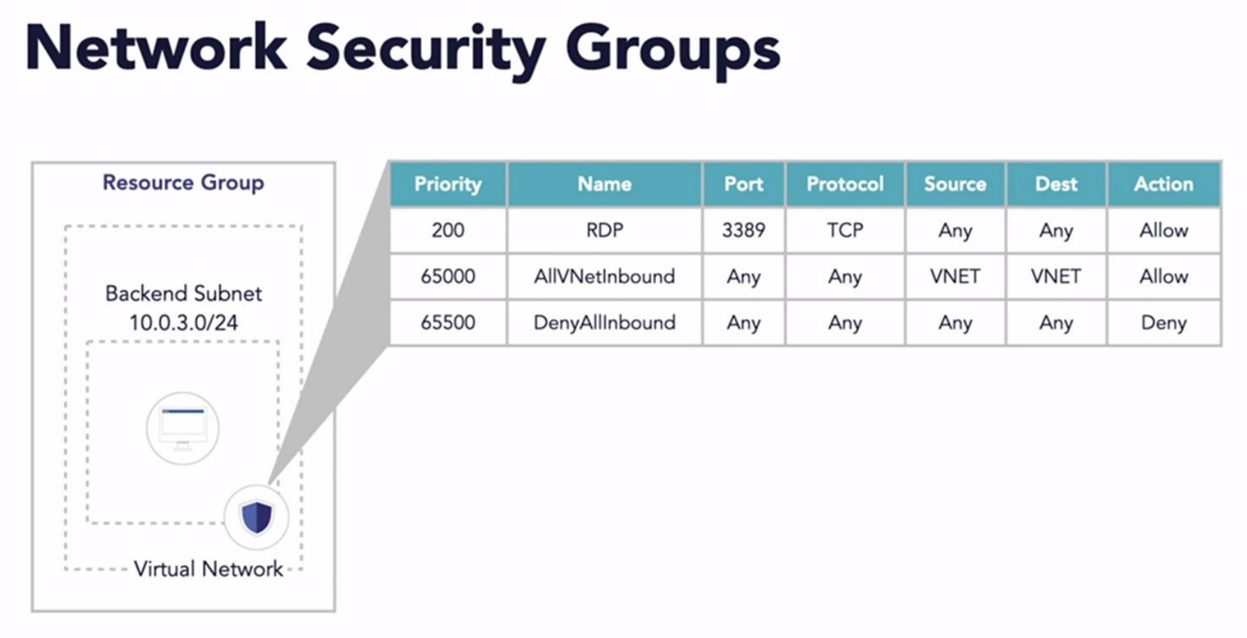
- **Encryption**: supports MACsec and IPsec for end-to-end connectivity encryption
- **Bandwidth**: supports high-bandwidth connectivity scenarios (up to 10 GB)



Exam Tip

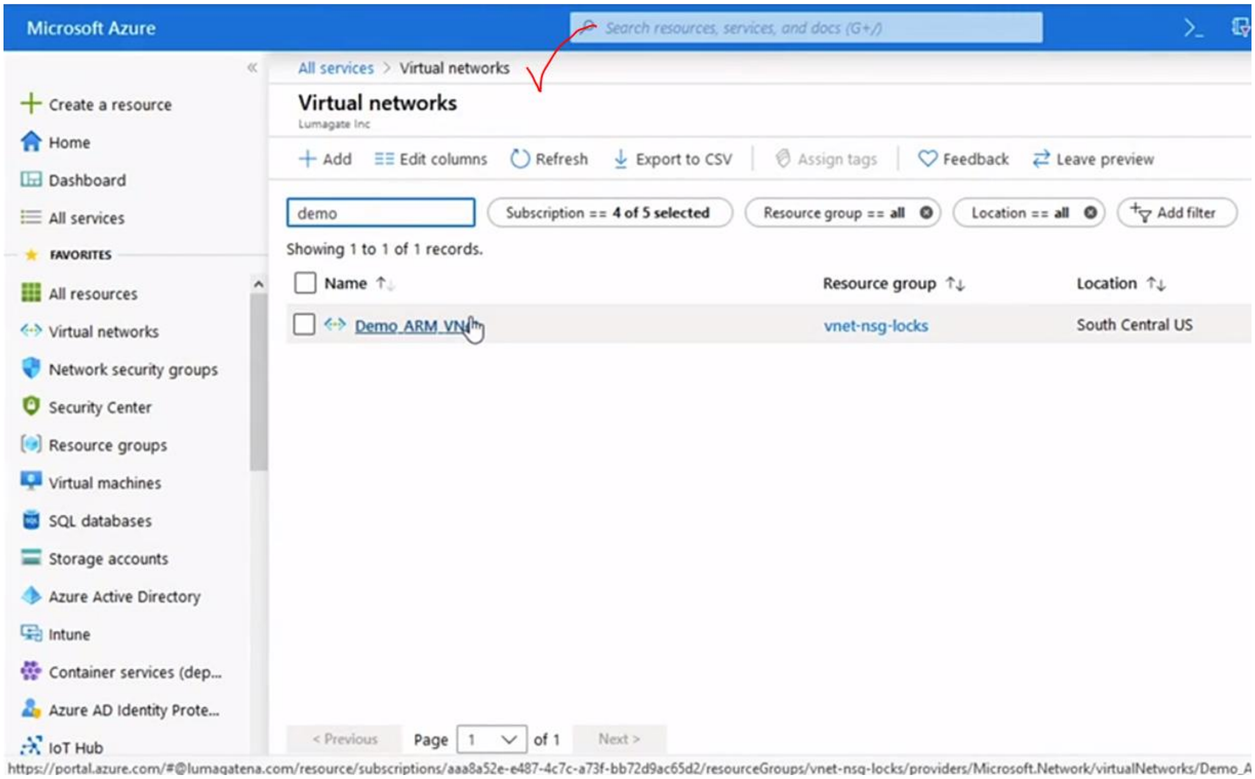
Know site-to-site config steps and the advantages of Azure ExpressRoute.

1.2 Secure the connectivity of virtual networks



Network Security Groups

Priority	Name	Port	Protocol	Source	Dest	Action
200	RDP	3389	TCP	Any	Any	Allow
65000	AllVNetInbound	Any	Any	VNET	VNET	Allow
65500	DenyAllInbound	Any	Any	Any	Any	Deny



Virtual networks

Lumagate Inc

demo

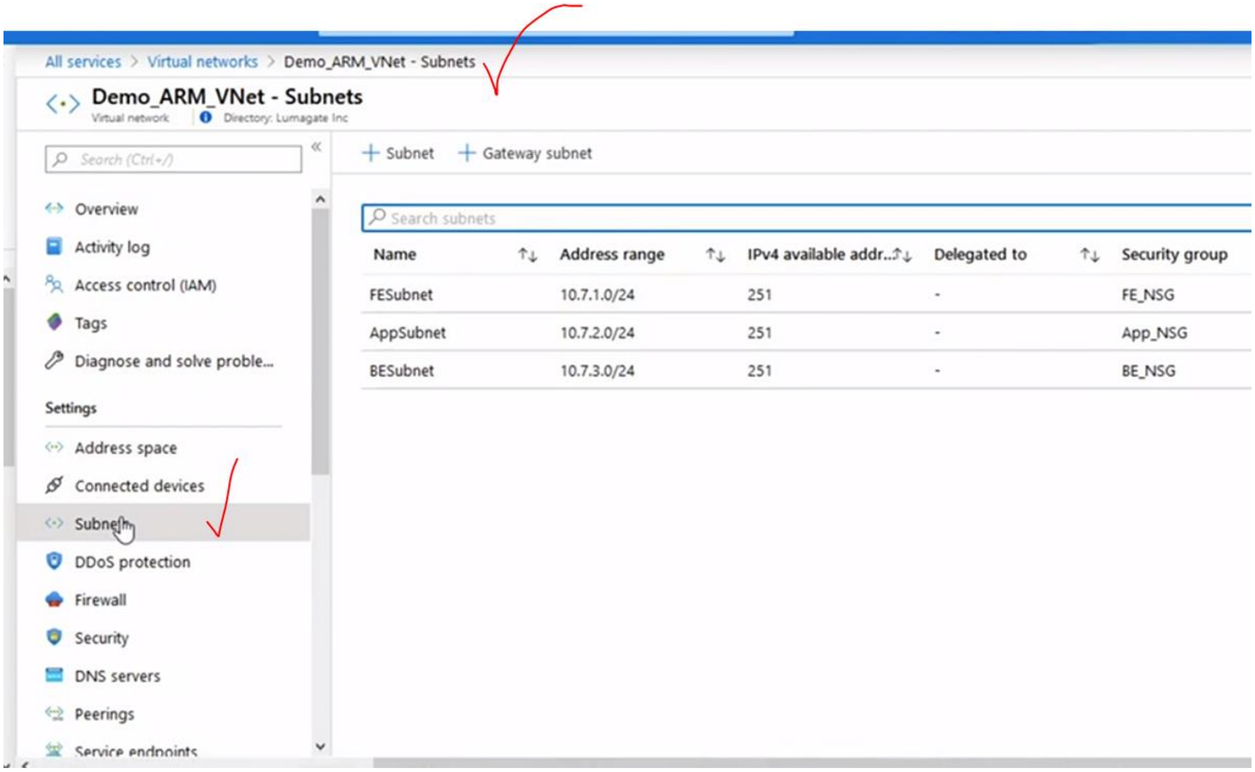
Subscription == 4 of 5 selected | Resource group == all | Location == all

Showing 1 to 1 of 1 records.

Name	Resource group	Location
Demo_ARM_VNet	vnet-nsg-locks	South Central US

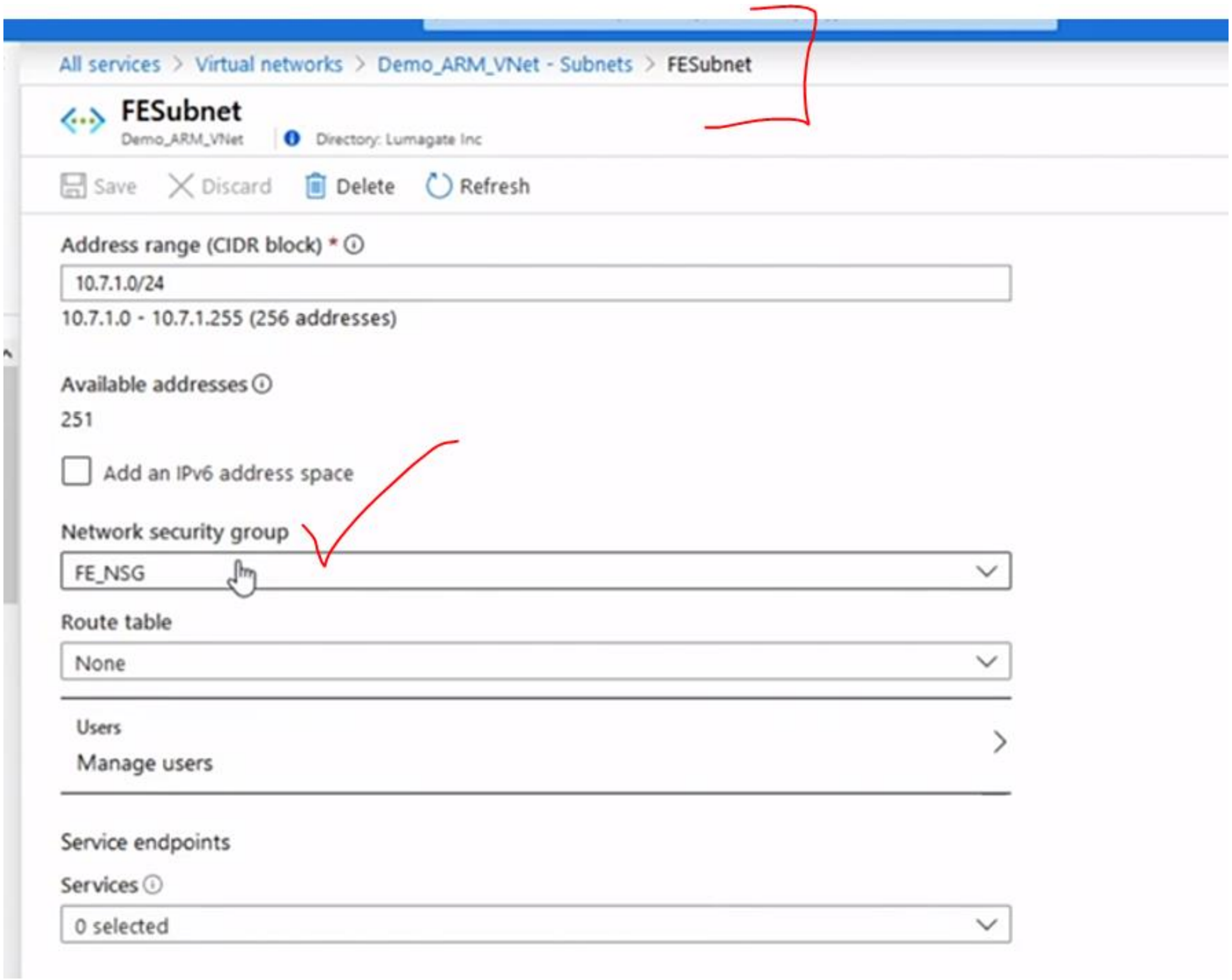
Page 1 of 1

https://portal.azure.com/#@lumagatena.com/resource/subscriptions/aaa8a52e-e487-4c7c-a73f-bb72d9ac65d2/resourceGroups/vnet-nsg-locks/providers/Microsoft.Network/virtualNetworks/Demo_A



Name	Address range	IPv4 available addr...	Delegated to	Security group
FESubnet	10.7.1.0/24	251	-	FE_NSG
AppSubnet	10.7.2.0/24	251	-	App_NSG
BESubnet	10.7.3.0/24	251	-	BE_NSG

The NSG or Network Security Group has been applied.



All services > Virtual networks > Demo_ARM_VNet - Subnets > FESubnet

FESubnet

Demo_ARM_VNet | Directory: Lumagate Inc

Save
Discard
Delete
Refresh

Address range (CIDR block) *

10.7.1.0/24

10.7.1.0 - 10.7.1.255 (256 addresses)

Available addresses

251

□ Add an IPv6 address space

Network security group

FE_NSG

Route table

None

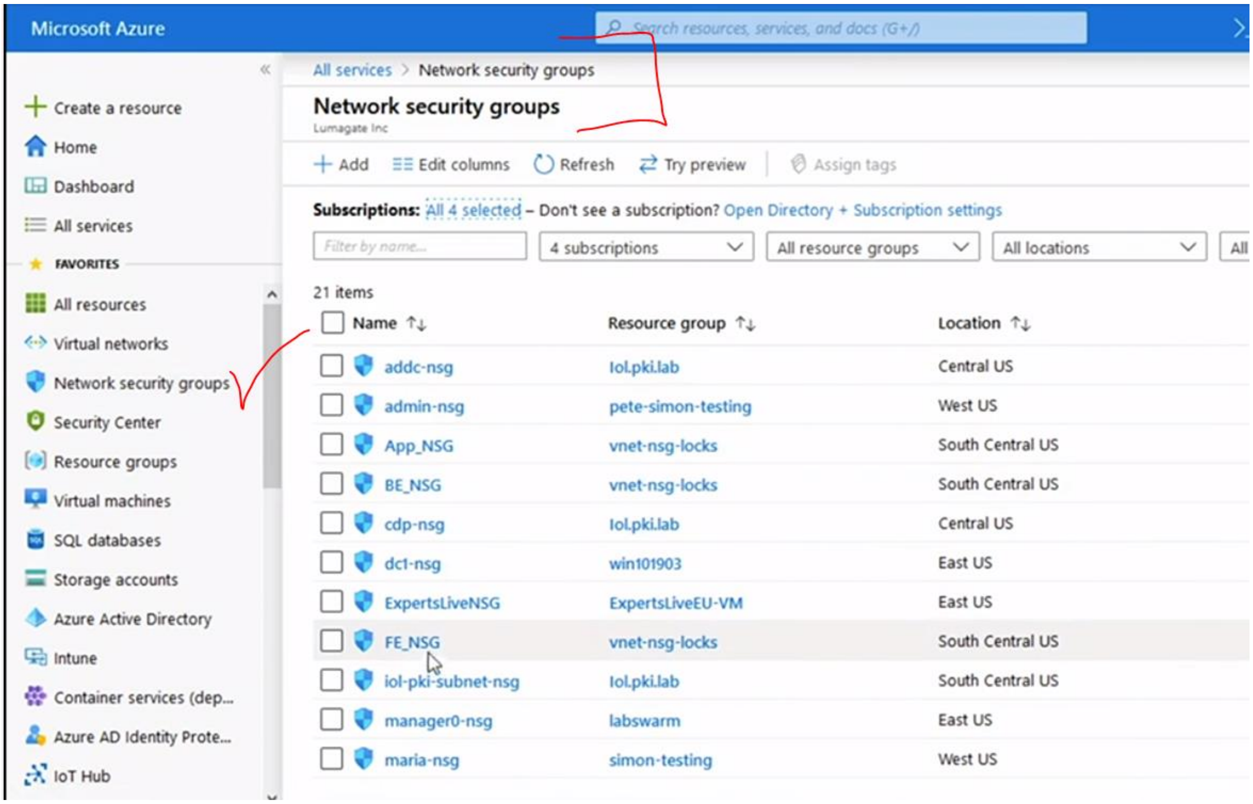
Users

Manage users

Service endpoints

Services

0 selected



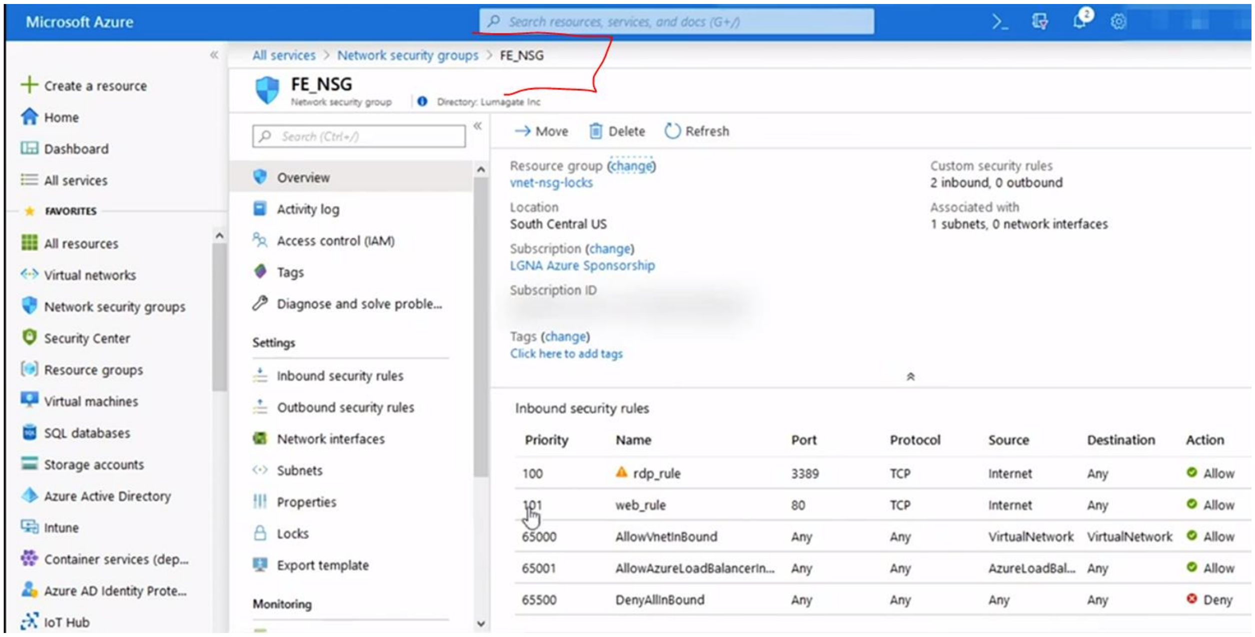
Network security groups
Lumagate Inc

Subscriptions: All 4 selected – Don't see a subscription? Open Directory + Subscription settings

21 items

Name	Resource group	Location
addc-nsg	lol.pki.lab	Central US
admin-nsg	pete-simon-testing	West US
App_NSG	vnet-nsg-locks	South Central US
BE_NSG	vnet-nsg-locks	South Central US
cdp-nsg	lol.pki.lab	Central US
dc1-nsg	win101903	East US
ExpertsLiveNSG	ExpertsLiveEU-VM	East US
FE_NSG	vnet-nsg-locks	South Central US
iol-pki-subnet-nsg	lol.pki.lab	South Central US
manager0-nsg	labswarm	East US
maria-nsg	simon-testing	West US

Looking at the properties of an NSG



FE_NSG
Network security group | Directory: Lumagate Inc

Resource group (change)
vnet-nsg-locks

Location
South Central US

Subscription (change)
LGNA Azure Sponsorship

Subscription ID
[redacted]

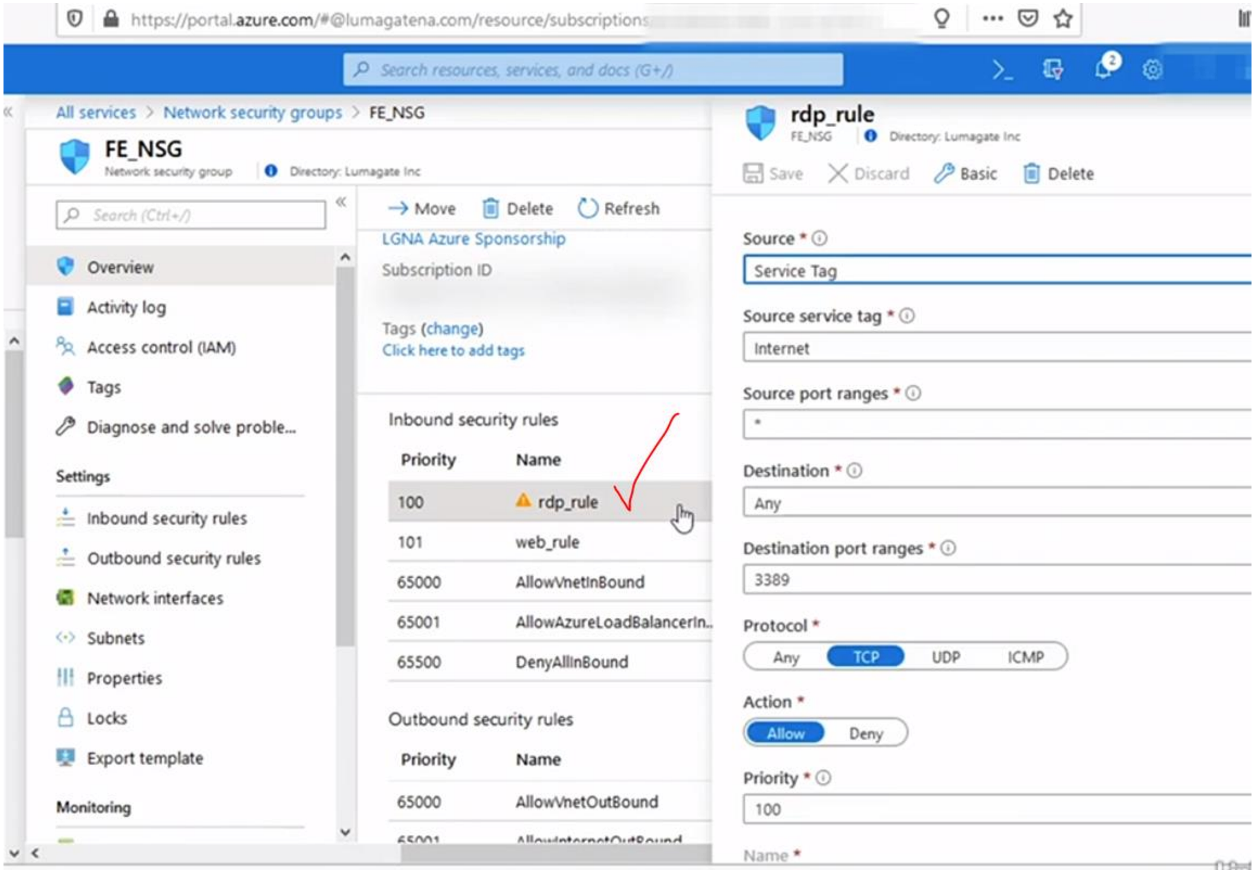
Tags (change)
Click here to add tags

Custom security rules
2 inbound, 0 outbound

Associated with
1 subnets, 0 network interfaces

Inbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
100	⚠ rdp_rule	3389	TCP	Internet	Any	✓ Allow
101	web_rule	80	TCP	Internet	Any	✓ Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBal...	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny



FE_NSG

Inbound security rules

Priority	Name
100	⚠ rdp_rule ✓
101	web_rule
65000	AllowVnetInBound
65001	AllowAzureLoadBalancerIn...
65500	DenyAllInBound

Outbound security rules

Priority	Name
65000	AllowVnetOutBound
65001	AllowInternetOutBound

rdp_rule

Source * : Service Tag

Source service tag * : Internet

Source port ranges * : *

Destination * : Any

Destination port ranges * : 3389

Protocol * : ○ Any ● TCP ○ UDP ○ ICMP

Action * : ● Allow ○ Deny

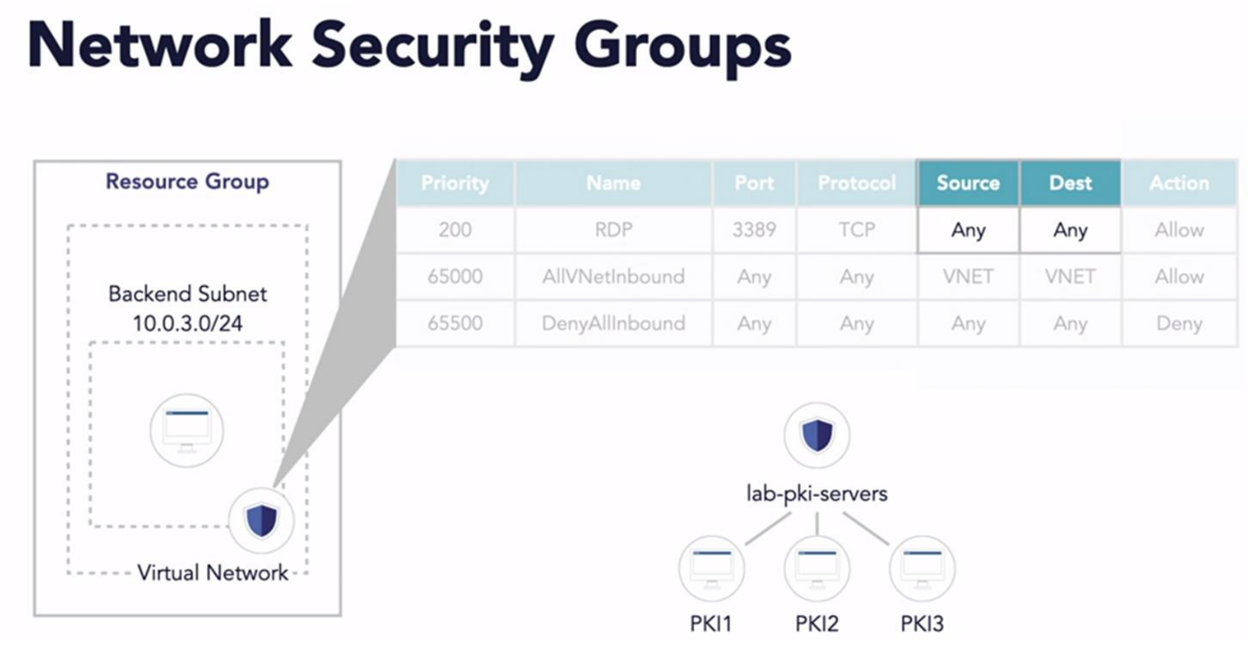
Priority * : 100

Name *

Exam Prep

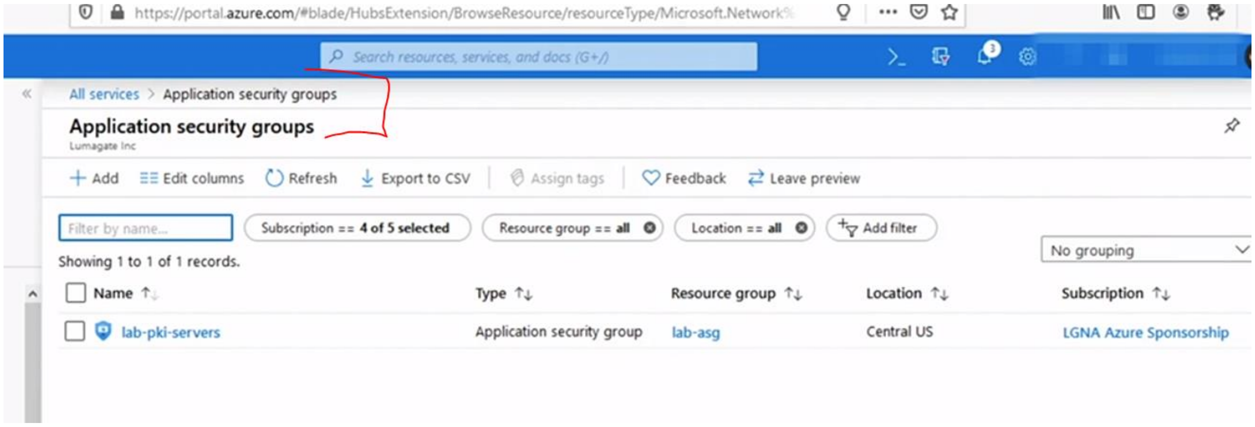
Understand NSG rule syntax, priority, and where NSGs can be applied.

Create and Configure Application Security Groups



Network Security Groups

Priority	Name	Port	Protocol	Source	Dest	Action
200	RDP	3389	TCP	Any	Any	Allow
65000	AllVNetInbound	Any	Any	VNET	VNET	Allow
65500	DenyAllInbound	Any	Any	Any	Any	Deny



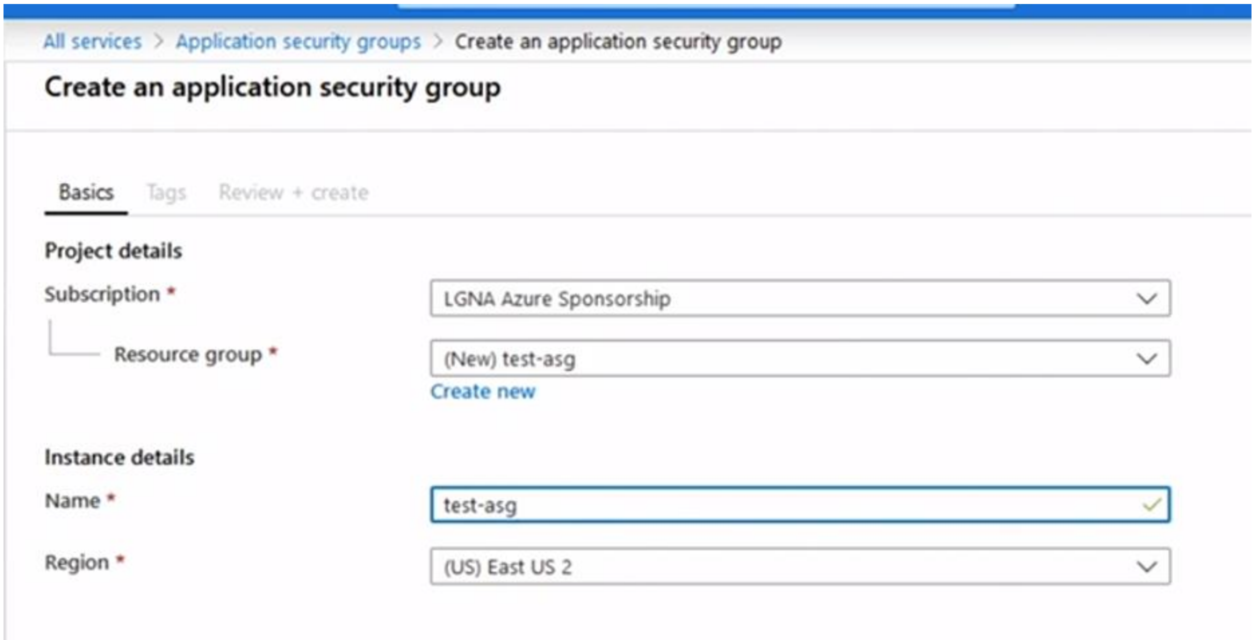
https://portal.azure.com/#blade/HubsExtension/BrowseResource/resourceType/Microsoft.Network
Search resources, services, and docs (G+/)
All services > Application security groups

Application security groups
Lumagate Inc

+ Add
Edit columns
Refresh
Export to CSV
Assign tags
Feedback
Leave preview
Filter by name...
Subscription == 4 of 5 selected
Resource group == all
Location == all
Add filter
No grouping

Showing 1 to 1 of 1 records.

Name	Type	Resource group	Location	Subscription
lab-pki-servers	Application security group	lab-asg	Central US	LGNA Azure Sponsorship


All services > Application security groups > Create an application security group
Basics
Tags
Review + create
Create new

Create an application security group

Project details

Subscription * LGNA Azure Sponsorship

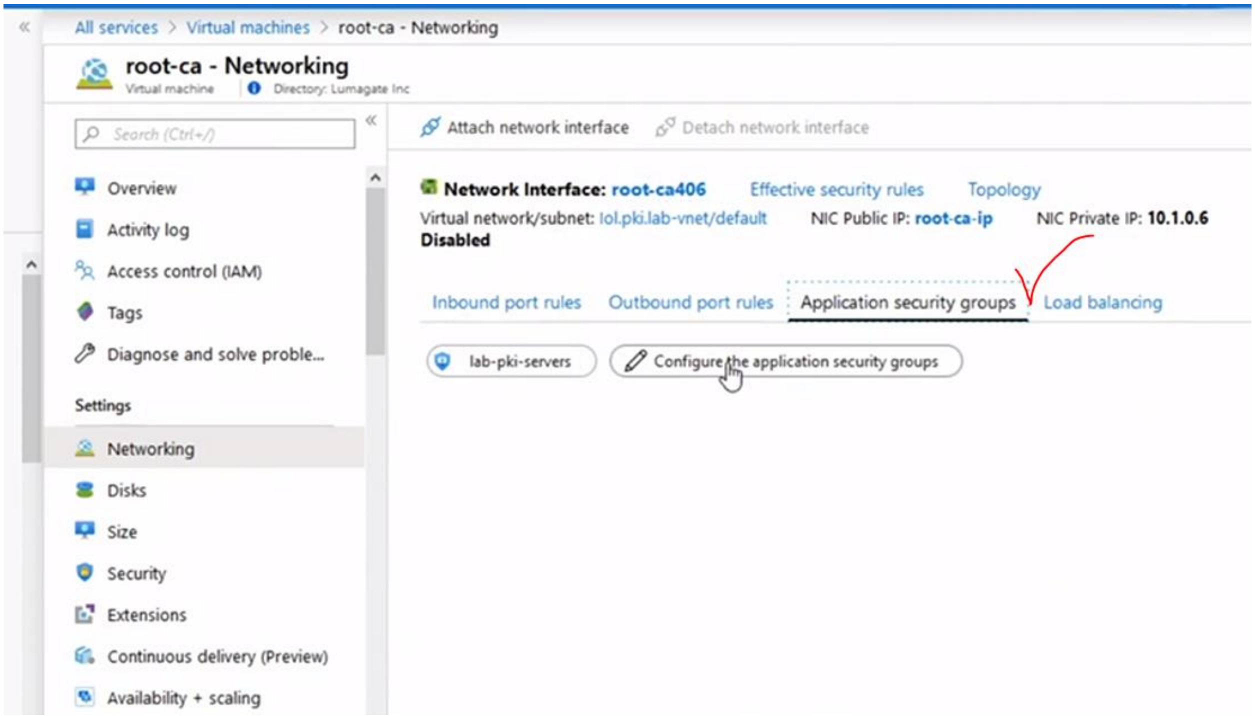
Resource group * (New) test-asg

Instance details

Name * test-asg

Region * (US) East US 2

How to associate ASG to a Server or VM

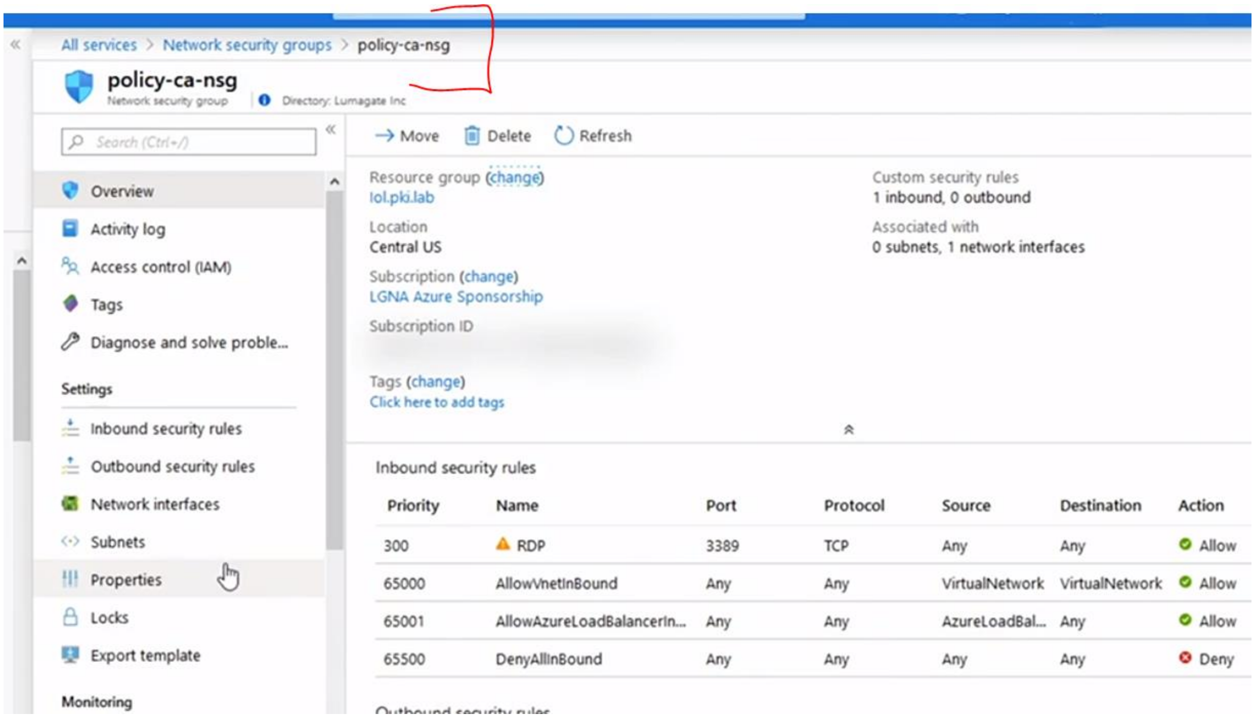


root-ca - Networking

Network Interface: root-ca406

Virtual network/subnet: lol.pki.lab-vnet/default NIC Public IP: root-ca-ip NIC Private IP: 10.1.0.6

Disabled



All services > Network security groups > policy-ca-nsg

policy-ca-nsg
Network security group | Directory: Lumagate Inc

Resource group (change)
lol.pki.lab

Location
Central US

Subscription (change)
LGNA Azure Sponsorship

Subscription ID
[redacted]

Tags (change)
Click here to add tags

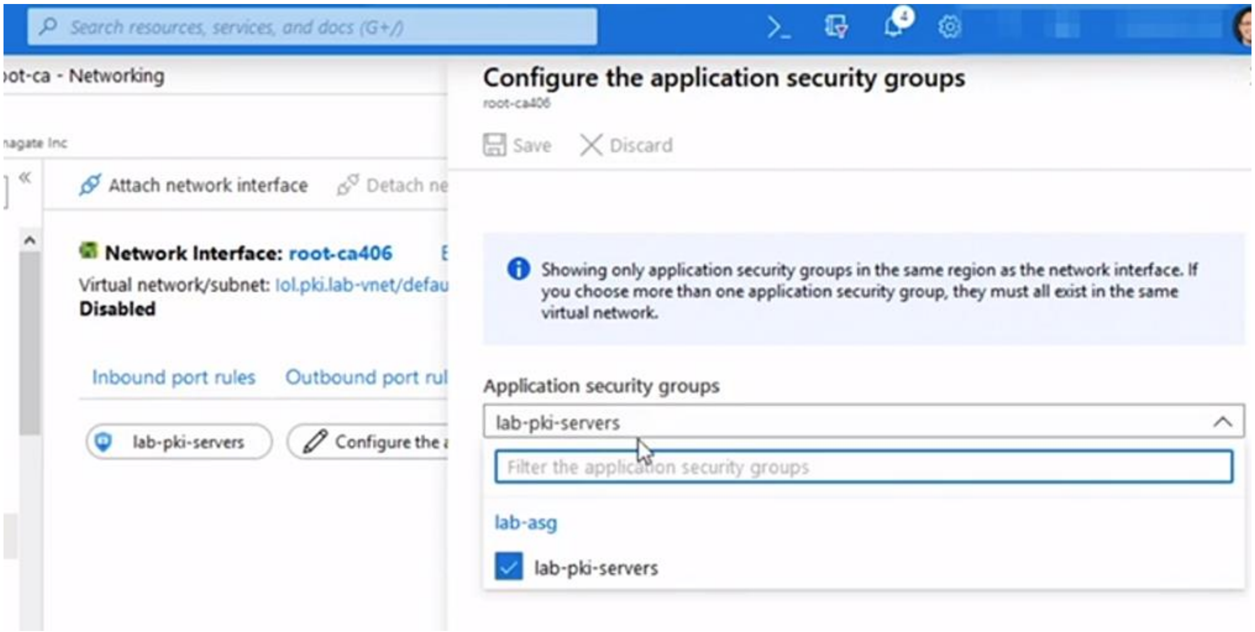
Custom security rules
1 inbound, 0 outbound

Associated with
0 subnets, 1 network interfaces

Inbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
300	⚠ RDP	3389	TCP	Any	Any	✓ Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBal...	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✕ Deny

Outbound security rules



ot-ca - Networking

nagate Inc

Network Interface: root-ca406

Virtual network/subnet: lol.pki.lab-vnet/defau

Disabled

Configure the application security groups

root-ca406

Showing only application security groups in the same region as the network interface. If you choose more than one application security group, they must all exist in the same virtual network.

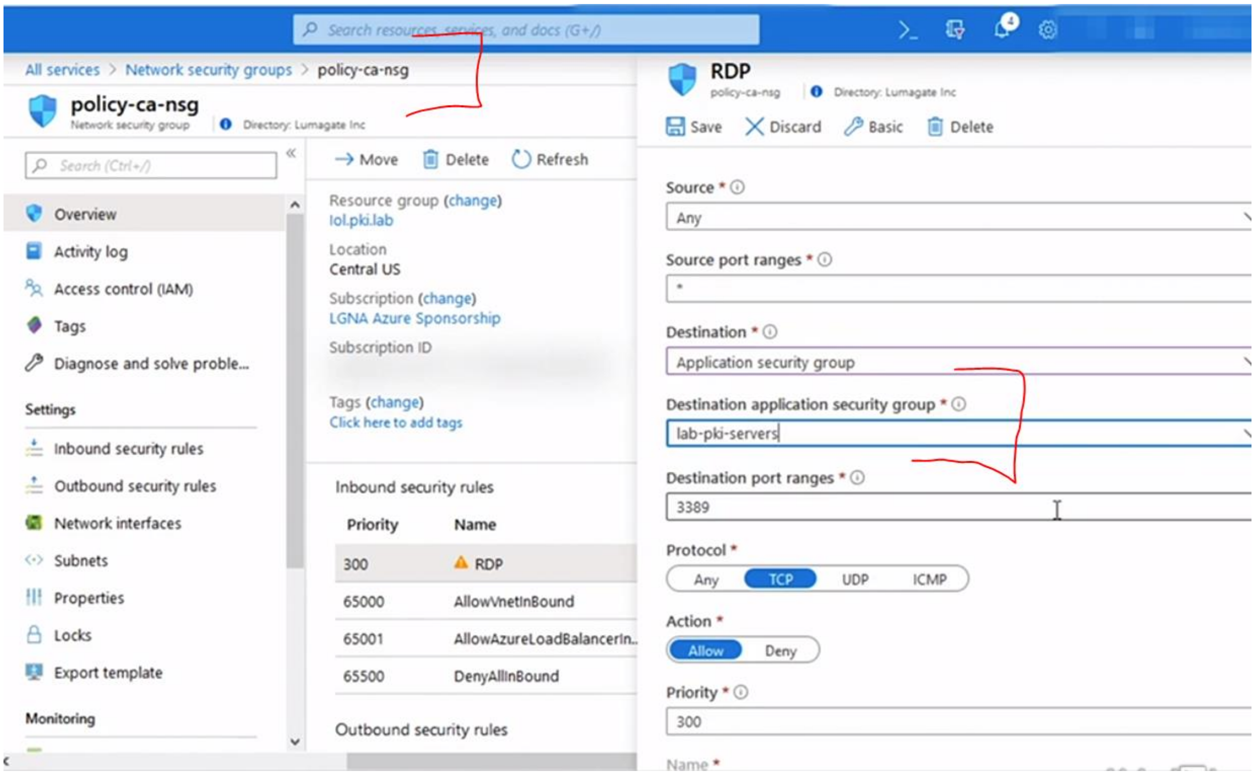
Application security groups

lab-pki-servers

Filter the application security groups

lab-asg

☑ lab-pki-servers



Resource group (change)
lol.pki.lab

Location
Central US

Subscription (change)
LGNA Azure Sponsorship

Subscription ID
[redacted]

Tags (change)
Click here to add tags

Inbound security rules

Priority	Name
300	⚠ RDP
65000	AllowVnetInBound
65001	AllowAzureLoadBalancerIn..
65500	DenyAllInBound

Outbound security rules

Source * ⓘ
Any

Source port ranges * ⓘ
*

Destination * ⓘ
Application security group

Destination application security group * ⓘ
lab-pki-servers

Destination port ranges * ⓘ
3389

Protocol *
Any [✓ TCP] UDP ICMP

Action *
[✓ Allow] Deny

Priority * ⓘ
300

Name *

Application Security Groups

Logical grouping of VM network interfaces for assignment in NSGs

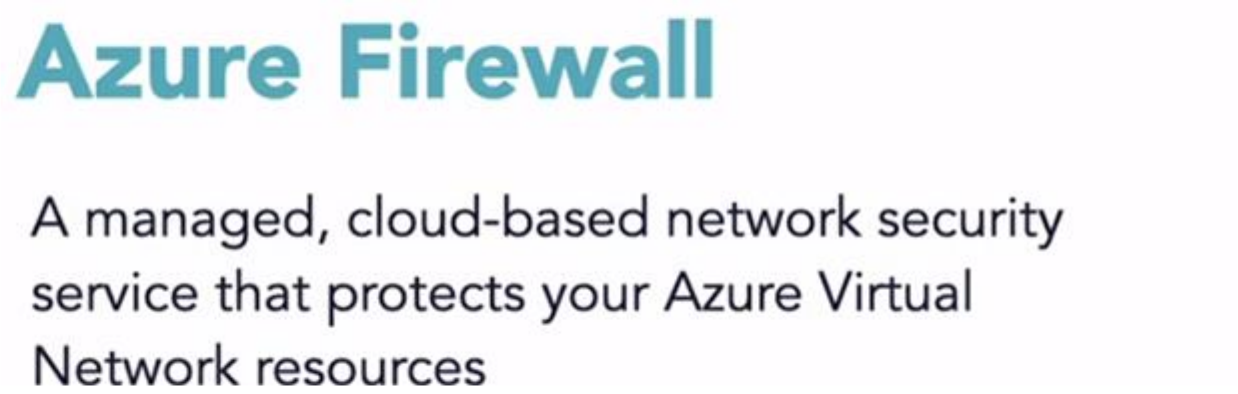
All network interfaces must be within the same virtual network (VNet)

ASGs used in the source and destination must be within the same VNet

ASG Summary

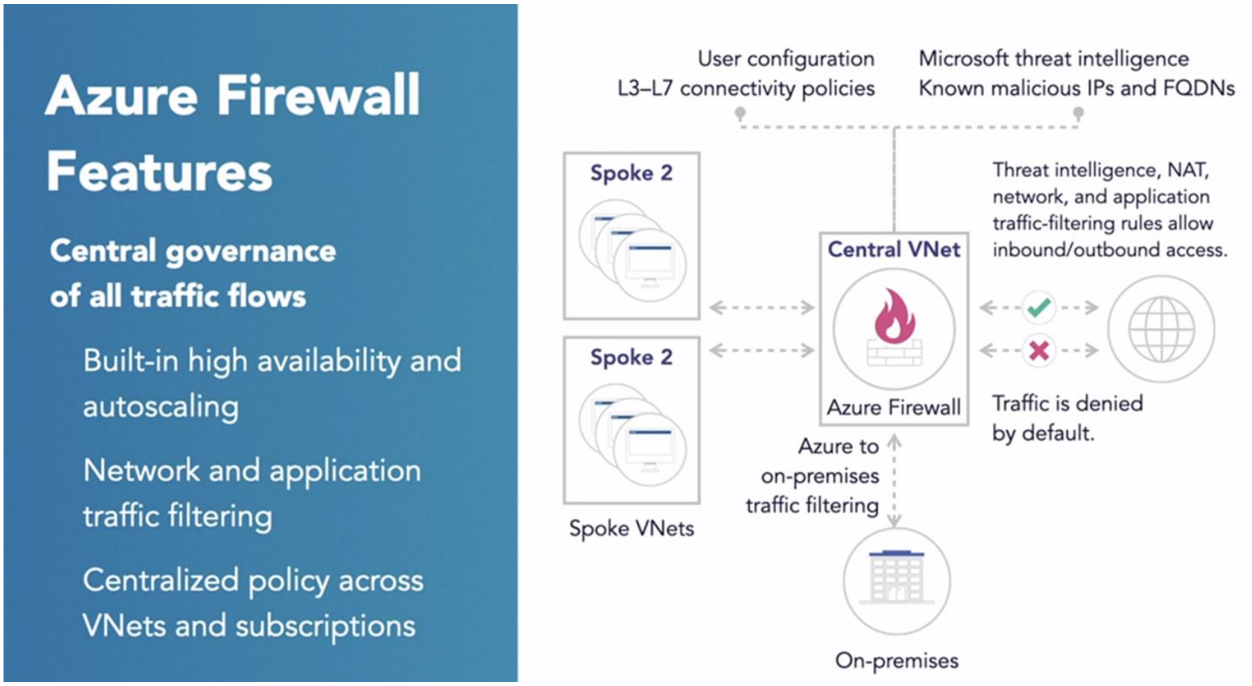
ASGs facilitate micro-segmentation—fine-grained traffic filtering based on the application patterns.

1.3 Create and configure Microsoft Azure Firewall



Azure Firewall

A managed, cloud-based network security service that protects your Azure Virtual Network resources

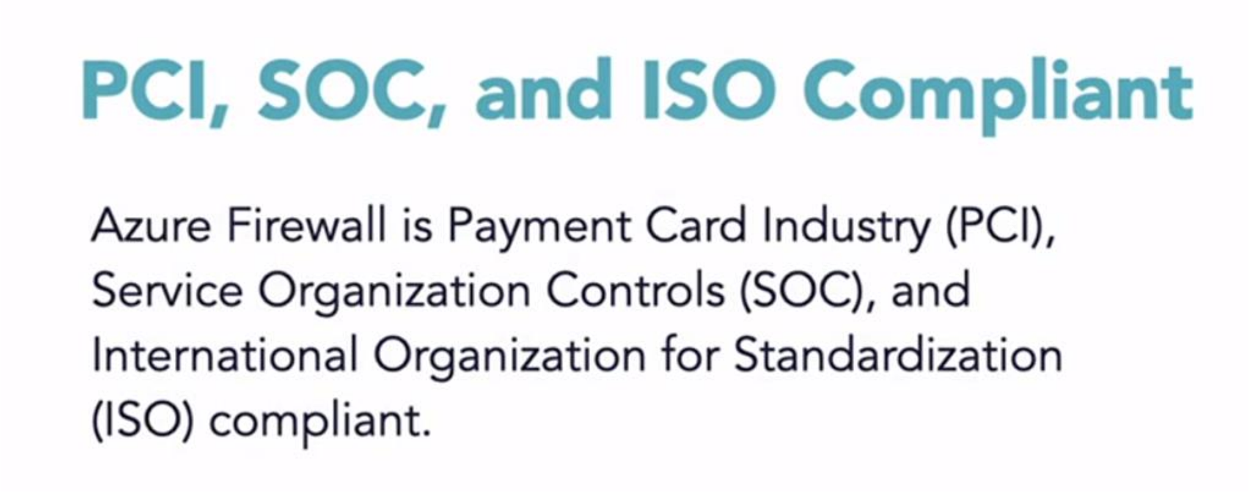


Azure Firewall Features

Central governance of all traffic flows

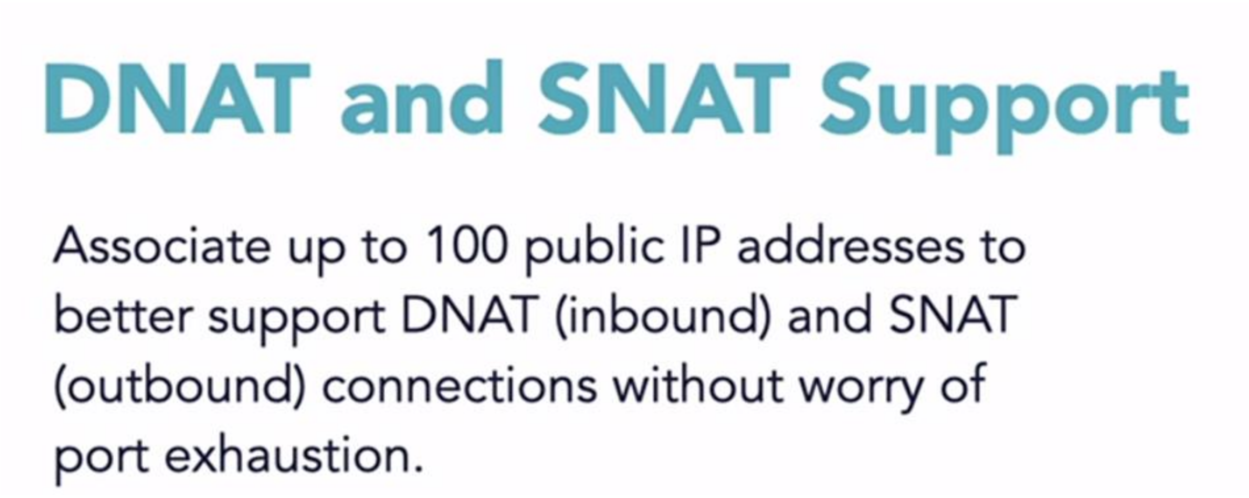
- Built-in high availability and autoscaling
- Network and application traffic filtering
- Centralized policy across VNets and subscriptions

User configuration
L3–L7 connectivity policies
Microsoft threat intelligence
Known malicious IPs and FQDNs
Spoke 2
Spoke 2
Spoke VNets
Central VNet
Azure Firewall
Threat intelligence, NAT, network, and application traffic-filtering rules allow inbound/outbound access.
Traffic is denied by default.
Azure to on-premises traffic filtering
On-premises



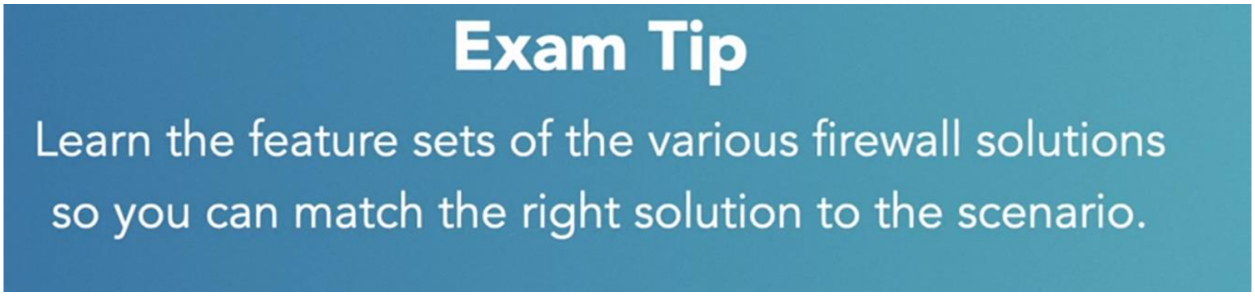
PCI, SOC, and ISO Compliant

Azure Firewall is Payment Card Industry (PCI), Service Organization Controls (SOC), and International Organization for Standardization (ISO) compliant.



DNAT and SNAT Support

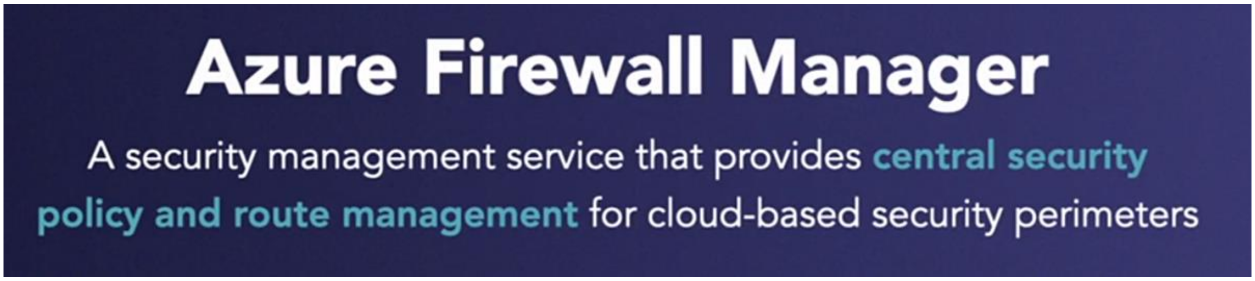
Associate up to 100 public IP addresses to better support DNAT (inbound) and SNAT (outbound) connections without worry of port exhaustion.



Exam Tip

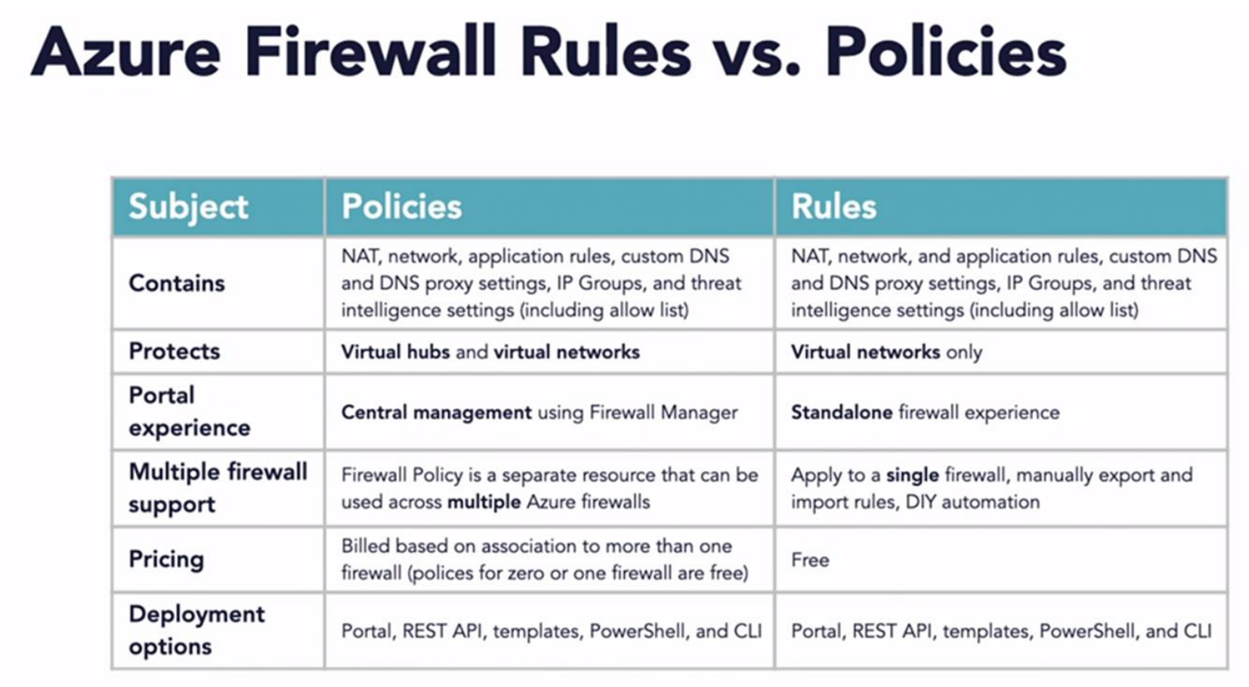
Learn the feature sets of the various firewall solutions so you can match the right solution to the scenario.

1.4 Create and configure Azure Firewall Manager



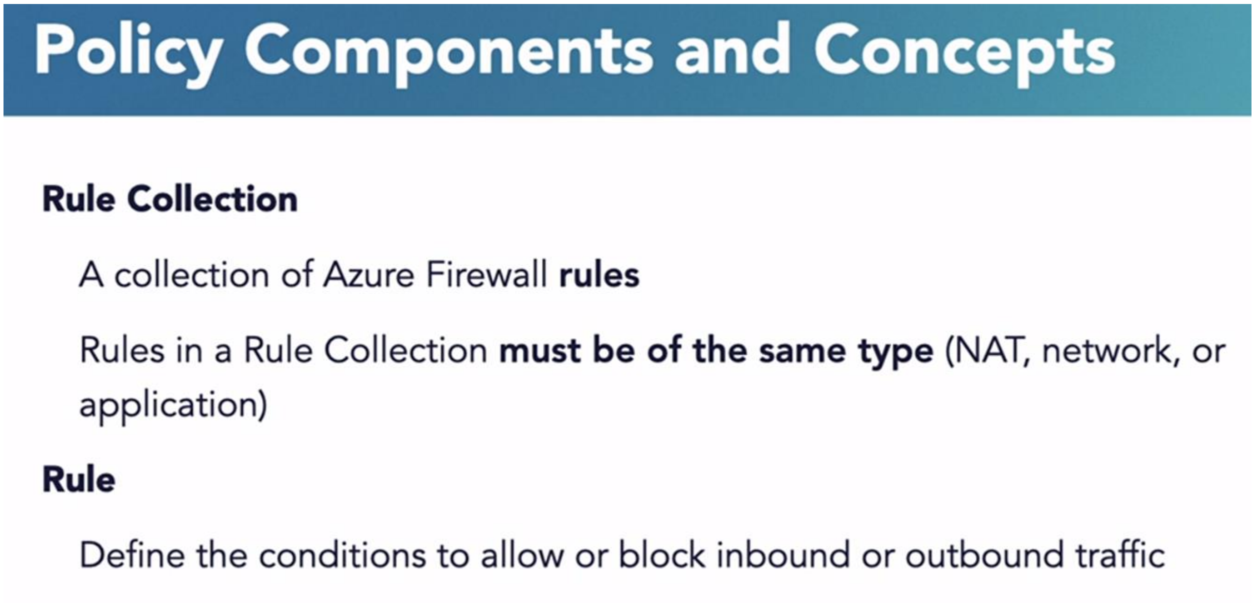
Azure Firewall Manager

A security management service that provides **central security policy and route management** for cloud-based security perimeters



Azure Firewall Rules vs. Policies

Subject	Policies	Rules
Contains	NAT, network, application rules, custom DNS and DNS proxy settings, IP Groups, and threat intelligence settings (including allow list)	NAT, network, and application rules, custom DNS and DNS proxy settings, IP Groups, and threat intelligence settings (including allow list)
Protects	**Virtual hubs** and **virtual networks**	**Virtual networks** only
Portal experience	**Central management** using Firewall Manager	**Standalone** firewall experience
Multiple firewall support	Firewall Policy is a separate resource that can be used across **multiple** Azure firewalls	Apply to a **single** firewall, manually export and import rules, DIY automation
Pricing	Billed based on association to more than one firewall (polices for zero or one firewall are free)	Free
Deployment options	Portal, REST API, templates, PowerShell, and CLI	Portal, REST API, templates, PowerShell, and CLI



Policy Components and Concepts

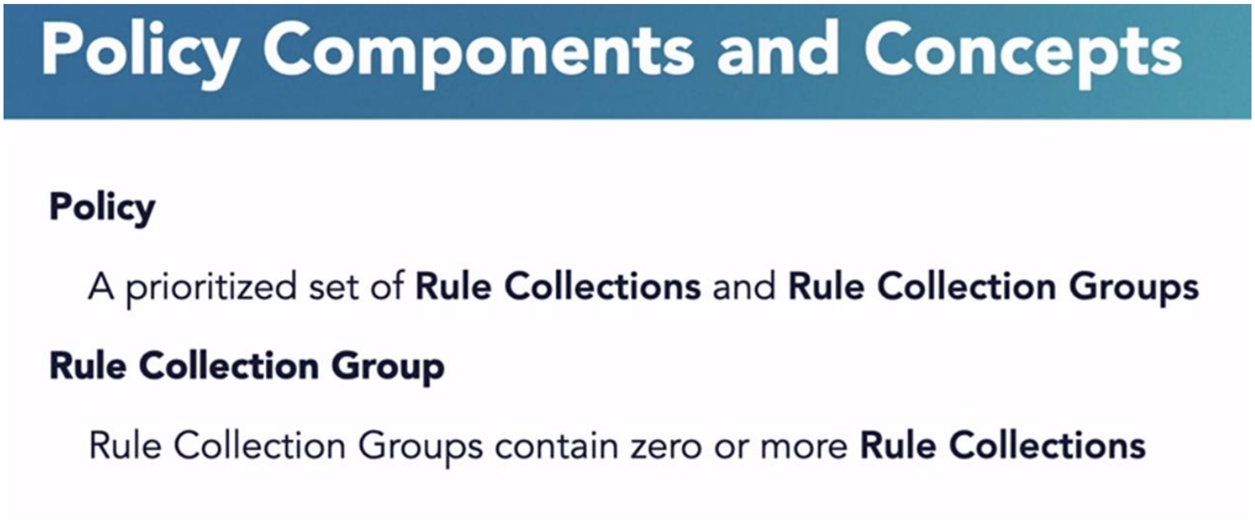
Rule Collection

A collection of Azure Firewall **rules**

Rules in a Rule Collection **must be of the same type** (NAT, network, or application)

Rule

Define the conditions to allow or block inbound or outbound traffic



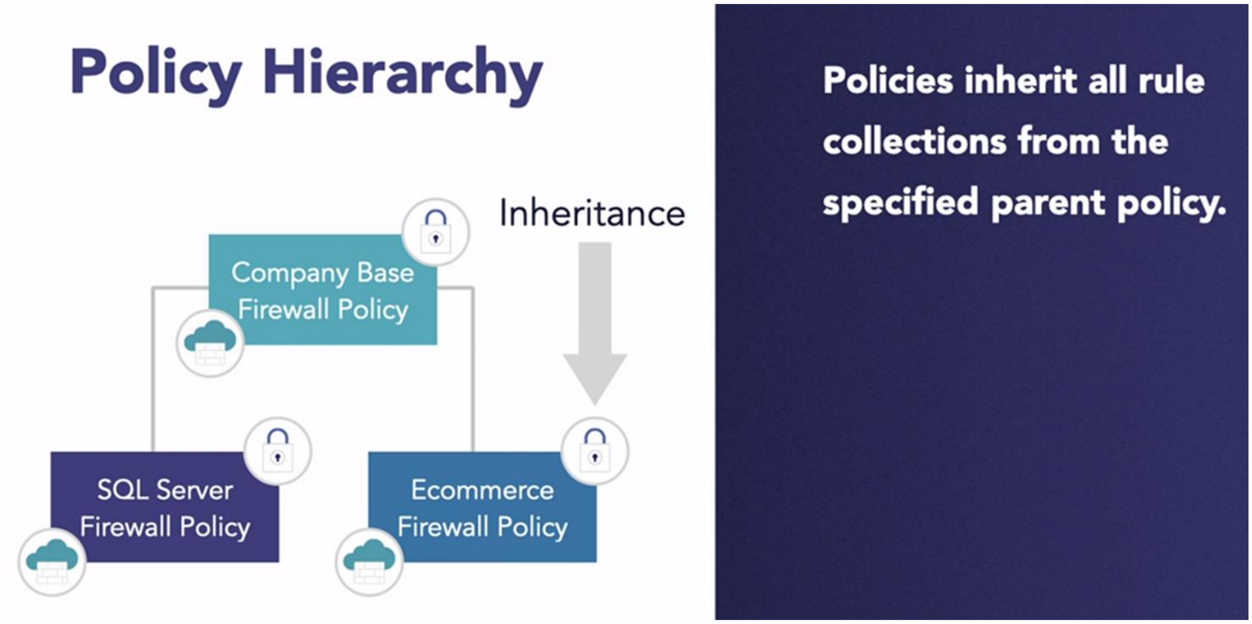
Policy Components and Concepts

Policy

A prioritized set of **Rule Collections** and **Rule Collection Groups**

Rule Collection Group

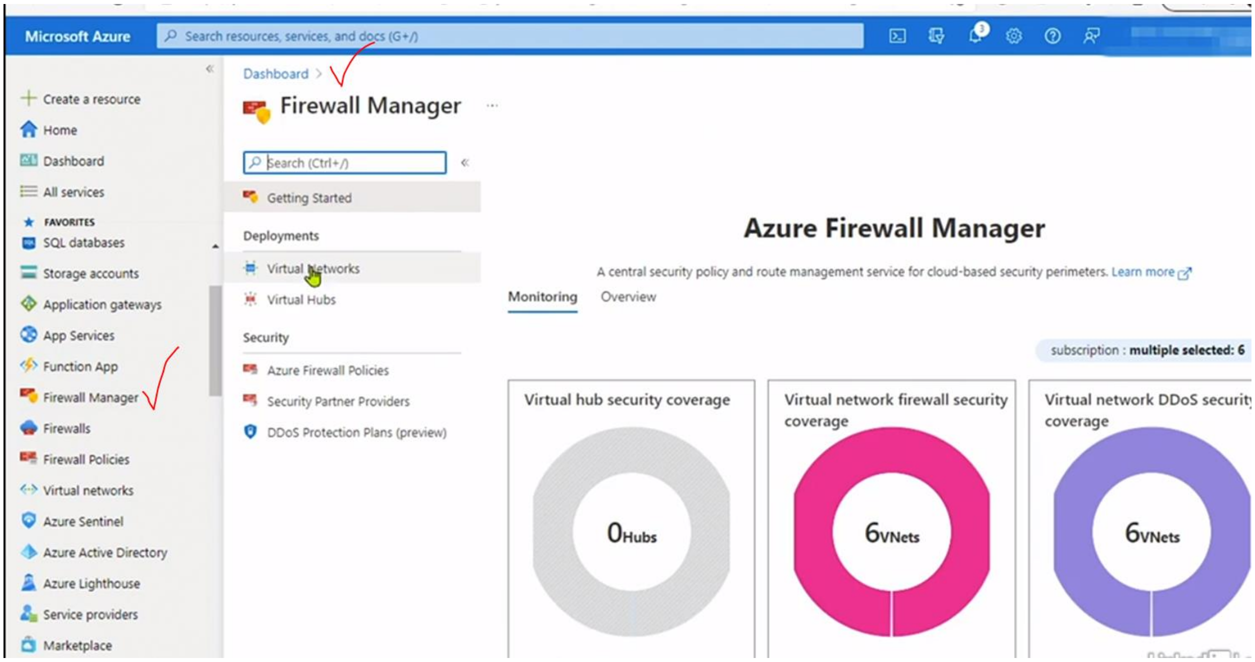
Rule Collection Groups contain zero or more **Rule Collections**



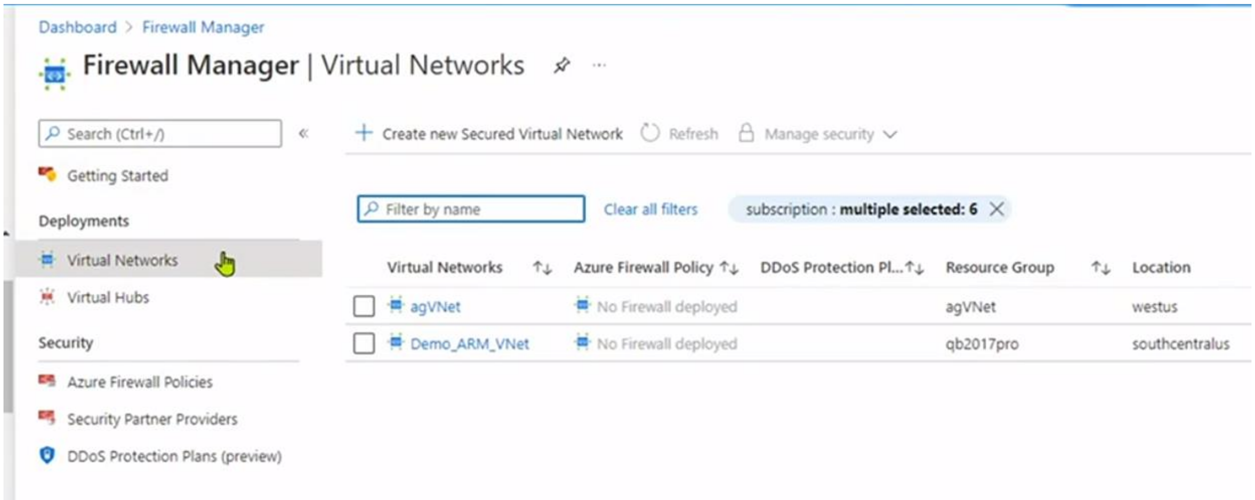
Policy Hierarchy

Inheritance
Company Base Firewall Policy
SQL Server Firewall Policy
Ecommerce Firewall Policy

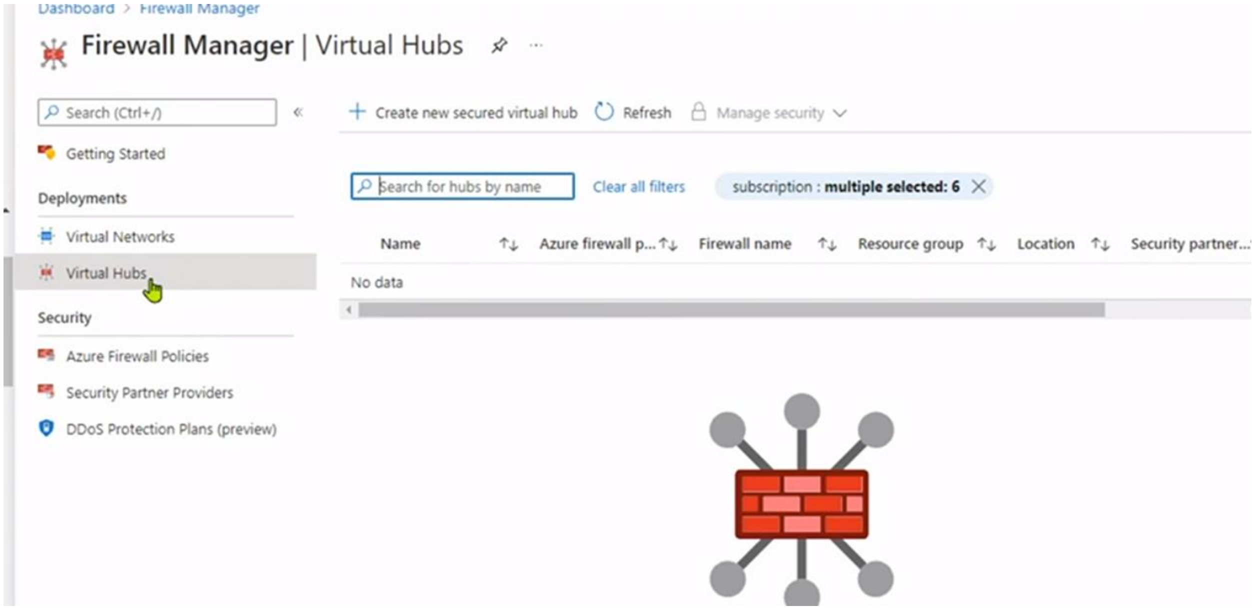
Policies inherit all rule collections from the specified parent policy.



A central security policy and route management service for cloud-based security perimeters. Learn more


Dashboard > Firewall Manager
Firewall Manager | Virtual Networks
Search (Ctrl+/)
Getting Started
Deployments
Virtual Networks
Virtual Hubs
Security
Azure Firewall Policies
Security Partner Providers
DDoS Protection Plans (preview)
Create new Secured Virtual Network
Refresh
Manage security
Filter by name
Clear all filters
subscription : multiple selected: 6

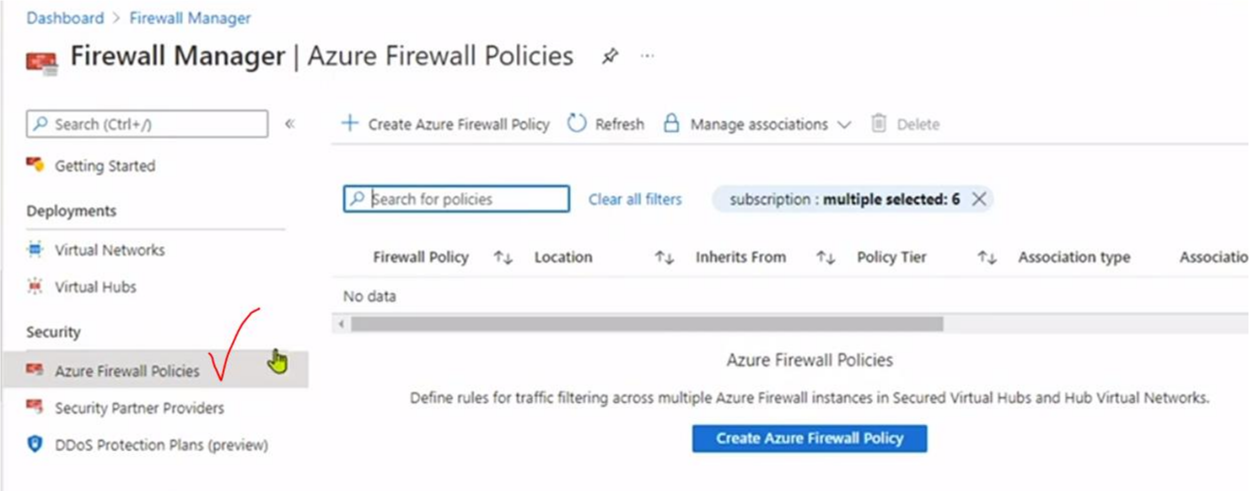
	Virtual Networks	Azure Firewall Policy	DDoS Protection Pl...	Resource Group	Location
□	agVNet	No Firewall deployed		agVNet	westus
□	Demo_ARM_VNet	No Firewall deployed		qb2017pro	southcentralus



Firewall Manager | Virtual Hubs

subscription : **multiple selected: 6**

Name	Azure firewall p...	Firewall name	Resource group	Location	Security partner...
No data					



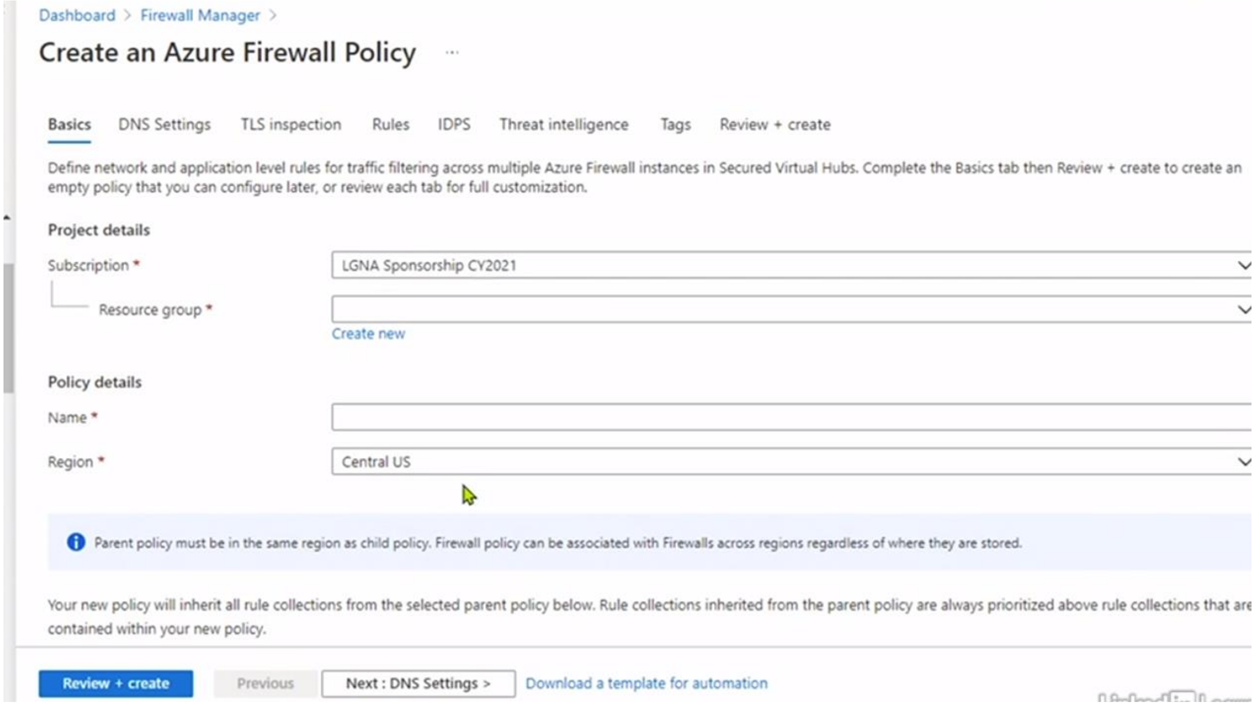
Firewall Manager | Azure Firewall Policies

subscription : **multiple selected: 6**

Firewall Policy	Location	Inherits From	Policy Tier	Association type	Associatio
No data					

Azure Firewall Policies

Define rules for traffic filtering across multiple Azure Firewall instances in Secured Virtual Hubs and Hub Virtual Networks.



Dashboard > Firewall Manager >

Create an Azure Firewall Policy ...

Basics | DNS Settings | TLS inspection | Rules | IDPS | Threat intelligence | Tags | Review + create

Define network and application level rules for traffic filtering across multiple Azure Firewall instances in Secured Virtual Hubs. Complete the Basics tab then Review + create to create an empty policy that you can configure later, or review each tab for full customization.

Project details

Subscription * : LGNA Sponsorship CY2021

Resource group * :

Create new

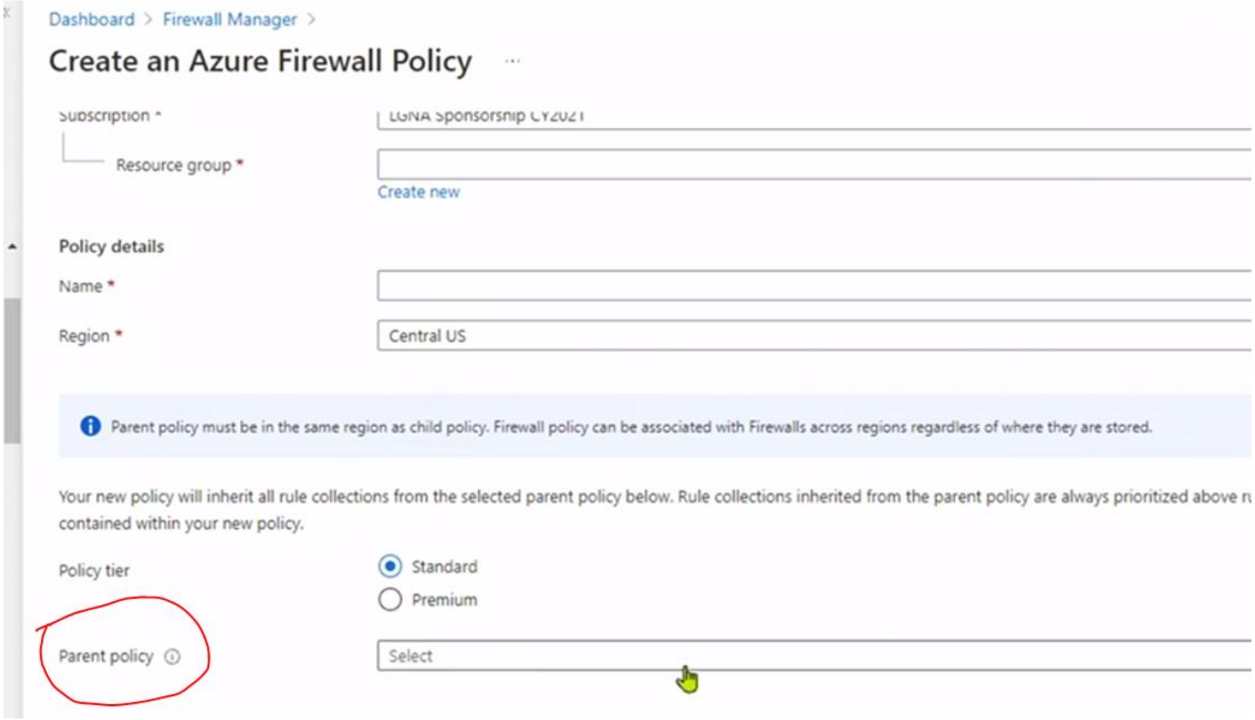
Policy details

Name * :

Region * : Central US

Parent policy must be in the same region as child policy. Firewall policy can be associated with Firewalls across regions regardless of where they are stored.

Your new policy will inherit all rule collections from the selected parent policy below. Rule collections inherited from the parent policy are always prioritized above rule collections that are contained within your new policy.



Dashboard > Firewall Manager >

Create an Azure Firewall Policy ...

Subscription * : LGNA Sponsorship CY2021

Resource group * :

Create new

Policy details

Name * :

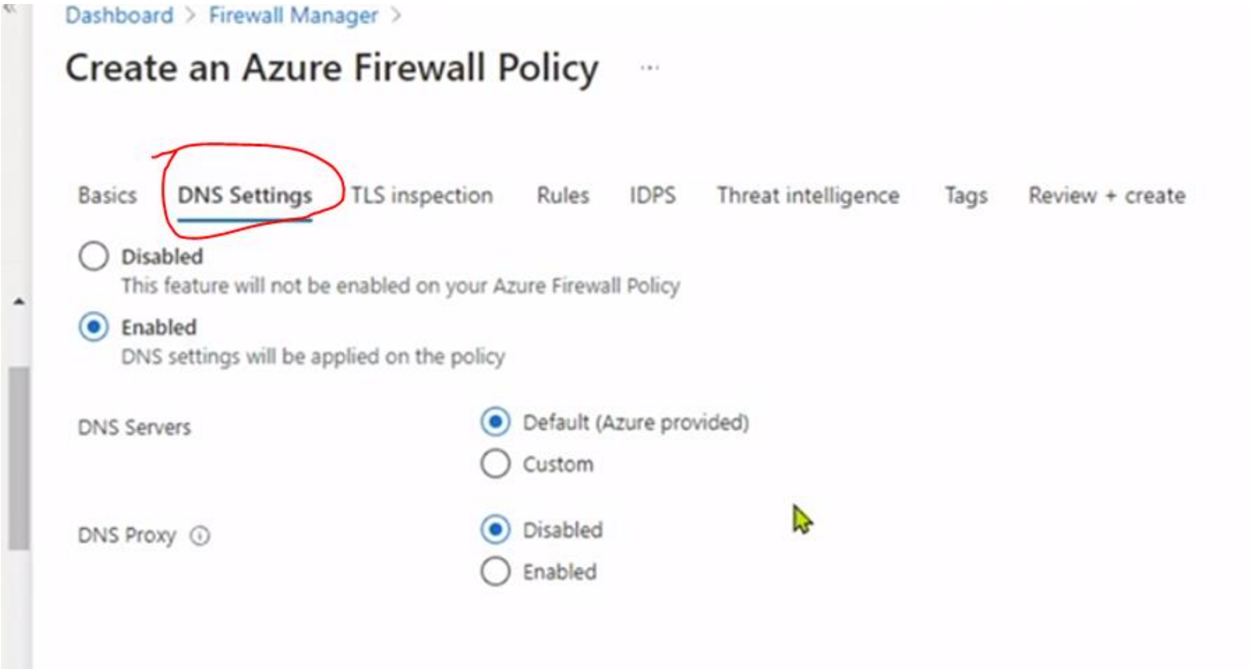
Region * : Central US

Parent policy must be in the same region as child policy. Firewall policy can be associated with Firewalls across regions regardless of where they are stored.

Your new policy will inherit all rule collections from the selected parent policy below. Rule collections inherited from the parent policy are always prioritized above r contained within your new policy.

Policy tier: ● Standard ○ Premium

Parent policy ⓘ : Select



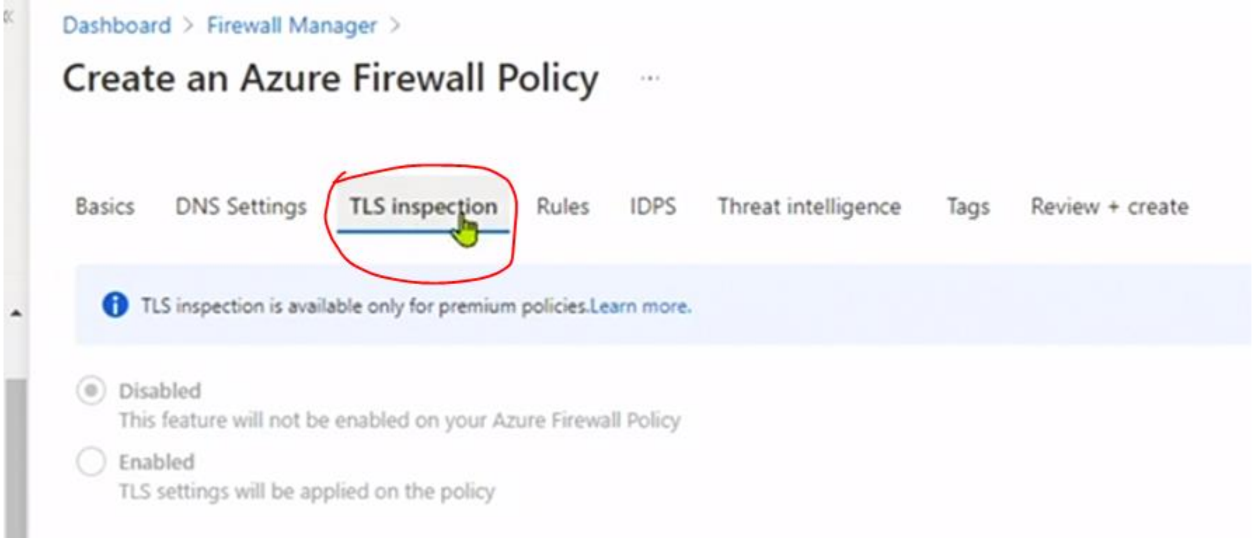
Create an Azure Firewall Policy

○ Disabled
This feature will not be enabled on your Azure Firewall Policy

● Enabled
DNS settings will be applied on the policy

DNS Servers: ● Default (Azure provided) ○ Custom

DNS Proxy: ● Disabled ○ Enabled

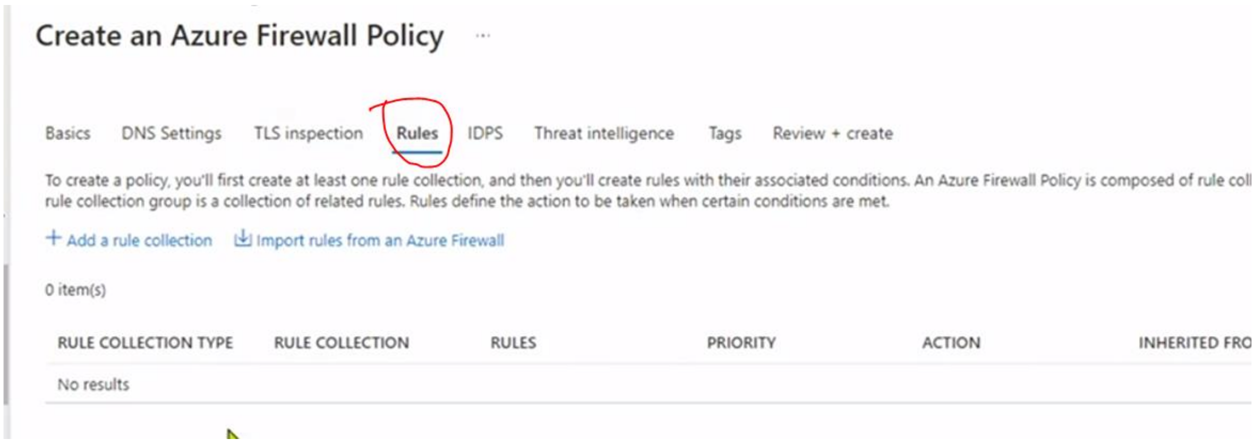


Create an Azure Firewall Policy

TLS inspection is available only for premium policies.Learn more.

● Disabled
This feature will not be enabled on your Azure Firewall Policy

○ Enabled
TLS settings will be applied on the policy

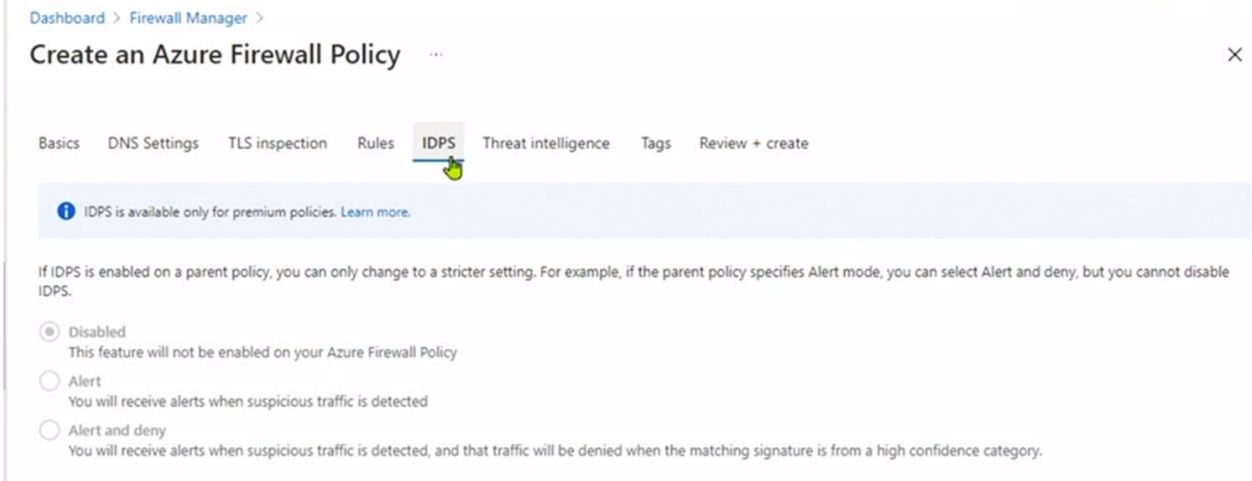


Create an Azure Firewall Policy

To create a policy, you'll first create at least one rule collection, and then you'll create rules with their associated conditions. An Azure Firewall Policy is composed of rule coll
rule collection group is a collection of related rules. Rules define the action to be taken when certain conditions are met.

0 item(s)

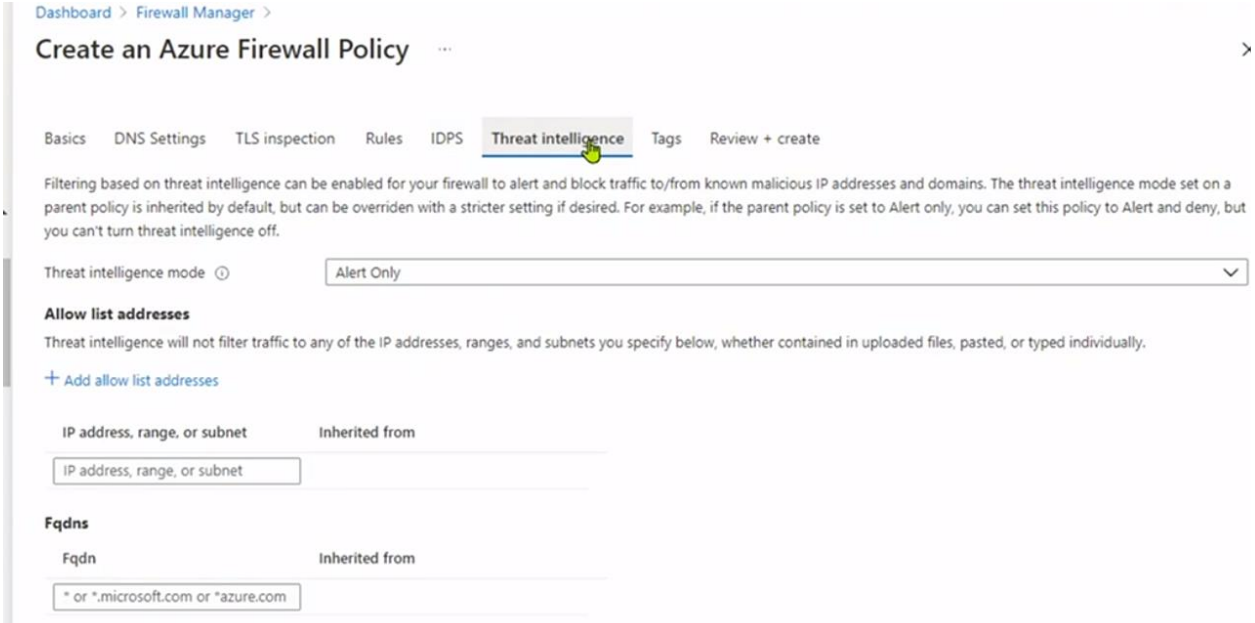
RULE COLLECTION TYPE	RULE COLLECTION	RULES	PRIORITY	ACTION	INHERITED FRO
No results					



IDPS is available only for premium policies. Learn more.

If IDPS is enabled on a parent policy, you can only change to a stricter setting. For example, if the parent policy specifies Alert mode, you can select Alert and deny, but you cannot disable IDPS.

- ● Disabled
  This feature will not be enabled on your Azure Firewall Policy
- ○ Alert
  You will receive alerts when suspicious traffic is detected
- ○ Alert and deny
  You will receive alerts when suspicious traffic is detected, and that traffic will be denied when the matching signature is from a high confidence category.



Filtering based on threat intelligence can be enabled for your firewall to alert and block traffic to/from known malicious IP addresses and domains. The threat intelligence mode set on a parent policy is inherited by default, but can be overriden with a stricter setting if desired. For example, if the parent policy is set to Alert only, you can set this policy to Alert and deny, but you can't turn threat intelligence off.

Threat intelligence mode: Alert Only

Allow list addresses

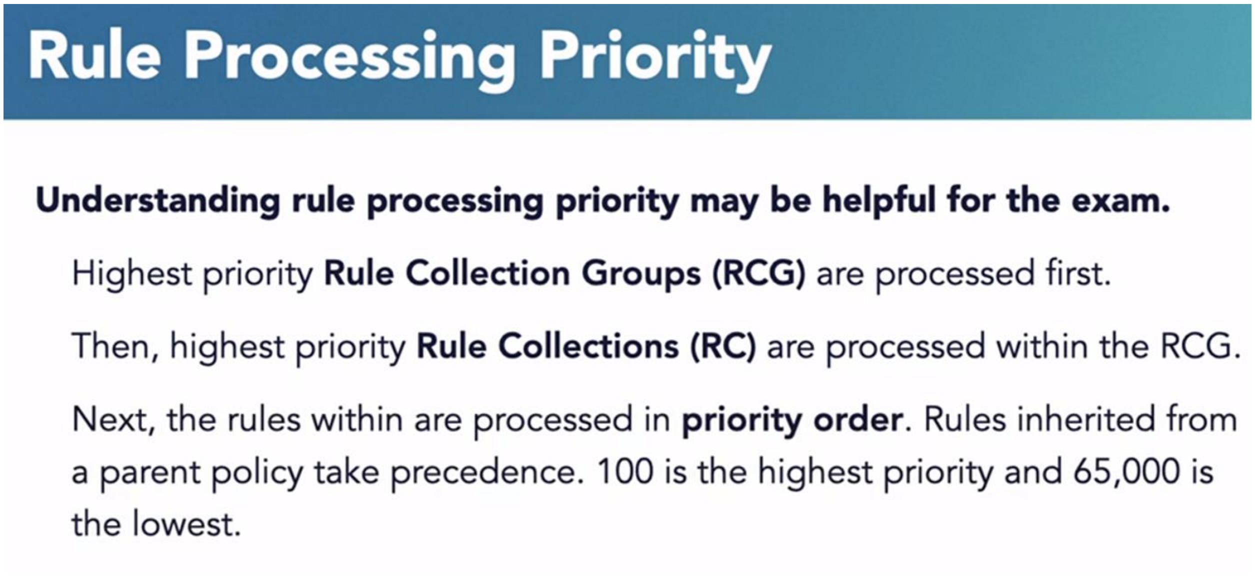
Threat intelligence will not filter traffic to any of the IP addresses, ranges, and subnets you specify below, whether contained in uploaded files, pasted, or typed individually.

+ Add allow list addresses

IP address, range, or subnet	Inherited from
IP address, range, or subnet	

Fqdns

Fqdn	Inherited from
* or *.microsoft.com or *azure.com	



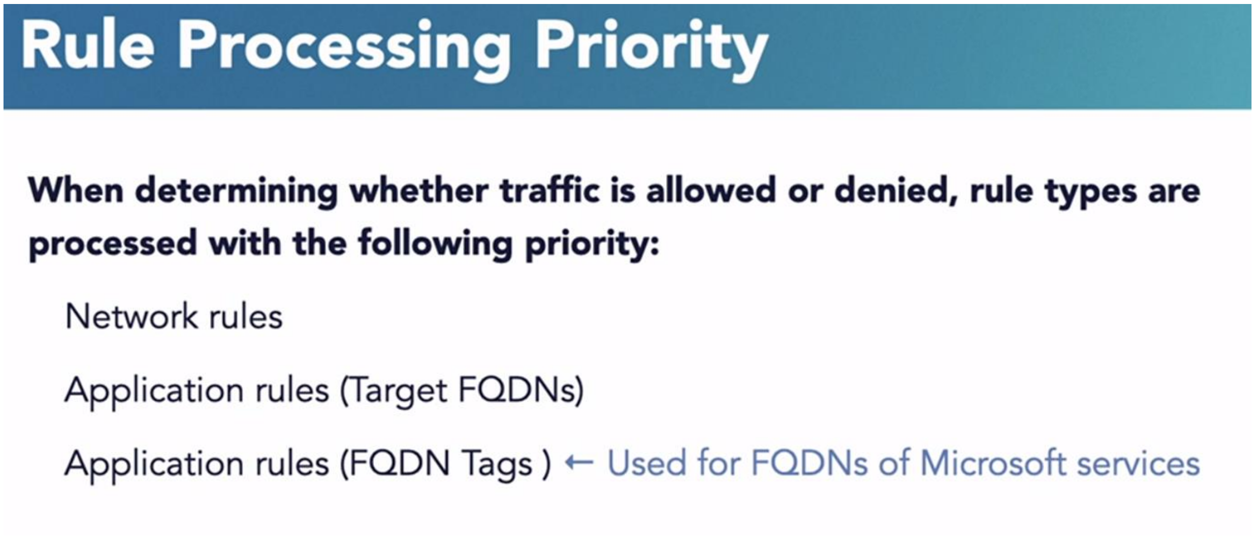
Rule Processing Priority

Understanding rule processing priority may be helpful for the exam.

Highest priority **Rule Collection Groups (RCG)** are processed first.

Then, highest priority **Rule Collections (RC)** are processed within the RCG.

Next, the rules within are processed in **priority order**. Rules inherited from a parent policy take precedence. 100 is the highest priority and 65,000 is the lowest.



Rule Processing Priority

When determining whether traffic is allowed or denied, rule types are processed with the following priority:

Network rules

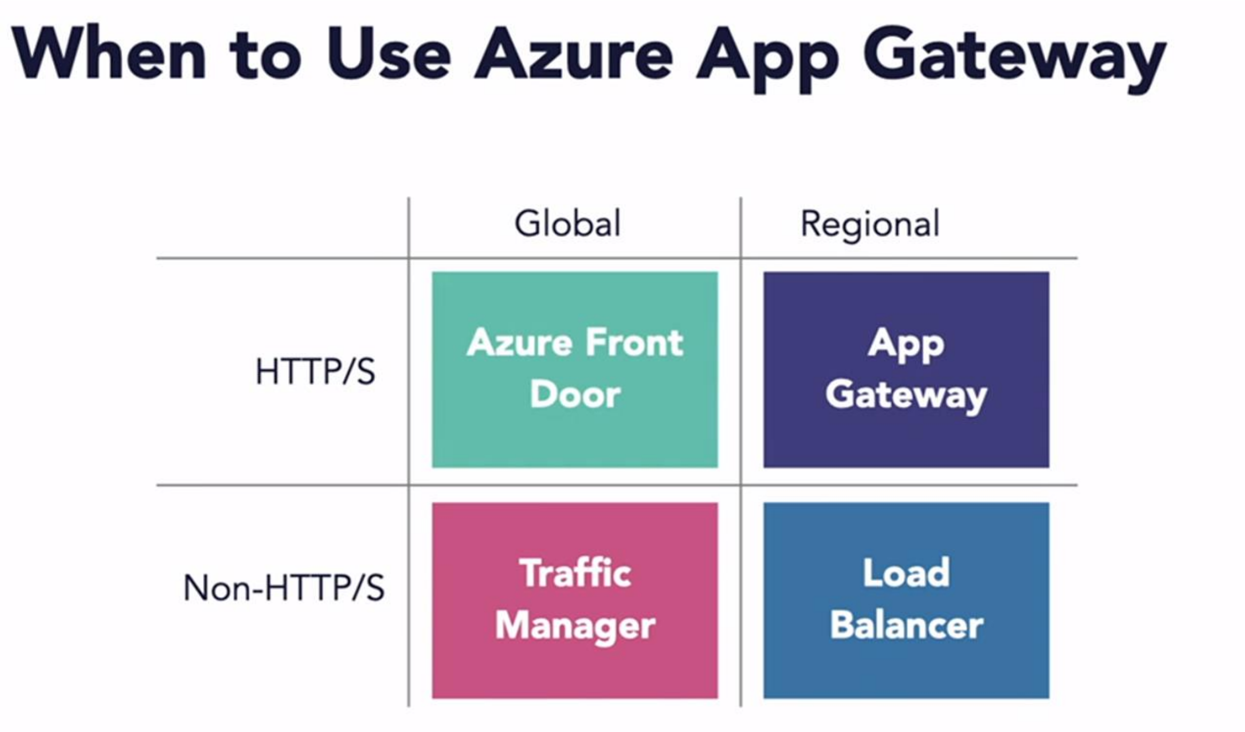
Application rules (Target FQDNs)

Application rules (FQDN Tags) ← Used for FQDNs of Microsoft services

Exam Tip

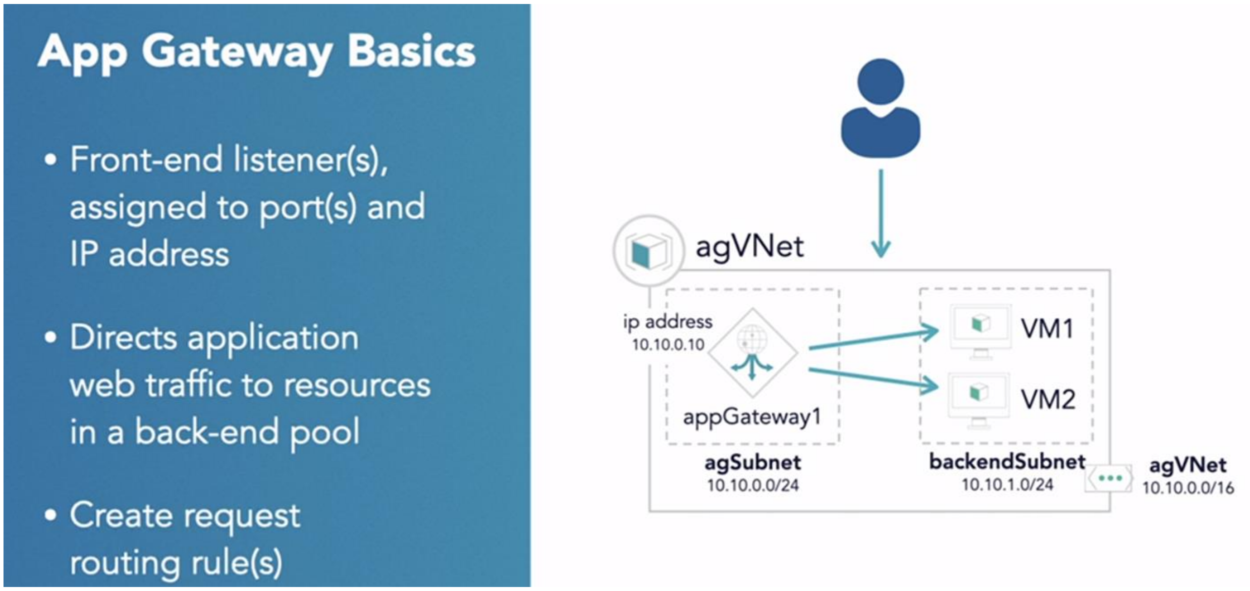
Complete the Azure Firewall Manager tutorial in the course download so you have hands-on experience before taking the exam.

1.5 Create and configure Azure Application Gateway



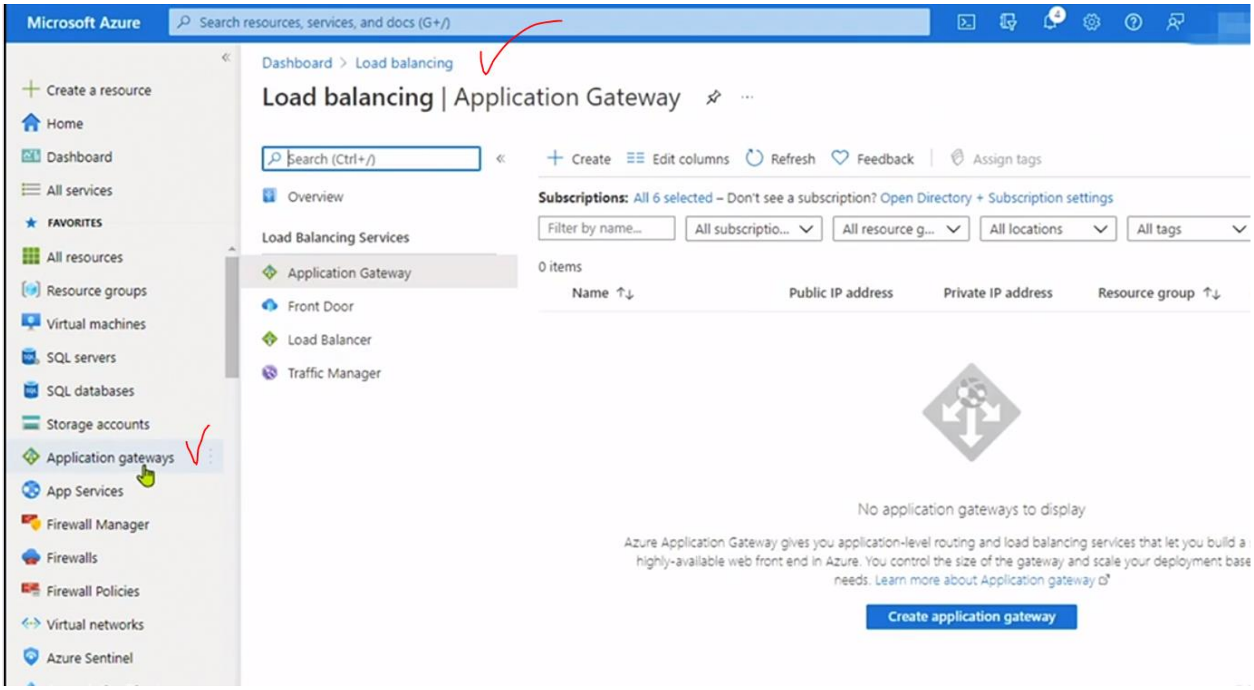
When to Use Azure App Gateway

	Global	Regional
HTTP/S	Azure Front Door	App Gateway
Non-HTTP/S	Traffic Manager	Load Balancer



App Gateway Basics

- Front-end listener(s), assigned to port(s) and IP address
- Directs application web traffic to resources in a back-end pool
- Create request routing rule(s)



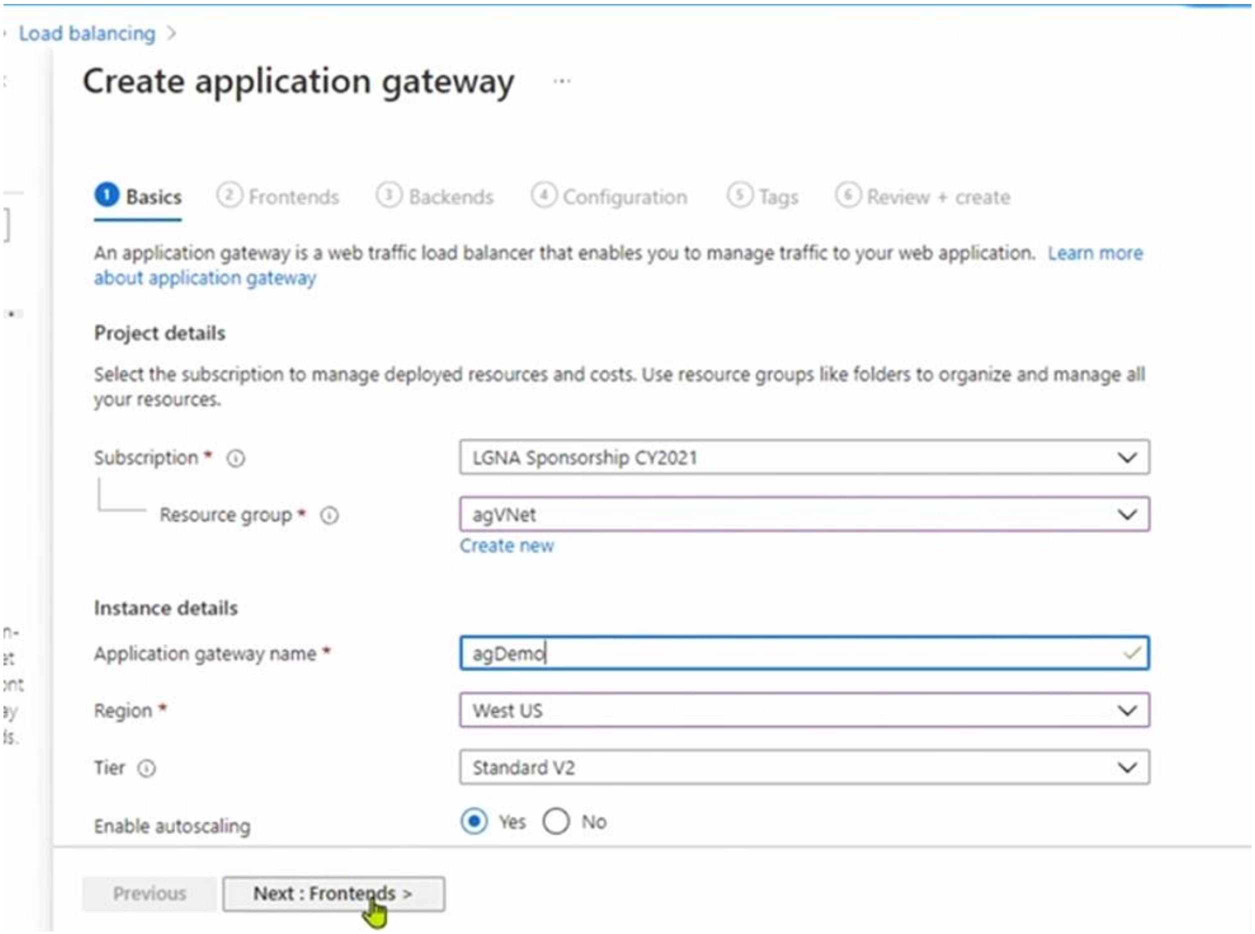
Subscriptions: All 6 selected – Don't see a subscription? Open Directory + Subscription settings

0 items

No application gateways to display

Azure Application Gateway gives you application-level routing and load balancing services that let you build a highly-available web front end in Azure. You control the size of the gateway and scale your deployment base needs. Learn more about Application gateway

Creating an application Gateway



Create application gateway

An application gateway is a web traffic load balancer that enables you to manage traffic to your web application. Learn more about application gateway

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : LGNA Sponsorship CY2021

Resource group * : agVNet

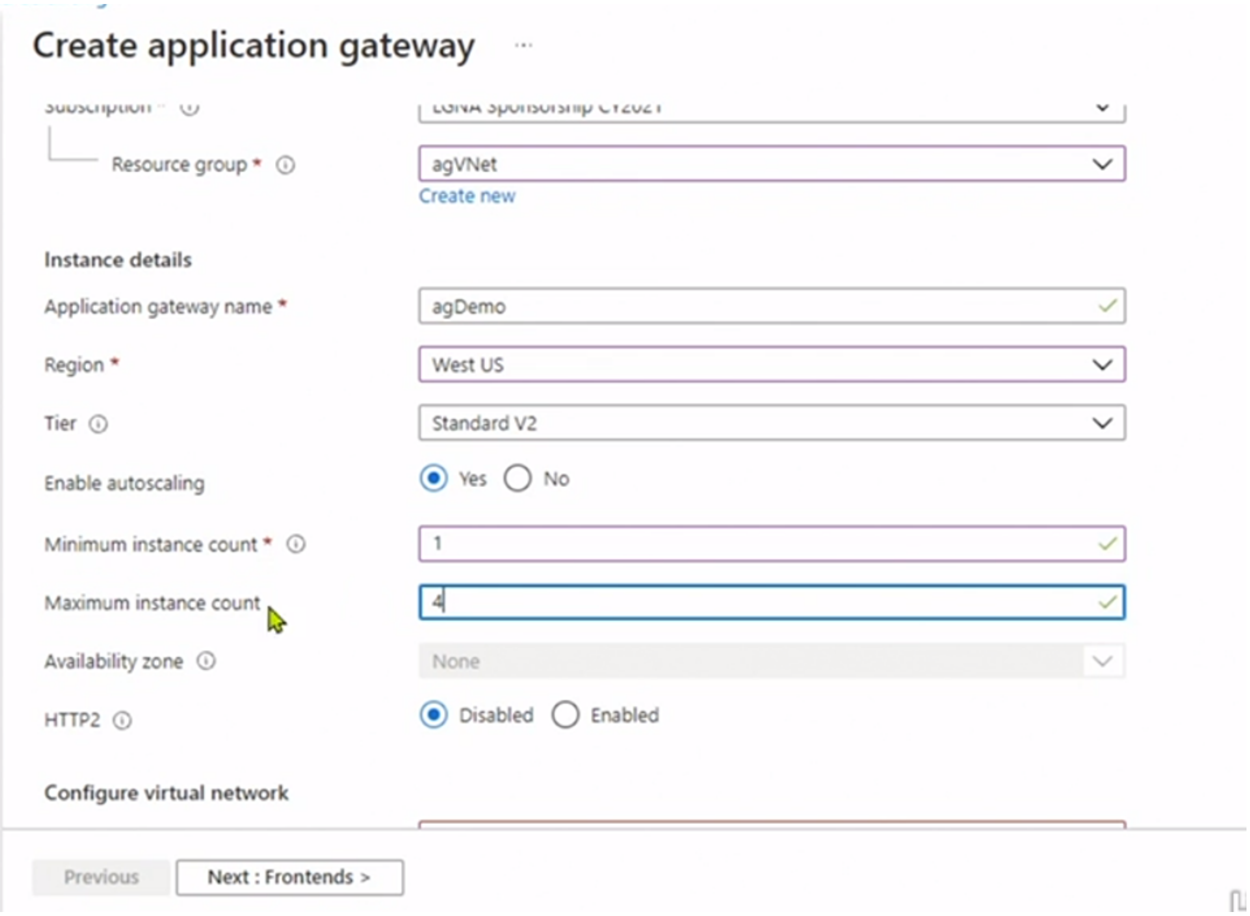
Instance details

Application gateway name * : agDemo

Region * : West US

Tier : Standard V2

Enable autoscaling: ● Yes ○ No



Create application gateway

Subscription * ⓘ LGNA Sponsorship CY2021

Resource group * ⓘ agVNet

Instance details

Application gateway name * agDemo

Region * West US

Tier ⓘ Standard V2

Enable autoscaling ● Yes ○ No

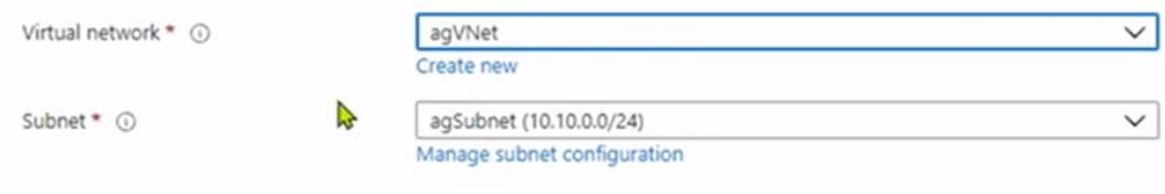
Minimum instance count * ⓘ 1

Maximum instance count 4

Availability zone ⓘ None

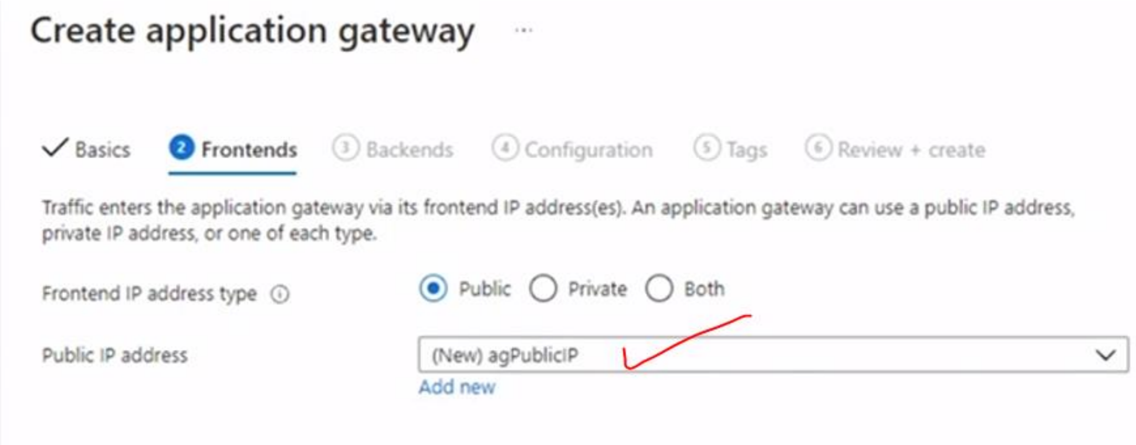
HTTP2 ⓘ ● Disabled ○ Enabled

Configure virtual network



Virtual network * ⓘ agVNet

Subnet * ⓘ agSubnet (10.10.0.0/24)

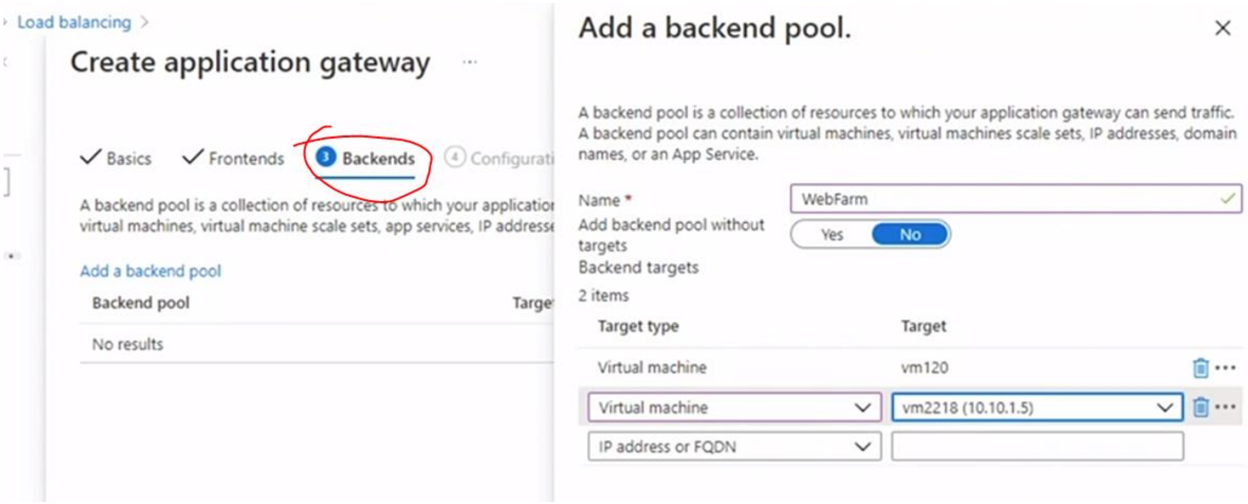


Create application gateway

Traffic enters the application gateway via its frontend IP address(es). An application gateway can use a public IP address, private IP address, or one of each type.

Frontend IP address type ⓘ ● Public ○ Private ○ Both

Public IP address (New) agPublicIP



Load balancing >

Create application gateway ...

✓ Basics ✓ Frontends 3 Backends 4 Configurati

A backend pool is a collection of resources to which your applicatio
virtual machines, virtual machine scale sets, app services, IP addresse

Add a backend pool

Backend pool	Targe
No results	

Add a backend pool.

A backend pool is a collection of resources to which your application gateway can send traffic. A backend pool can contain virtual machines, virtual machines scale sets, IP addresses, domain names, or an App Service.

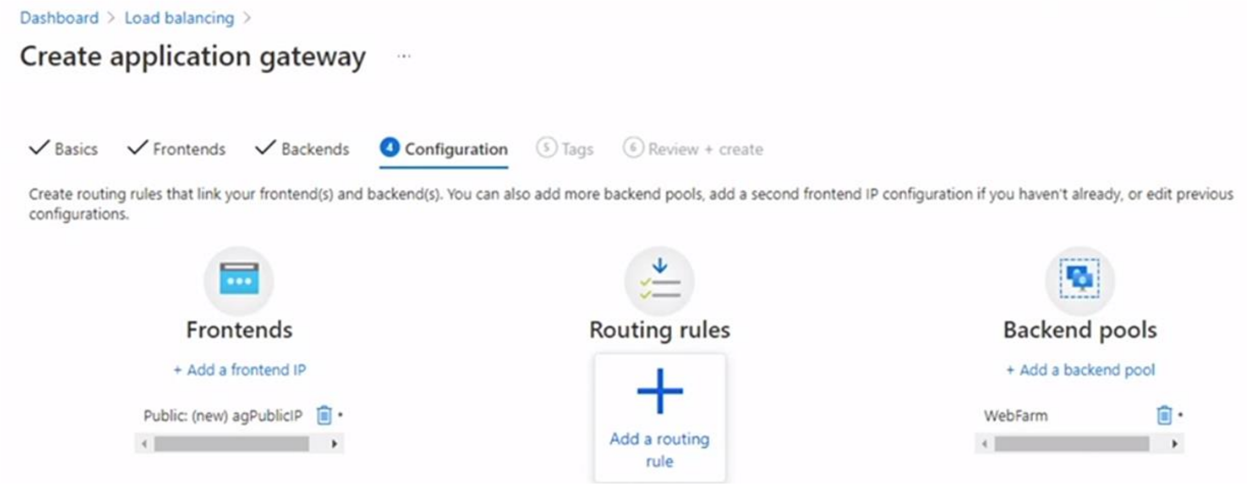
Name * WebFarm

Add backend pool without targets: Yes [✓ No]

Backend targets

2 items

Target type	Target
Virtual machine	vm120
Virtual machine	vm2218 (10.10.1.5)
IP address or FQDN	



Dashboard > Load balancing >

Create application gateway ...

✓ Basics ✓ Frontends ✓ Backends 4 Configuration 5 Tags 6 Review + create

Create routing rules that link your frontend(s) and backend(s). You can also add more backend pools, add a second frontend IP configuration if you haven't already, or edit previous configurations.

Frontends

+ Add a frontend IP

Public: (new) agPublicIP

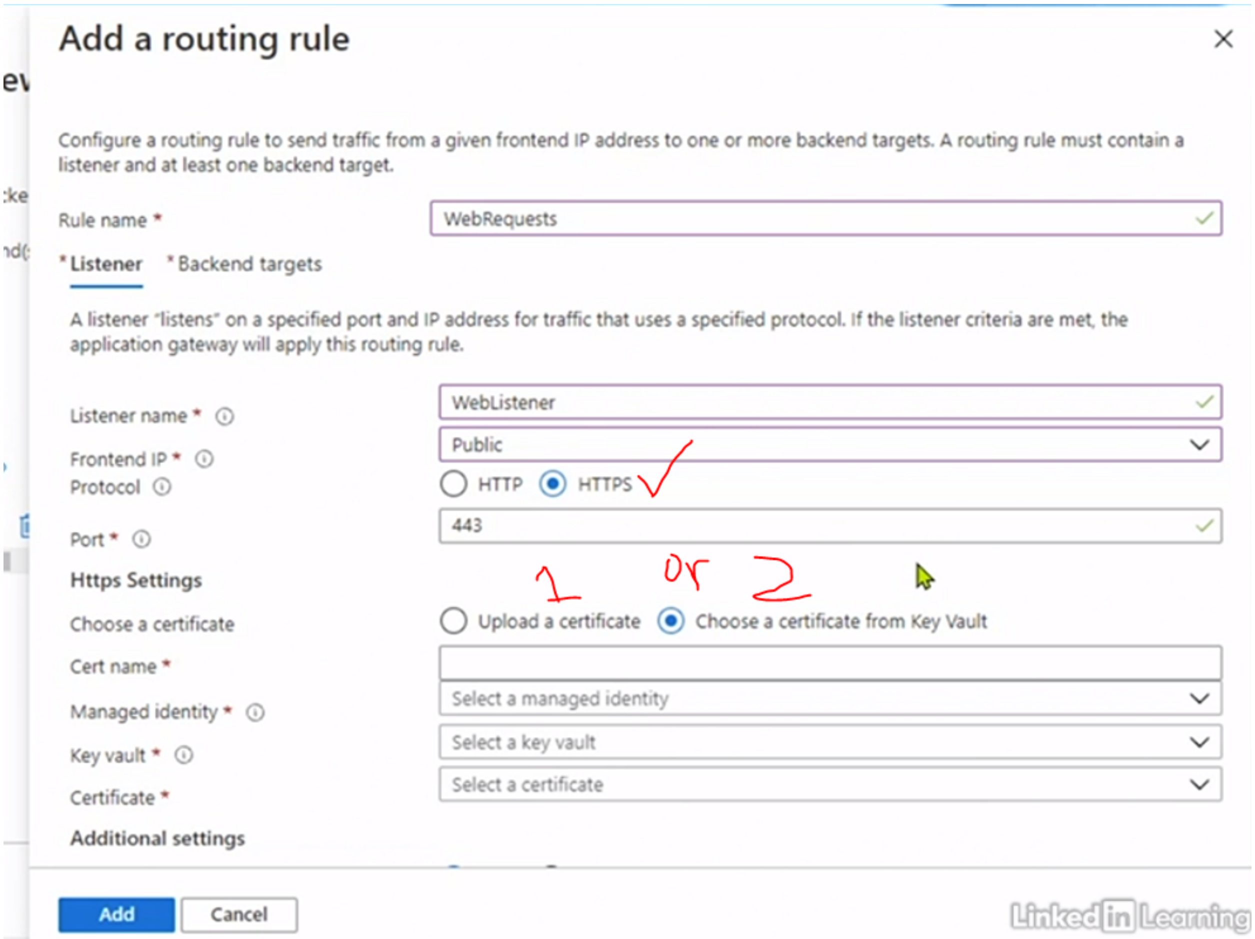
Routing rules

Add a routing rule

Backend pools

+ Add a backend pool

WebFarm



Add a routing rule

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name * WebRequests

*Listener *Backend targets

A listener "listens" on a specified port and IP address for traffic that uses a specified protocol. If the listener criteria are met, the application gateway will apply this routing rule.

Listener name * WebListener

Frontend IP * Public

Protocol ○ HTTP ● HTTPS ✓

Port * 443

Https Settings

1 or 2

Choose a certificate ○ Upload a certificate ● Choose a certificate from Key Vault

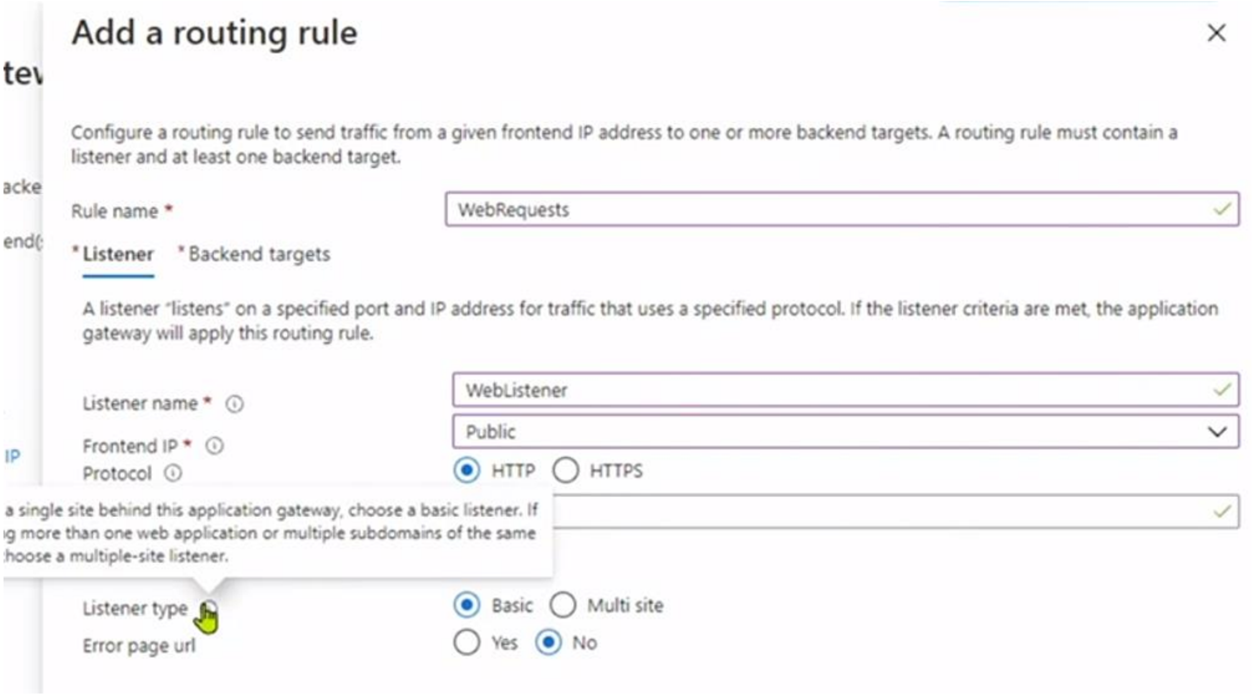
Cert name *

Managed identity * Select a managed identity

Key vault * Select a key vault

Certificate * Select a certificate

Additional settings



Add a routing rule

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name * WebRequests

*Listener *Backend targets

A listener "listens" on a specified port and IP address for traffic that uses a specified protocol. If the listener criteria are met, the application gateway will apply this routing rule.

Listener name * WebListener

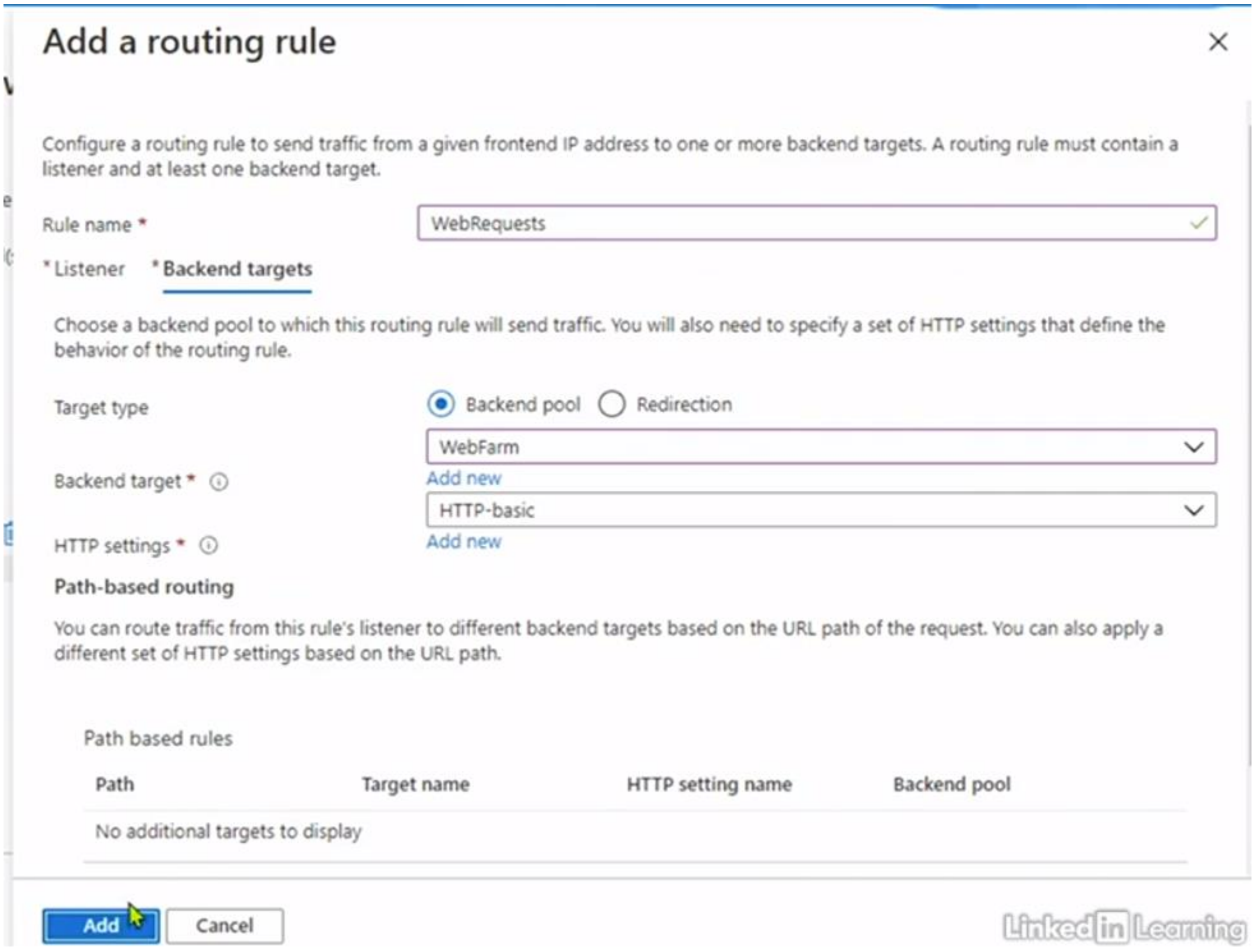
Frontend IP * Public

Protocol ● HTTP ○ HTTPS

a single site behind this application gateway, choose a basic listener. If g more than one web application or multiple subdomains of the same hoose a multiple-site listener.

Listener type ● Basic ○ Multi site

Error page url ○ Yes ● No



Add a routing rule

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name * WebRequests ✓

* Listener * **Backend targets**

Choose a backend pool to which this routing rule will send traffic. You will also need to specify a set of HTTP settings that define the behavior of the routing rule.

Target type ● Backend pool ○ Redirection

Backend target * ⓘ WebFarm

HTTP settings * ⓘ HTTP-basic

Path-based routing

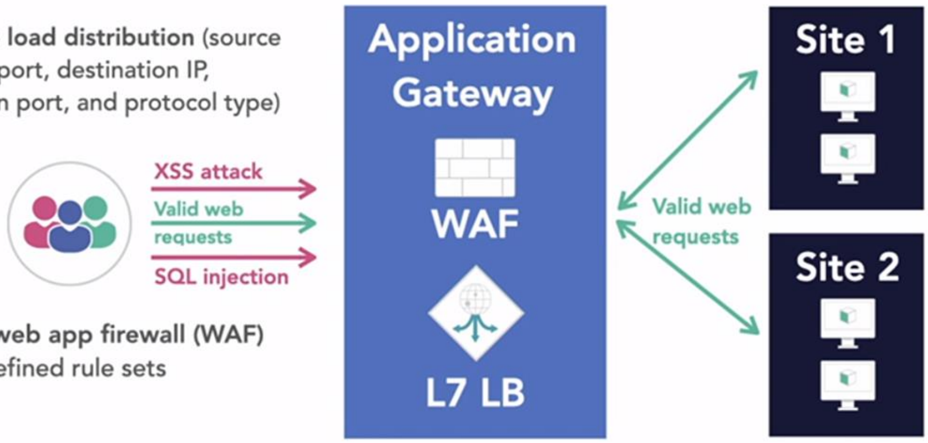
You can route traffic from this rule's listener to different backend targets based on the URL path of the request. You can also apply a different set of HTTP settings based on the URL path.

Path based rules

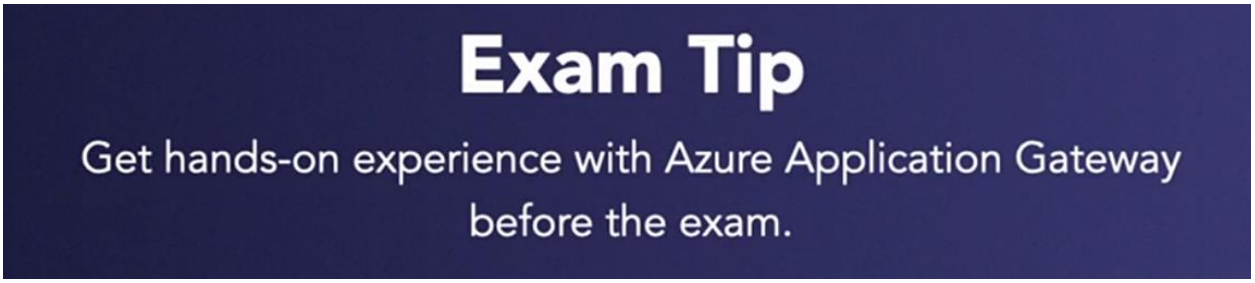
Path	Target name	HTTP setting name	Backend pool
No additional targets to display			

App Gateway Functionality

Five-tuple load distribution (source IP, source port, destination IP, destination port, and protocol type)



Optional **web app firewall (WAF)** with predefined rule sets



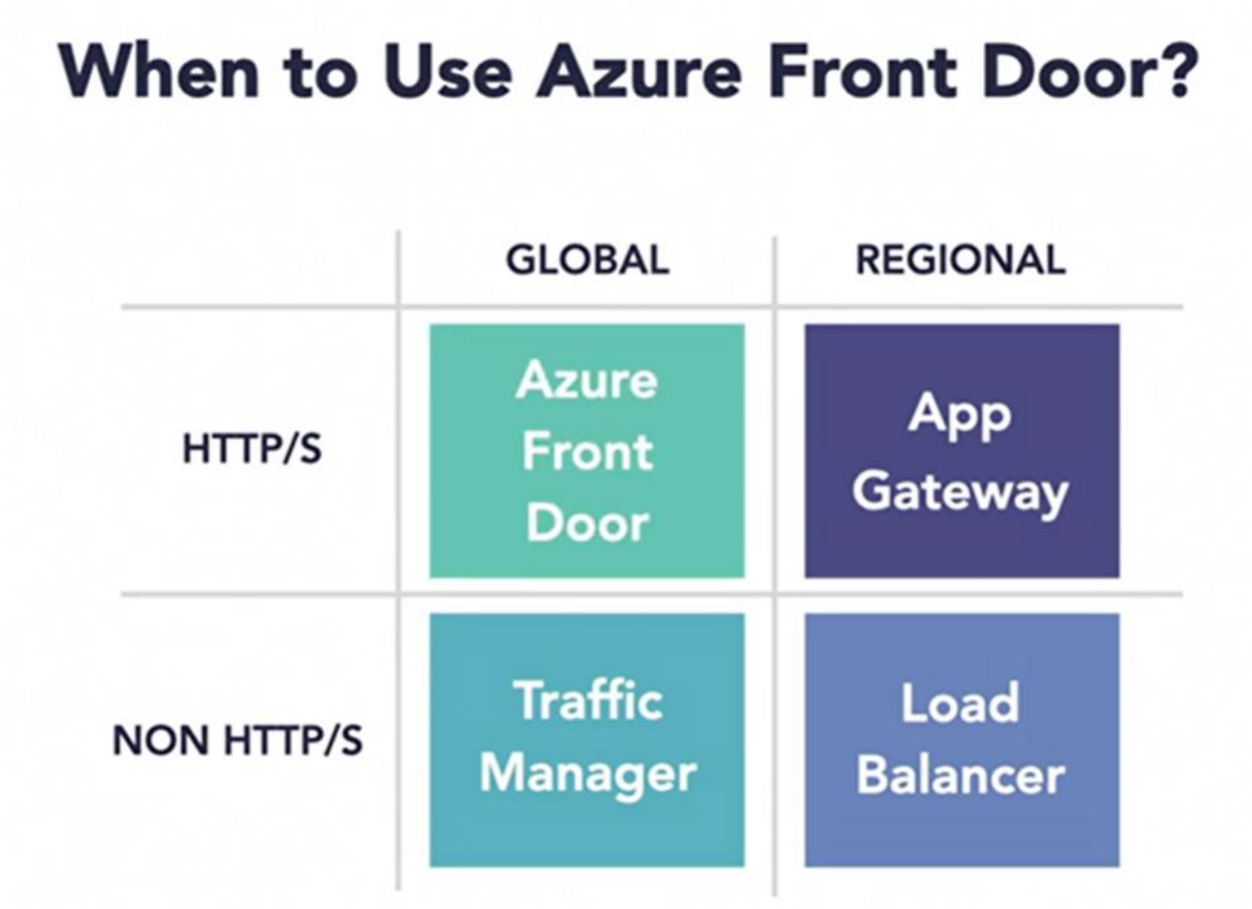
Exam Tip

Get hands-on experience with Azure Application Gateway before the exam.

1.6 Create and configure Azure Front Door

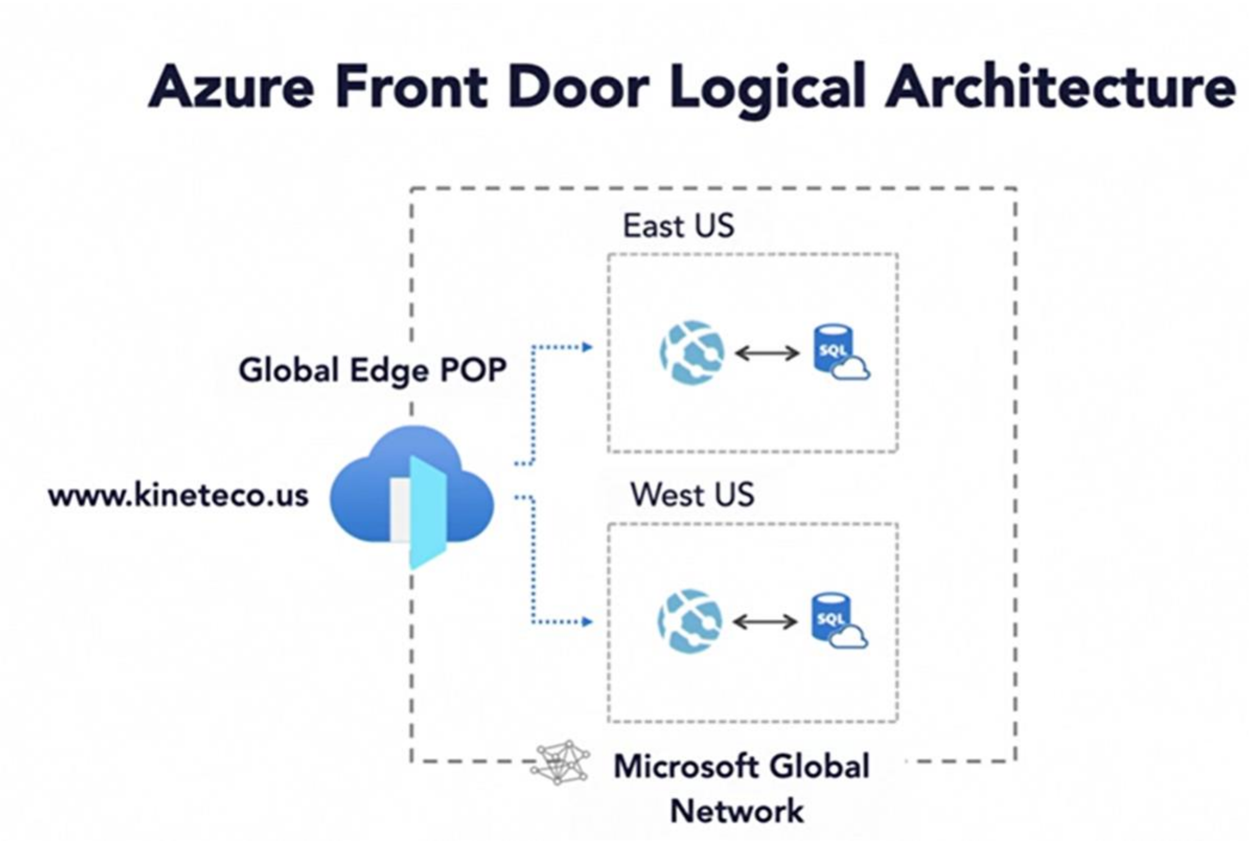
What Is Azure Front Door?

A “web application acceleration platform” for **global routing of web traffic**, optimizing performance, availability, and scalability.

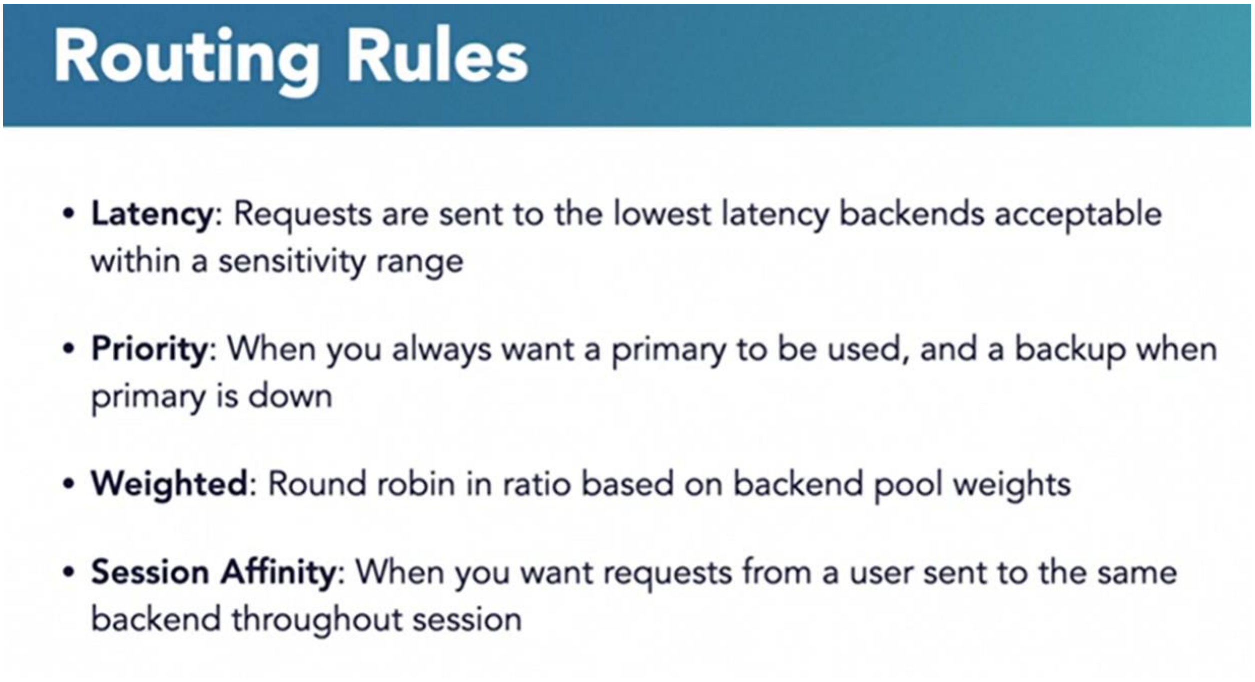


When to Use Azure Front Door?

	GLOBAL	REGIONAL
HTTP/S	Azure Front Door	App Gateway
NON HTTP/S	Traffic Manager	Load Balancer

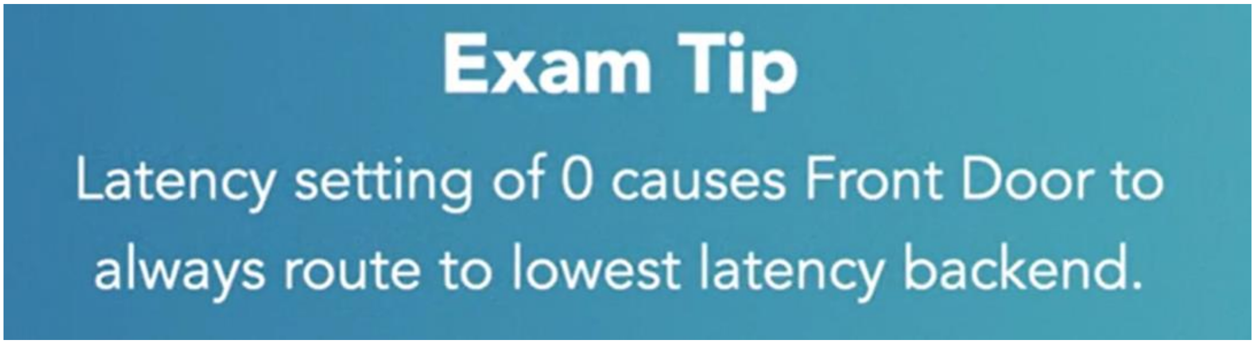


Azure Front Door Logical Architecture



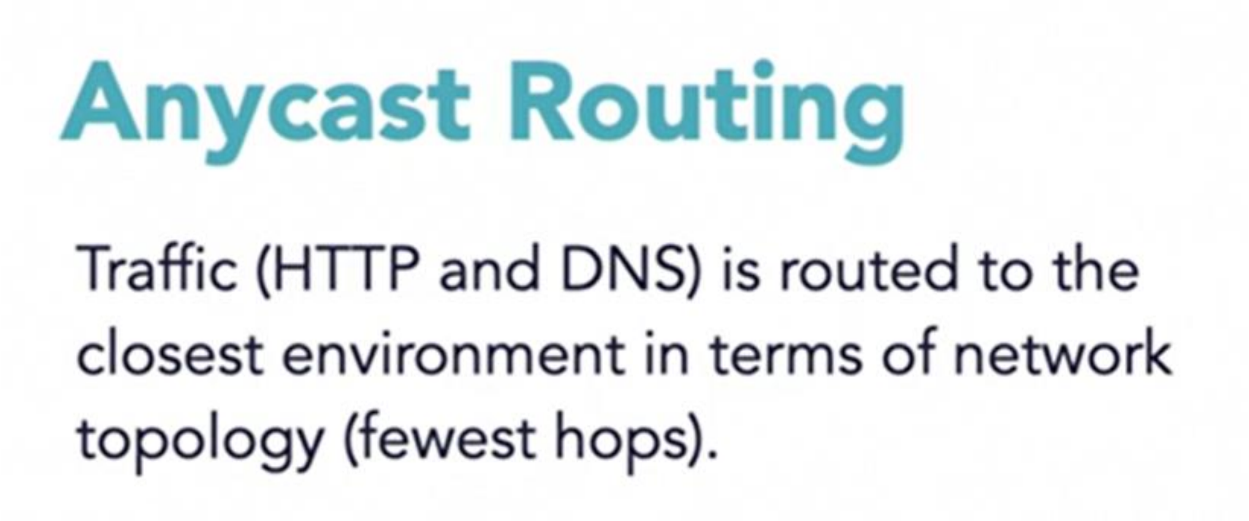
Routing Rules

- **Latency**: Requests are sent to the lowest latency backends acceptable within a sensitivity range
- **Priority**: When you always want a primary to be used, and a backup when primary is down
- **Weighted**: Round robin in ratio based on backend pool weights
- **Session Affinity**: When you want requests from a user sent to the same backend throughout session



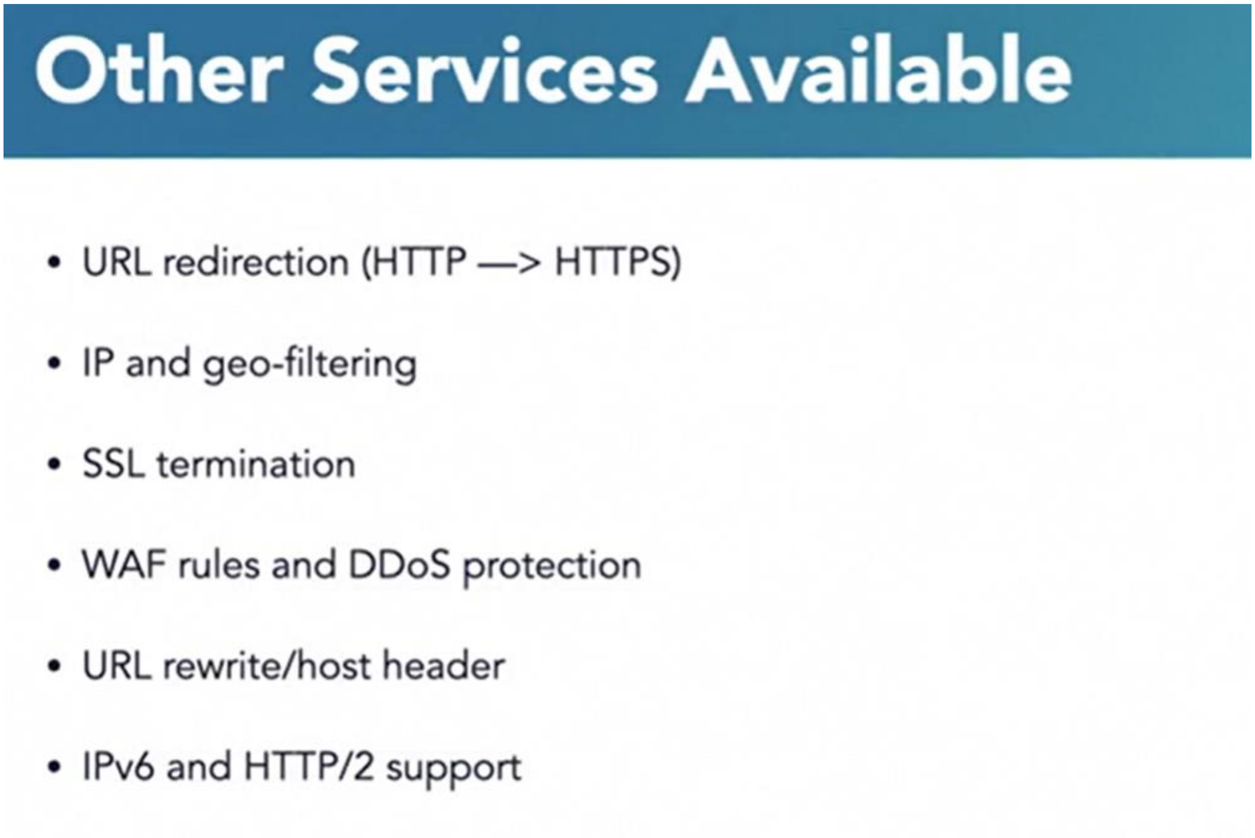
Exam Tip

Latency setting of 0 causes Front Door to always route to lowest latency backend.



Anycast Routing

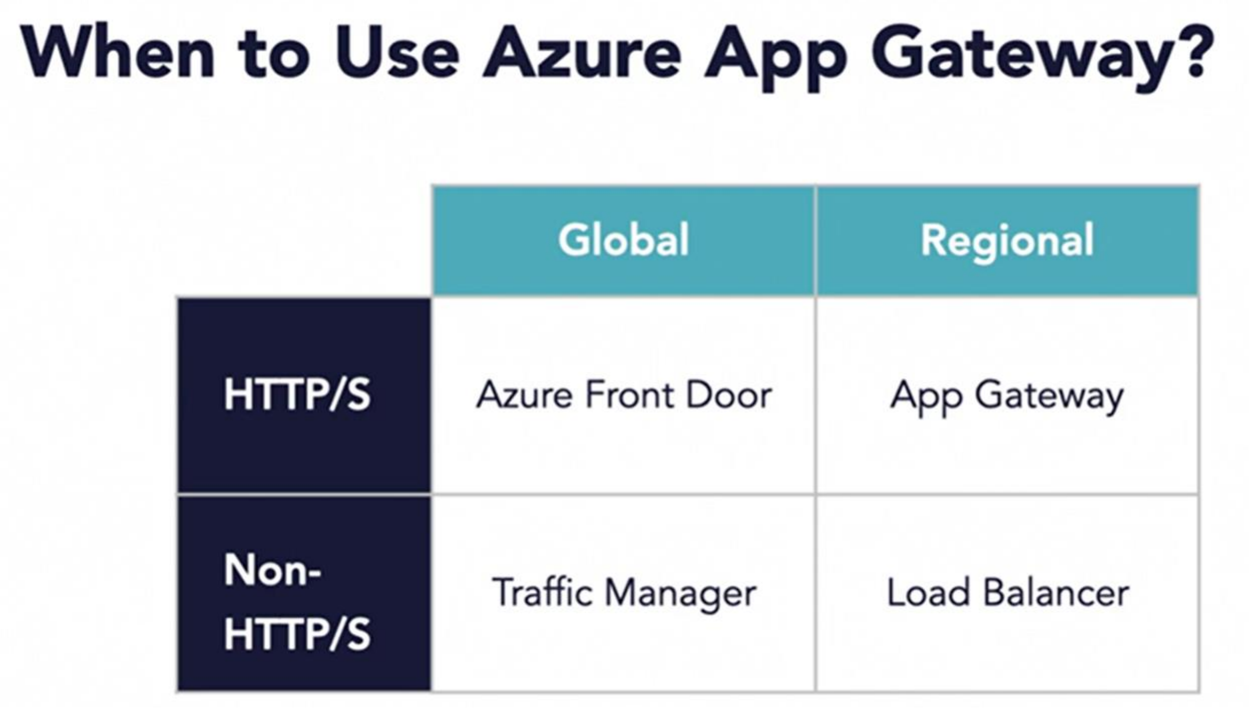
Traffic (HTTP and DNS) is routed to the closest environment in terms of network topology (fewest hops).



Other Services Available

- URL redirection (HTTP —> HTTPS)
- IP and geo-filtering
- SSL termination
- WAF rules and DDoS protection
- URL rewrite/host header
- IPv6 and HTTP/2 support

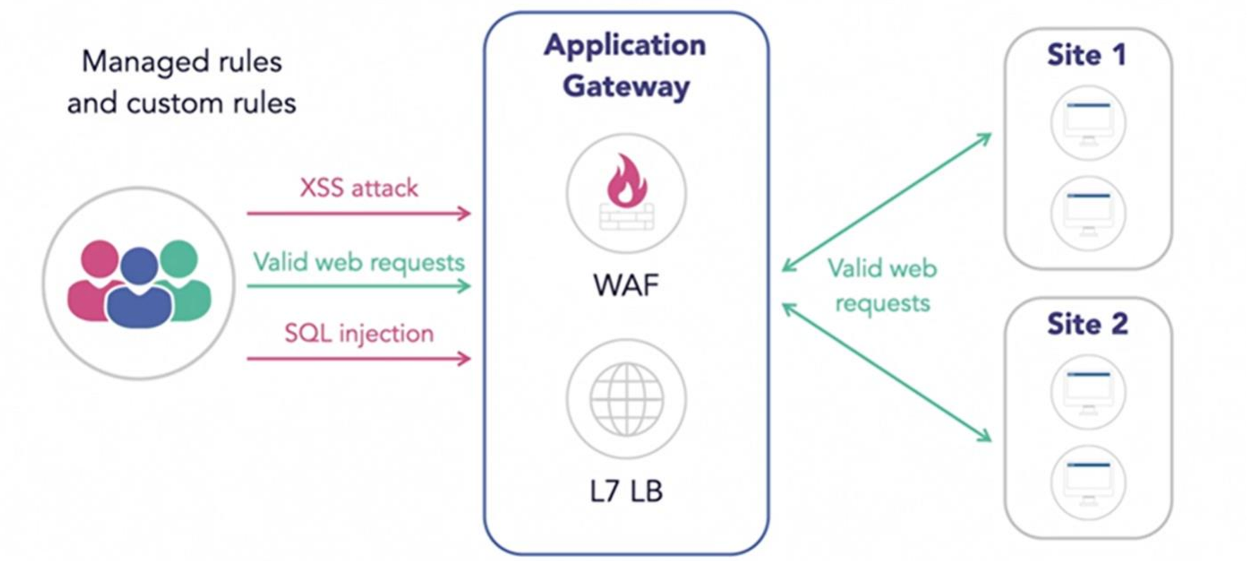
1.7 Create and configure Web Application Firewall



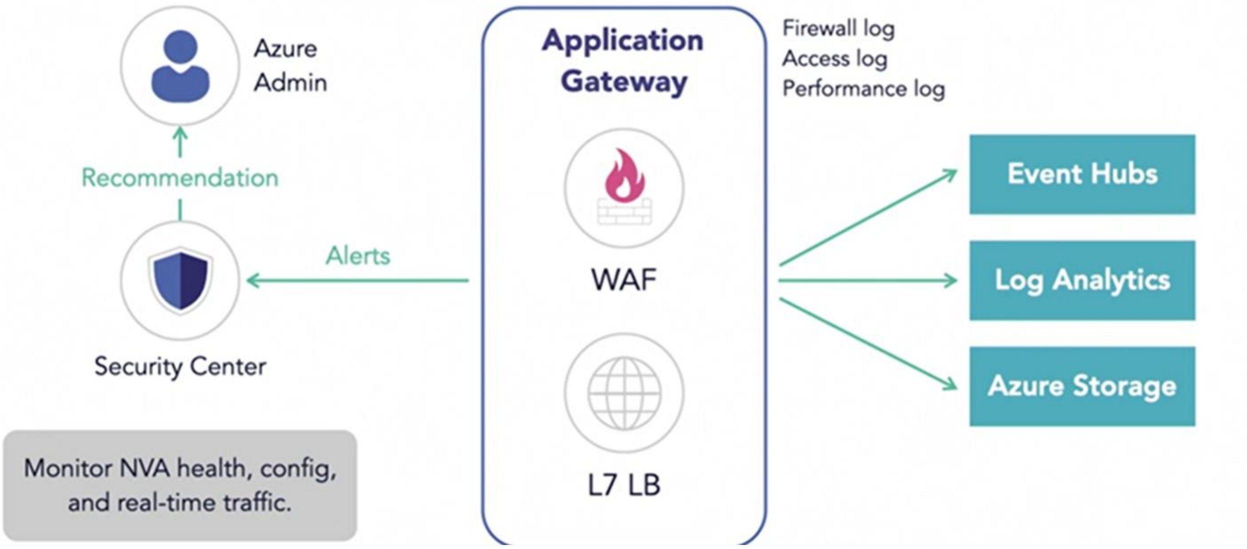
When to Use Azure App Gateway?

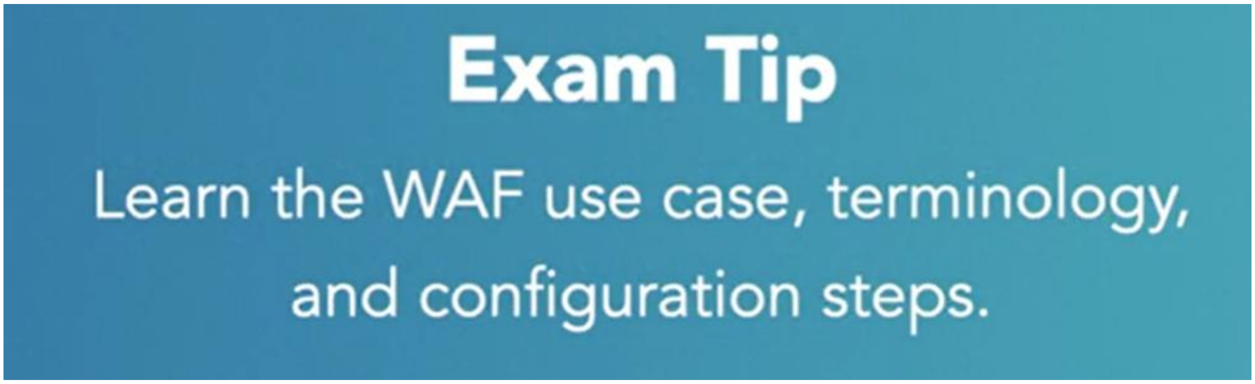
	Global	Regional
HTTP/S	Azure Front Door	App Gateway
Non-HTTP/S	Traffic Manager	Load Balancer

Web App Firewall on Azure App Gateway



Monitoring Web App Firewall on Azure App Gateway

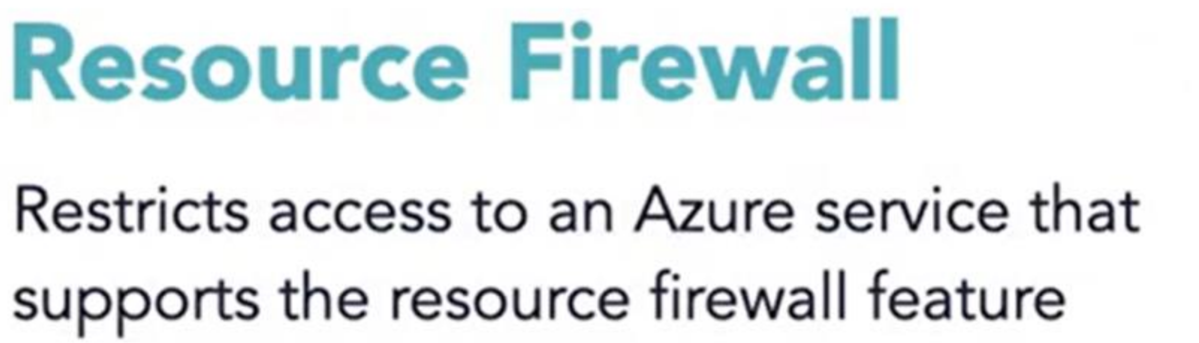




Exam Tip

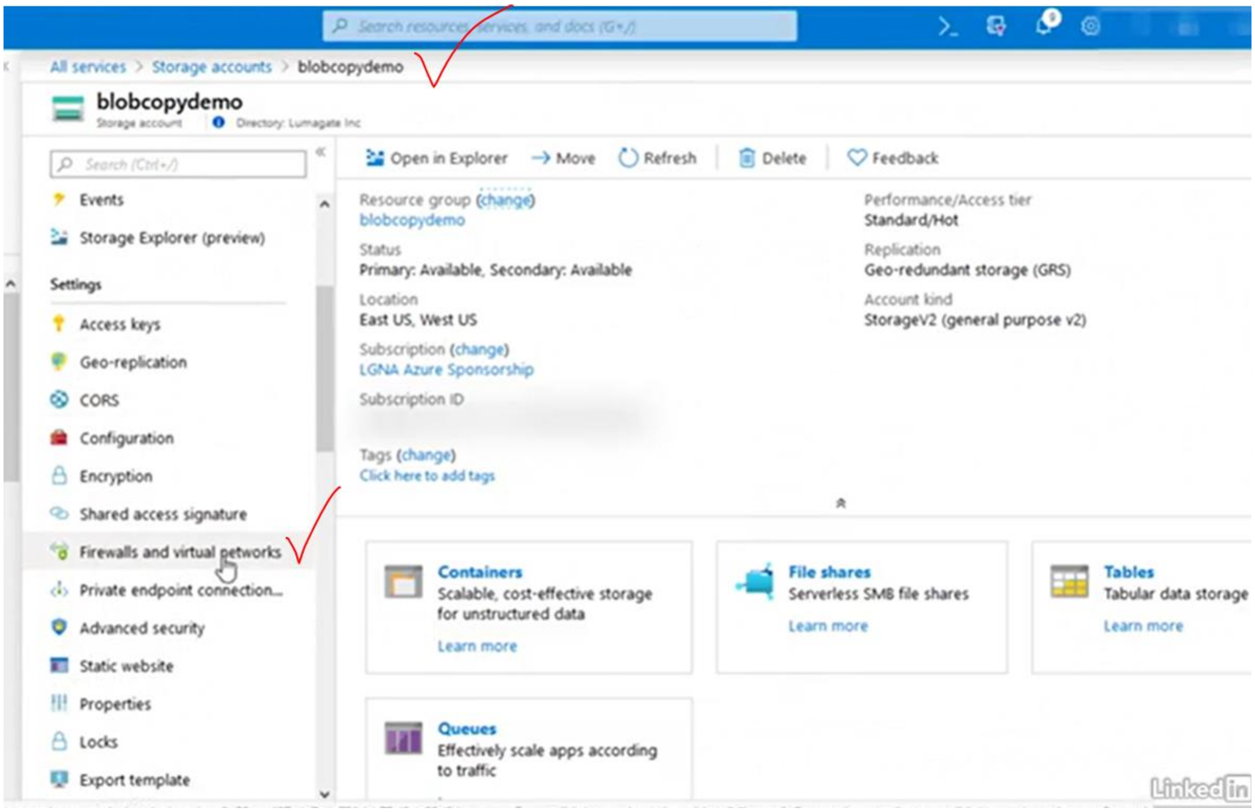
Learn the WAF use case, terminology, and configuration steps.

1.8 Configure firewall for Storage, SQL, Key Vault, App Service



Resource Firewall

Restricts access to an Azure service that supports the resource firewall feature



Resource group (change)
blobcopydemo

Status
Primary: Available, Secondary: Available

Location
East US, West US

Subscription (change)
LGNA Azure Sponsorship

Subscription ID
[redacted]

Tags (change)
Click here to add tags

Performance/Access tier
Standard/Hot

Replication
Geo-redundant storage (GRS)

Account kind
StorageV2 (general purpose v2)

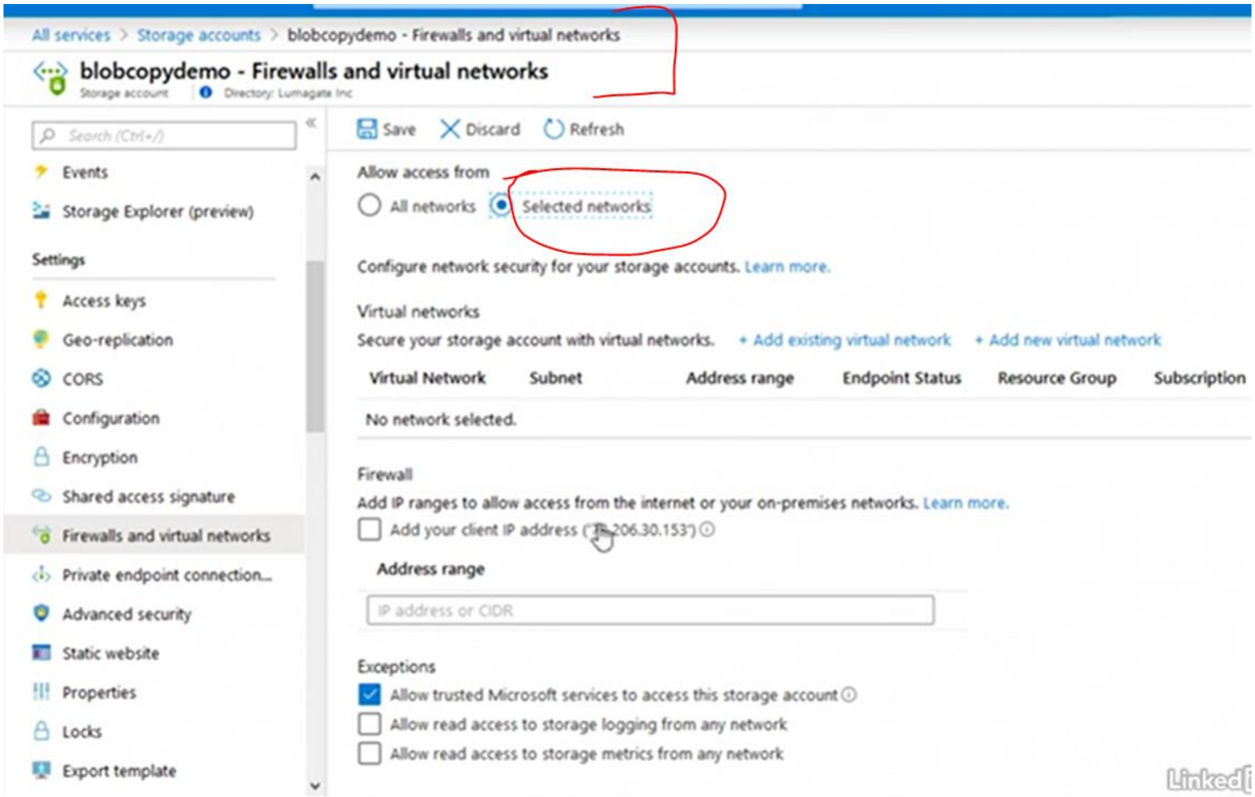
Containers
Scalable, cost-effective storage for unstructured data
Learn more

File shares
Serverless SMB file shares
Learn more

Tables
Tabular data storage
Learn more

Queues
Effectively scale apps according to traffic

This is a way to create a service endpoint.


All services > Storage accounts > blobcopydemo - Firewalls and virtual networks
Search (Ctrl+/)
Events
Storage Explorer (preview)
Settings
Access keys
Geo-replication
CORS
Configuration
Encryption
Shared access signature
Firewalls and virtual networks
Private endpoint connection...
Advanced security
Static website
Properties
Locks
Export template
Save
Discard
Refresh
+ Add existing virtual network
+ Add new virtual network
Linked

blobcopydemo - Firewalls and virtual networks
Storage account | Directory: Lumagate Inc

Allow access from

○ All networks ● Selected networks

Configure network security for your storage accounts. Learn more.

Virtual networks

Secure your storage account with virtual networks.

Virtual Network	Subnet	Address range	Endpoint Status	Resource Group	Subscription
No network selected.					

Firewall

Add IP ranges to allow access from the internet or your on-premises networks. Learn more.

□ Add your client IP address ('1.206.30.153')

Address range

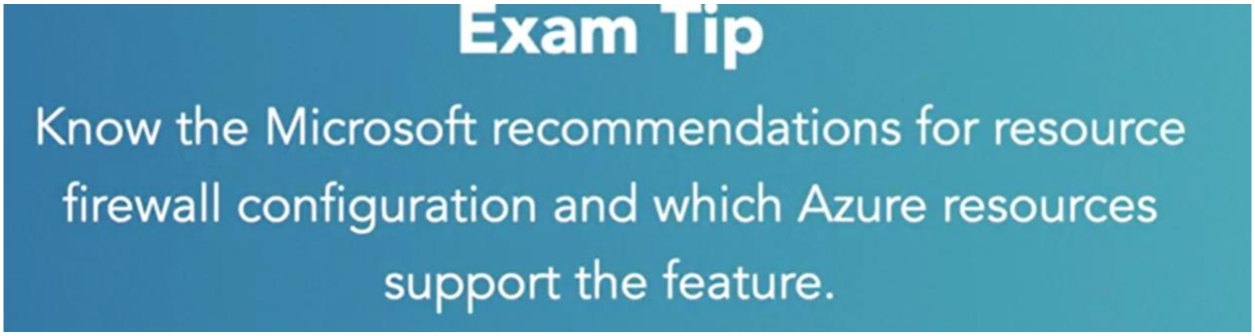
IP address or CIDR

Exceptions

☑ Allow trusted Microsoft services to access this storage account

□ Allow read access to storage logging from any network

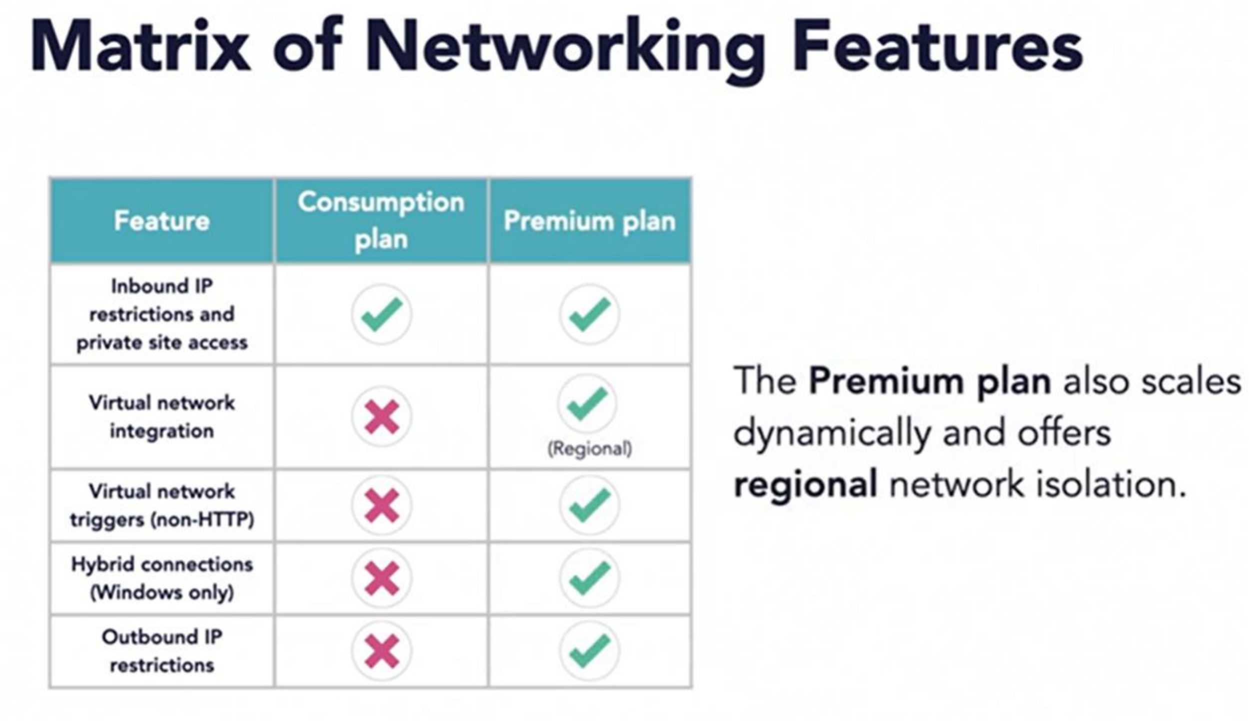
□ Allow read access to storage metrics from any network



Exam Tip

Know the Microsoft recommendations for resource firewall configuration and which Azure resources support the feature.

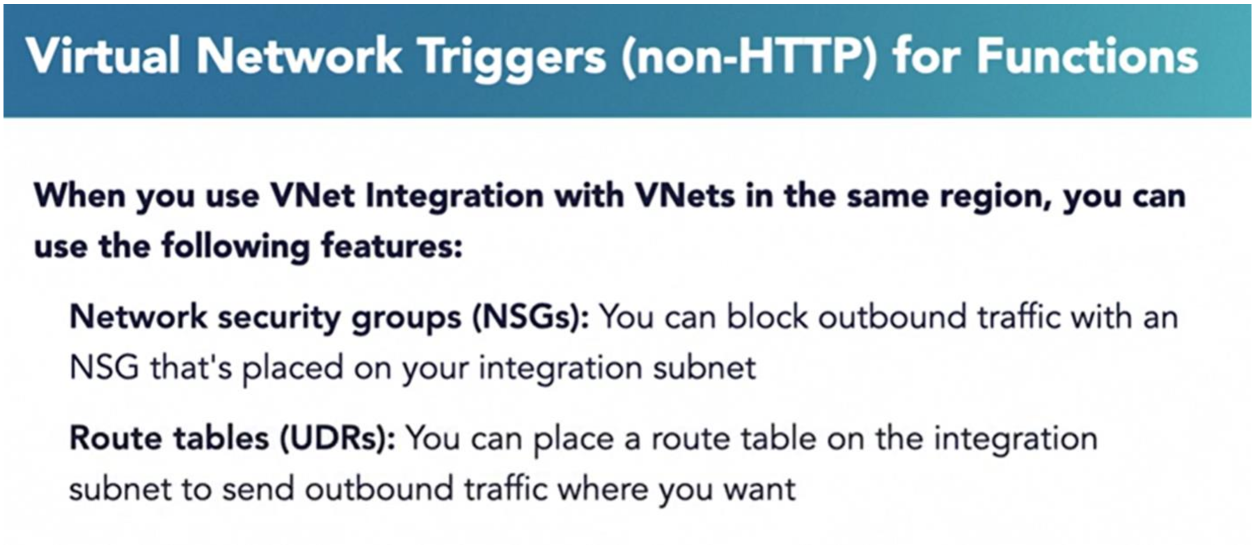
1.9 Configure network isolation for web Apps and Azure Functions



Matrix of Networking Features

Feature	Consumption plan	Premium plan
Inbound IP restrictions and private site access	✓	✓
Virtual network integration	✗	✓ (Regional)
Virtual network triggers (non-HTTP)	✗	✓
Hybrid connections (Windows only)	✗	✓
Outbound IP restrictions	✗	✓

The **Premium plan** also scales dynamically and offers **regional** network isolation.

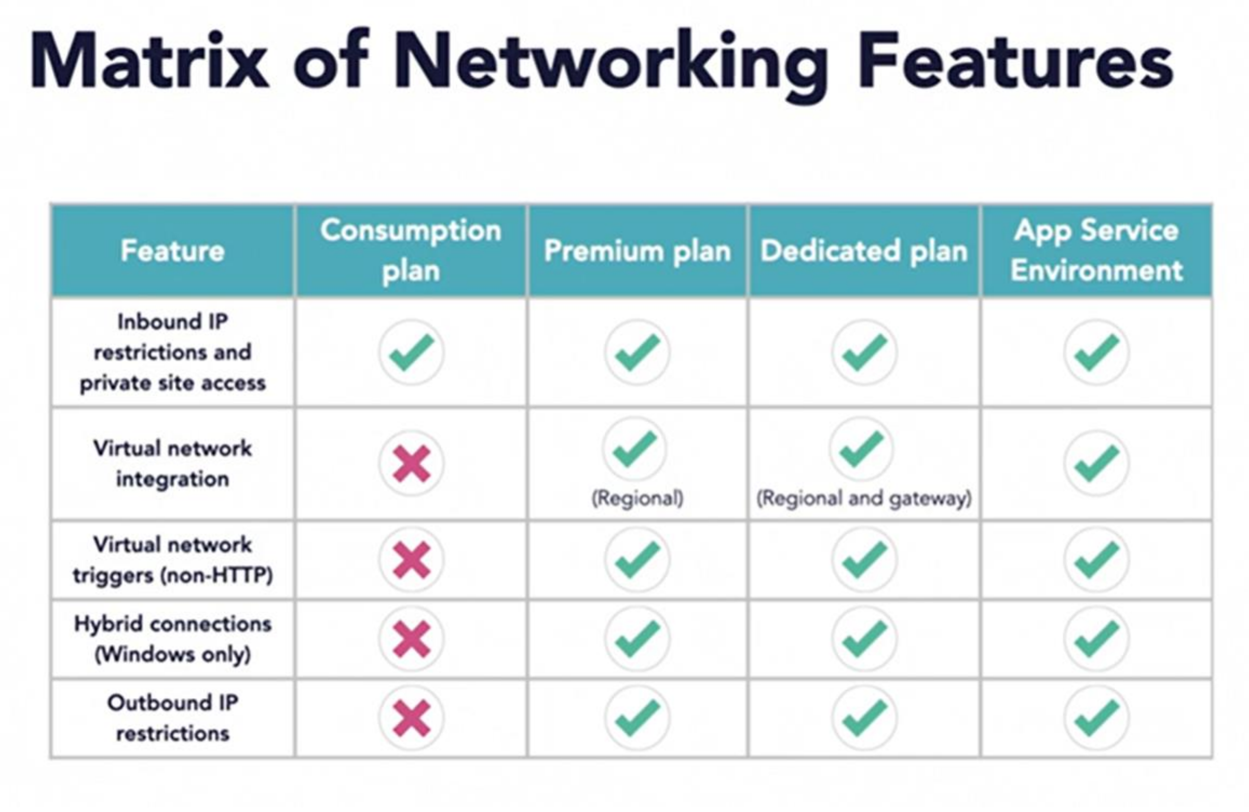


Virtual Network Triggers (non-HTTP) for Functions

When you use VNet Integration with VNets in the same region, you can use the following features:

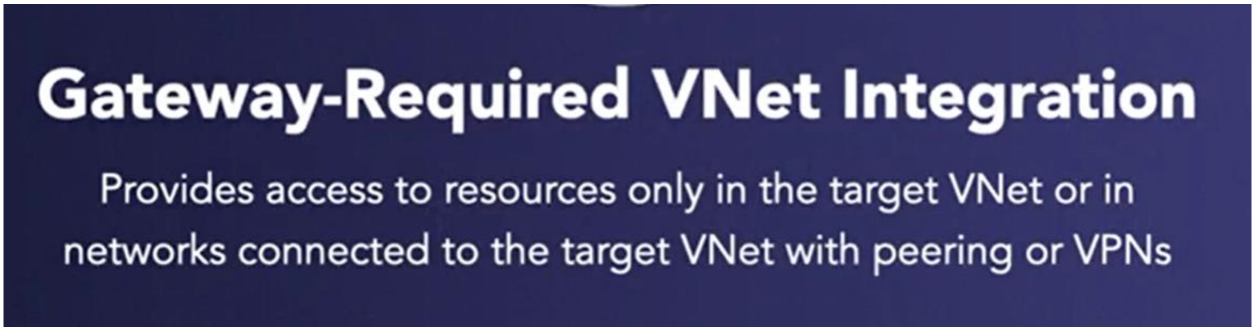
Network security groups (NSGs): You can block outbound traffic with an NSG that's placed on your integration subnet

Route tables (UDRs): You can place a route table on the integration subnet to send outbound traffic where you want



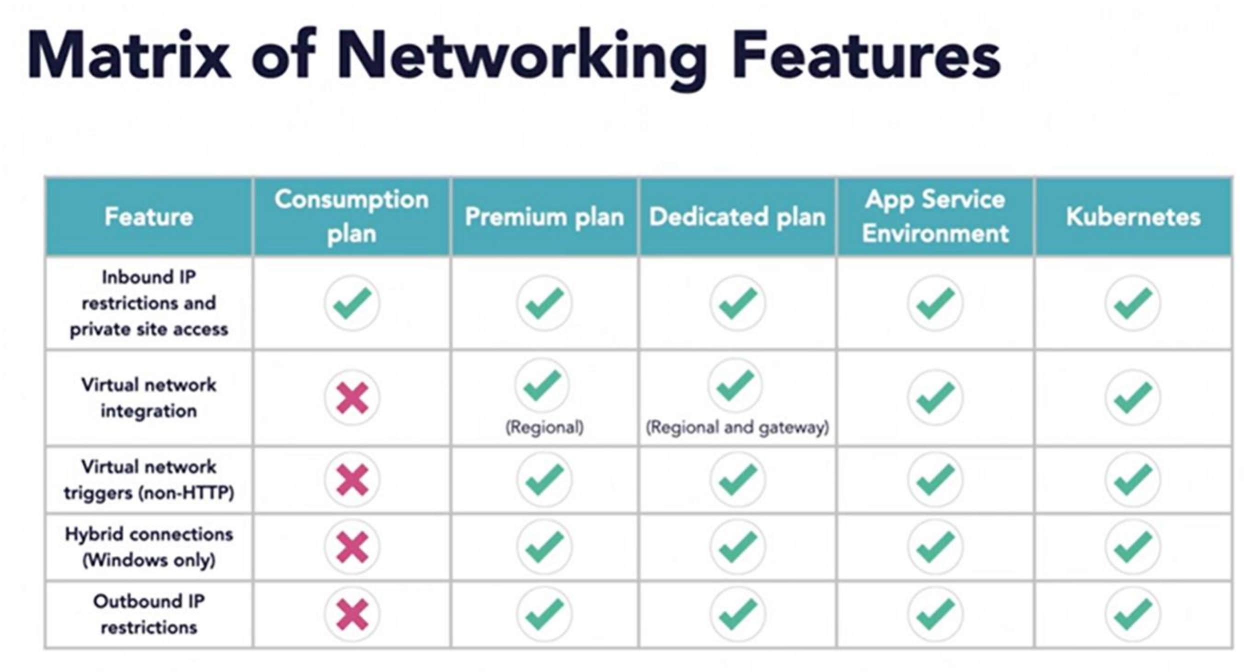
Matrix of Networking Features

Feature	Consumption plan	Premium plan	Dedicated plan	App Service Environment
Inbound IP restrictions and private site access	✓	✓	✓	✓
Virtual network integration	✗	✓ (Regional)	✓ (Regional and gateway)	✓
Virtual network triggers (non-HTTP)	✗	✓	✓	✓
Hybrid connections (Windows only)	✗	✓	✓	✓
Outbound IP restrictions	✗	✓	✓	✓



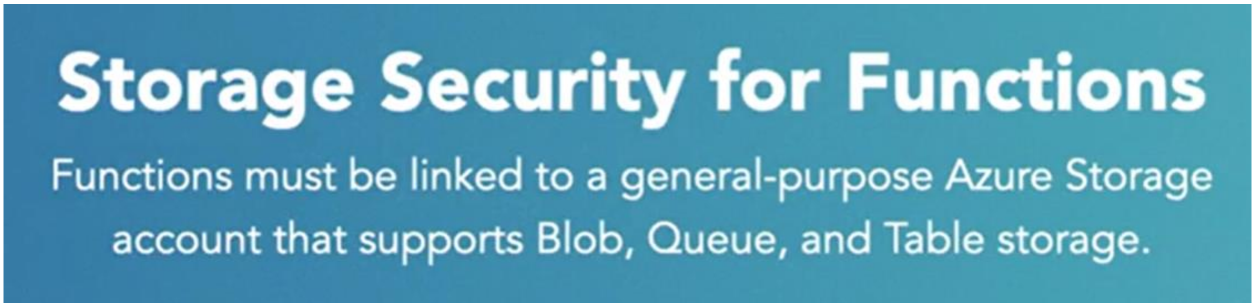
Gateway-Required VNet Integration

Provides access to resources only in the target VNet or in networks connected to the target VNet with peering or VPNs



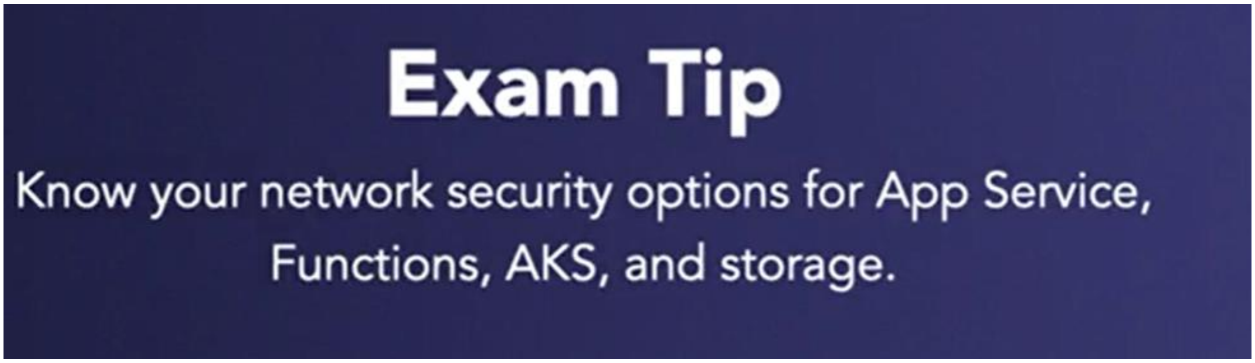
Matrix of Networking Features

Feature	Consumption plan	Premium plan	Dedicated plan	App Service Environment	Kubernetes
Inbound IP restrictions and private site access	✓	✓	✓	✓	✓
Virtual network integration	✗	✓ (Regional)	✓ (Regional and gateway)	✓	✓
Virtual network triggers (non-HTTP)	✗	✓	✓	✓	✓
Hybrid connections (Windows only)	✗	✓	✓	✓	✓
Outbound IP restrictions	✗	✓	✓	✓	✓



Storage Security for Functions

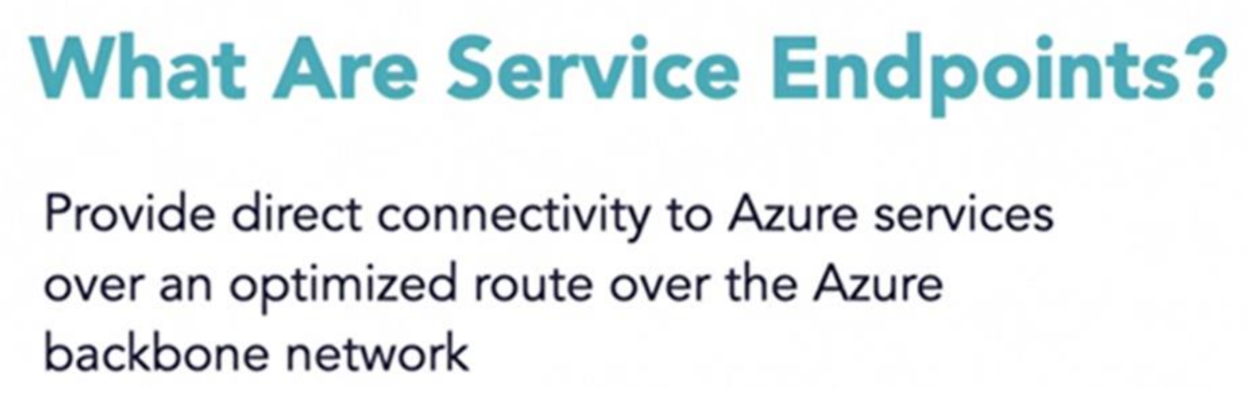
Functions must be linked to a general-purpose Azure Storage account that supports Blob, Queue, and Table storage.



Exam Tip

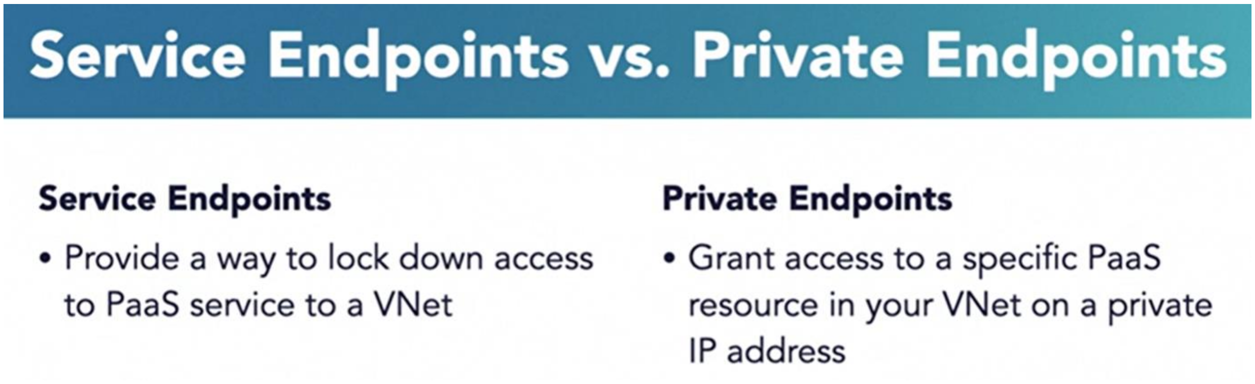
Know your network security options for App Service, Functions, AKS, and storage.

1.10 Implement service endpoints



What Are Service Endpoints?

Provide direct connectivity to Azure services over an optimized route over the Azure backbone network



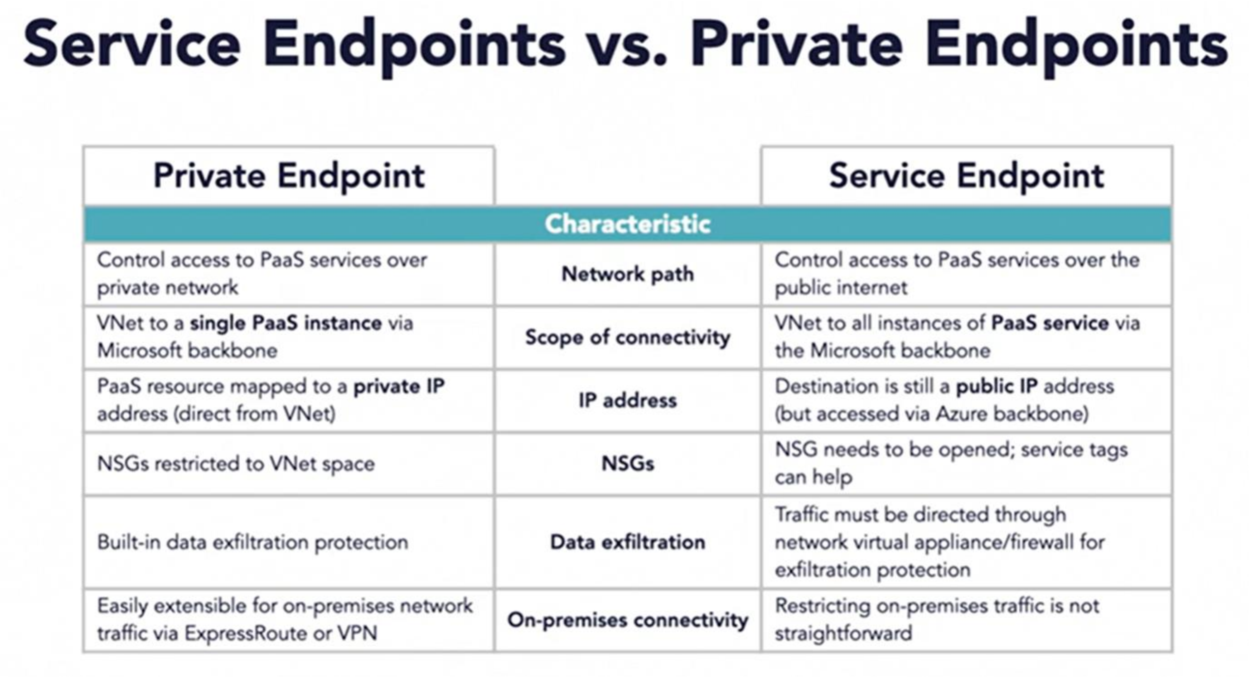
Service Endpoints vs. Private Endpoints

Service Endpoints

- Provide a way to lock down access to PaaS service to a VNet

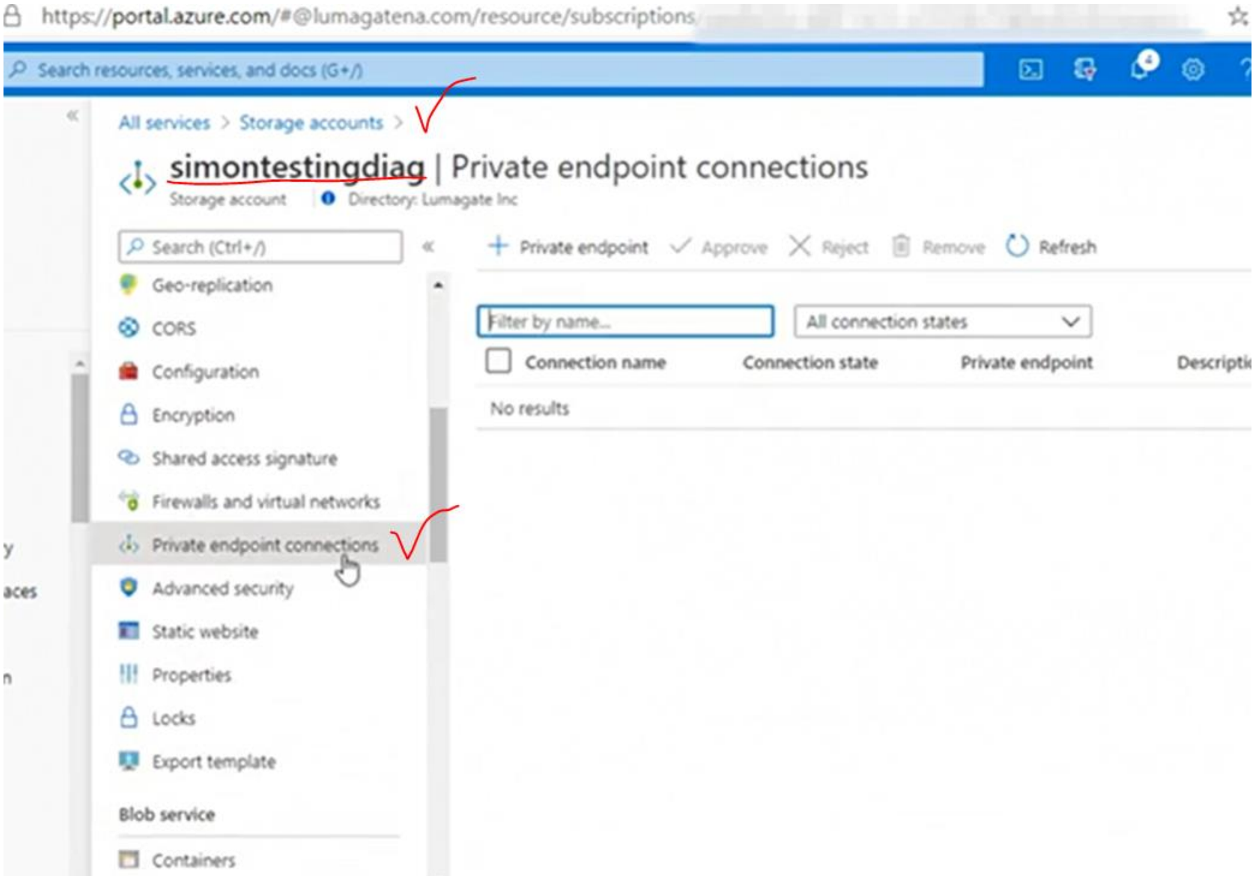
Private Endpoints

- Grant access to a specific PaaS resource in your VNet on a private IP address

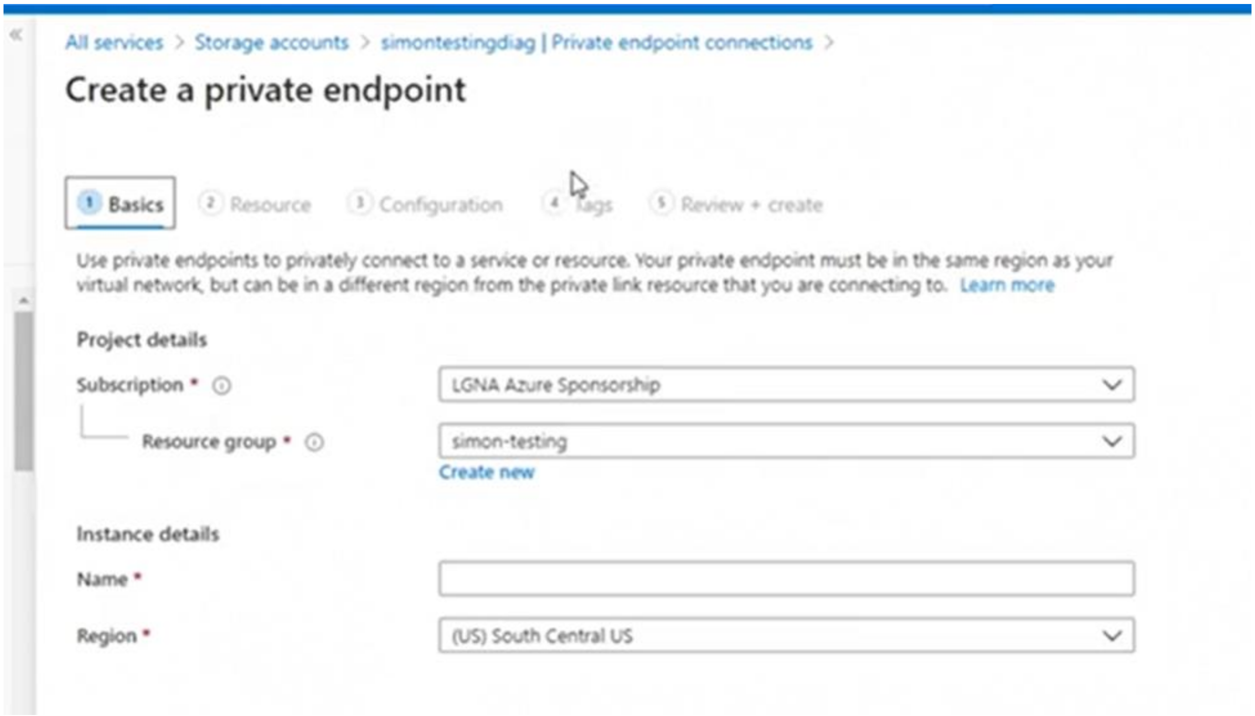


Service Endpoints vs. Private Endpoints

Private Endpoint		Service Endpoint
	Characteristic	
Control access to PaaS services over private network	**Network path**	Control access to PaaS services over the public internet
VNet to a **single PaaS instance** via Microsoft backbone	**Scope of connectivity**	VNet to all instances of **PaaS service** via the Microsoft backbone
PaaS resource mapped to a **private IP** address (direct from VNet)	**IP address**	Destination is still a **public IP** address (but accessed via Azure backbone)
NSGs restricted to VNet space	**NSGs**	NSG needs to be opened; service tags can help
Built-in data exfiltration protection	**Data exfiltration**	Traffic must be directed through network virtual appliance/firewall for exfiltration protection
Easily extensible for on-premises network traffic via ExpressRoute or VPN	**On-premises connectivity**	Restricting on-premises traffic is not straightforward



Creating a private endpoint


All services > Storage accounts > simontestingdiag | Private endpoint connections >

Create a private endpoint

1 Basics
2 Resource
3 Configuration
4 Tags
5 Review + create

Use private endpoints to privately connect to a service or resource. Your private endpoint must be in the same region as your virtual network, but can be in a different region from the private link resource that you are connecting to. Learn more

Project details

Subscription * : LGNA Azure Sponsorship

Resource group * : simon-testing

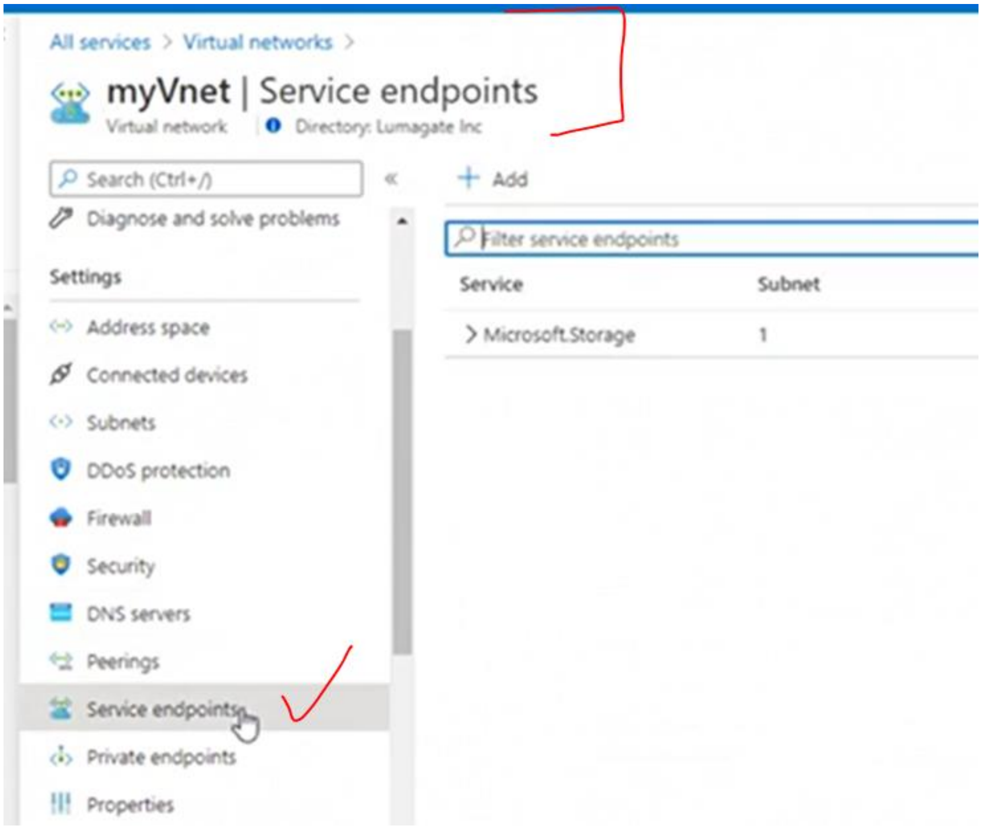
Create new

Instance details

Name * :

Region * : (US) South Central US

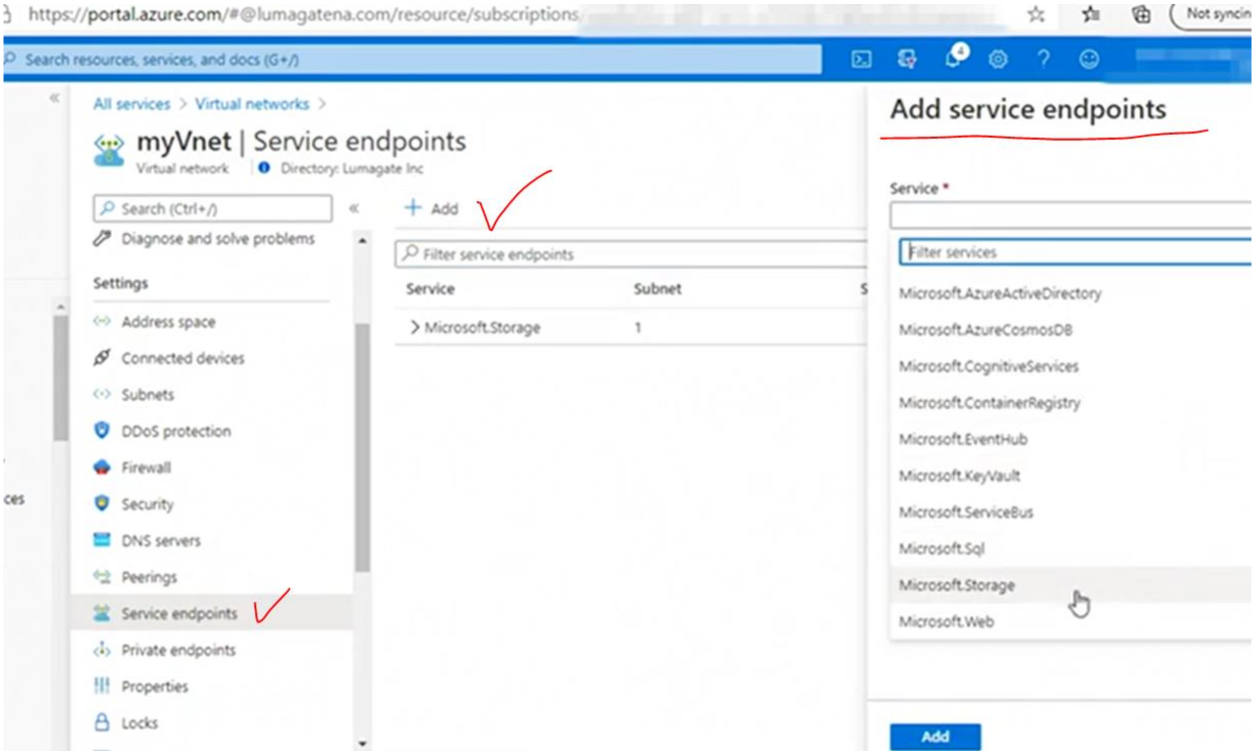
Service Endpoint is available at the VNet level, not Storage account.



myVnet | Service endpoints

Virtual network | Directory: Lumagate Inc

Service	Subnet
> Microsoft.Storage	1


https://portal.azure.com/#@lumagatena.com/resource/subscriptions

Search resources, services, and docs (G+/)
Not syncin
All services > Virtual networks >

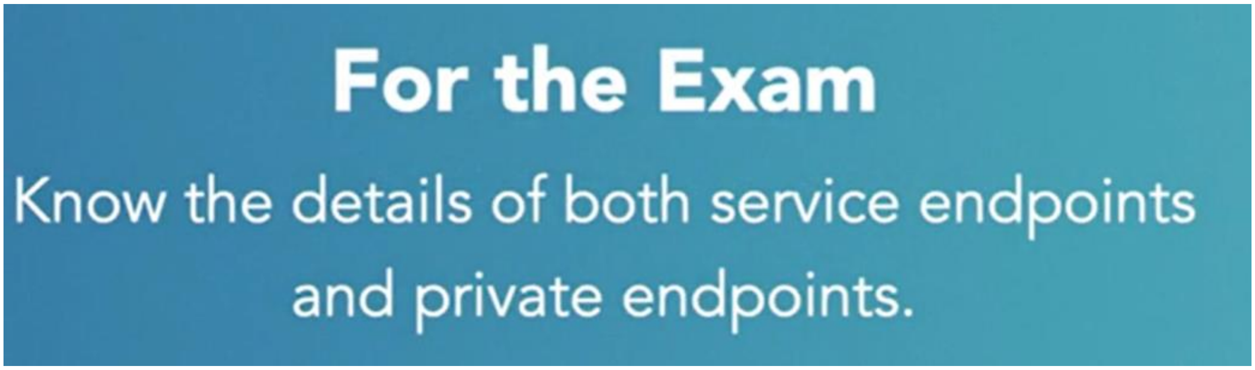
myVnet | Service endpoints

Virtual network | Directory: Lumagate Inc

Service	Subnet
> Microsoft.Storage	1

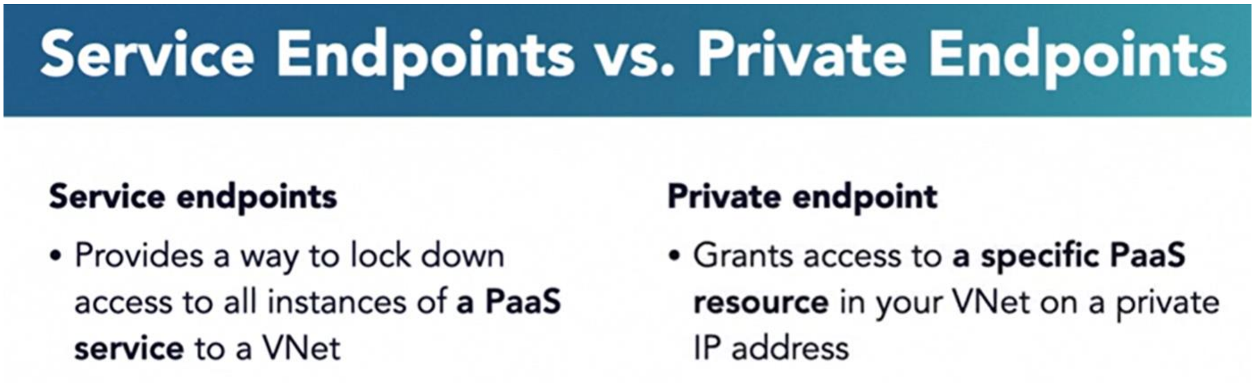
Add service endpoints

Service *


For the Exam

Know the details of both service endpoints and private endpoints.

1.11 Implement Azure Private Links

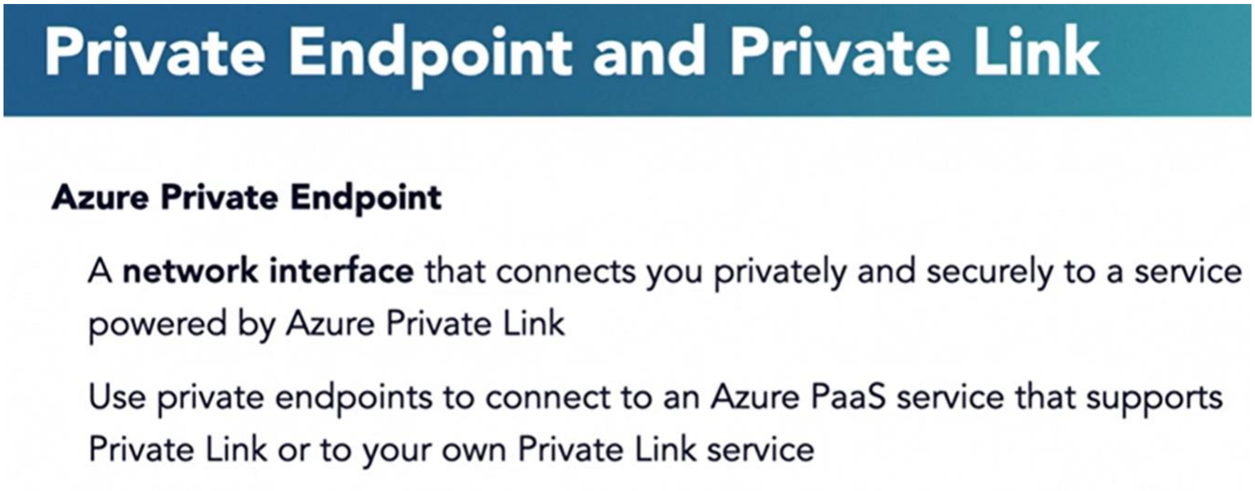

Service Endpoints vs. Private Endpoints

Service endpoints

- Provides a way to lock down access to all instances of **a PaaS service** to a VNet

Private endpoint

- Grants access to **a specific PaaS resource** in your VNet on a private IP address

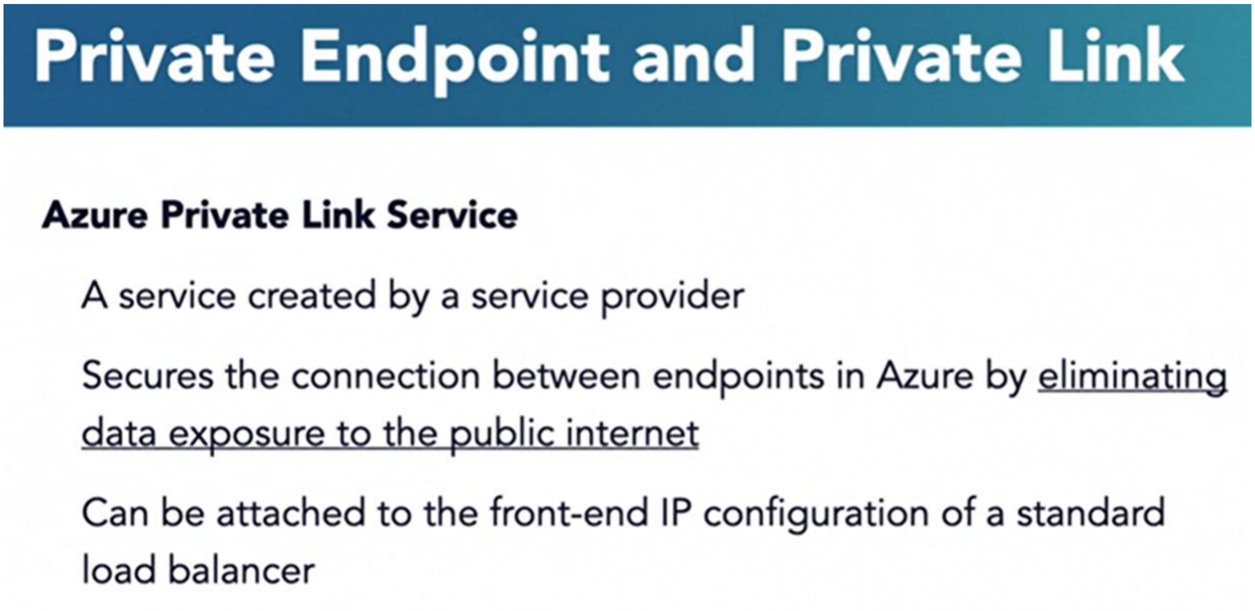


Private Endpoint and Private Link

Azure Private Endpoint

A **network interface** that connects you privately and securely to a service powered by Azure Private Link

Use private endpoints to connect to an Azure PaaS service that supports Private Link or to your own Private Link service



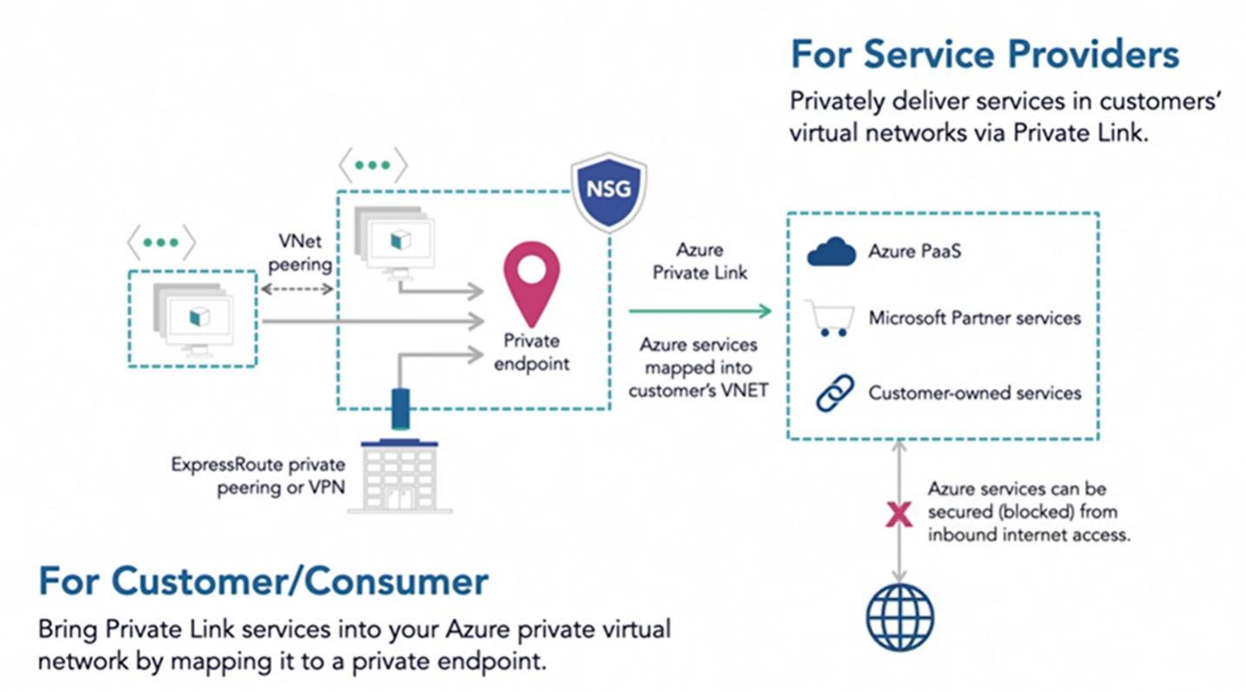
Private Endpoint and Private Link

Azure Private Link Service

A service created by a service provider

Secures the connection between endpoints in Azure by eliminating data exposure to the public internet

Can be attached to the front-end IP configuration of a standard load balancer



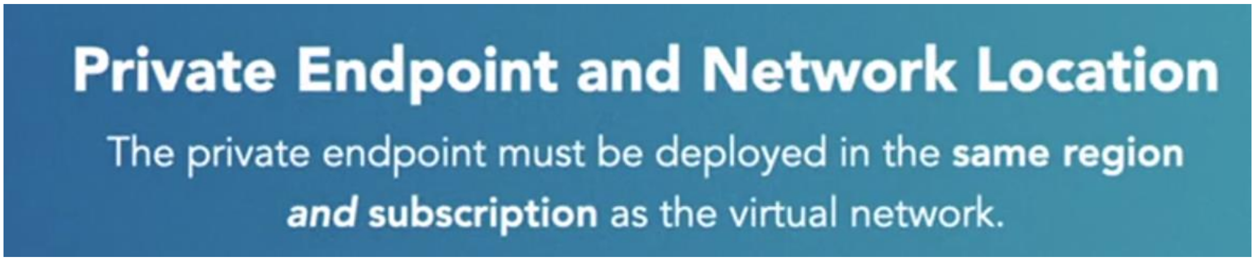
For Service Providers

Privately deliver services in customers' virtual networks via Private Link.

NSG
VNet peering
Private endpoint
Azure Private Link
Azure services mapped into customer's VNET
Azure PaaS
Microsoft Partner services
Customer-owned services
ExpressRoute private peering or VPN
Azure services can be secured (blocked) from inbound internet access.

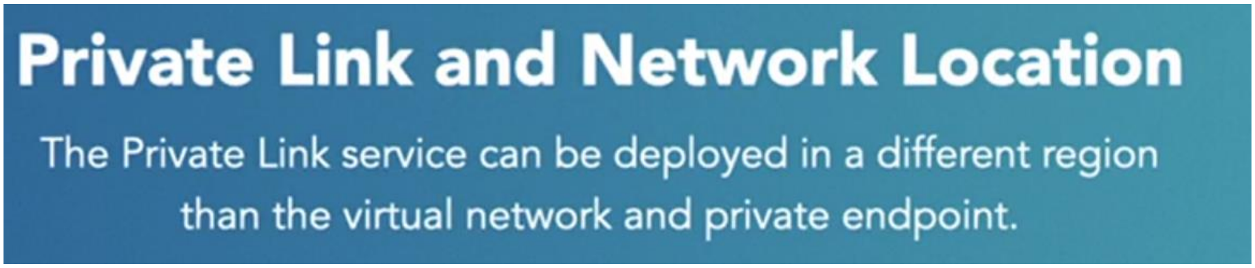
For Customer/Consumer

Bring Private Link services into your Azure private virtual network by mapping it to a private endpoint.



Private Endpoint and Network Location

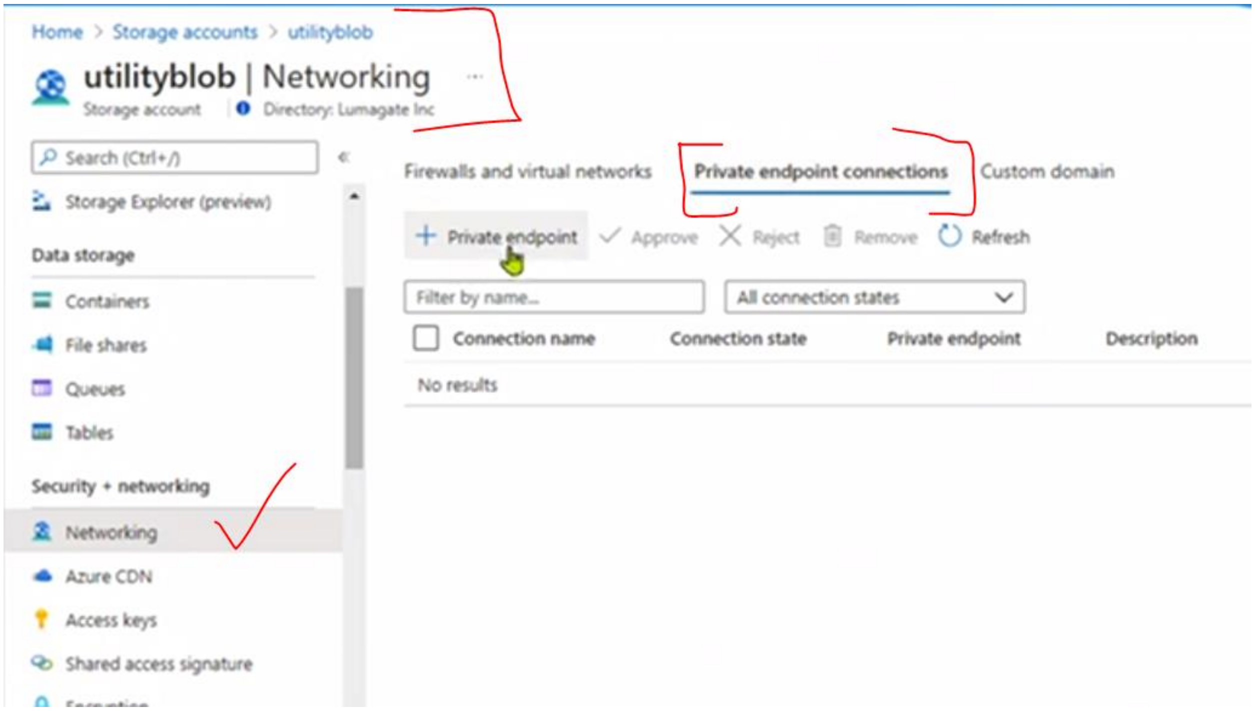
The private endpoint must be deployed in the **same region** ***and* subscription** as the virtual network.



Private Link and Network Location

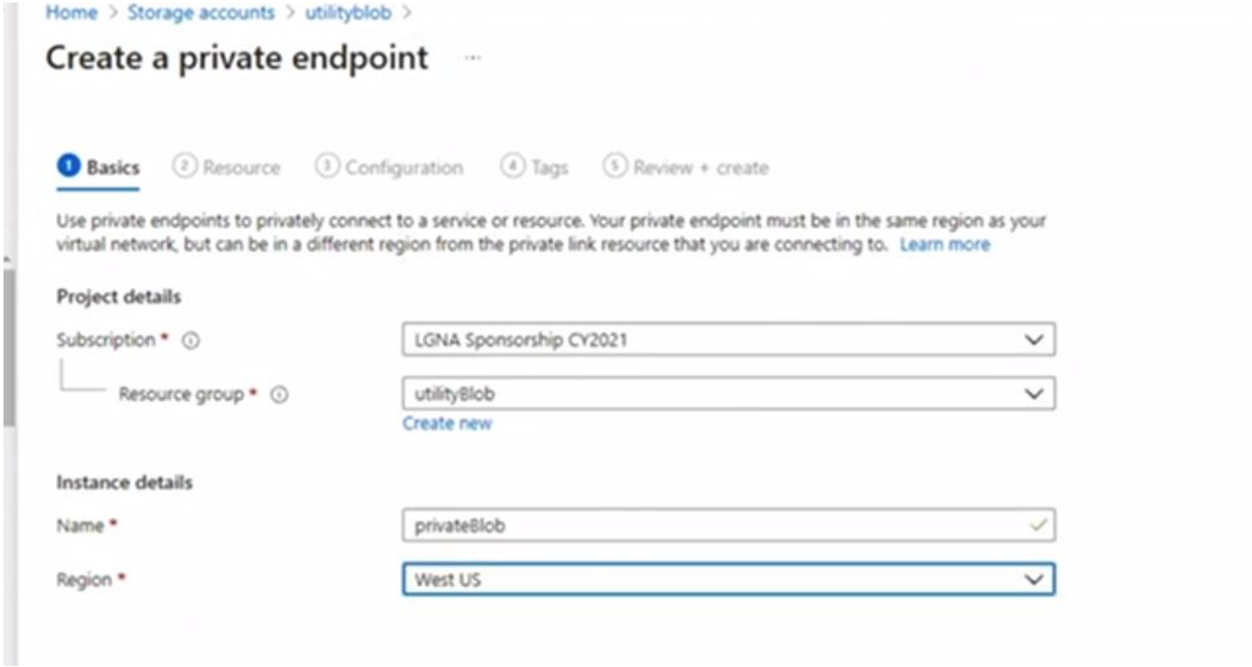
The Private Link service can be deployed in a different region than the virtual network and private endpoint.

Remember that a Private endpoint is a Network Interface.



□ Connection name	Connection state	Private endpoint	Description
No results			

Create a Private Endpoint.



Create a private endpoint ···

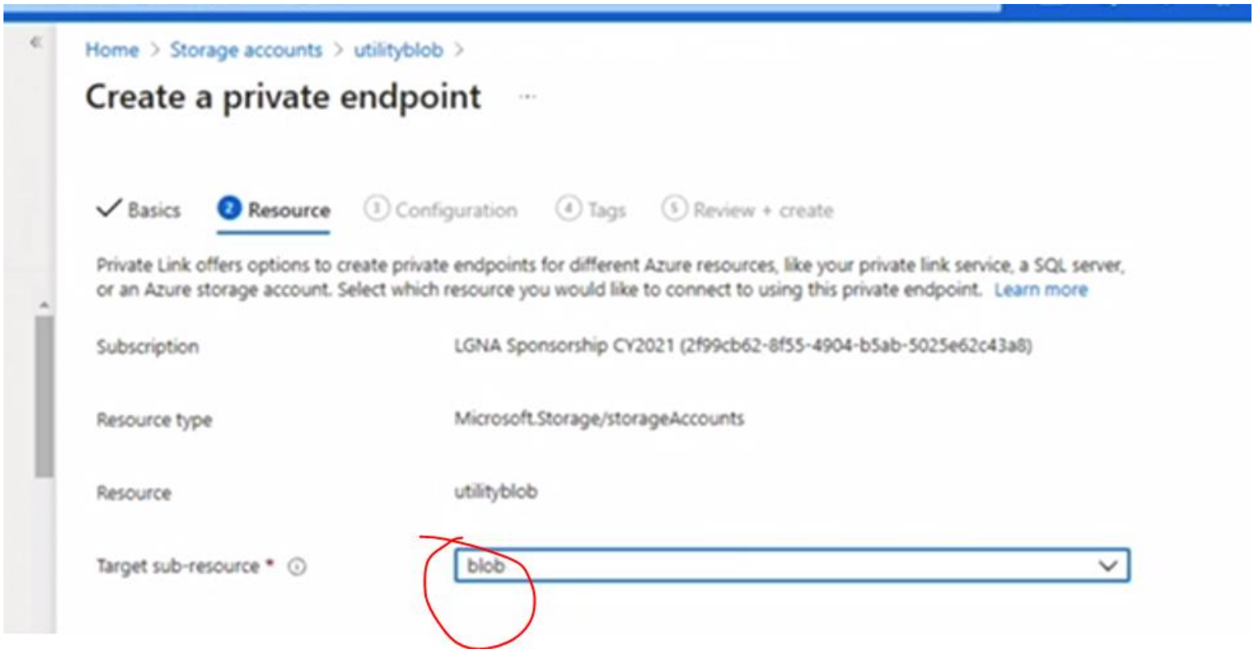
Use private endpoints to privately connect to a service or resource. Your private endpoint must be in the same region as your virtual network, but can be in a different region from the private link resource that you are connecting to. Learn more

Project details

Subscription *	LGNA Sponsorship CY2021
Resource group *	utilityBlob

Instance details

Name *	privateBlob
Region *	West US



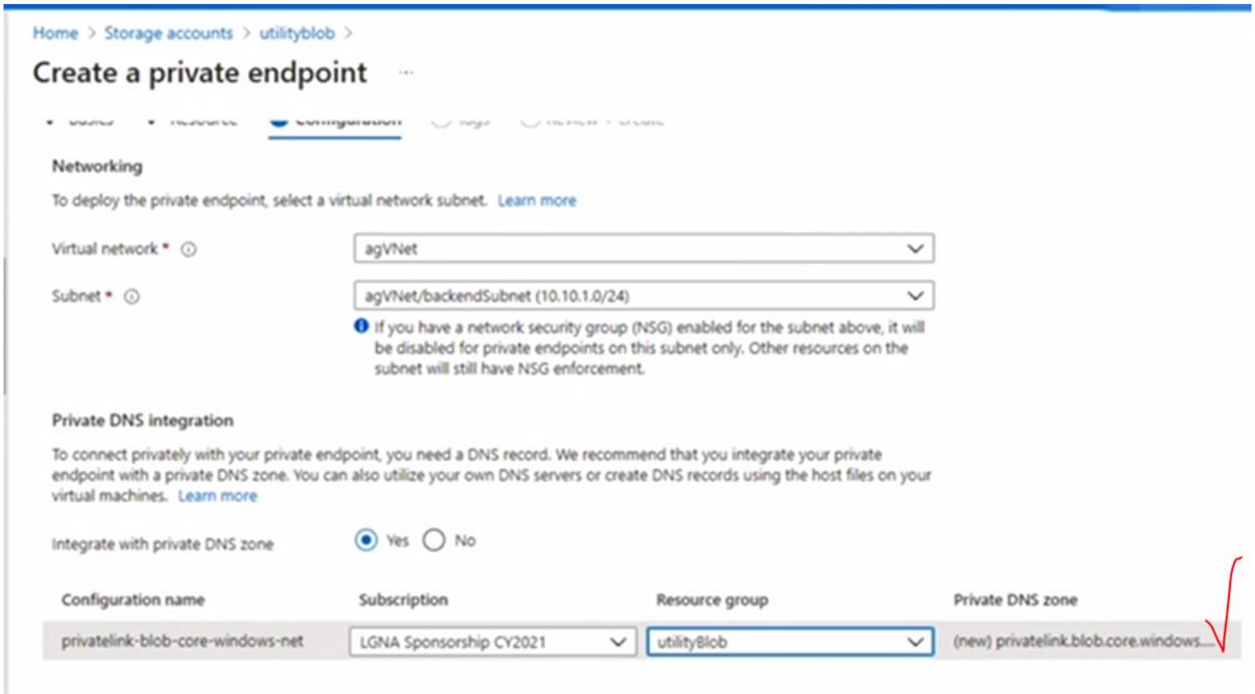
Home > Storage accounts > utilityblob >

Create a private endpoint

✓ Basics ❷ Resource ③ Configuration ④ Tags ⑤ Review + create

Private Link offers options to create private endpoints for different Azure resources, like your private link service, a SQL server, or an Azure storage account. Select which resource you would like to connect to using this private endpoint. Learn more

Subscription	LGNA Sponsorship CY2021 (2f99cb62-8f55-4904-b5ab-5025e62c43a8)
Resource type	Microsoft.Storage/storageAccounts
Resource	utilityblob
Target sub-resource * ⓘ	blob



Home > Storage accounts > utilityblob >

Create a private endpoint

Networking

To deploy the private endpoint, select a virtual network subnet. Learn more

Virtual network * ⓘ	agVNet
Subnet * ⓘ	agVNet/backendSubnet (10.10.1.0/24)

If you have a network security group (NSG) enabled for the subnet above, it will be disabled for private endpoints on this subnet only. Other resources on the subnet will still have NSG enforcement.

Private DNS integration

To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone. You can also utilize your own DNS servers or create DNS records using the host files on your virtual machines. Learn more

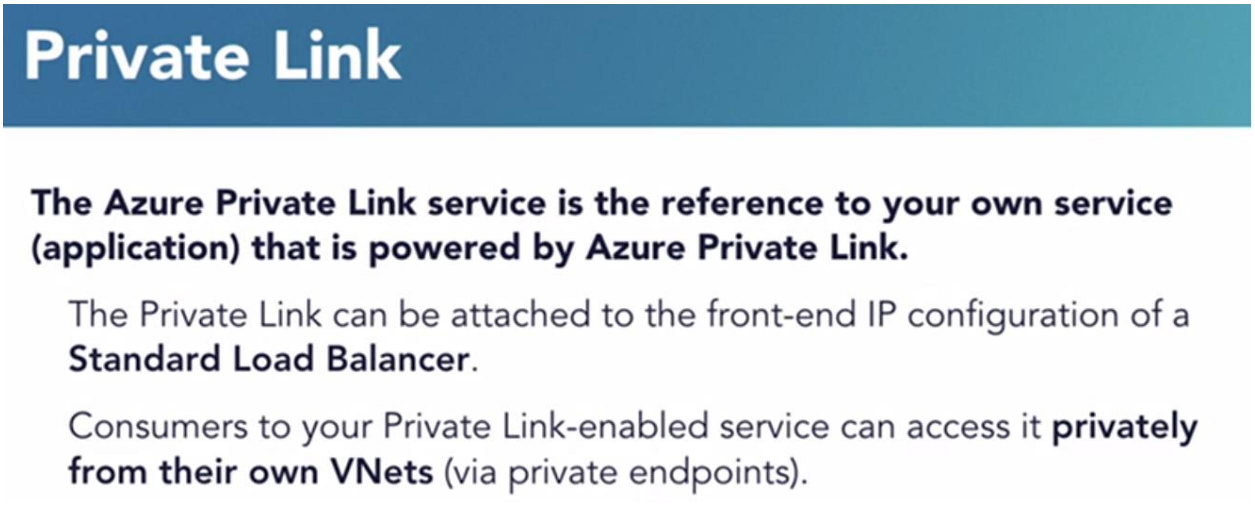
Integrate with private DNS zone ● Yes ○ No

Configuration name	Subscription	Resource group	Private DNS zone
privatelink-blob-core-windows-net	LGNA Sponsorship CY2021	utilityBlob	(new) privatelink.blob.core.windows....

For the Exam

Know the use cases for private endpoints and how to configure them.

1.12 Implement Azure Private Links

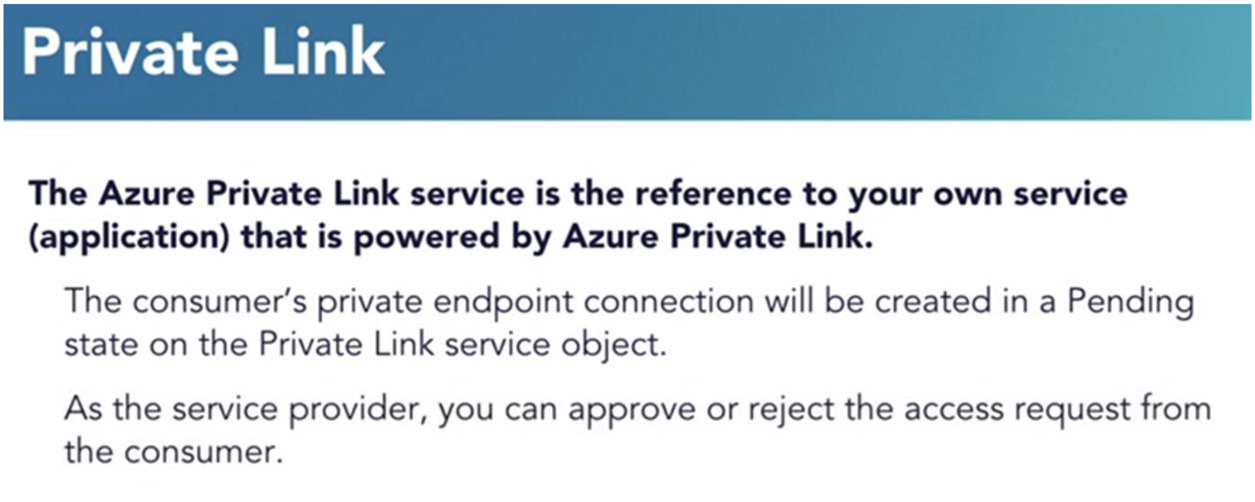


Private Link

The Azure Private Link service is the reference to your own service (application) that is powered by Azure Private Link.

The Private Link can be attached to the front-end IP configuration of a **Standard Load Balancer**.

Consumers to your Private Link-enabled service can access it **privately from their own VNets** (via private endpoints).

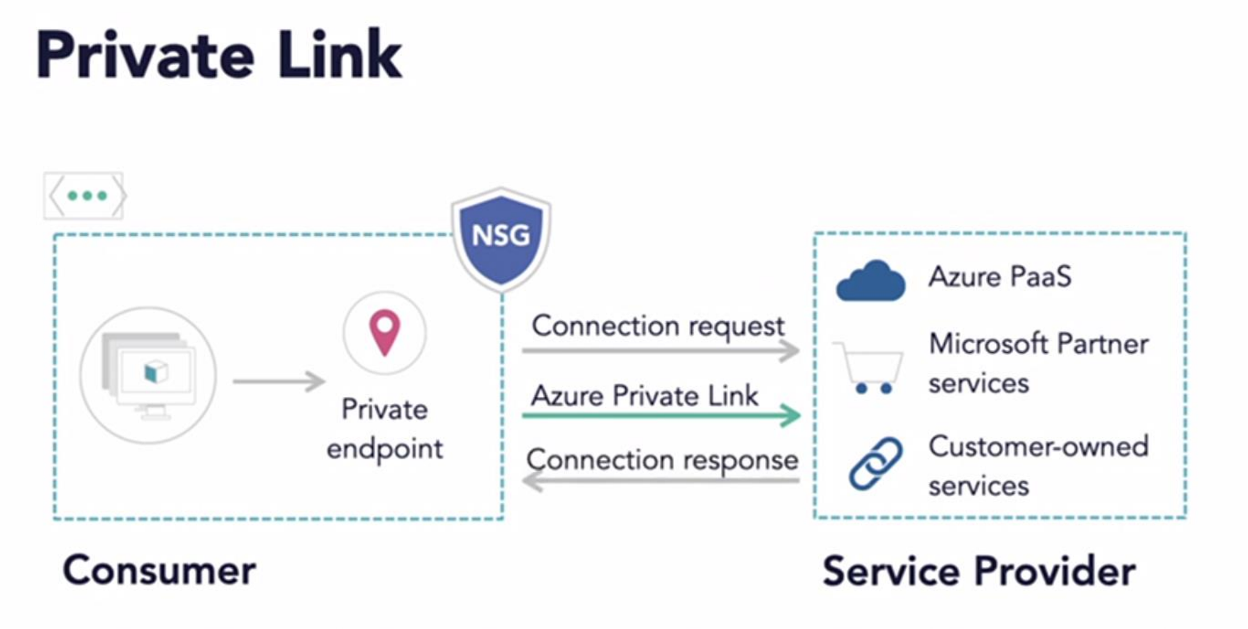


Private Link

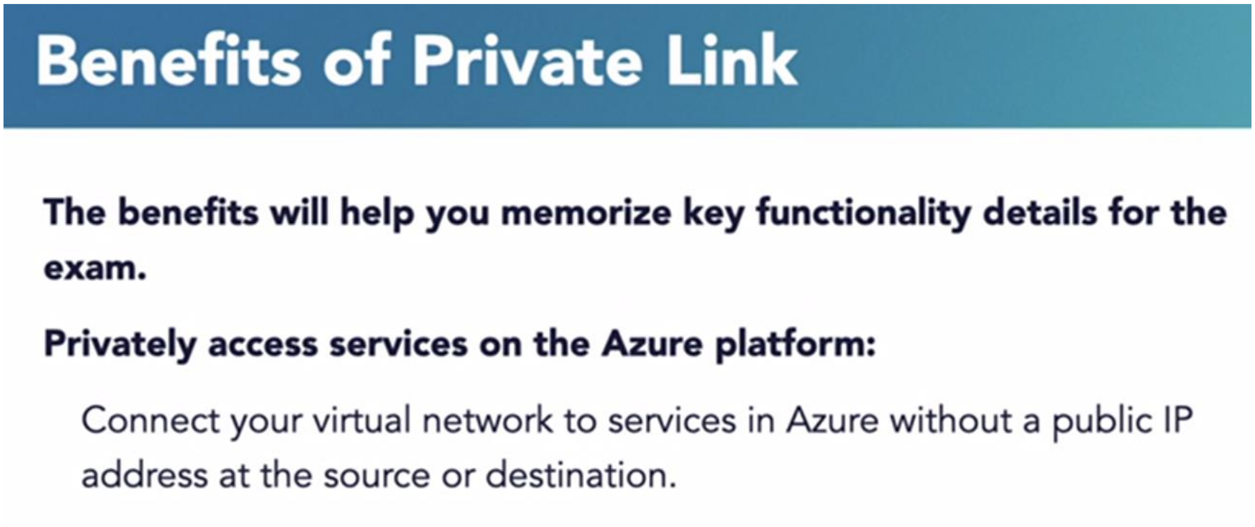
The Azure Private Link service is the reference to your own service (application) that is powered by Azure Private Link.

The consumer’s private endpoint connection will be created in a Pending state on the Private Link service object.

As the service provider, you can approve or reject the access request from the consumer.



Private Link

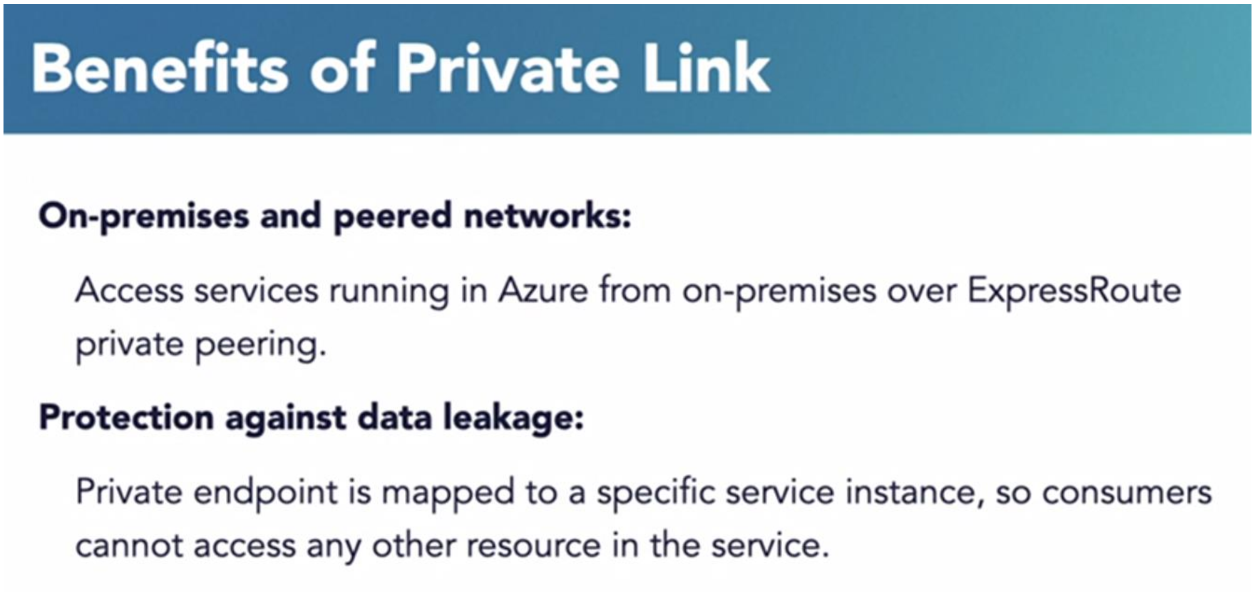


Benefits of Private Link

The benefits will help you memorize key functionality details for the exam.

Privately access services on the Azure platform:

Connect your virtual network to services in Azure without a public IP address at the source or destination.



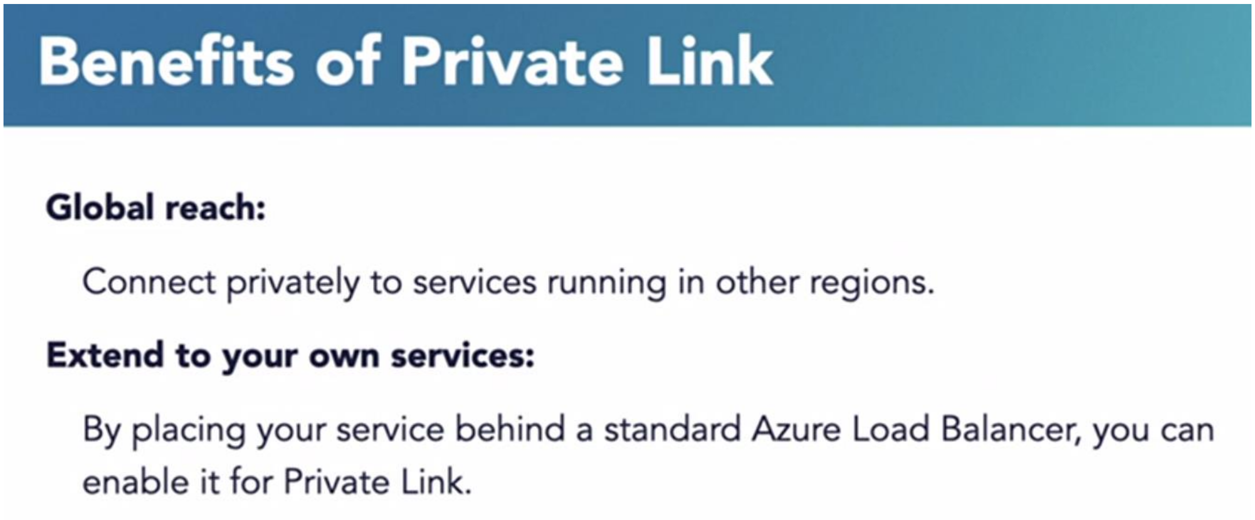
Benefits of Private Link

On-premises and peered networks:

Access services running in Azure from on-premises over ExpressRoute private peering.

Protection against data leakage:

Private endpoint is mapped to a specific service instance, so consumers cannot access any other resource in the service.



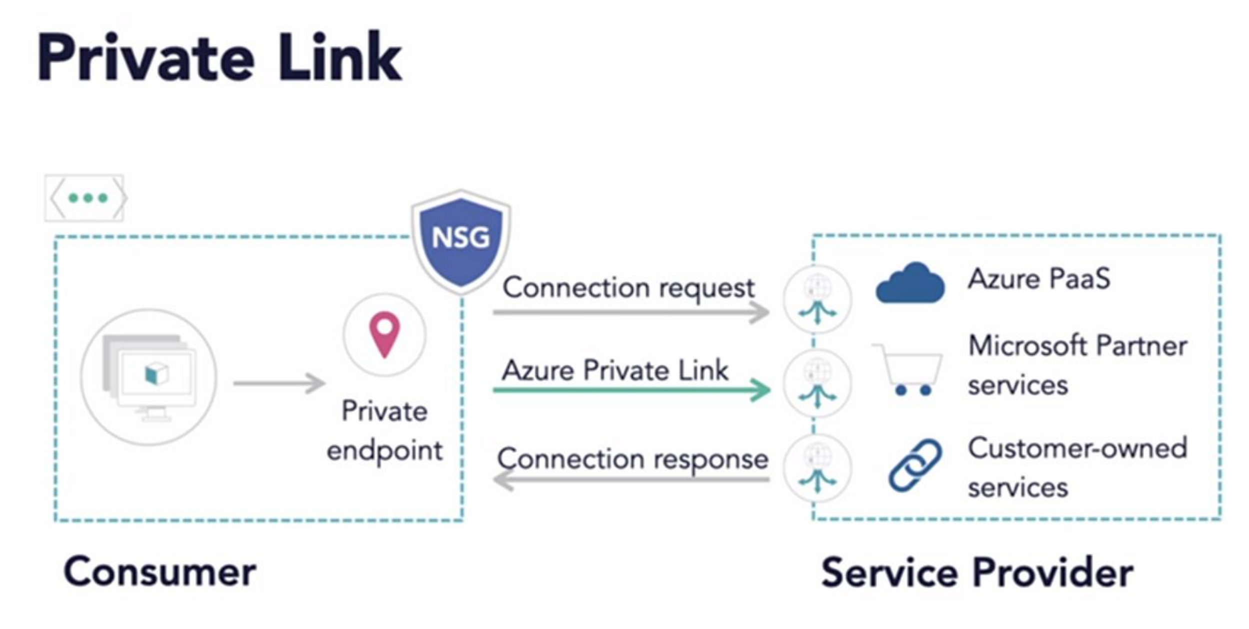
Benefits of Private Link

Global reach:

Connect privately to services running in other regions.

Extend to your own services:

By placing your service behind a standard Azure Load Balancer, you can enable it for Private Link.



Private Link

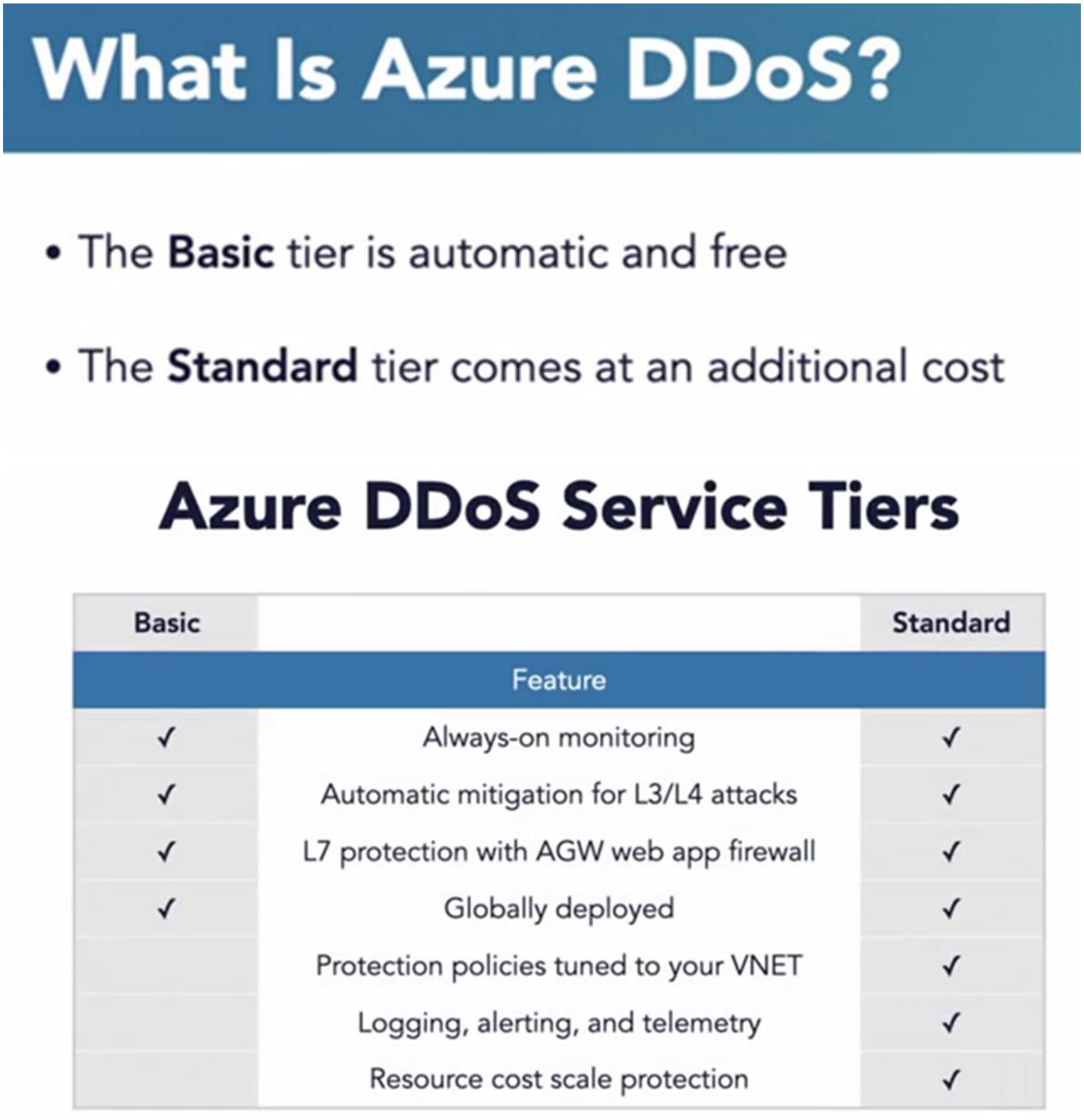
For the Exam

Know how to enable a service for Private Link and your options for controlling access to that Private Link-enabled service.

1.13 Implement Azure DDoS protection

What Is Azure DDoS?

VNET-integrated service that provides protection for Azure applications from impacts of DDoS attacks

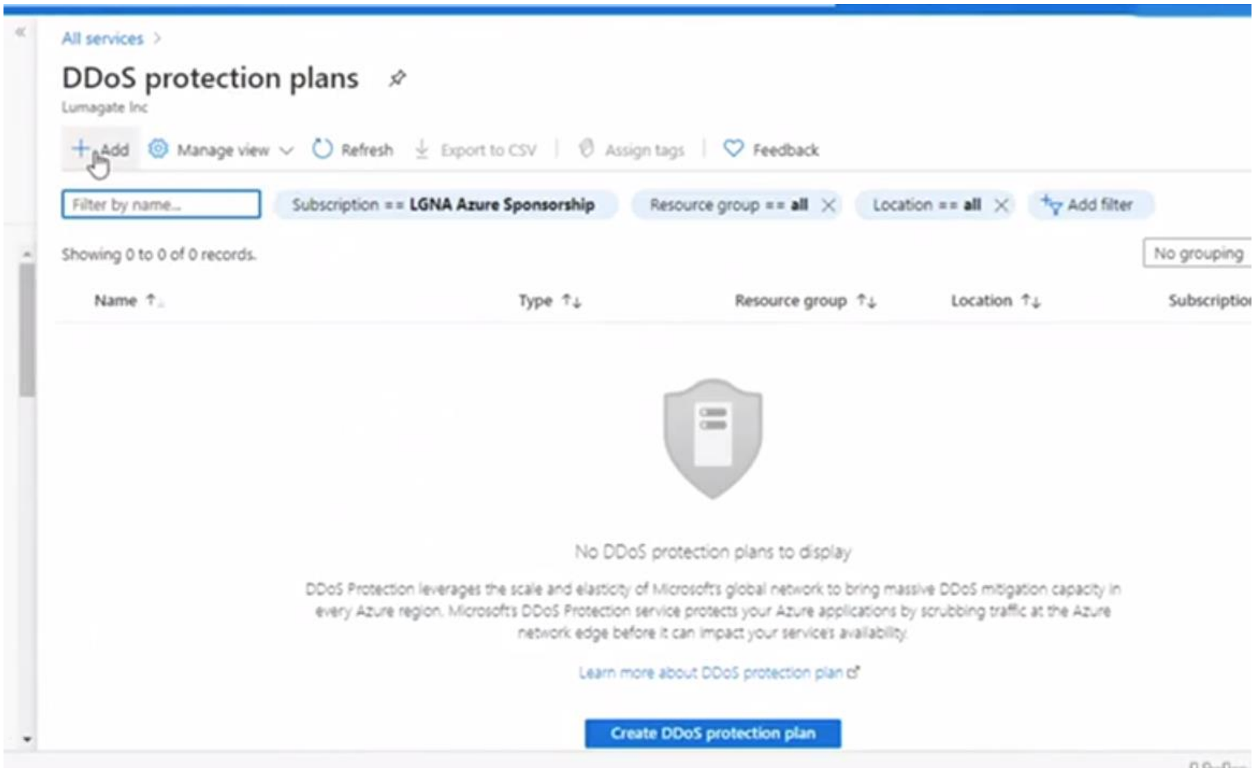


What Is Azure DDoS?

- The **Basic** tier is automatic and free
- The **Standard** tier comes at an additional cost

Azure DDoS Service Tiers

Basic		Standard
	Feature	
✓	Always-on monitoring	✓
✓	Automatic mitigation for L3/L4 attacks	✓
✓	L7 protection with AGW web app firewall	✓
✓	Globally deployed	✓
	Protection policies tuned to your VNET	✓
	Logging, alerting, and telemetry	✓
	Resource cost scale protection	✓


All services >

DDoS protection plans

Lumagate Inc

Subscription == LGNA Azure Sponsorship

Resource group == all

Location == all

Showing 0 to 0 of 0 records.

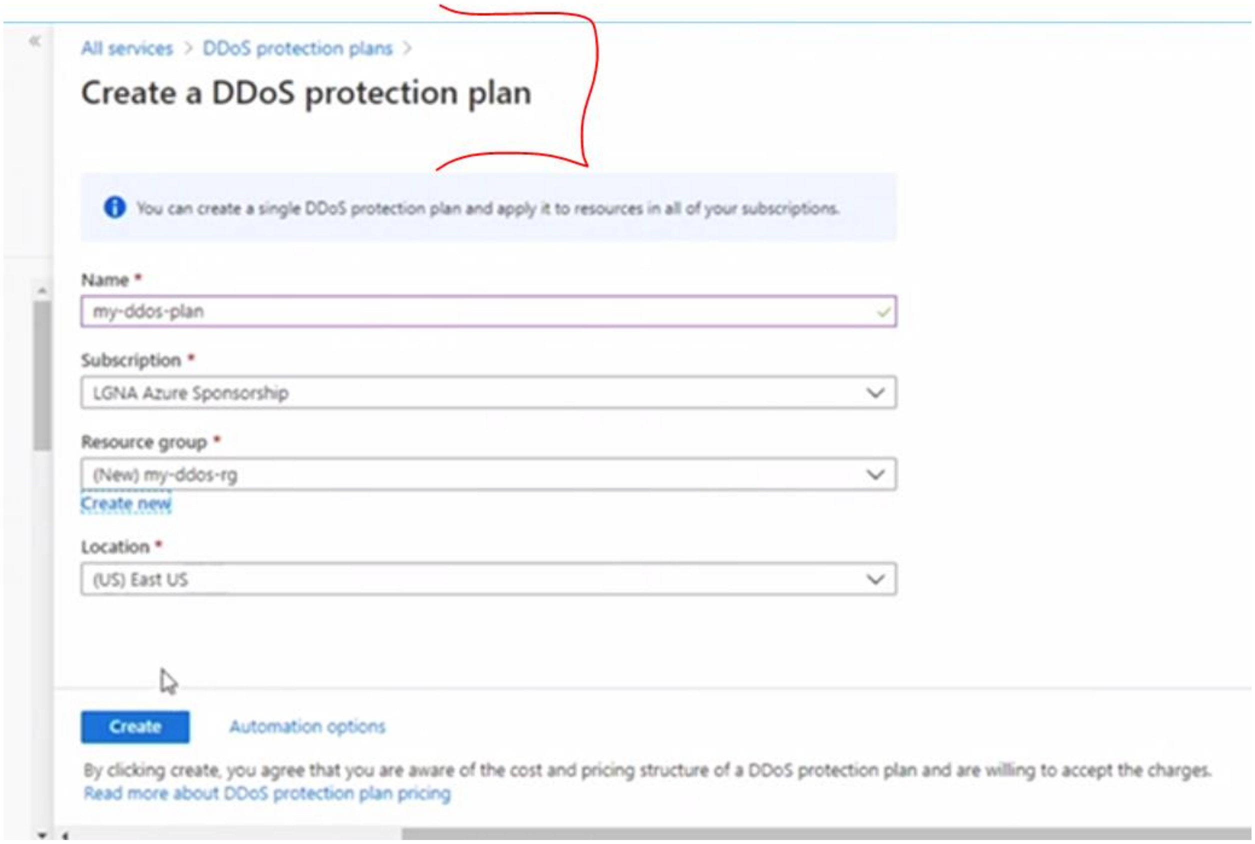
Name	Type	Resource group	Location	Subscriptio

No DDoS protection plans to display

DDoS Protection leverages the scale and elasticity of Microsoft's global network to bring massive DDoS mitigation capacity in every Azure region. Microsoft's DDoS Protection service protects your Azure applications by scrubbing traffic at the Azure network edge before it can impact your services availability.

Learn more about DDoS protection plan

Create a DDoS protection plan



Create a DDoS protection plan

You can create a single DDoS protection plan and apply it to resources in all of your subscriptions.

Name *
my-ddos-plan

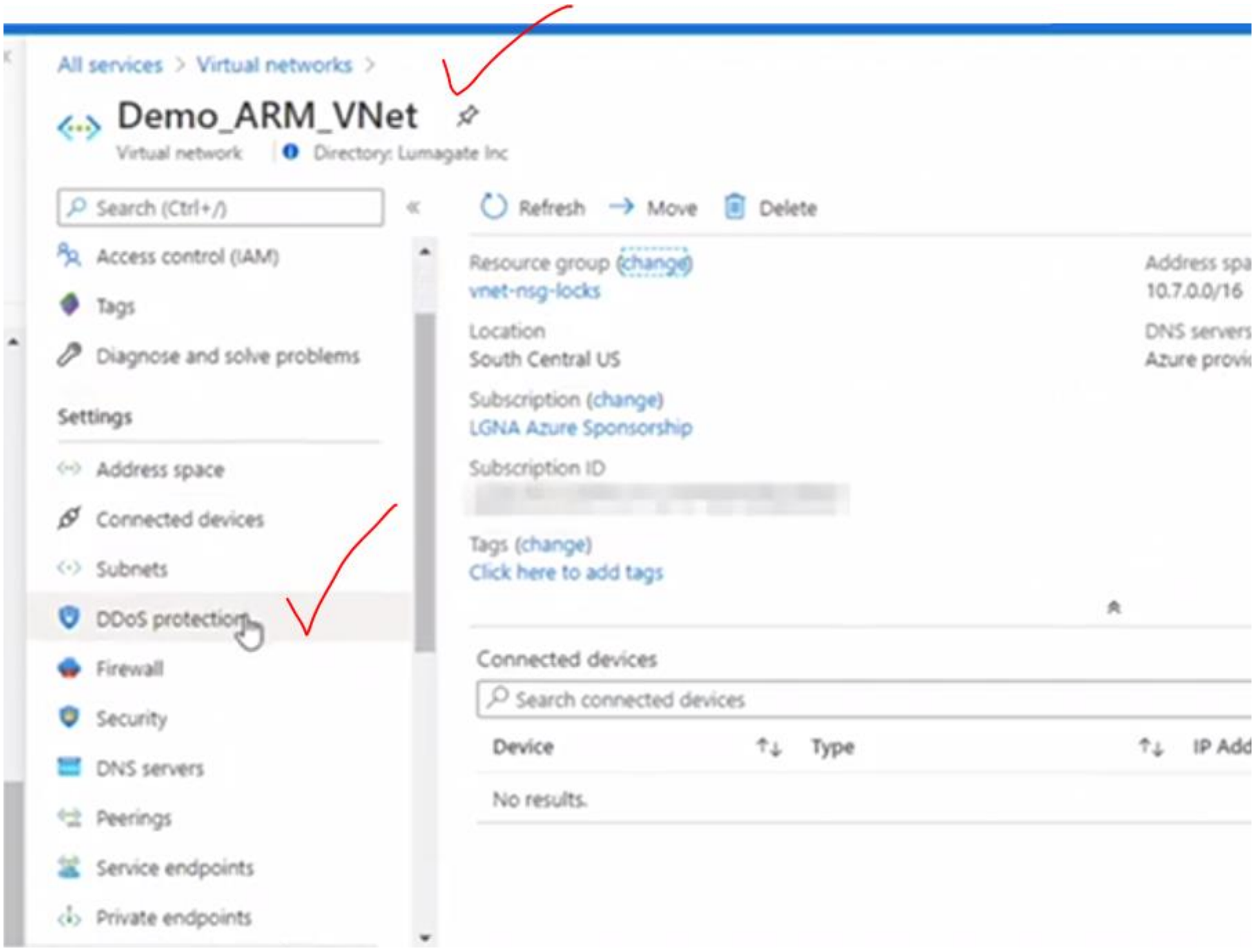
Subscription *
LGNA Azure Sponsorship

Resource group *
(New) my-ddos-rg
Create new

Location *
(US) East US

By clicking create, you agree that you are aware of the cost and pricing structure of a DDoS protection plan and are willing to accept the charges.
Read more about DDoS protection plan pricing

The next step is to assign that plan to existing and new VNETs



Demo_ARM_VNet

Resource group (change)
vnet-nsg-locks

Location
South Central US

Subscription (change)
LGNA Azure Sponsorship

Subscription ID
[redacted]

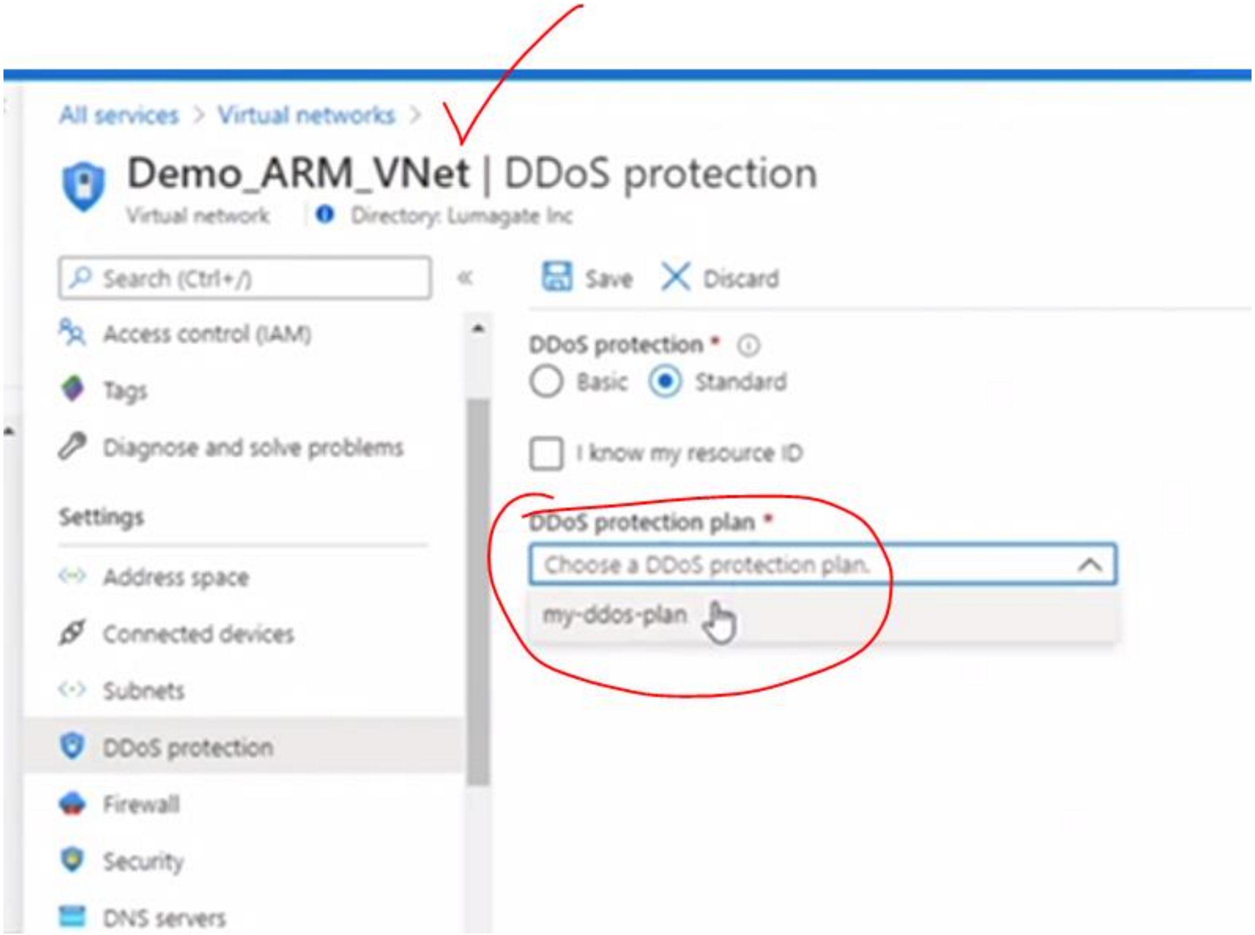
Tags (change)
Click here to add tags

Address spa
10.7.0.0/16

DNS servers
Azure provi

Connected devices

Device	Type	IP Add
No results.		



All services > Virtual networks >

Demo_ARM_VNet | DDoS protection

Virtual network | Directory: Lumagate Inc

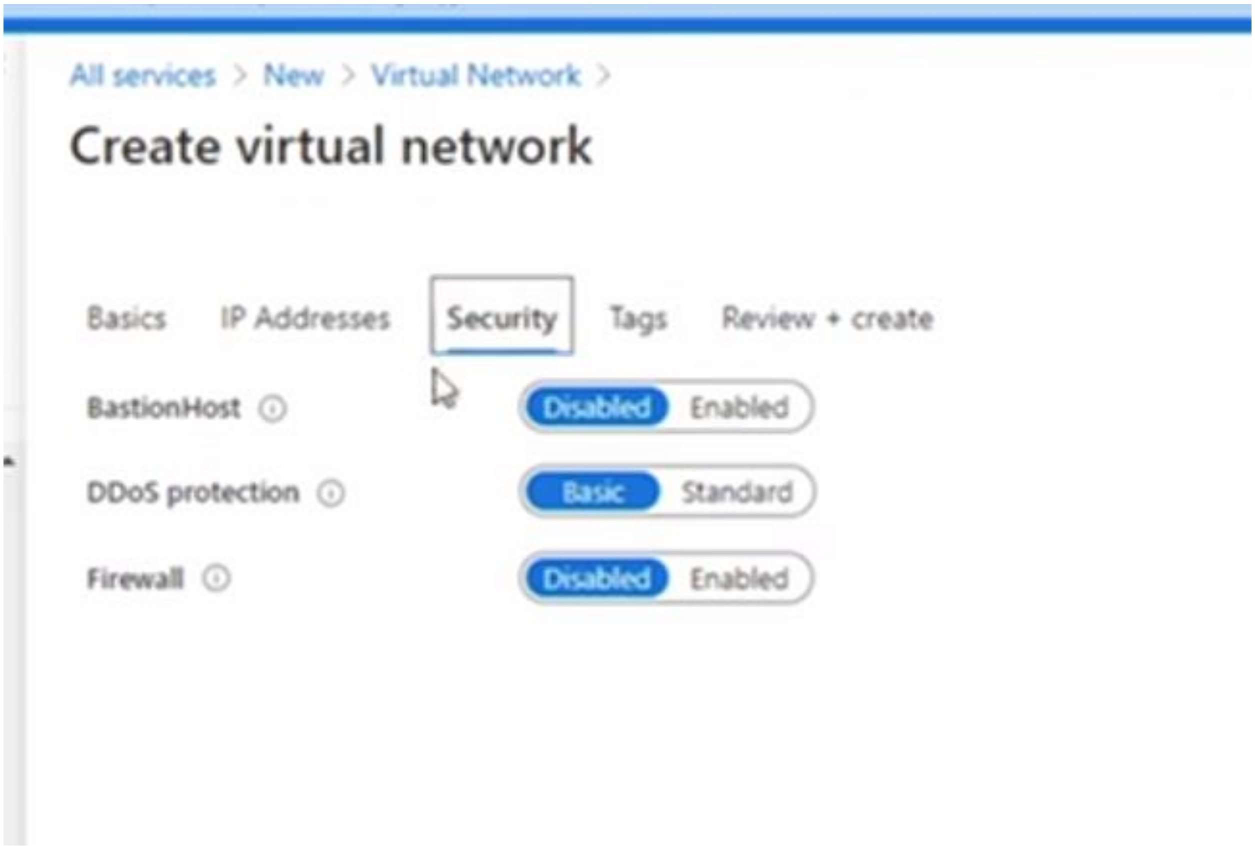
DDoS protection * ○ Basic ● Standard

□ I know my resource ID

DDoS protection plan *

Choose a DDoS protection plan.

my-ddos-plan

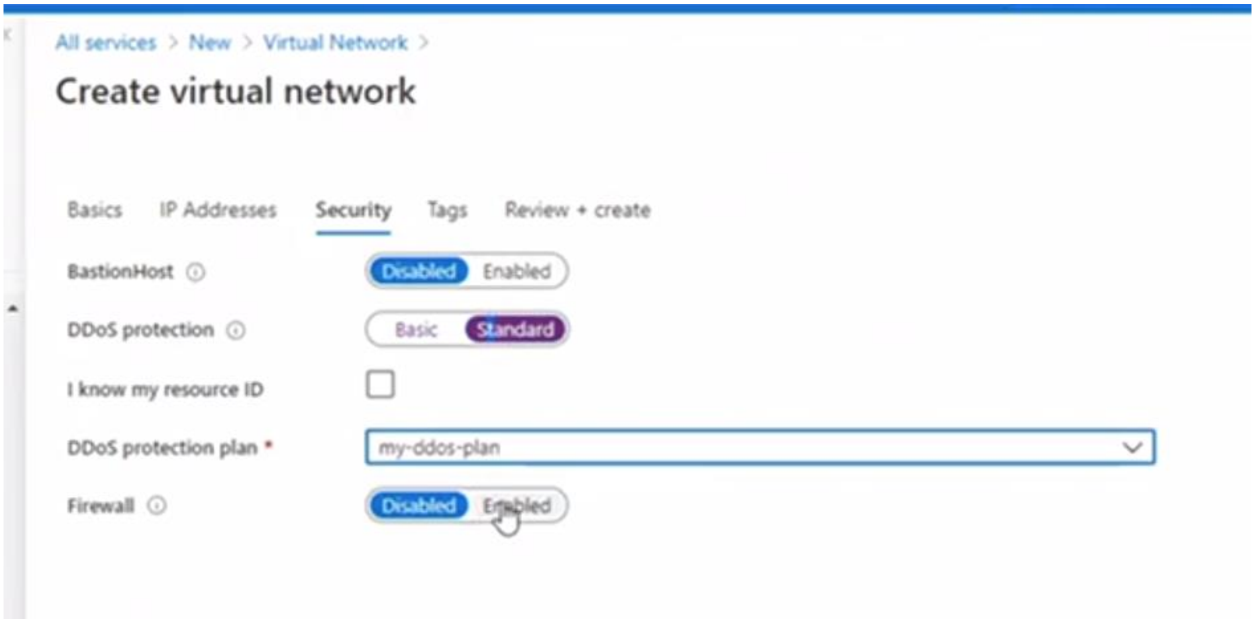


Create virtual network

BastionHost: [✓ Disabled] Enabled

DDoS protection: [✓ Basic] Standard

Firewall: [✓ Disabled] Enabled



Create virtual network

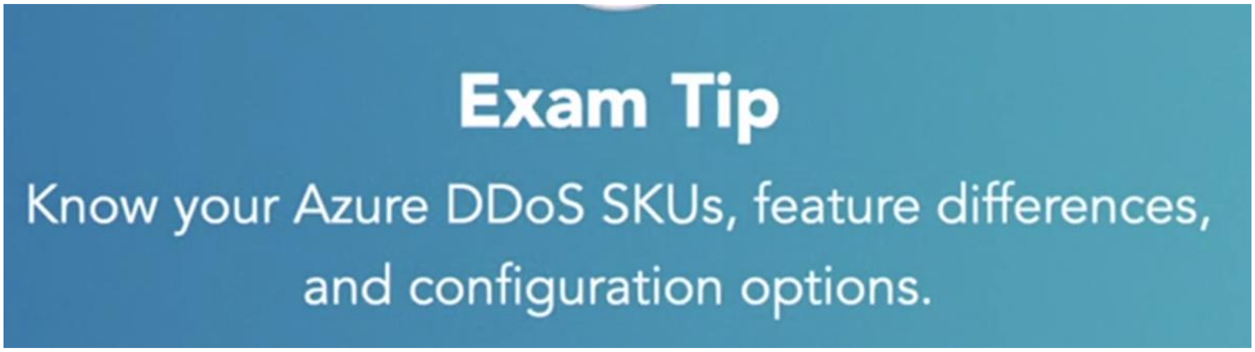
BastionHost: [✓ Disabled] Enabled

DDoS protection: Basic [✓ Standard]

I know my resource ID: □

DDoS protection plan *: my-ddos-plan

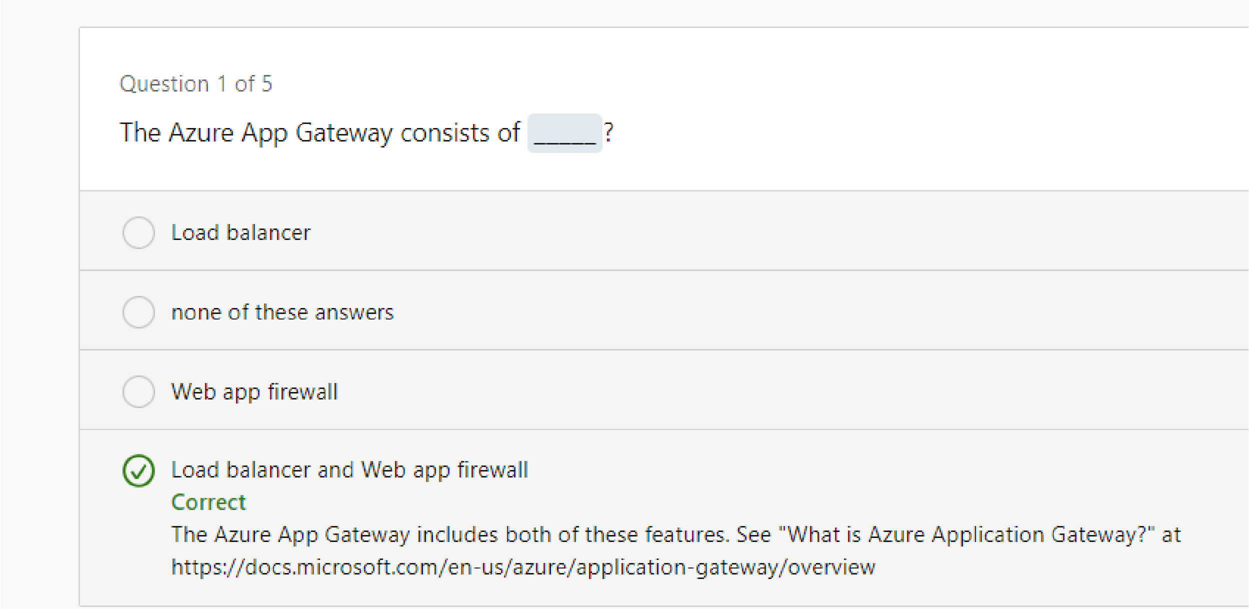
Firewall: [✓ Disabled] Enabled



Exam Tip

Know your Azure DDoS SKUs, feature differences, and configuration options.

1.14 Quiz



Question 1 of 5

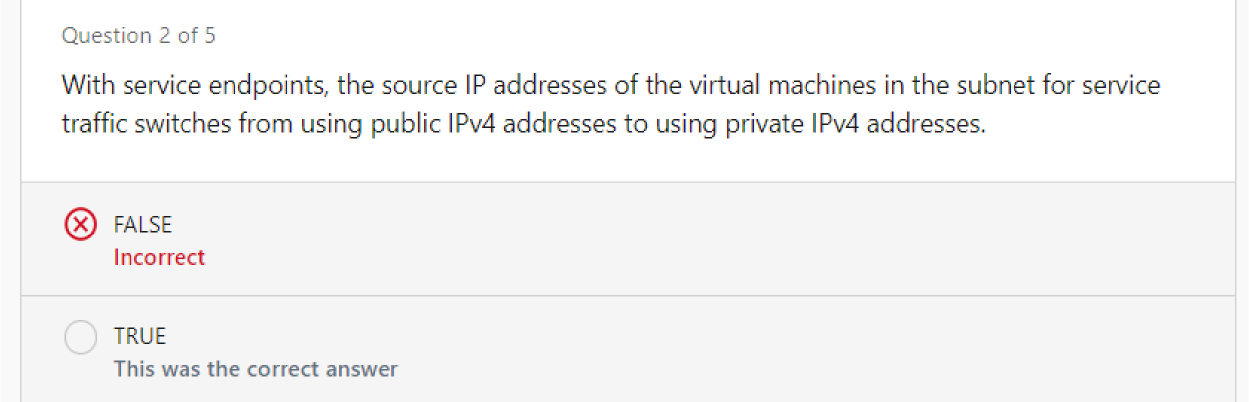
The Azure App Gateway consists of _____?

○ Load balancer

○ none of these answers

○ Web app firewall

✓ Load balancer and Web app firewall
Correct
The Azure App Gateway includes both of these features. See "What is Azure Application Gateway?" at https://docs.microsoft.com/en-us/azure/application-gateway/overview

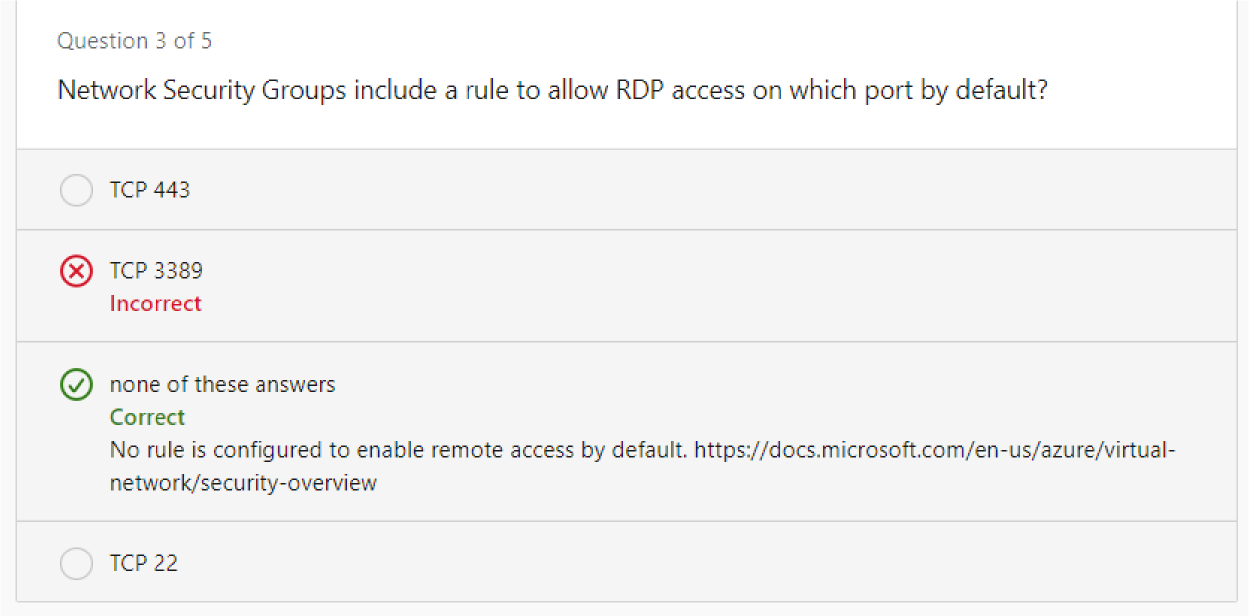


Question 2 of 5

With service endpoints, the source IP addresses of the virtual machines in the subnet for service traffic switches from using public IPv4 addresses to using private IPv4 addresses.

☒ FALSE
Incorrect

○ TRUE
This was the correct answer



Question 3 of 5

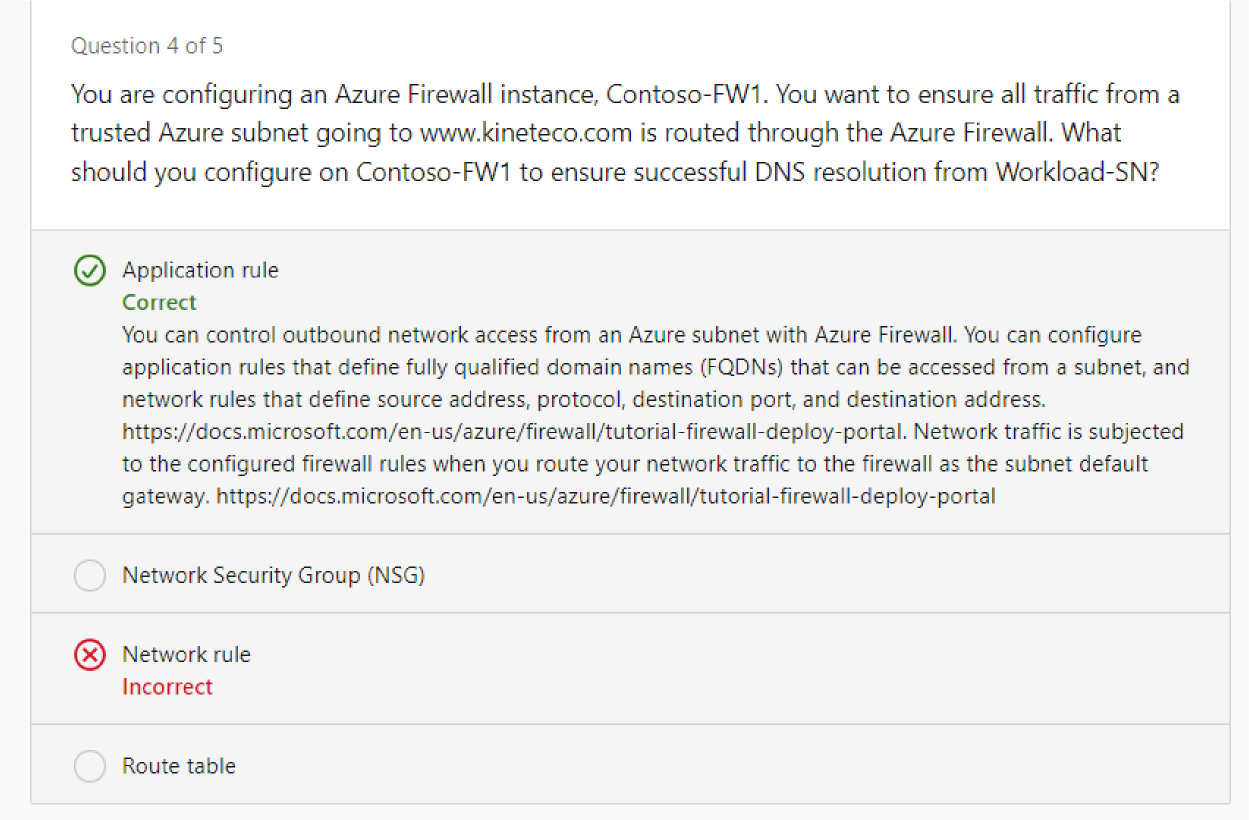
Network Security Groups include a rule to allow RDP access on which port by default?

○ TCP 443

⊗ TCP 3389
Incorrect

✓ none of these answers
Correct
No rule is configured to enable remote access by default. https://docs.microsoft.com/en-us/azure/virtual-network/security-overview

○ TCP 22



Question 4 of 5

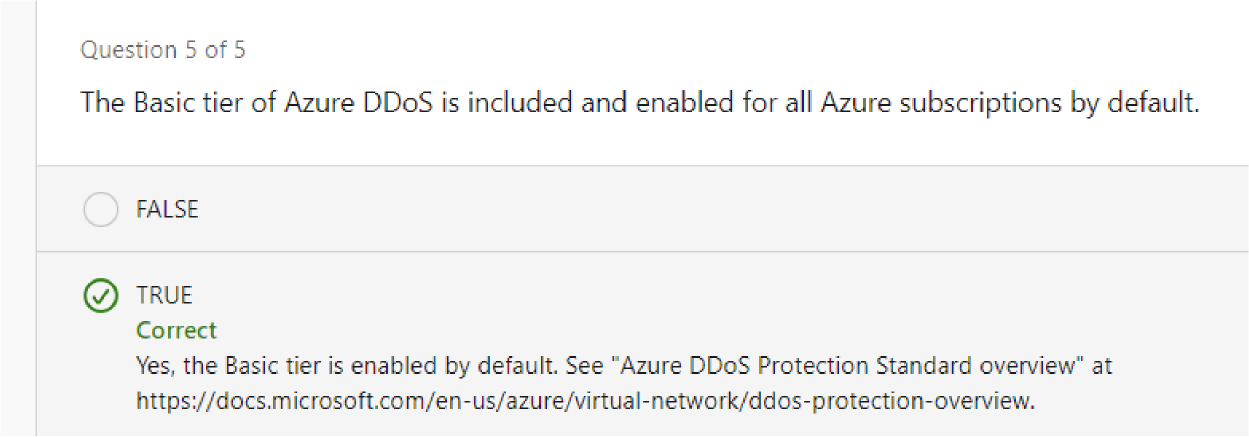
You are configuring an Azure Firewall instance, Contoso-FW1. You want to ensure all traffic from a trusted Azure subnet going to www.kineteco.com is routed through the Azure Firewall. What should you configure on Contoso-FW1 to ensure successful DNS resolution from Workload-SN?

✓ Application rule
Correct
You can control outbound network access from an Azure subnet with Azure Firewall. You can configure application rules that define fully qualified domain names (FQDNs) that can be accessed from a subnet, and network rules that define source address, protocol, destination port, and destination address. https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal. Network traffic is subjected to the configured firewall rules when you route your network traffic to the firewall as the subnet default gateway. https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal

○ Network Security Group (NSG)

⊗ Network rule
Incorrect

○ Route table



Question 5 of 5

The Basic tier of Azure DDoS is included and enabled for all Azure subscriptions by default.

○ FALSE

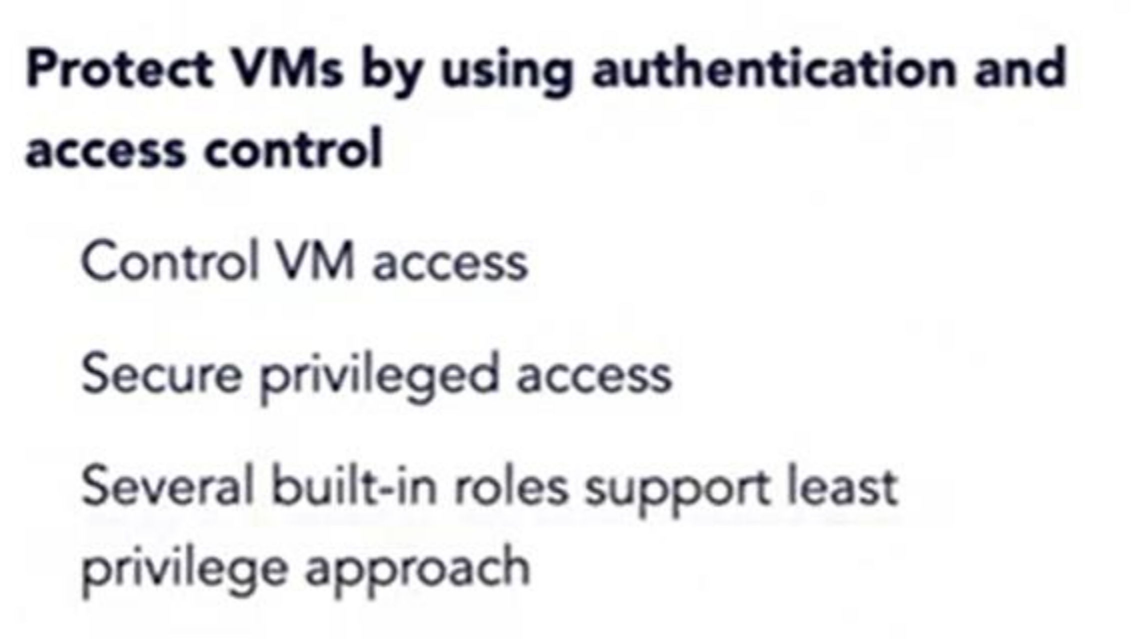
✓ TRUE

Correct

Yes, the Basic tier is enabled by default. See "Azure DDoS Protection Standard overview" at https://docs.microsoft.com/en-us/azure/virtual-network/ddos-protection-overview.

2. Configure Advanced Security for Compute

2.1 Configure Azure Endpoint Protection for VMs

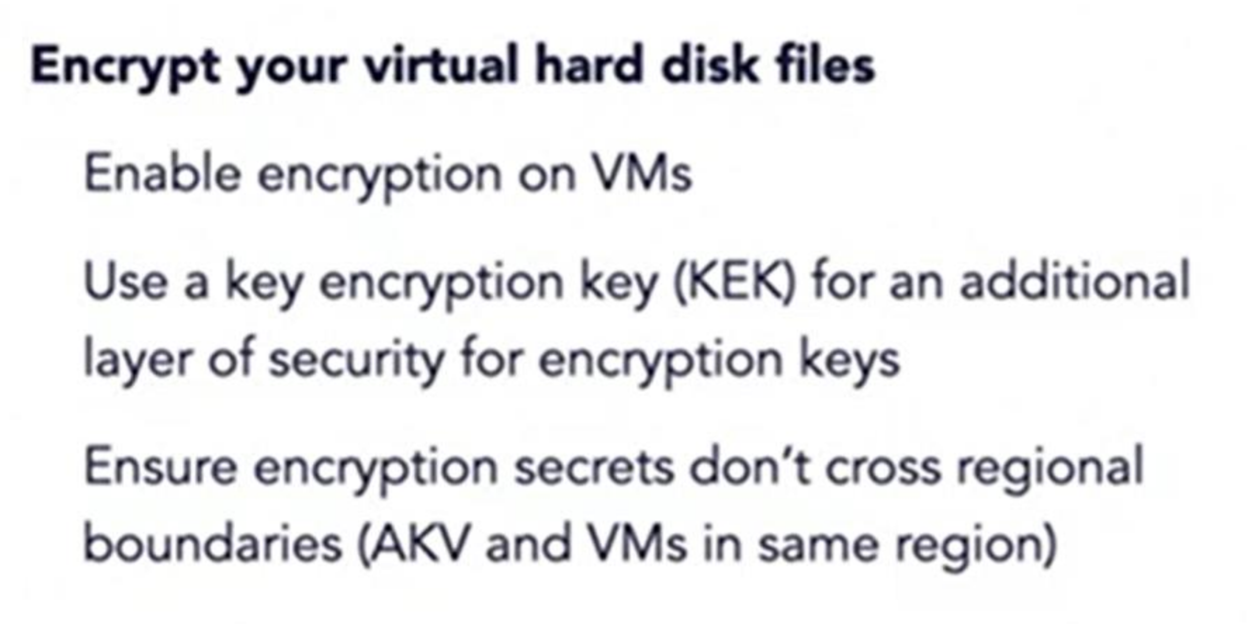


Protect VMs by using authentication and access control

Control VM access

Secure privileged access

Several built-in roles support least privilege approach



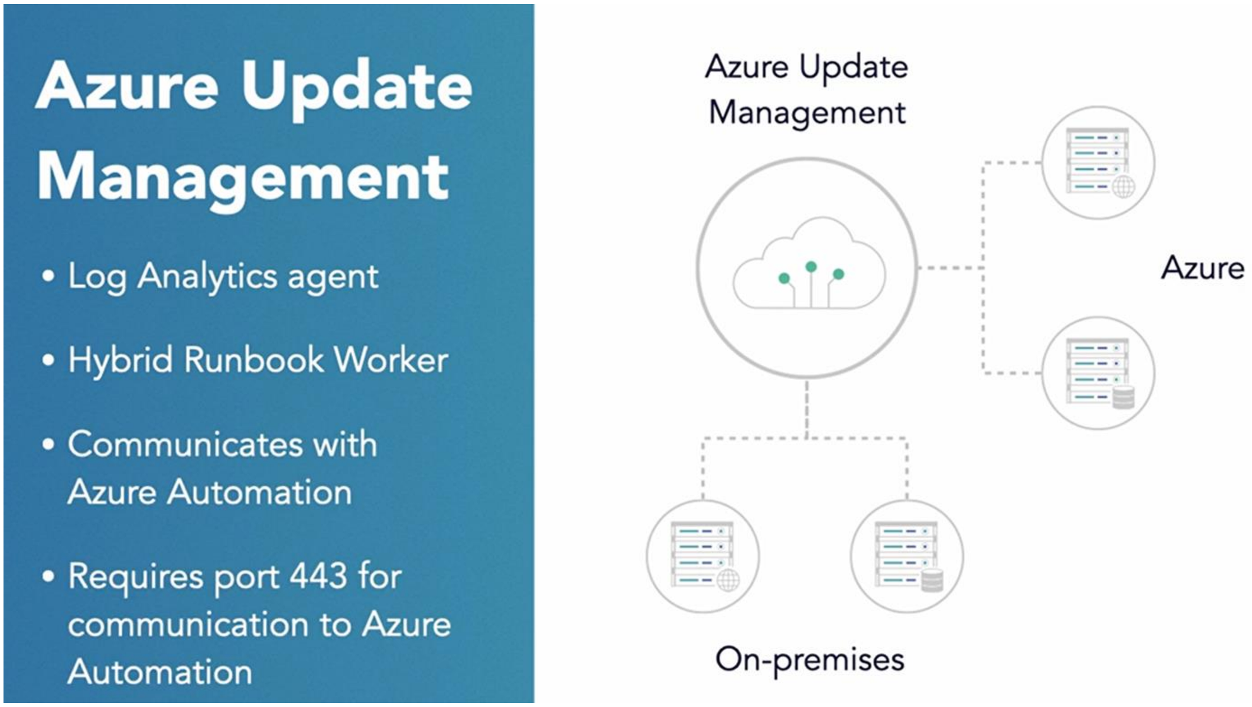
Encrypt your virtual hard disk files

Enable encryption on VMs

Use a key encryption key (KEK) for an additional layer of security for encryption keys

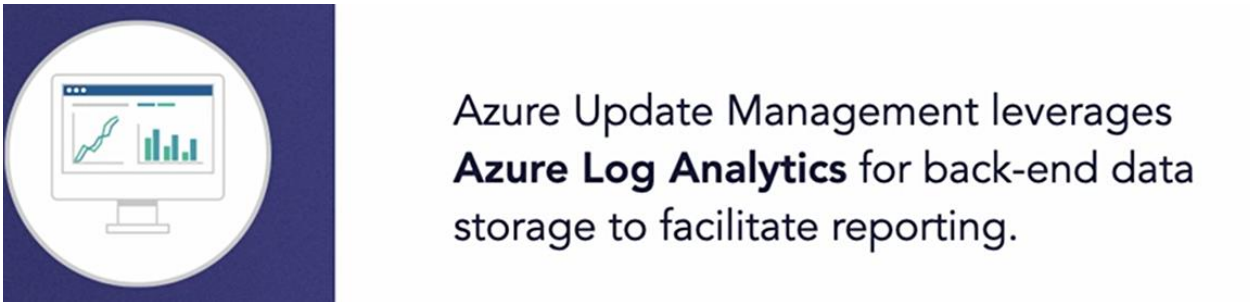
Ensure encryption secrets don't cross regional boundaries (AKV and VMs in same region)

2.2 Implement and manage security updates for VMs

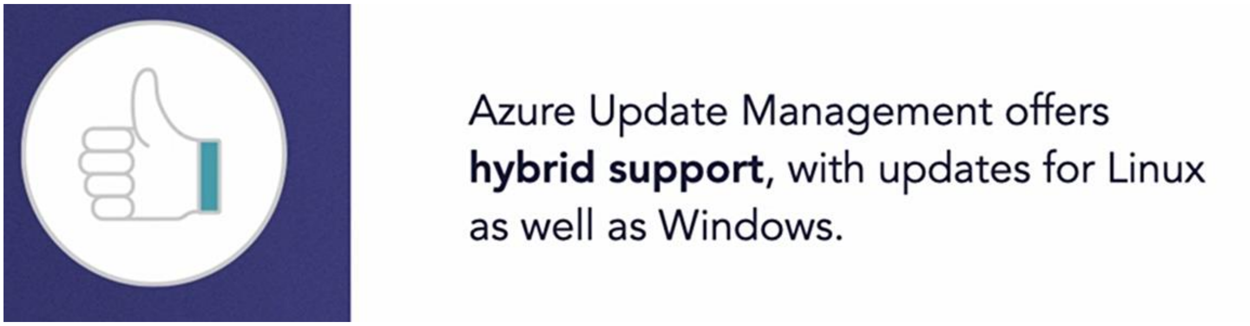


Azure Update Management

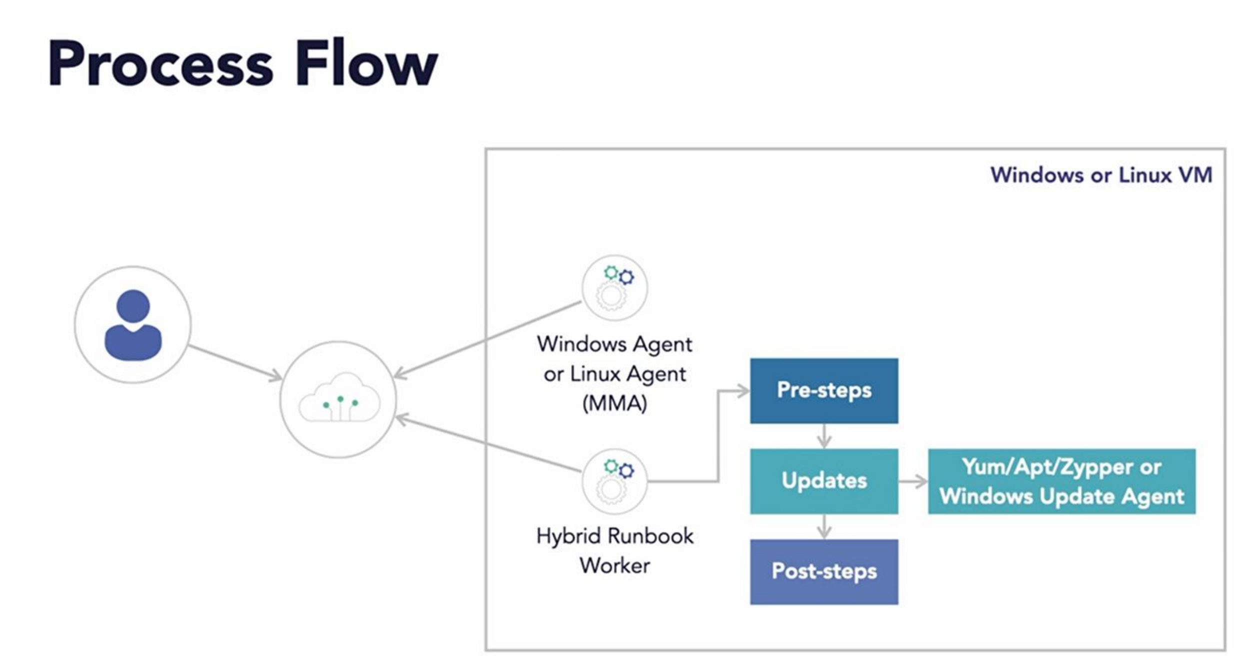
- Log Analytics agent
- Hybrid Runbook Worker
- Communicates with Azure Automation
- Requires port 443 for communication to Azure Automation



Azure Update Management leverages **Azure Log Analytics** for back-end data storage to facilitate reporting.

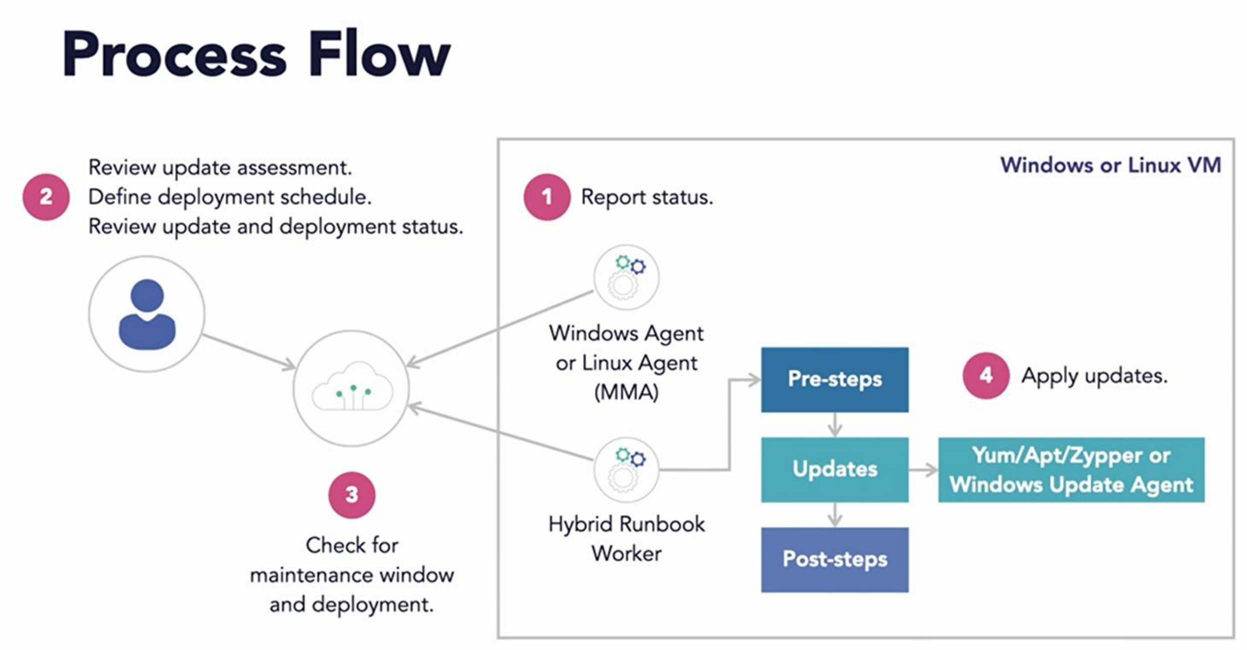


Azure Update Management offers **hybrid support**, with updates for Linux as well as Windows.



Process Flow

Windows or Linux VM
Windows Agent or Linux Agent (MMA)
Hybrid Runbook Worker
Pre-steps
Updates
Post-steps
Yum/Apt/Zypper or Windows Update Agent



Process Flow

2 Review update assessment.
Define deployment schedule.
Review update and deployment status.

Windows or Linux VM

1 Report status.

Windows Agent
or Linux Agent
(MMA)

Hybrid Runbook
Worker

3 Check for
maintenance window
and deployment.

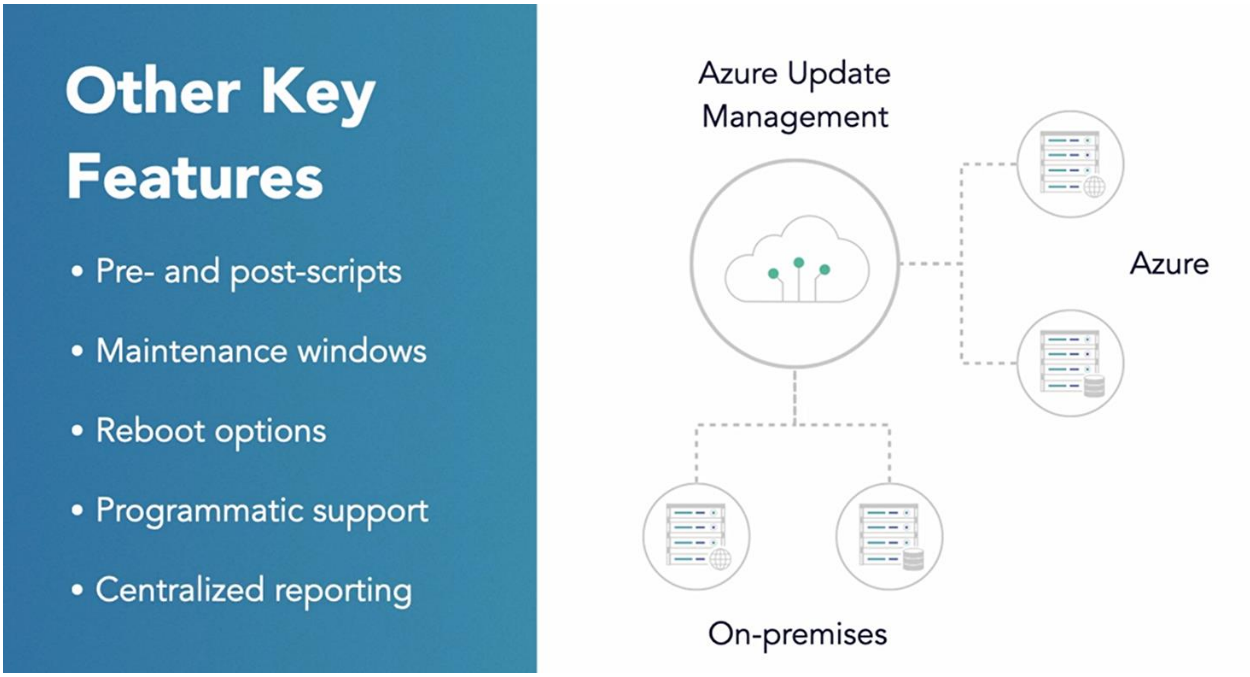
Pre-steps

Updates

Post-steps

4 Apply updates.

Yum/Apt/Zypper or
Windows Update Agent



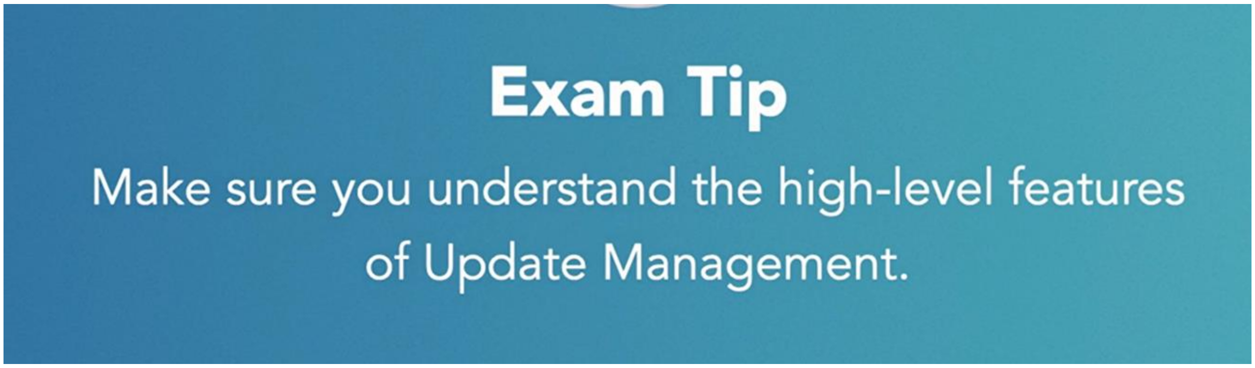
Other Key Features

- Pre- and post-scripts
- Maintenance windows
- Reboot options
- Programmatic support
- Centralized reporting

Azure Update
Management

Azure

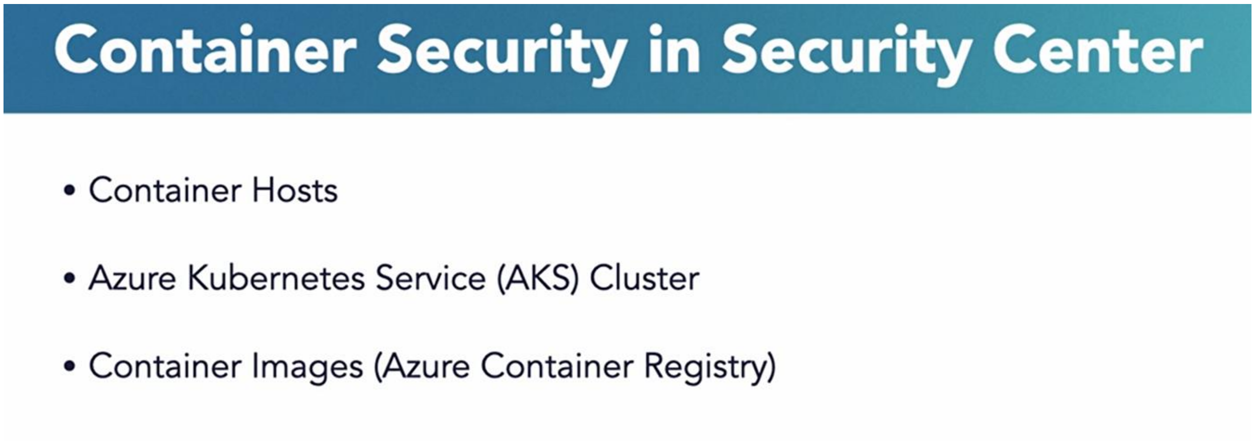
On-premises



Exam Tip

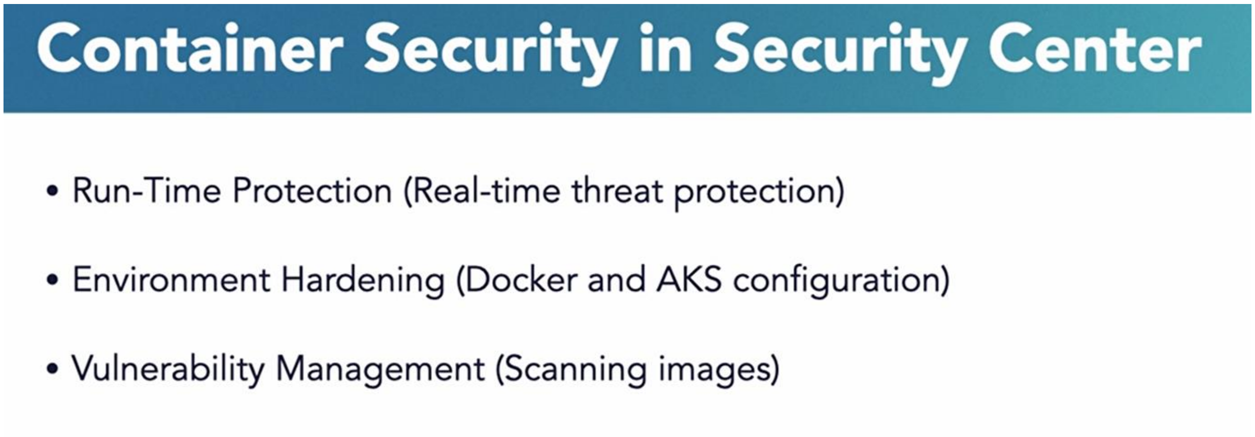
Make sure you understand the high-level features of Update Management.

2.3 Configure security for different types of container services



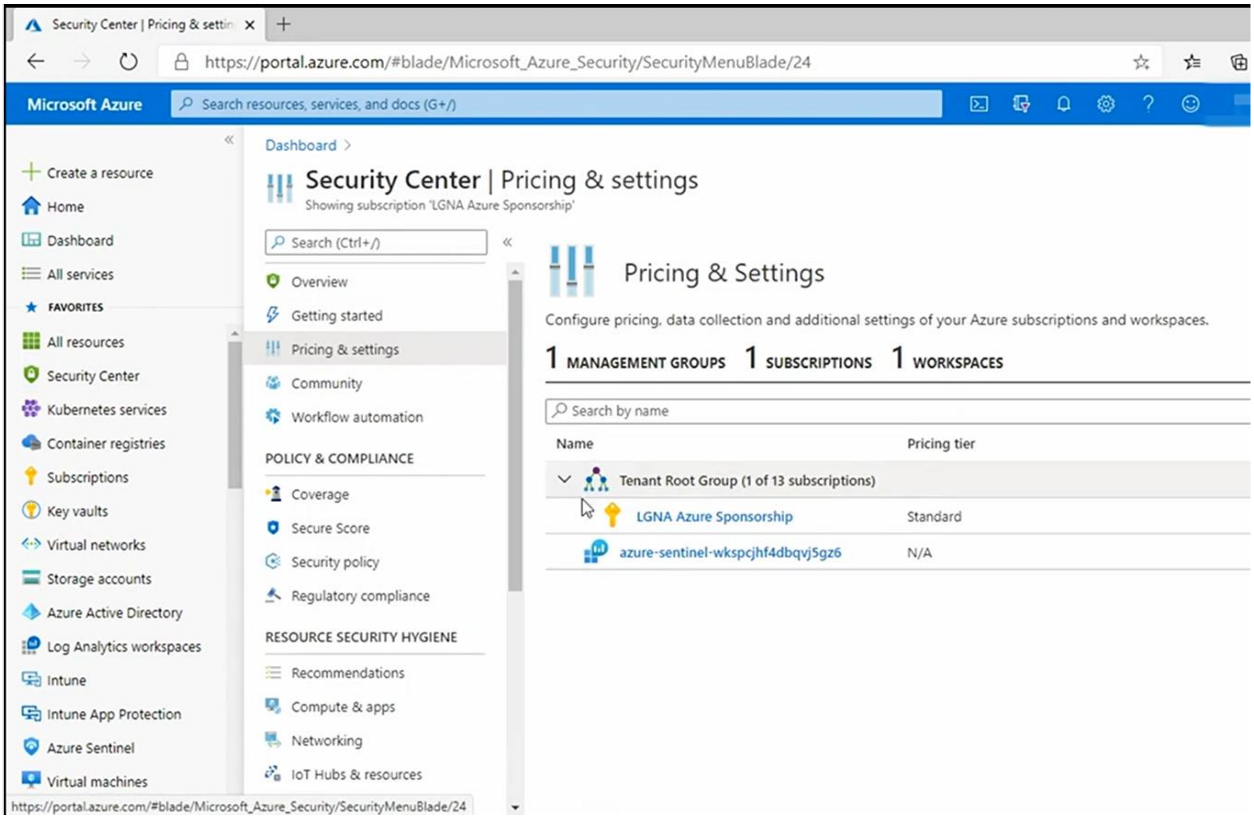
Container Security in Security Center

- Container Hosts
- Azure Kubernetes Service (AKS) Cluster
- Container Images (Azure Container Registry)



Container Security in Security Center

- Run-Time Protection (Real-time threat protection)
- Environment Hardening (Docker and AKS configuration)
- Vulnerability Management (Scanning images)



Security Center | Pricing & settings

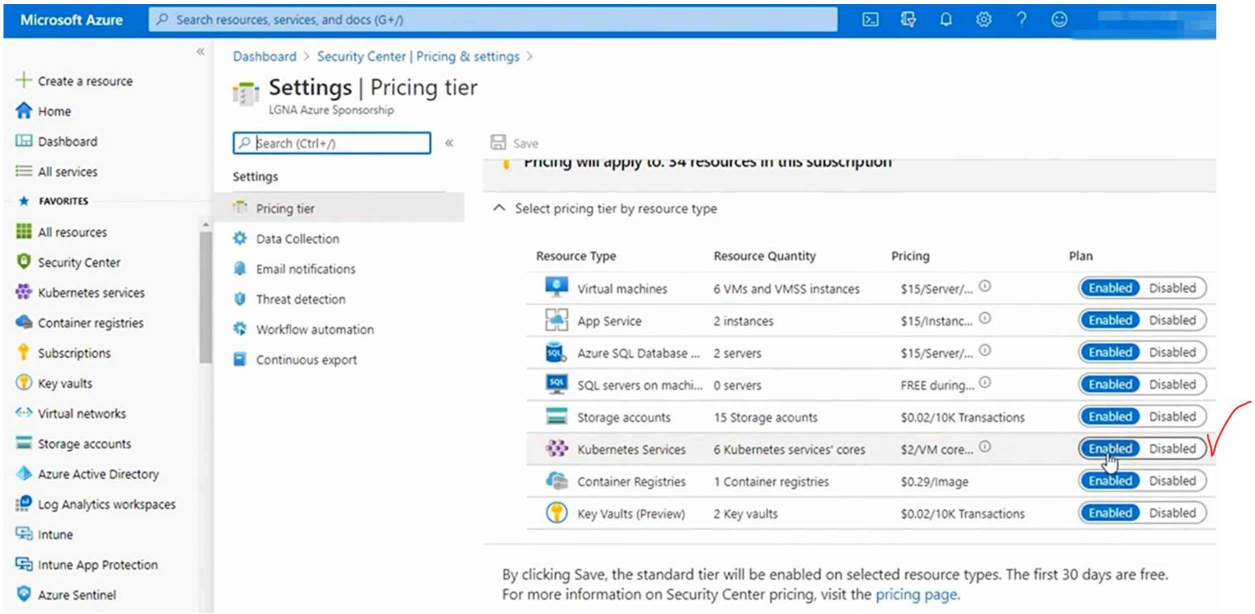
Showing subscription 'LGNA Azure Sponsorship'

Pricing & Settings

Configure pricing, data collection and additional settings of your Azure subscriptions and workspaces.

1 MANAGEMENT GROUPS 1 SUBSCRIPTIONS 1 WORKSPACES

Name	Pricing tier
Tenant Root Group (1 of 13 subscriptions)	
LGNA Azure Sponsorship	Standard
azure-sentinel-wkspcjhf4dbqvj5gz6	N/A



Settings | Pricing tier

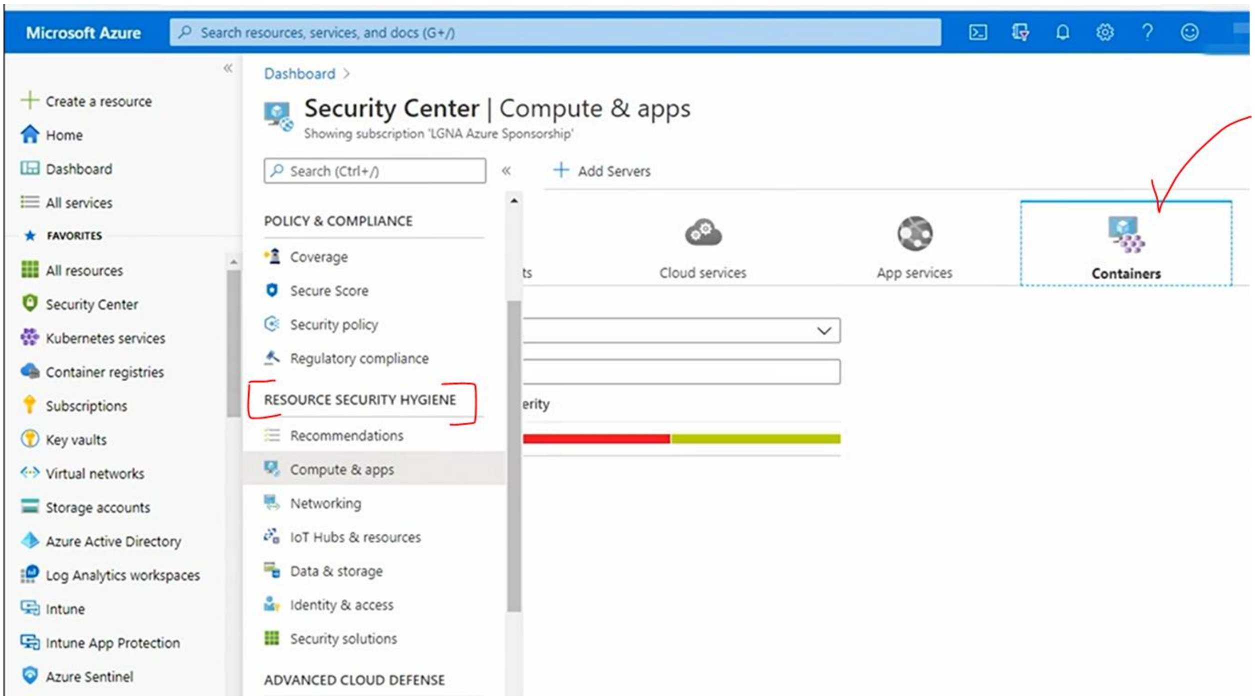
LGNA Azure Sponsorship

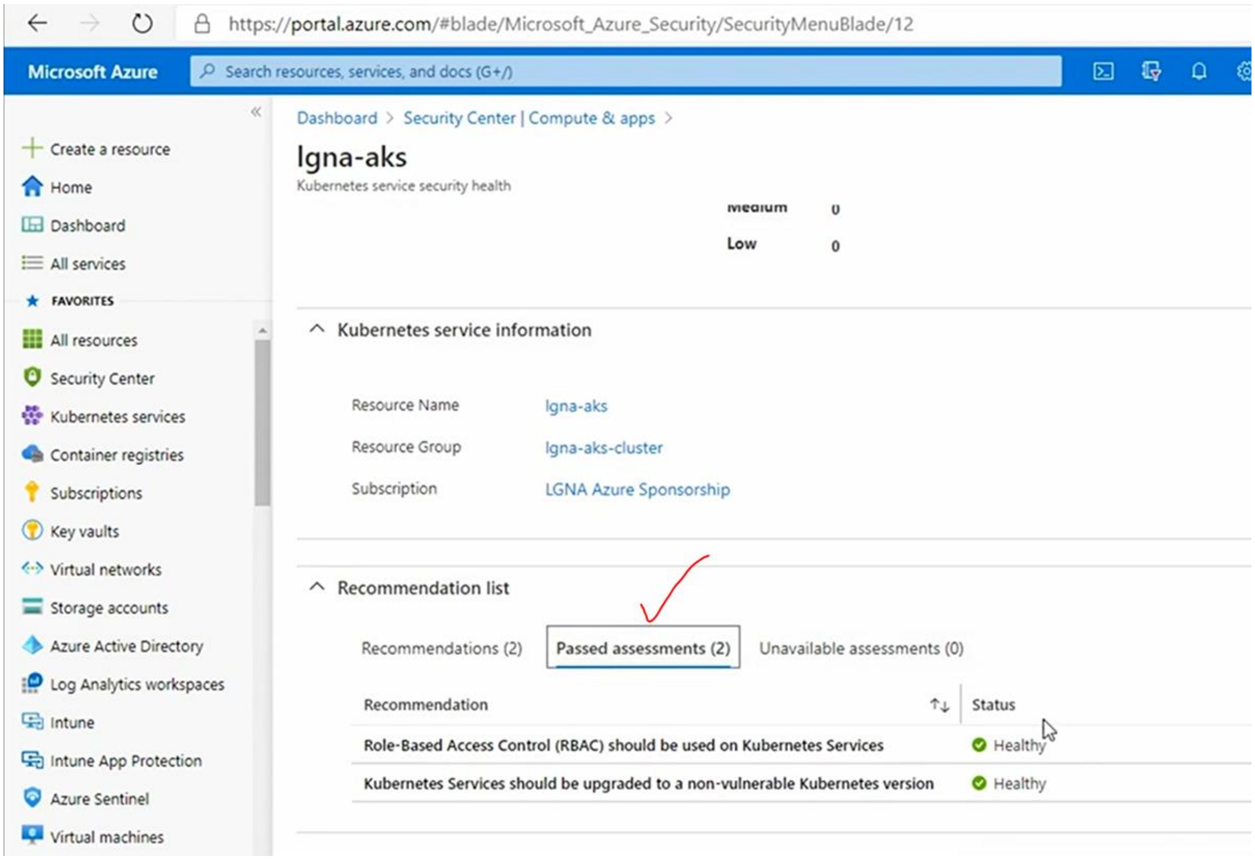
Pricing will apply to: 34 resources in this subscription

Select pricing tier by resource type

Resource Type	Resource Quantity	Pricing	Plan
Virtual machines	6 VMs and VMSS instances	$15/Server/...	Enabled Disabled
App Service	2 instances	$15/Instanc...	Enabled Disabled
Azure SQL Database ...	2 servers	$15/Server/...	Enabled Disabled
SQL servers on machi...	0 servers	FREE during...	Enabled Disabled
Storage accounts	15 Storage acounts	$0.02/10K Transactions	Enabled Disabled
Kubernetes Services	6 Kubernetes services' cores	$2/VM core...	Enabled Disabled ✓
Container Registries	1 Container registries	$0.29/Image	Enabled Disabled
Key Vaults (Preview)	2 Key vaults	$0.02/10K Transactions	Enabled Disabled

By clicking Save, the standard tier will be enabled on selected resource types. The first 30 days are free. For more information on Security Center pricing, visit the pricing page.





lgna-aks

Kubernetes service security health

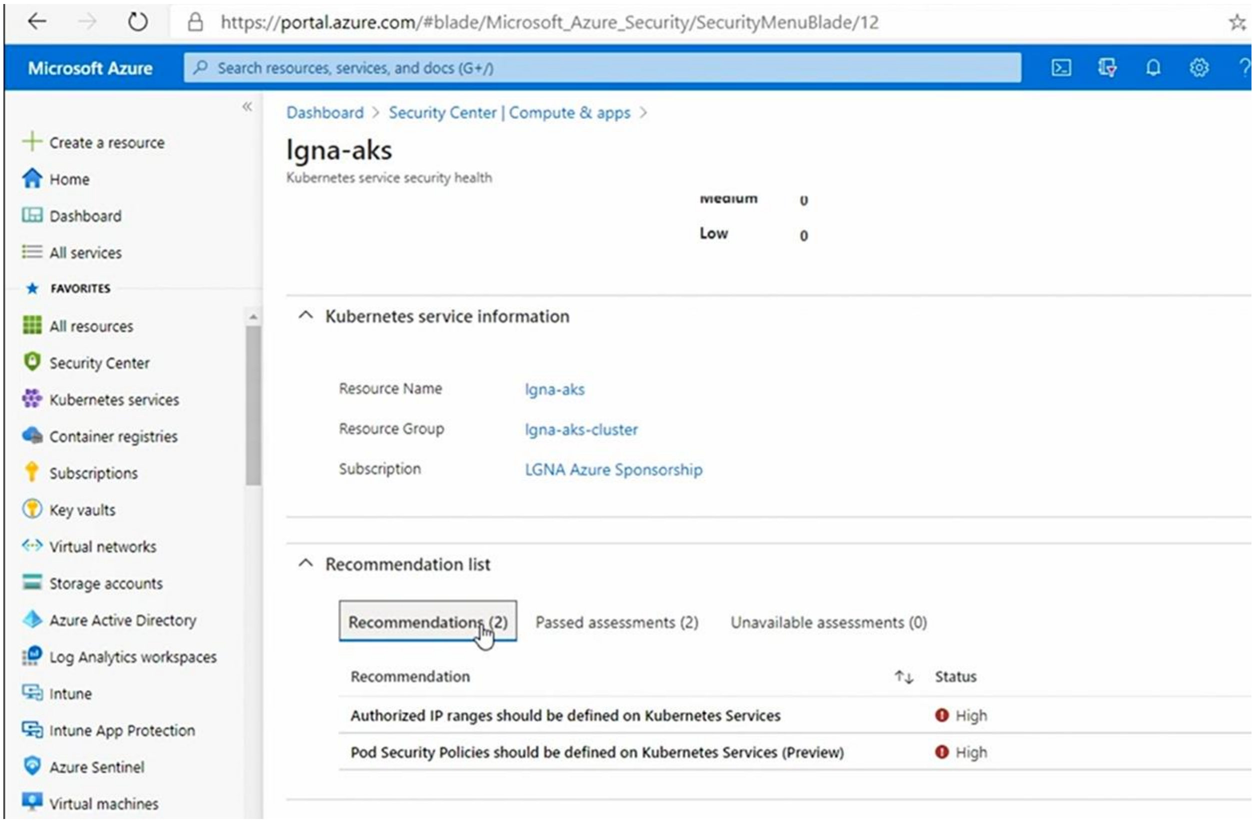
Medium	0
Low	0

Kubernetes service information

Resource Name	lgna-aks
Resource Group	lgna-aks-cluster
Subscription	LGNA Azure Sponsorship

Recommendation list

Recommendation	Status
Role-Based Access Control (RBAC) should be used on Kubernetes Services	Healthy
Kubernetes Services should be upgraded to a non-vulnerable Kubernetes version	Healthy



Igna-aks

Kubernetes service security health

Medium 0

Low 0

Kubernetes service information

Resource Name	Igna-aks
Resource Group	Igna-aks-cluster
Subscription	LGNA Azure Sponsorship

Recommendation list

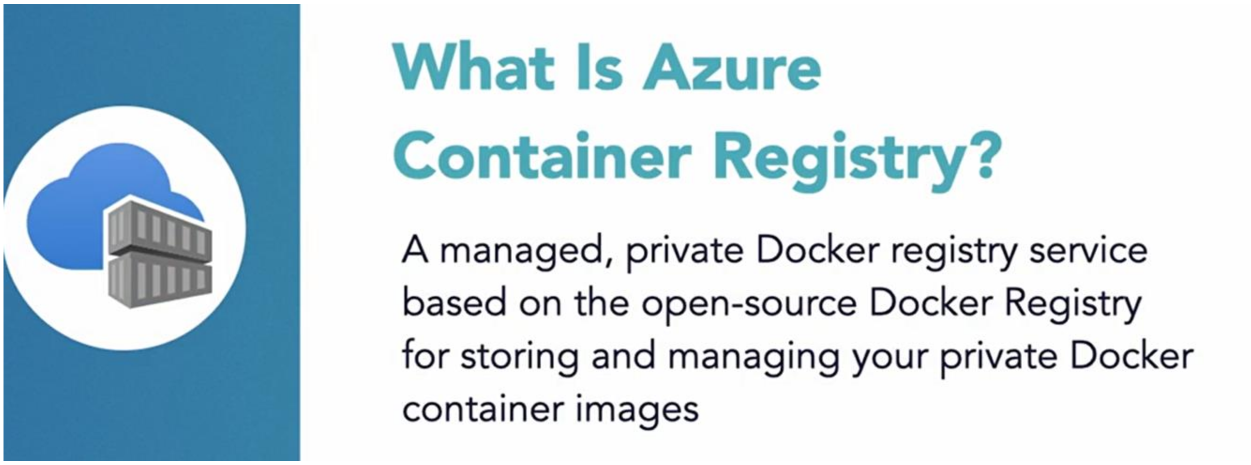
Recommendations (2) | Passed assessments (2) | Unavailable assessments (0)

Recommendation	Status
Authorized IP ranges should be defined on Kubernetes Services	● High
Pod Security Policies should be defined on Kubernetes Services (Preview)	● High

Exam Tip

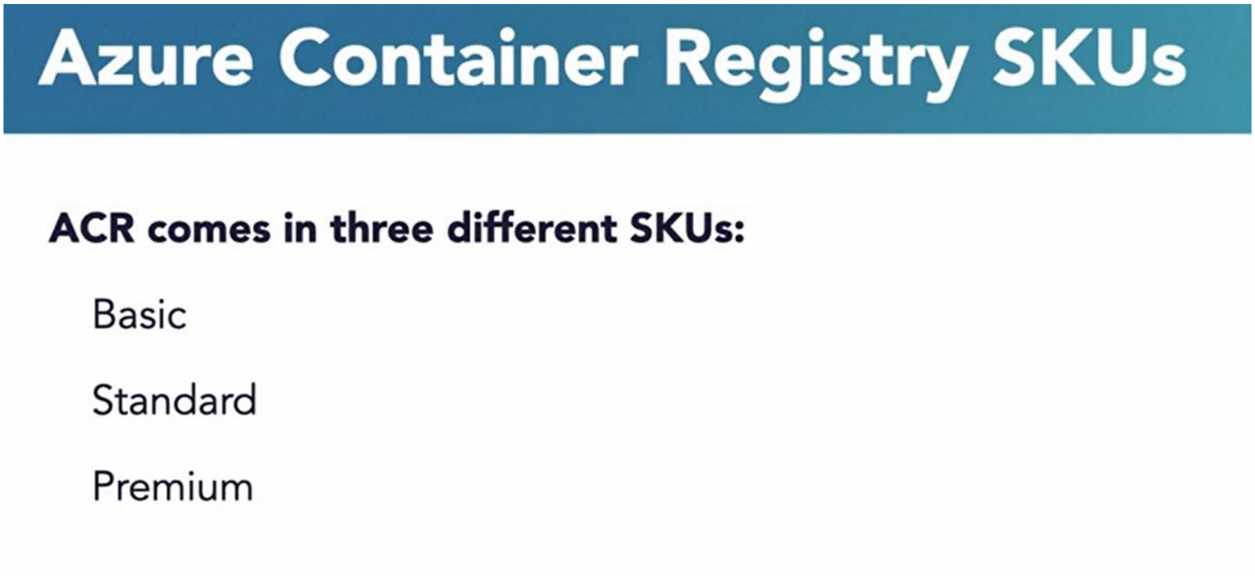
Deploy an AKS cluster with the integrations with ASC Standard enabled.

2.4 Manage access to Azure Container Registry



What Is Azure Container Registry?

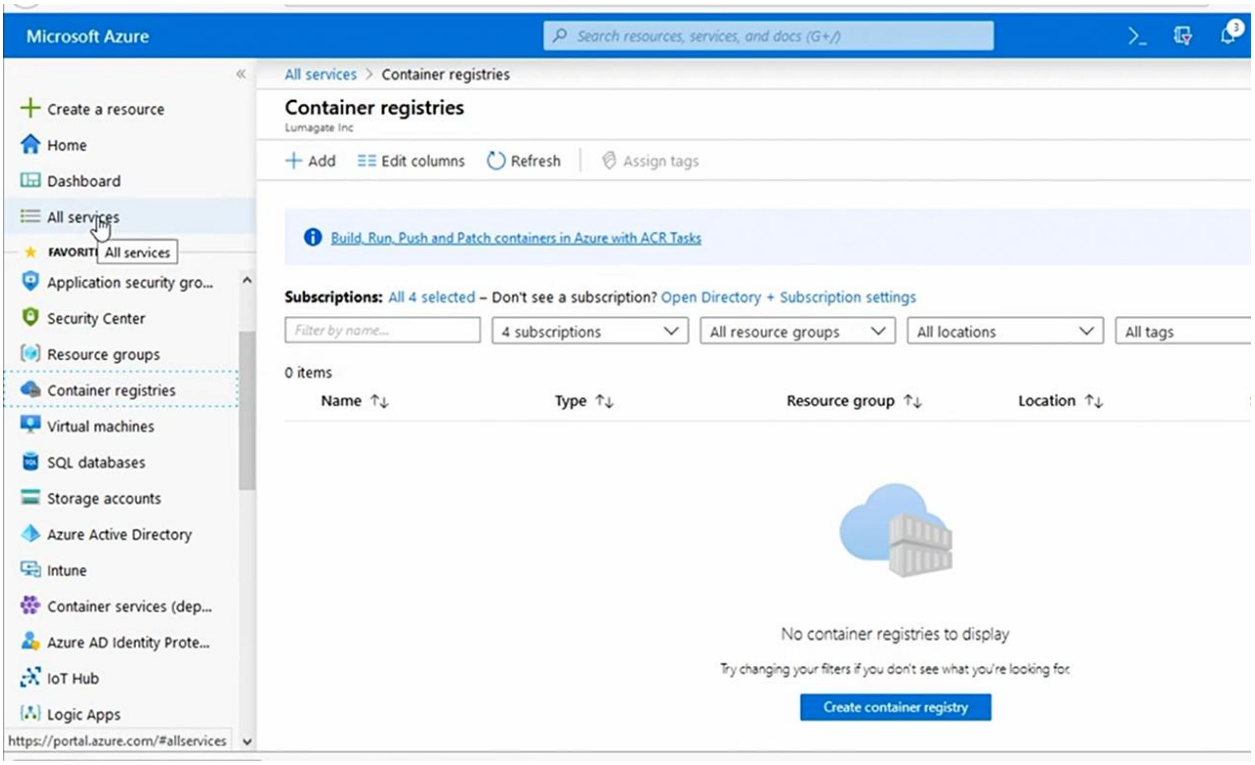
A managed, private Docker registry service based on the open-source Docker Registry for storing and managing your private Docker container images



Azure Container Registry SKUs

ACR comes in three different SKUs:

- Basic
- Standard
- Premium

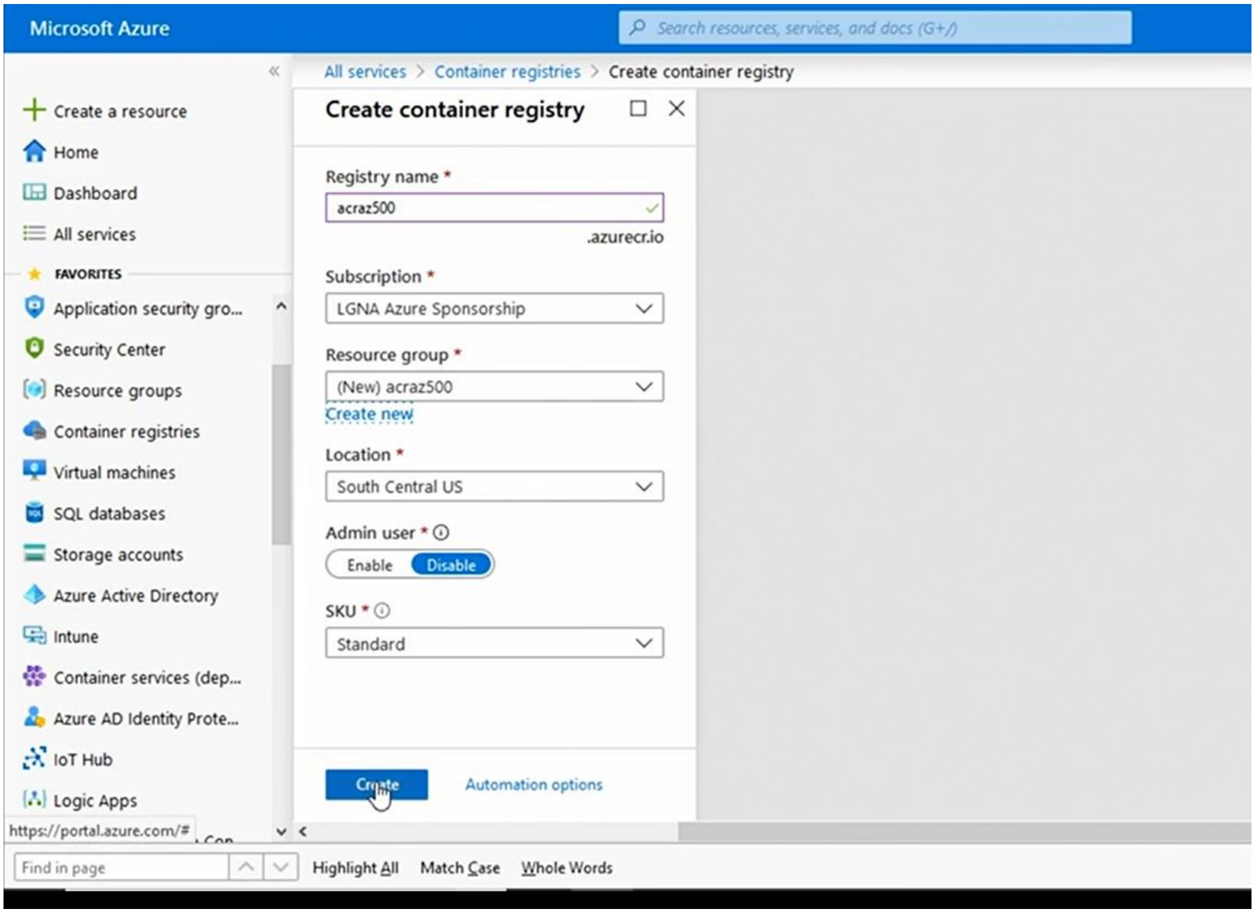


Subscriptions: All 4 selected – Don't see a subscription? Open Directory + Subscription settings

No container registries to display

Try changing your filters if you don't see what you're looking for.

Creating a Container Registry



All services > Container registries > Create container registry

Create container registry

Registry name * acraz500 .azurecr.io

Subscription * LGNA Azure Sponsorship

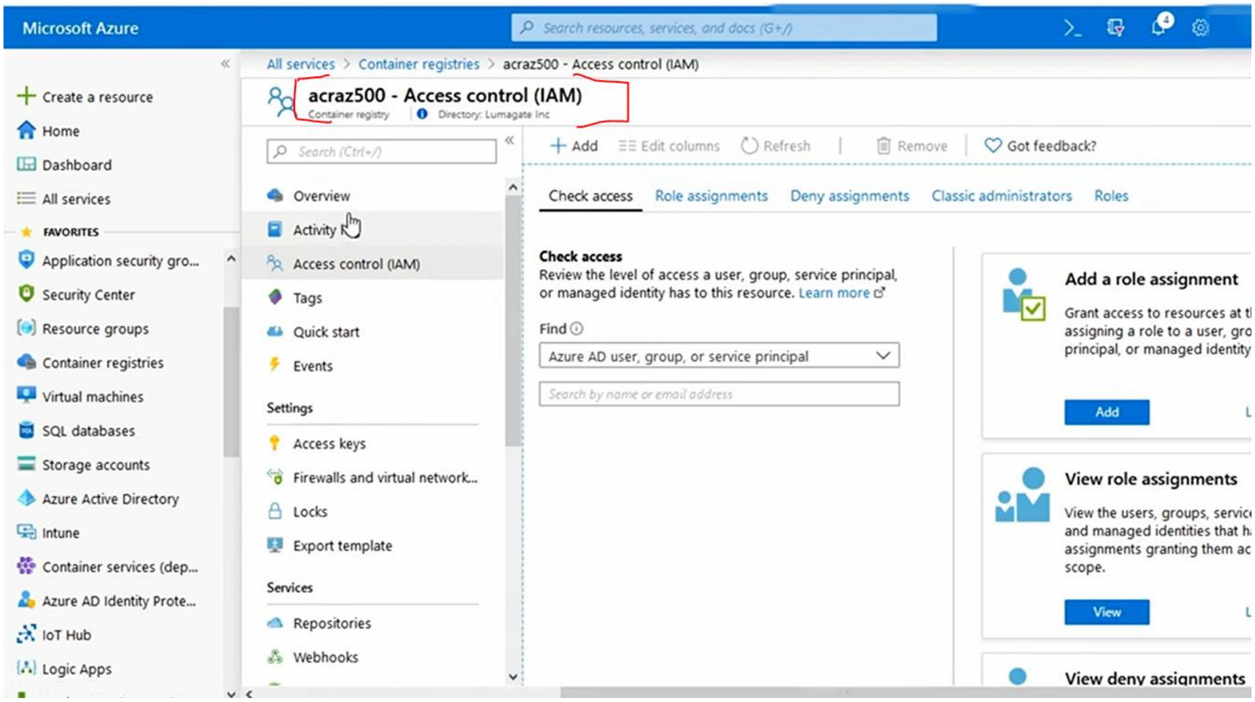
Resource group * (New) acraz500

Create new

Location * South Central US

Admin user * Enable [✓ Disable]

SKU * Standard



All services > Container registries > acraz500 - Access control (IAM)

acraz500 - Access control (IAM)

Container registry | Directory: Lumagate Inc

Check access

Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more

Find: Azure AD user, group, or service principal

Search by name or email address

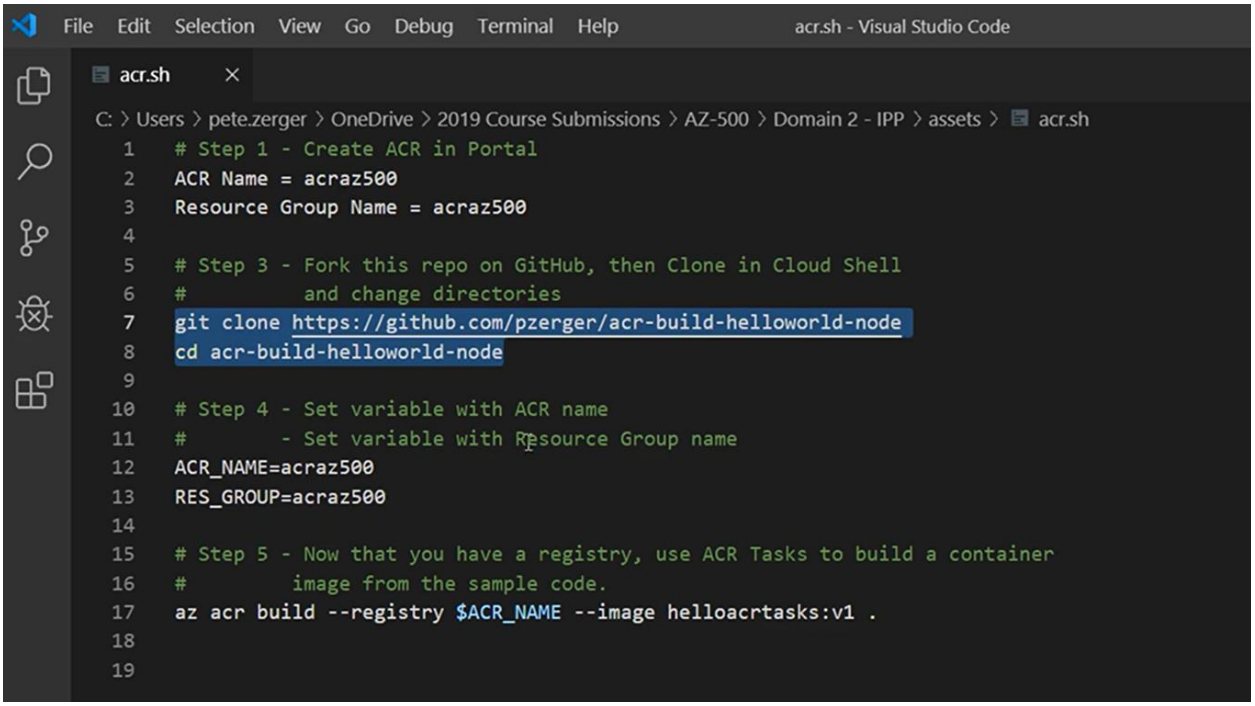
Add a role assignment

Grant access to resources at t assigning a role to a user, gro principal, or managed identity

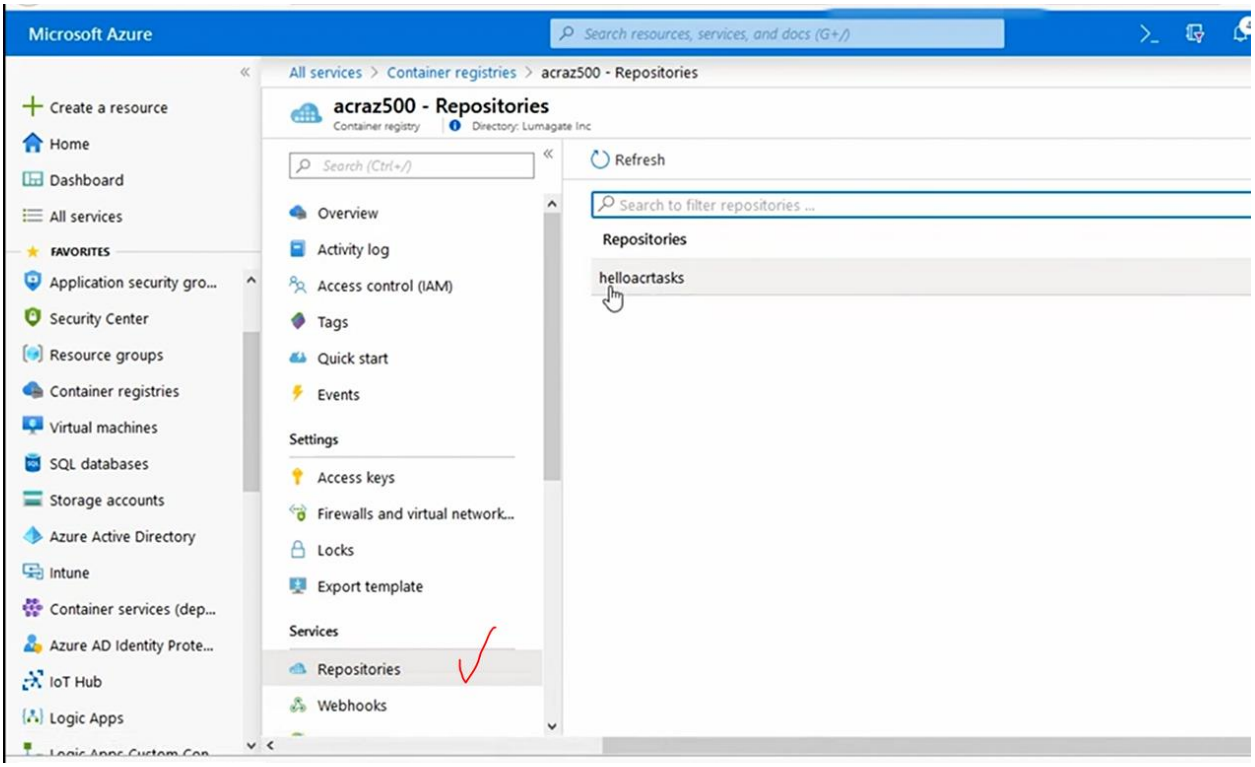
View role assignments

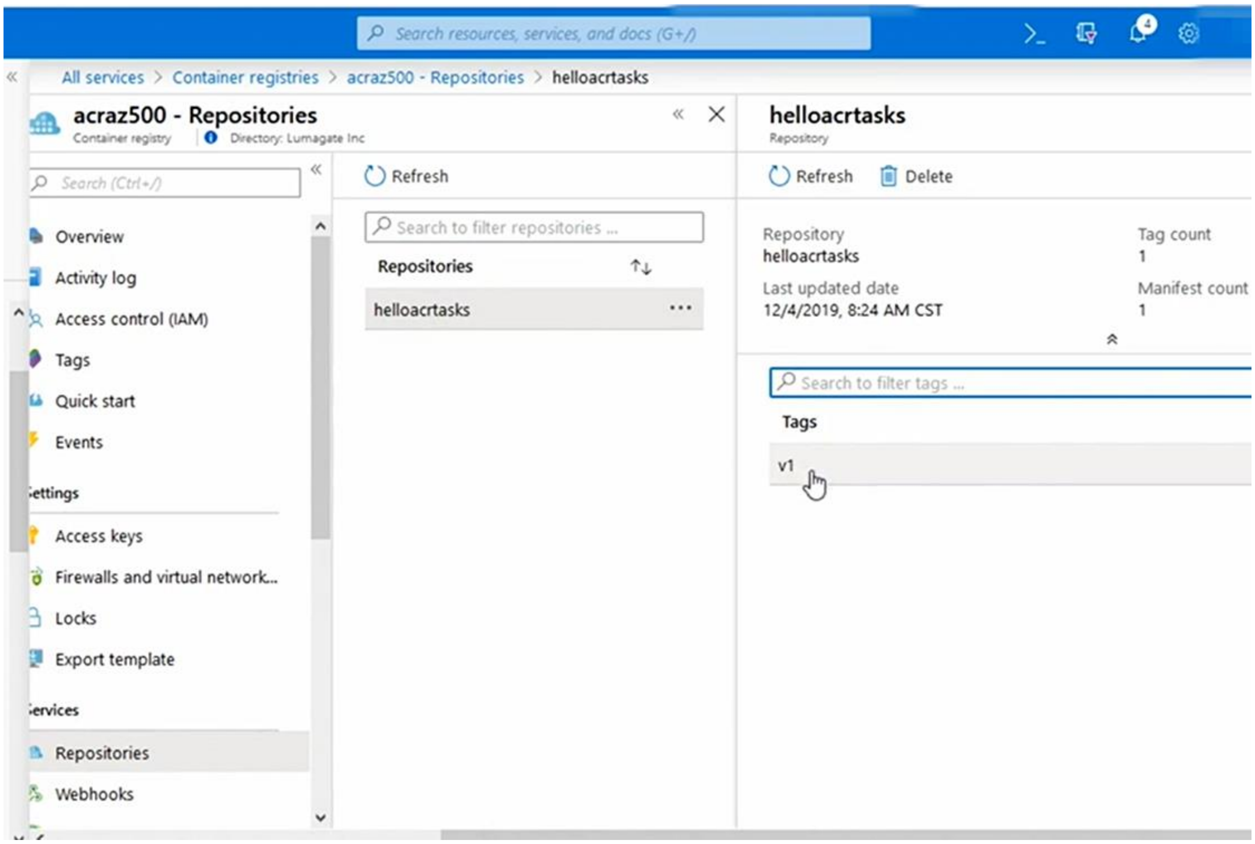
View the users, groups, servic and managed identities that h assignments granting them ac scope.

View deny assignments


File Edit Selection View Go Debug Terminal Help
acr.sh - Visual Studio Code
acr.sh
C: > Users > pete.zerger > OneDrive > 2019 Course Submissions > AZ-500 > Domain 2 - IPP > assets > acr.sh

```
# Step 1 - Create ACR in Portal
ACR Name = acraz500
Resource Group Name = acraz500

# Step 3 - Fork this repo on GitHub, then Clone in Cloud Shell
#         and change directories
git clone https://github.com/pzerger/acr-build-helloworld-node
cd acr-build-helloworld-node

# Step 4 - Set variable with ACR name
#        - Set variable with Resource Group name
ACR_NAME=acraz500
RES_GROUP=acraz500

# Step 5 - Now that you have a registry, use ACR Tasks to build a container
#         image from the sample code.
az acr build --registry $ACR_NAME --image helloacrtasks:v1 .


```





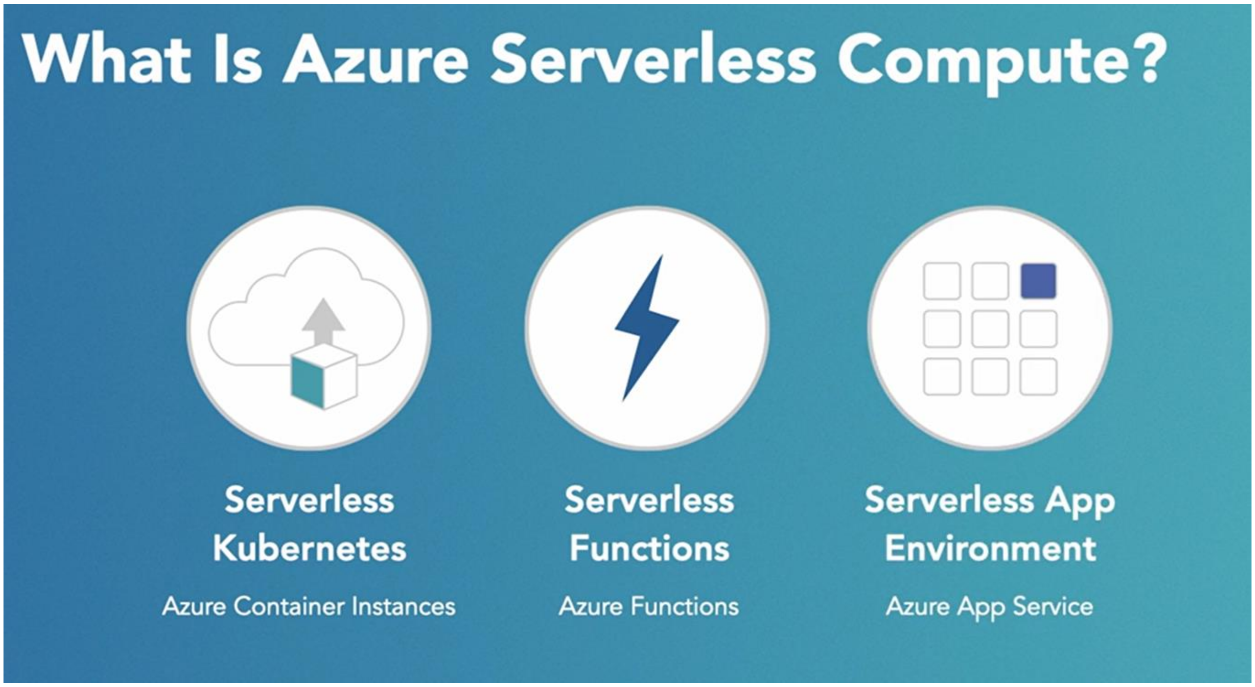
Repository
helloacrtasks

Last updated date
12/4/2019, 8:24 AM CST

Tag count
1

Manifest count
1

2.5 Configure security for serverless compute

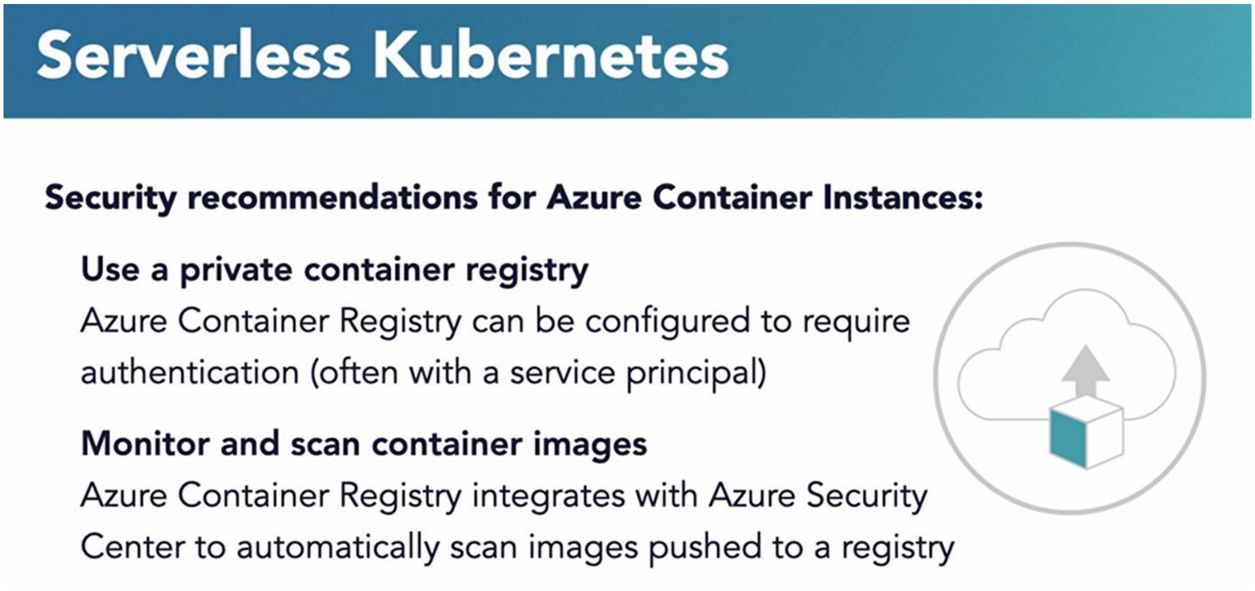


What Is Azure Serverless Compute?

Serverless Kubernetes
Azure Container Instances

Serverless Functions
Azure Functions

Serverless App Environment
Azure App Service

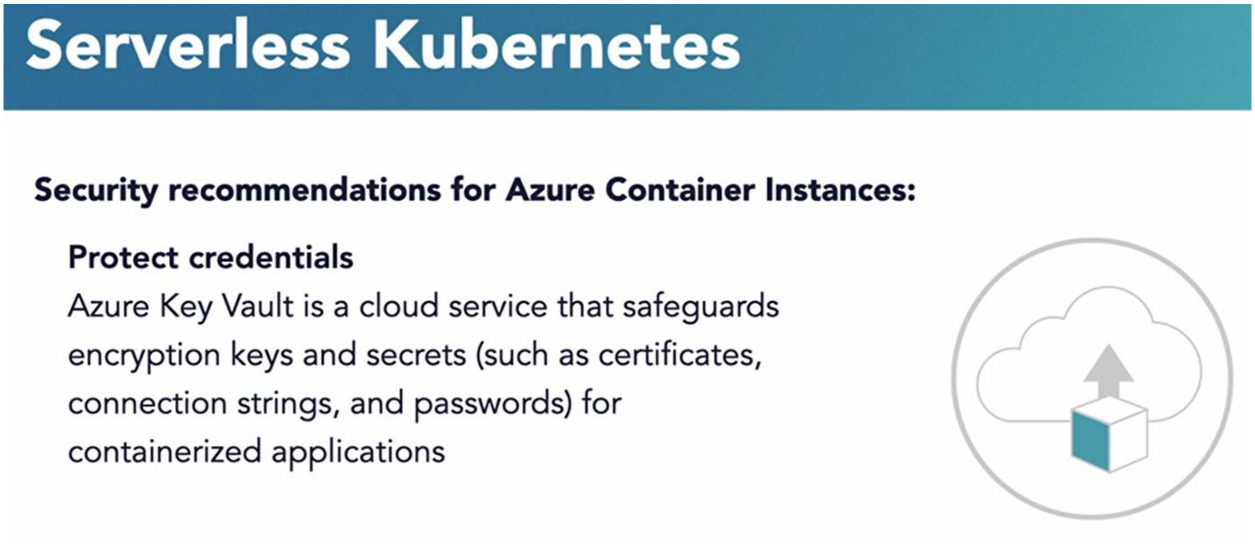


Serverless Kubernetes

Security recommendations for Azure Container Instances:

Use a private container registry
Azure Container Registry can be configured to require authentication (often with a service principal)

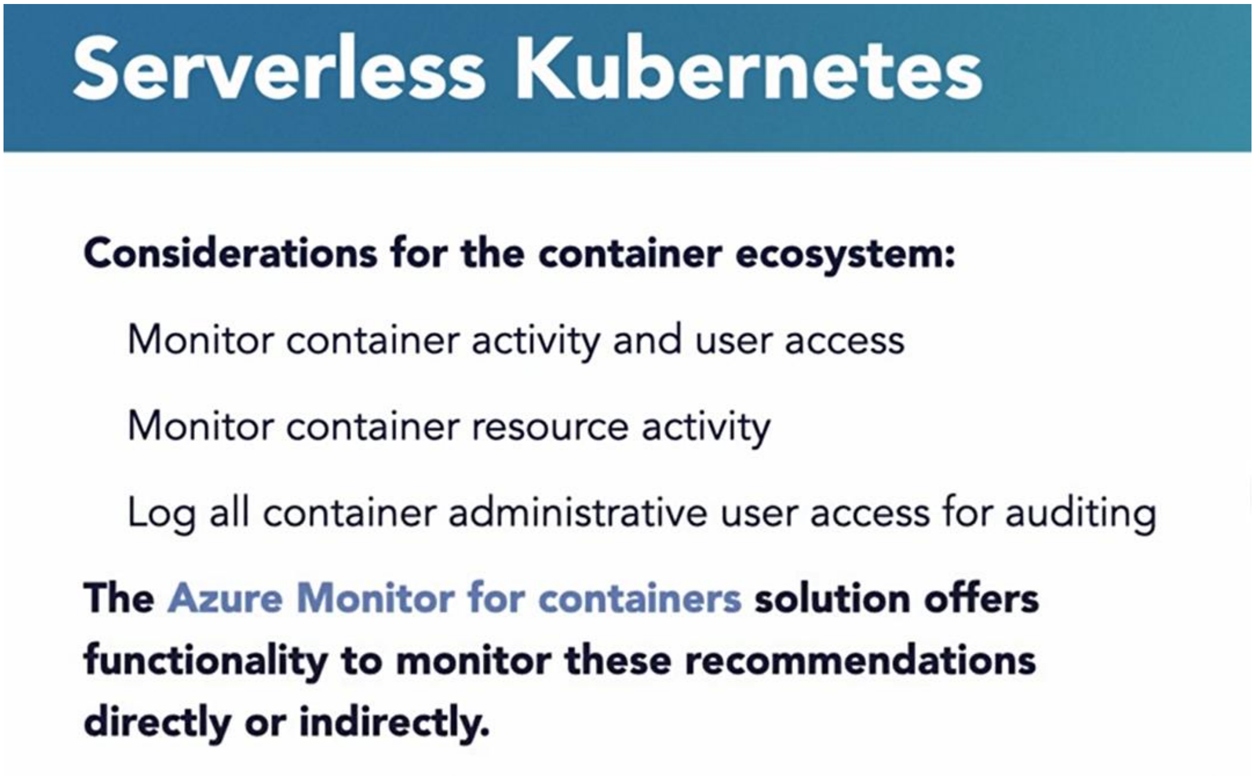
Monitor and scan container images
Azure Container Registry integrates with Azure Security Center to automatically scan images pushed to a registry



Serverless Kubernetes

Security recommendations for Azure Container Instances:

Protect credentials
Azure Key Vault is a cloud service that safeguards encryption keys and secrets (such as certificates, connection strings, and passwords) for containerized applications



Serverless Kubernetes

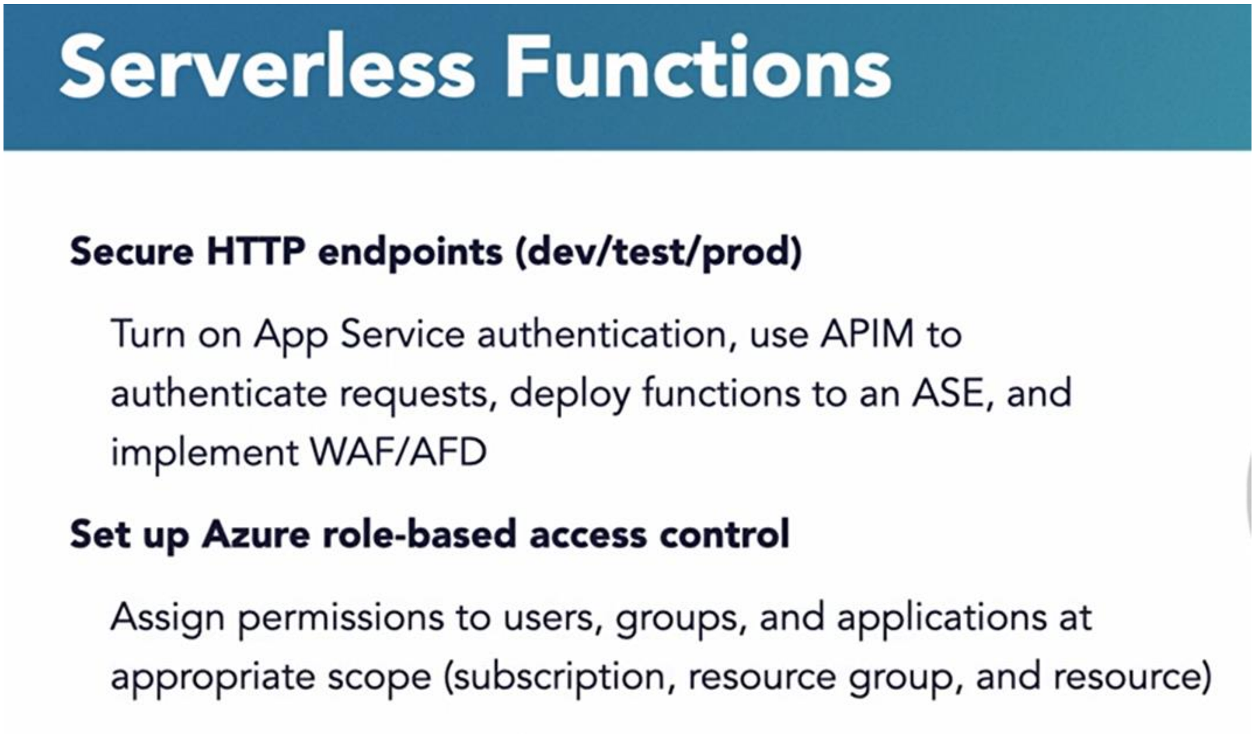
Considerations for the container ecosystem:

Monitor container activity and user access

Monitor container resource activity

Log all container administrative user access for auditing

The Azure Monitor for containers solution offers functionality to monitor these recommendations directly or indirectly.



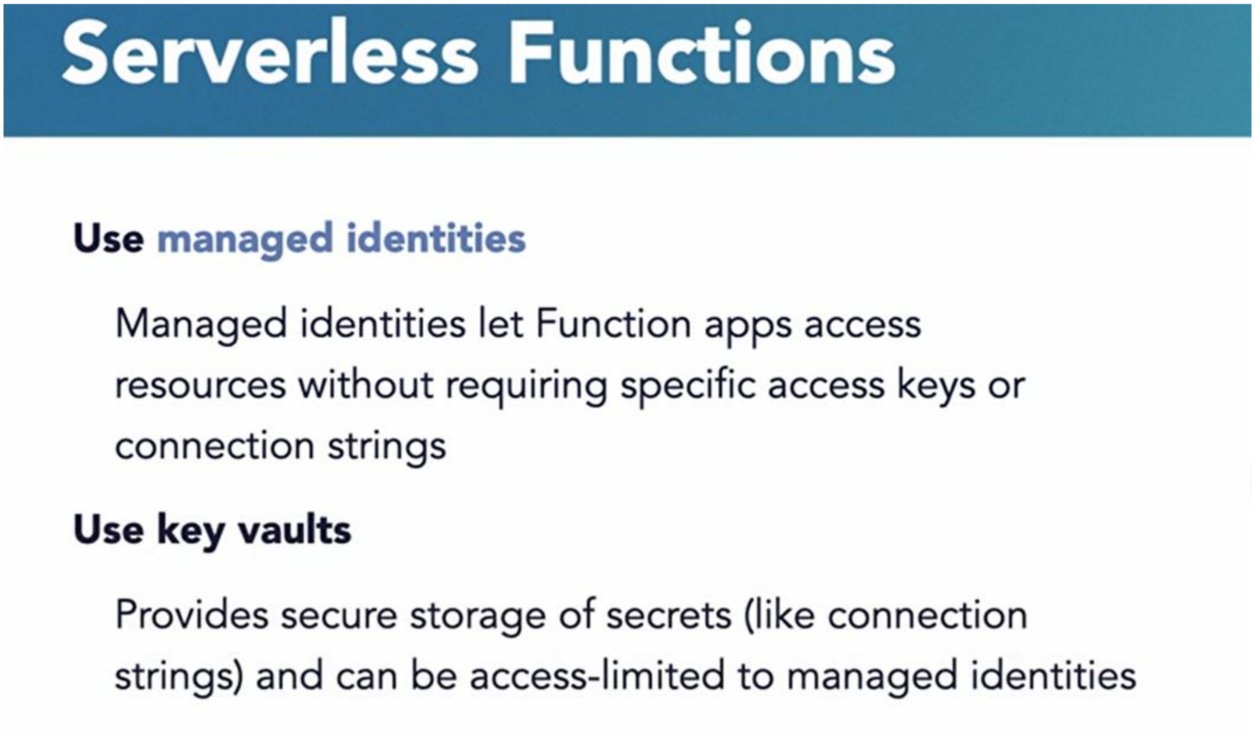
Serverless Functions

Secure HTTP endpoints (dev/test/prod)

Turn on App Service authentication, use APIM to authenticate requests, deploy functions to an ASE, and implement WAF/AFD

Set up Azure role-based access control

Assign permissions to users, groups, and applications at appropriate scope (subscription, resource group, and resource)



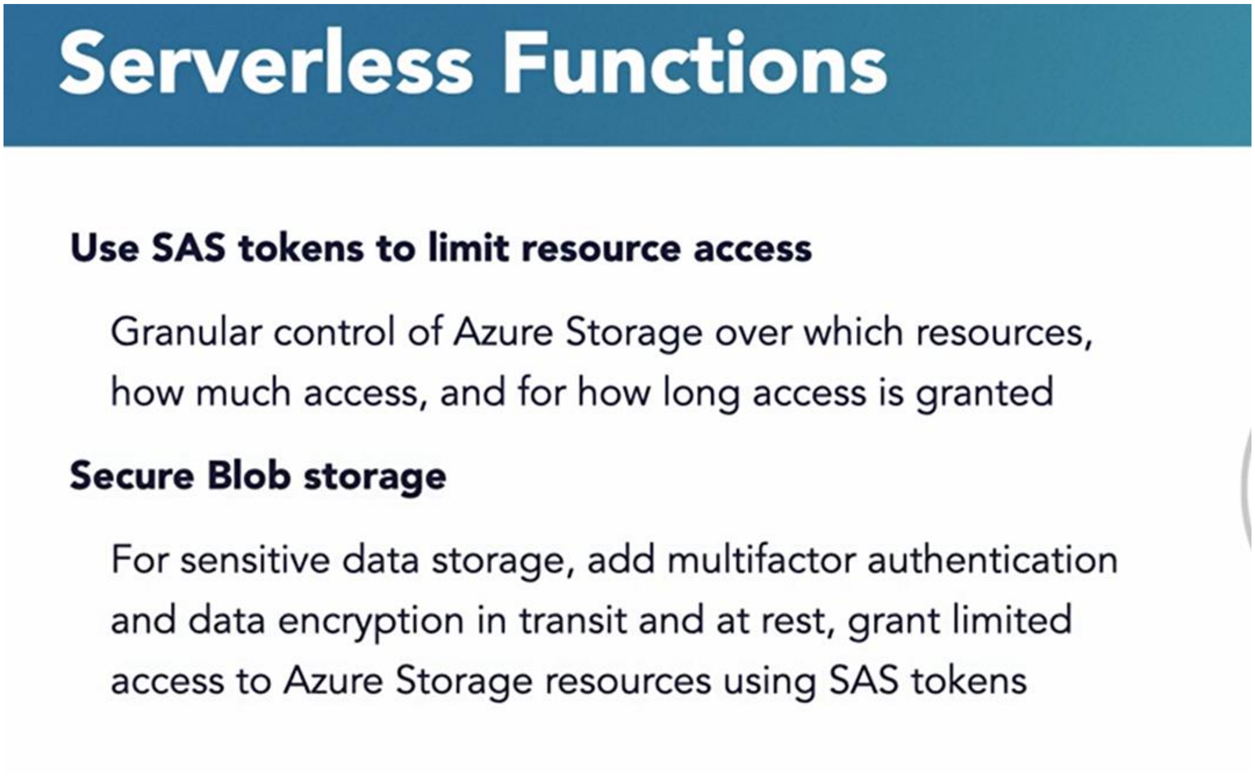
Serverless Functions

Use managed identities

Managed identities let Function apps access resources without requiring specific access keys or connection strings

Use key vaults

Provides secure storage of secrets (like connection strings) and can be access-limited to managed identities



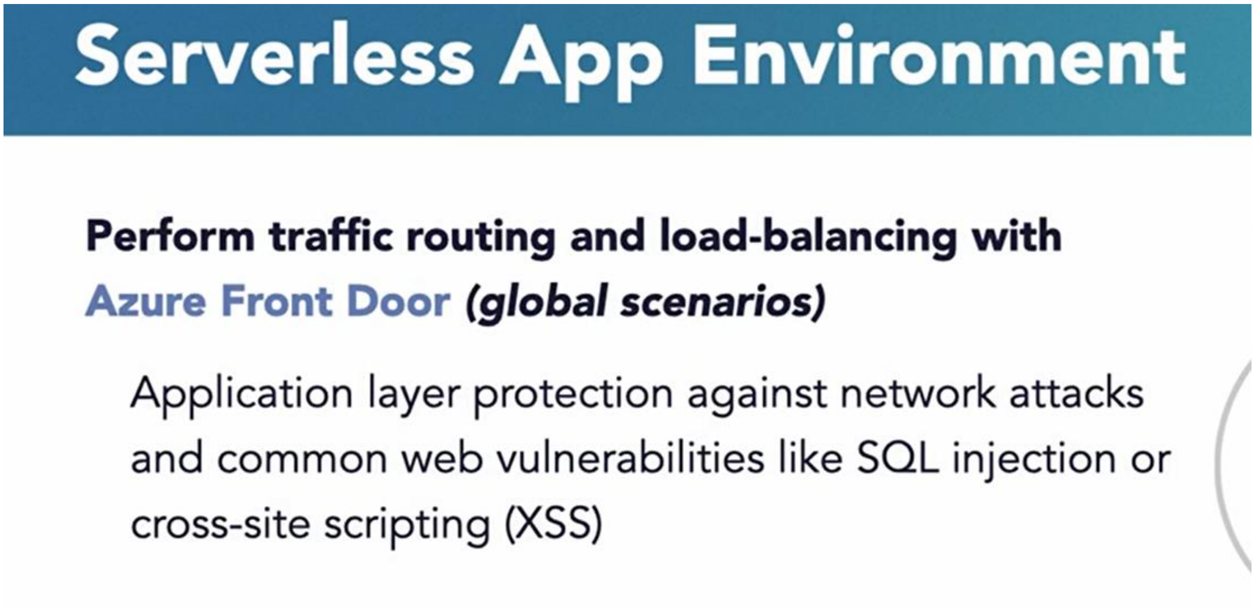
Serverless Functions

Use SAS tokens to limit resource access

Granular control of Azure Storage over which resources, how much access, and for how long access is granted

Secure Blob storage

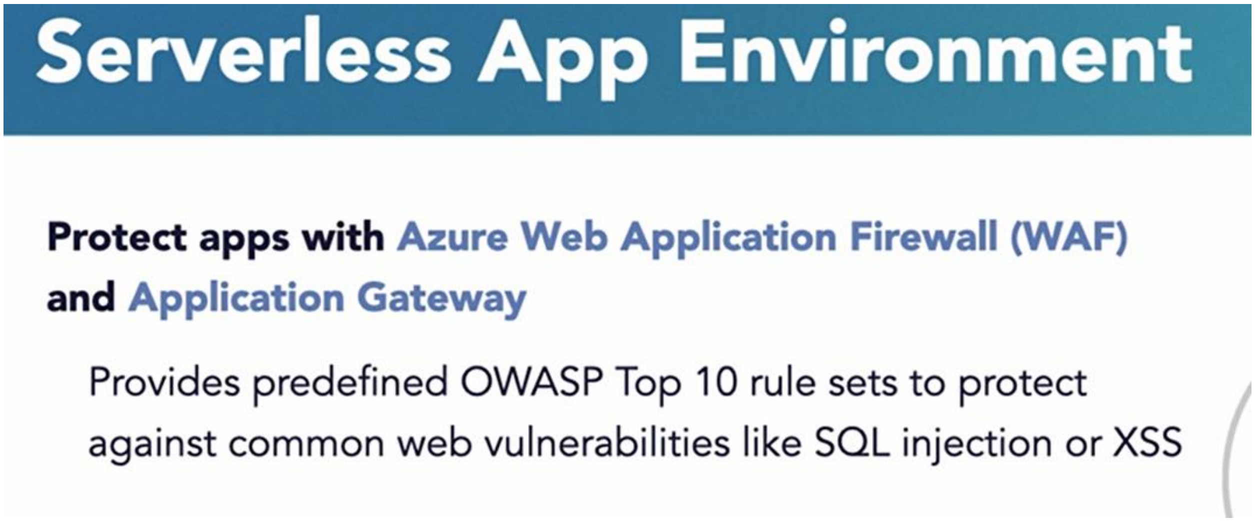
For sensitive data storage, add multifactor authentication and data encryption in transit and at rest, grant limited access to Azure Storage resources using SAS tokens



Serverless App Environment

Perform traffic routing and load-balancing with Azure Front Door *(global scenarios)*

Application layer protection against network attacks and common web vulnerabilities like SQL injection or cross-site scripting (XSS)



Serverless App Environment

Protect apps with Azure Web Application Firewall (WAF) and Application Gateway

Provides predefined OWASP Top 10 rule sets to protect against common web vulnerabilities like SQL injection or XSS

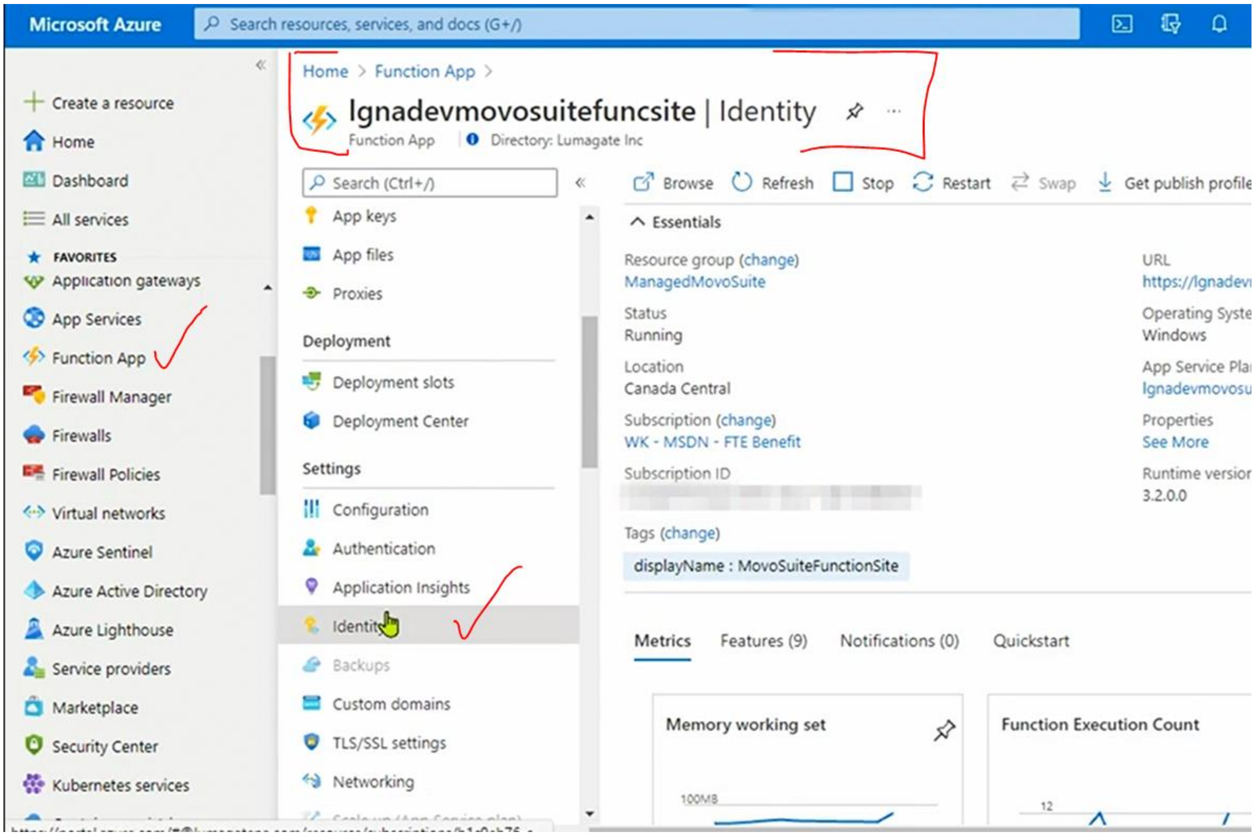
Serverless App Environment

Protect apps with Azure Web Application Firewall (WAF) and Application Gateway

Provides predefined OWASP Top 10 rule sets to protect against common web vulnerabilities like SQL injection or XSS

Protect apps with Azure Firewall

Centrally creates, enforces, and logs application and network connectivity policies across subscriptions and virtual networks



lgnadevmovosuitefuncsite | Identity

Resource group (change)
ManagedMovoSuite

Status
Running

Location
Canada Central

Subscription (change)
WK - MSDN - FTE Benefit

Subscription ID
[redacted]

Tags (change)
displayName : MovoSuiteFunctionSite

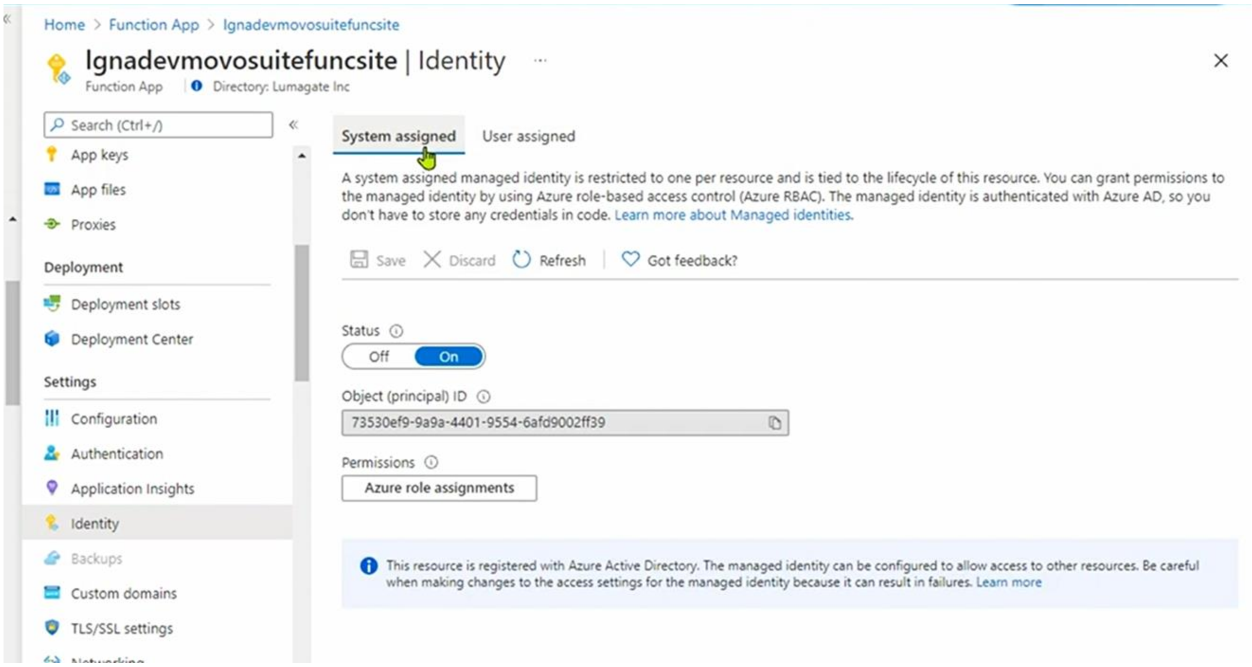
URL
https://lgnadev

Operating Syste
Windows

App Service Pla
lgnadevmovosu

Properties
See More

Runtime versior
3.2.0.0



Ignadevmovosuitefuncsite | Identity

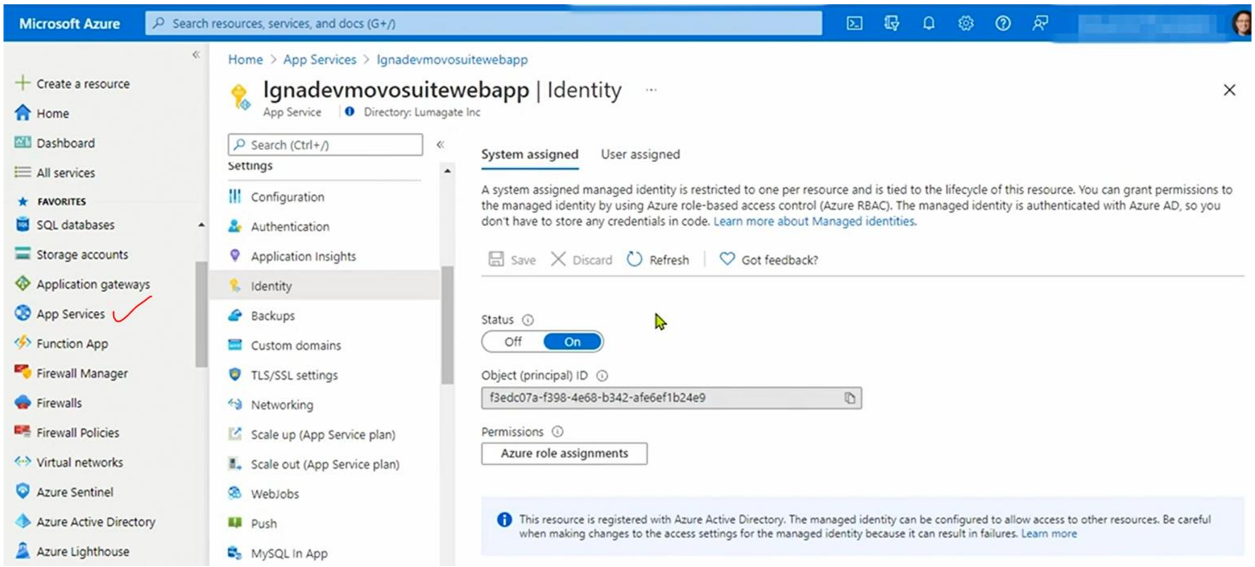
A system assigned managed identity is restricted to one per resource and is tied to the lifecycle of this resource. You can grant permissions to the managed identity by using Azure role-based access control (Azure RBAC). The managed identity is authenticated with Azure AD, so you don't have to store any credentials in code. Learn more about Managed identities.

Status: Off [✓ On]

Object (principal) ID: 73530ef9-9a9a-4401-9554-6afd9002ff39

Permissions: Azure role assignments

This resource is registered with Azure Active Directory. The managed identity can be configured to allow access to other resources. Be careful when making changes to the access settings for the managed identity because it can result in failures. Learn more



Ignadevmovosuitewebapp | Identity

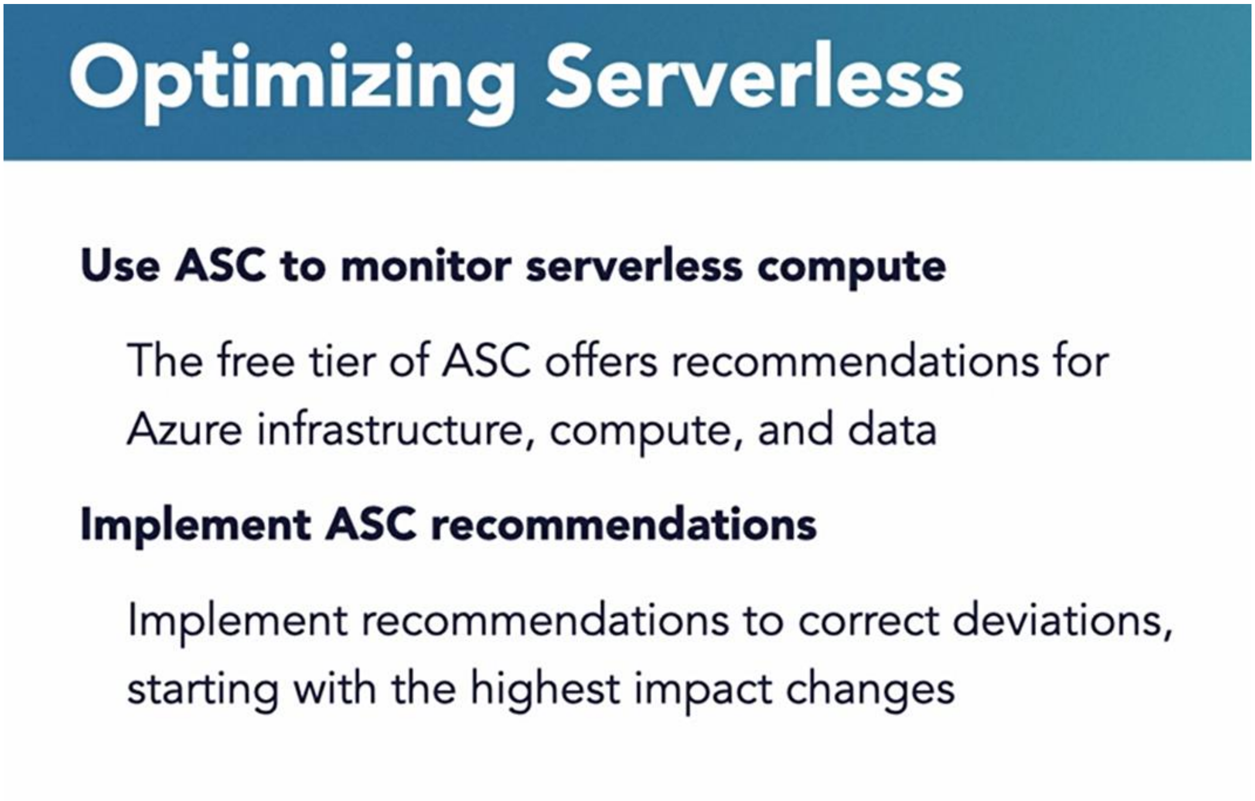
A system assigned managed identity is restricted to one per resource and is tied to the lifecycle of this resource. You can grant permissions to the managed identity by using Azure role-based access control (Azure RBAC). The managed identity is authenticated with Azure AD, so you don't have to store any credentials in code. Learn more about Managed identities.

Status: Off [✓ On]

Object (principal) ID: f3edc07a-f398-4e68-b342-afe6ef1b24e9

Permissions: Azure role assignments

This resource is registered with Azure Active Directory. The managed identity can be configured to allow access to other resources. Be careful when making changes to the access settings for the managed identity because it can result in failures. Learn more



Optimizing Serverless

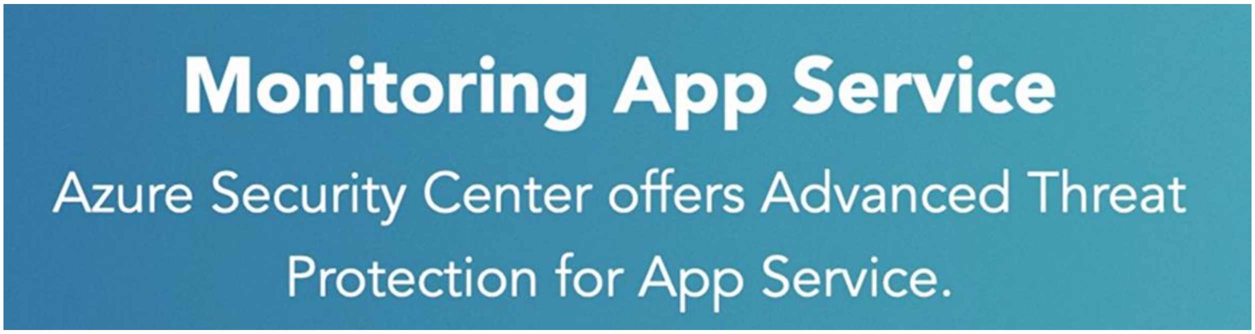
Use ASC to monitor serverless compute

The free tier of ASC offers recommendations for Azure infrastructure, compute, and data

Implement ASC recommendations

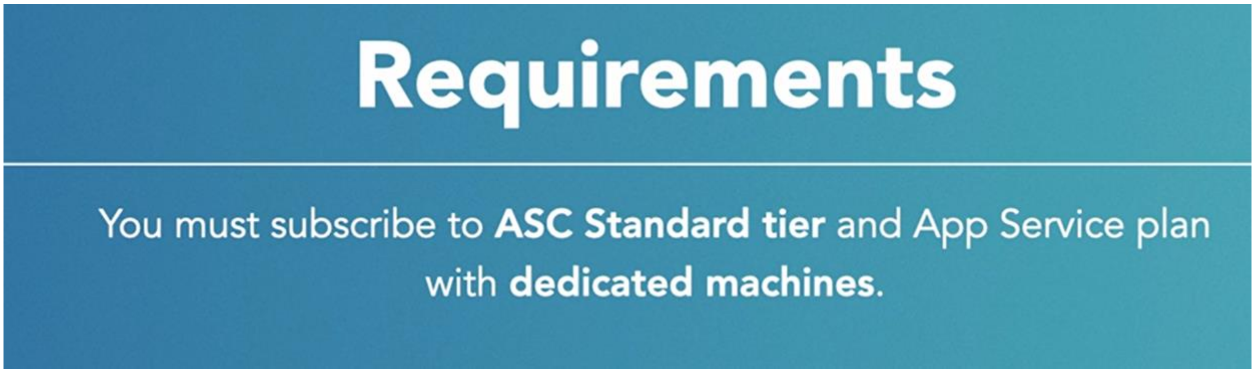
Implement recommendations to correct deviations, starting with the highest impact changes

2.6 Configure security for Azure App Service



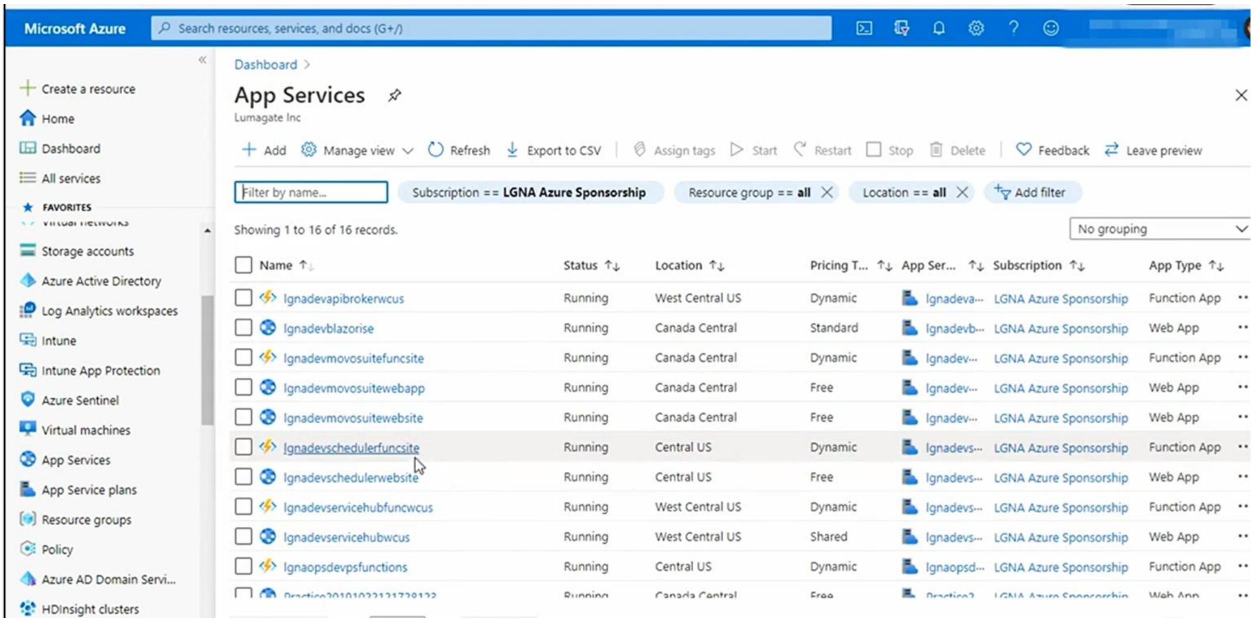
Monitoring App Service

Azure Security Center offers Advanced Threat Protection for App Service.



Requirements

You must subscribe to **ASC Standard tier** and App Service plan with **dedicated machines**.



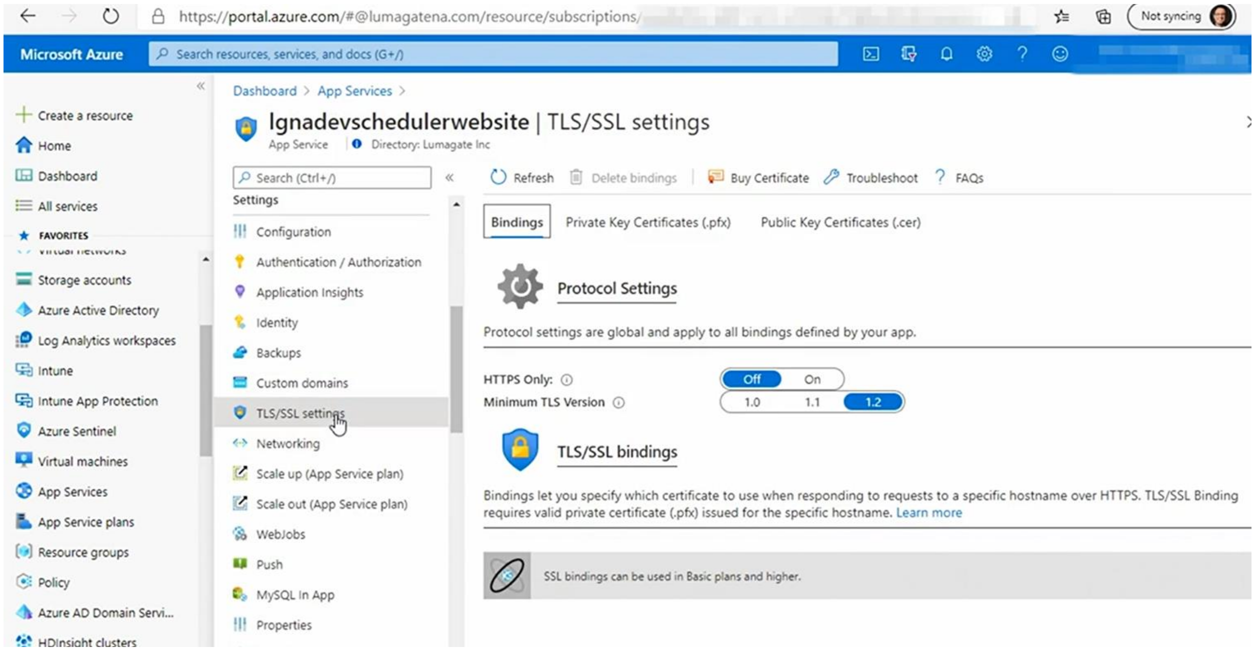
App Services

Lumagate Inc

Subscription == **LGNA Azure Sponsorship** | Resource group == **all** | Location == **all**

Showing 1 to 16 of 16 records.

Name	Status	Location	Pricing T...	App Ser...	Subscription	App Type
lgnadevapibrokerwcus	Running	West Central US	Dynamic	lgnadeva...	LGNA Azure Sponsorship	Function App
lgnadevblazorise	Running	Canada Central	Standard	lgnadevb...	LGNA Azure Sponsorship	Web App
lgnadevmovosuitefuncsite	Running	Canada Central	Dynamic	lgnadev...	LGNA Azure Sponsorship	Function App
lgnadevmovosuitewebapp	Running	Canada Central	Free	lgnadev...	LGNA Azure Sponsorship	Web App
lgnadevmovosuitewebsite	Running	Canada Central	Free	lgnadev...	LGNA Azure Sponsorship	Web App
lgnadevschedulerfuncsite	Running	Central US	Dynamic	lgnadevs...	LGNA Azure Sponsorship	Function App
lgnadevschedulerwebsite	Running	Central US	Free	lgnadevs...	LGNA Azure Sponsorship	Web App
lgnadevservicehubfuncwcus	Running	West Central US	Dynamic	lgnadevs...	LGNA Azure Sponsorship	Function App
lgnadevservicehubwcus	Running	West Central US	Shared	lgnadevs...	LGNA Azure Sponsorship	Web App
lgnaopsdevpsfunctions	Running	Central US	Dynamic	lgnaopsd...	LGNA Azure Sponsorship	Function App
Practice2019102212172812?	Running	Canada Central	Free	Practice2	LGNA Azure Sponsorship	Web App



lgnadevschedulerwebsite | TLS/SSL settings

App Service · Directory: Lumagate Inc

Protocol Settings

Protocol settings are global and apply to all bindings defined by your app.

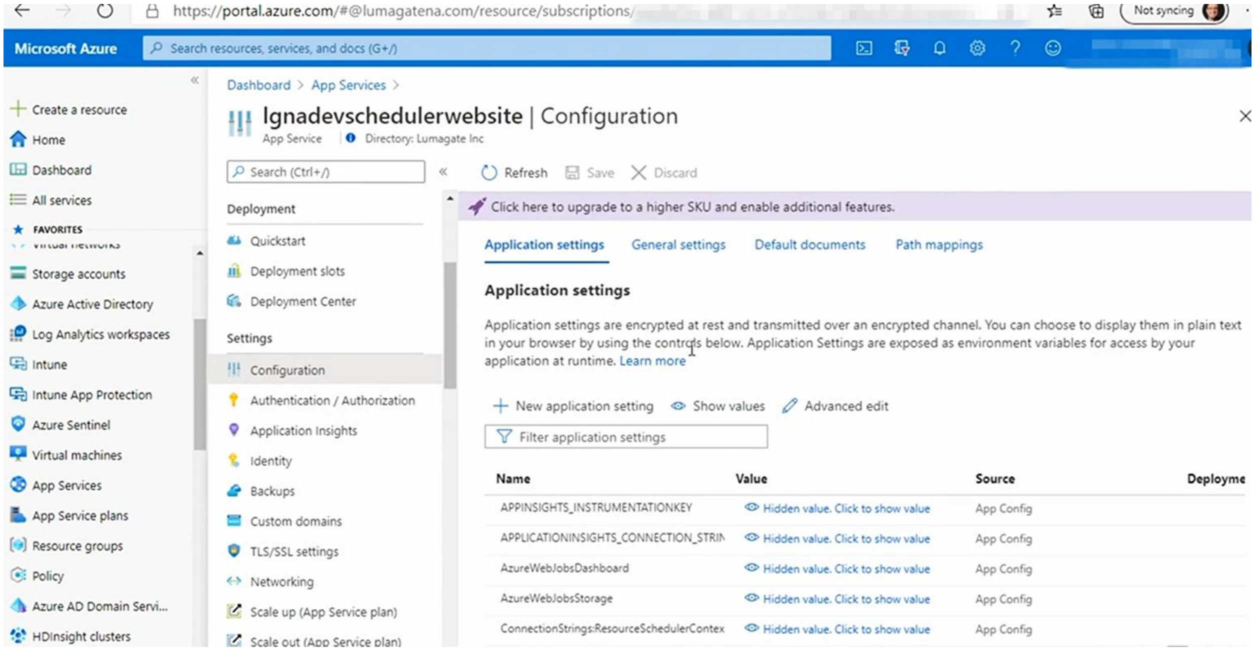
HTTPS Only: [✓ Off] On

Minimum TLS Version: 1.0 1.1 [✓ 1.2]

TLS/SSL bindings

Bindings let you specify which certificate to use when responding to requests to a specific hostname over HTTPS. TLS/SSL Binding requires valid private certificate (.pfx) issued for the specific hostname. Learn more

SSL bindings can be used in Basic plans and higher.



lgnadevschedulerwebsite | Configuration

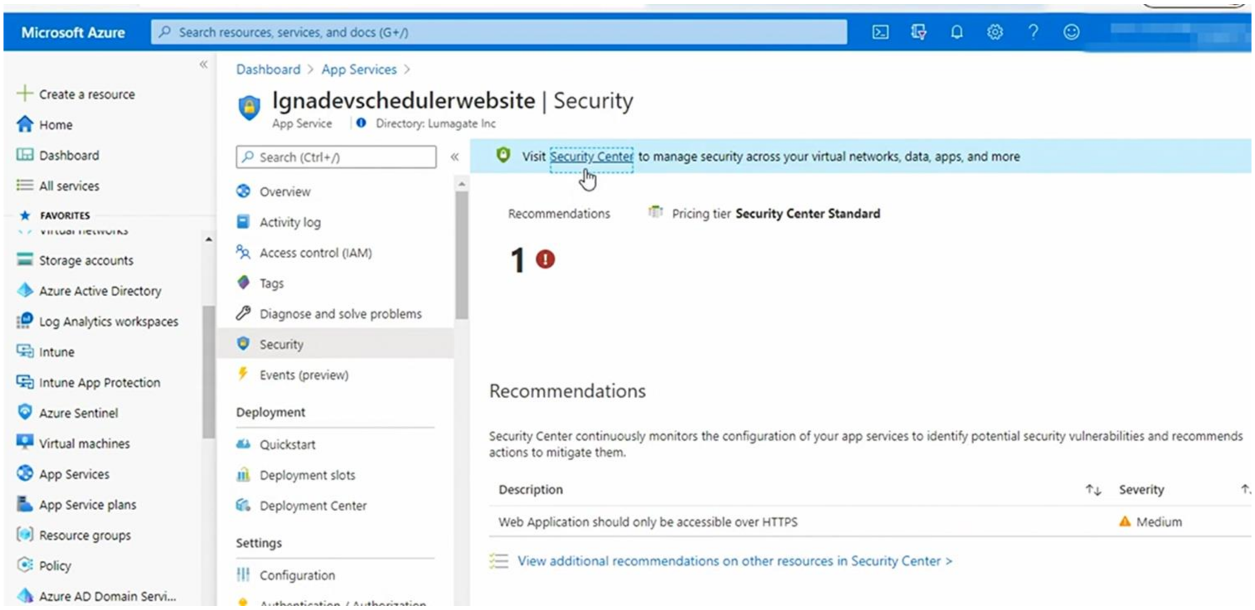
App Service | Directory: Lumagate Inc

Click here to upgrade to a higher SKU and enable additional features.

Application settings

Application settings are encrypted at rest and transmitted over an encrypted channel. You can choose to display them in plain text in your browser by using the controls below. Application Settings are exposed as environment variables for access by your application at runtime. Learn more

Name	Value	Source	Deployme
APPINSIGHTS_INSTRUMENTATIONKEY	Hidden value. Click to show value	App Config	
APPLICATIONINSIGHTS_CONNECTION_STRIN	Hidden value. Click to show value	App Config	
AzureWebJobsDashboard	Hidden value. Click to show value	App Config	
AzureWebJobsStorage	Hidden value. Click to show value	App Config	
ConnectionStrings:ResourceSchedulerContex	Hidden value. Click to show value	App Config	



lgnadevschedulerwebsite | Security

App Service | Directory: Lumagate Inc

Visit Security Center to manage security across your virtual networks, data, apps, and more

Recommendations — Pricing tier **Security Center Standard**

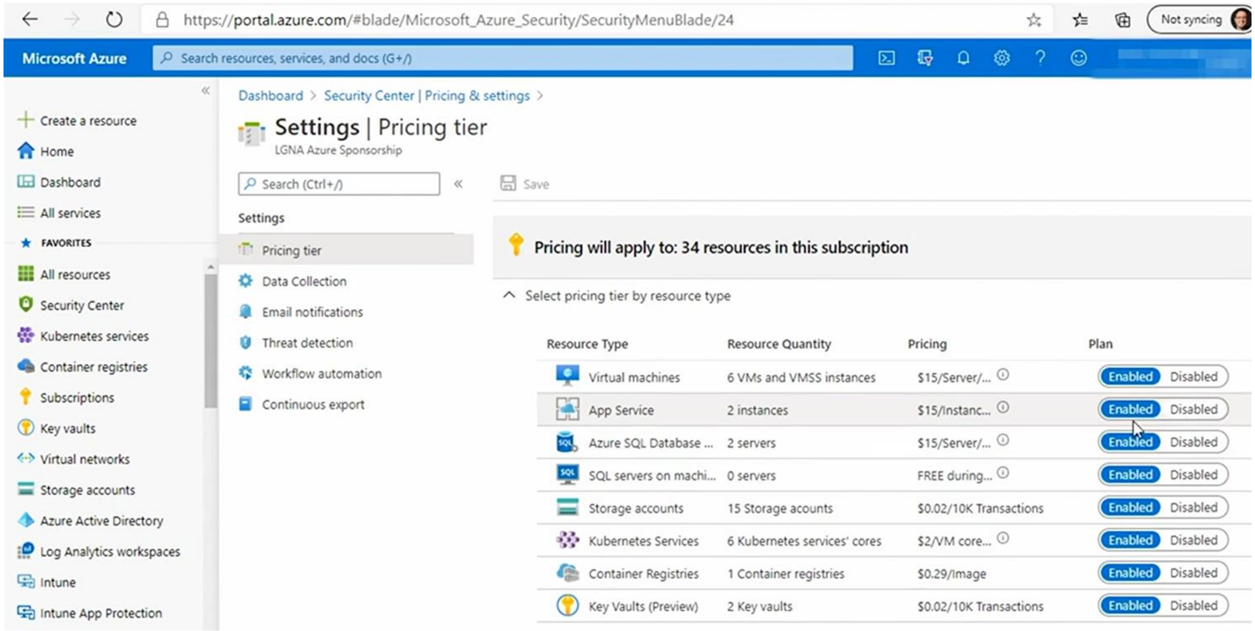
1

Recommendations

Security Center continuously monitors the configuration of your app services to identify potential security vulnerabilities and recommends actions to mitigate them.

Description	Severity
Web Application should only be accessible over HTTPS	Medium

View additional recommendations on other resources in Security Center >



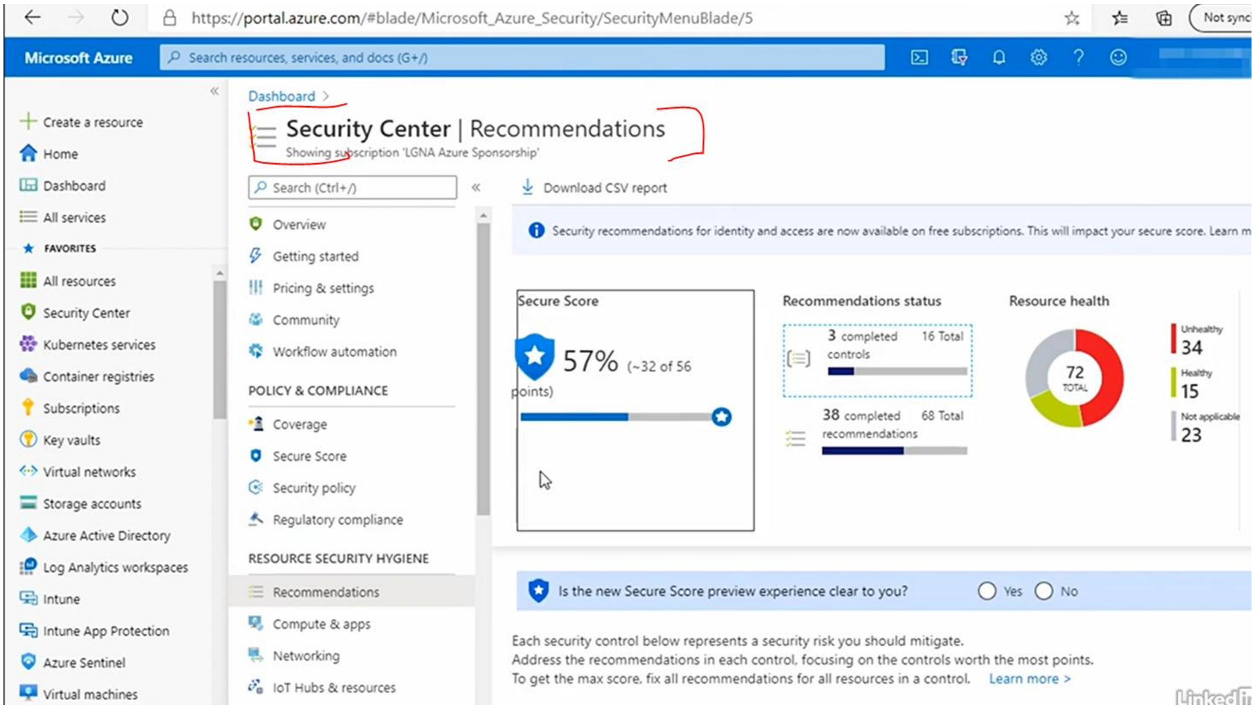
Settings | Pricing tier

LGNA Azure Sponsorship

Pricing will apply to: 34 resources in this subscription

Select pricing tier by resource type

Resource Type	Resource Quantity	Pricing	Plan
Virtual machines	6 VMs and VMSS instances	$15/Server/...	Enabled Disabled
App Service	2 instances	$15/Instanc...	Enabled Disabled
Azure SQL Database ...	2 servers	$15/Server/...	Enabled Disabled
SQL servers on machi...	0 servers	FREE during...	Enabled Disabled
Storage accounts	15 Storage acounts	$0.02/10K Transactions	Enabled Disabled
Kubernetes Services	6 Kubernetes services' cores	$2/VM core...	Enabled Disabled
Container Registries	1 Container registries	$0.29/Image	Enabled Disabled
Key Vaults (Preview)	2 Key vaults	$0.02/10K Transactions	Enabled Disabled



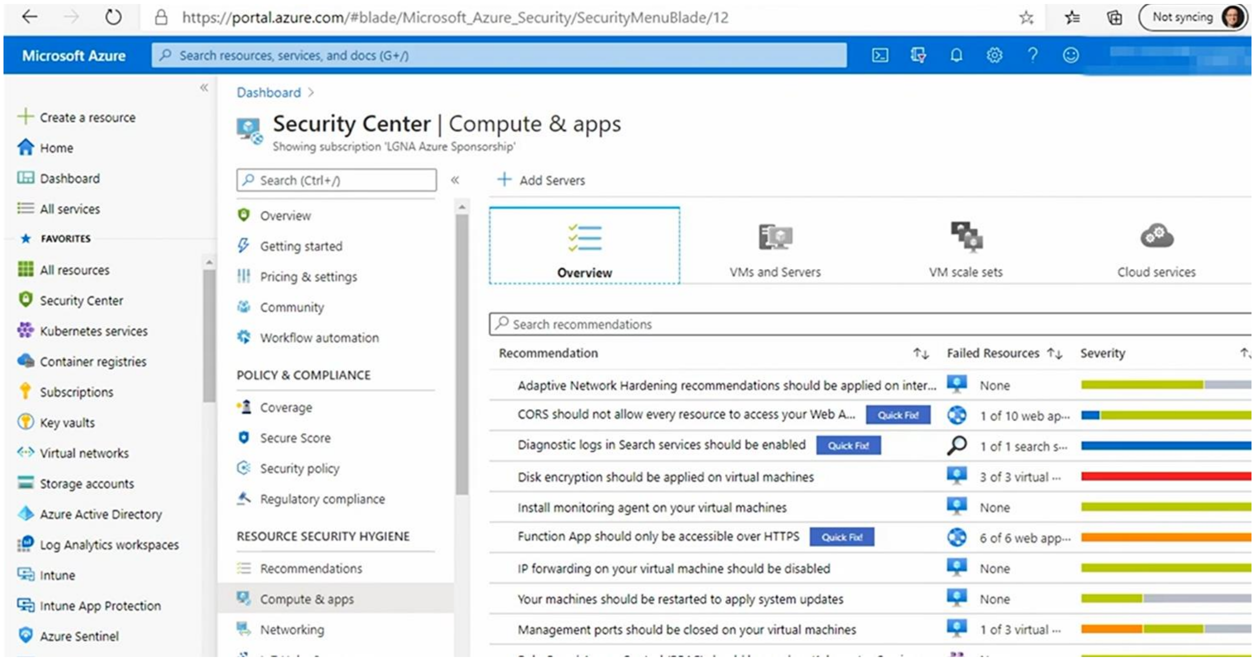
Security Center | Recommendations

Showing subscription 'LGNA Azure Sponsorship'

Security recommendations for identity and access are now available on free subscriptions. This will impact your secure score. Learn m

Is the new Secure Score preview experience clear to you? ○ Yes ○ No

Each security control below represents a security risk you should mitigate.
Address the recommendations in each control, focusing on the controls worth the most points.
To get the max score, fix all recommendations for all resources in a control. Learn more >

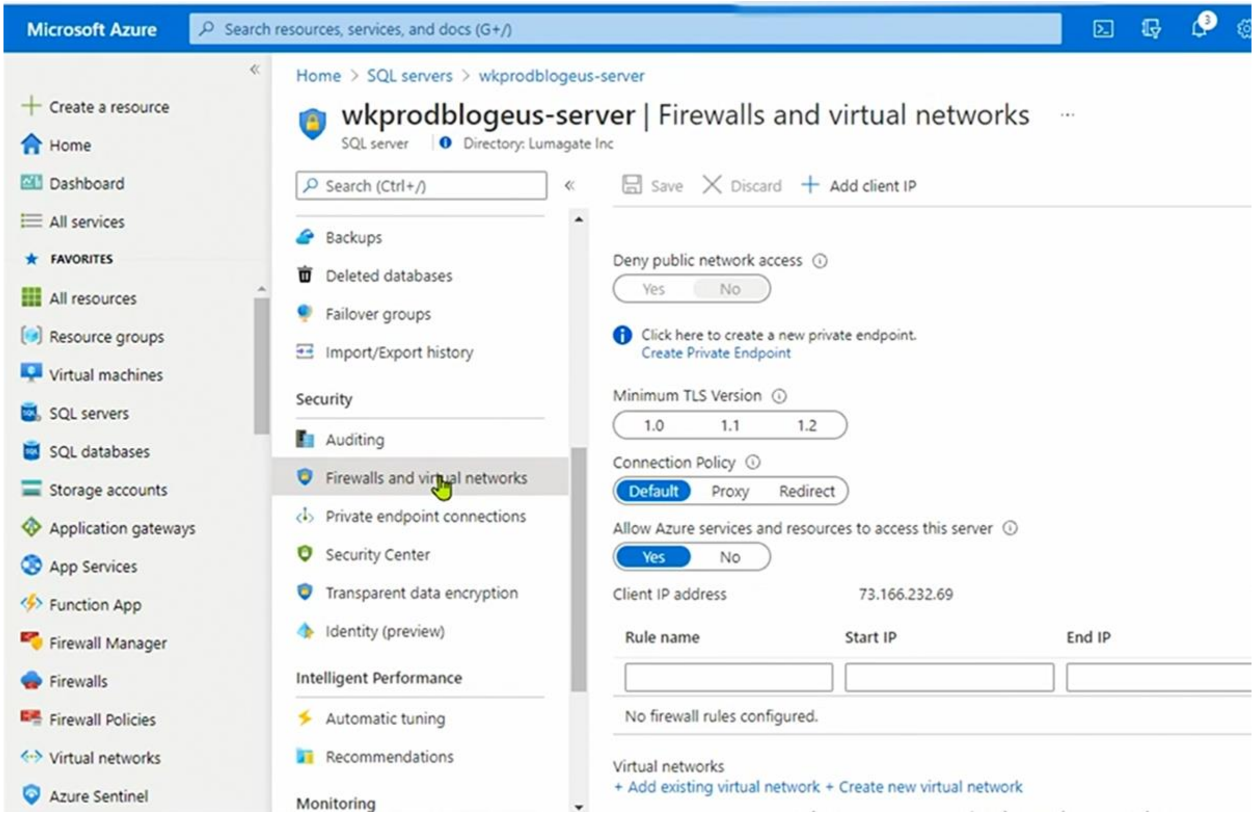


Recommendation	Failed Resources	Severity
Adaptive Network Hardening recommendations should be applied on inter...	None	🟩⬜
CORS should not allow every resource to access your Web A... Quick Fix!	1 of 10 web ap...	🟦🟩
Diagnostic logs in Search services should be enabled Quick Fix!	1 of 1 search s...	🟦
Disk encryption should be applied on virtual machines	3 of 3 virtual ...	🟥
Install monitoring agent on your virtual machines	None	🟩
Function App should only be accessible over HTTPS Quick Fix!	6 of 6 web app...	🟧
IP forwarding on your virtual machine should be disabled	None	🟩
Your machines should be restarted to apply system updates	None	🟩⬜
Management ports should be closed on your virtual machines	1 of 3 virtual ...	🟧🟩⬜

Exam Tip

Be familiar with Azure Security Center features for App Service and how to configure.

2.7 Configure encryption in transit



wkprodblogeus-server | Firewalls and virtual networks

SQL server | Directory: Lumagate Inc

Deny public network access: Yes [✓ No]

Click here to create a new private endpoint. Create Private Endpoint

Minimum TLS Version: 1.0 1.1 1.2

Connection Policy: [✓ Default] Proxy Redirect

Allow Azure services and resources to access this server: [✓ Yes] No

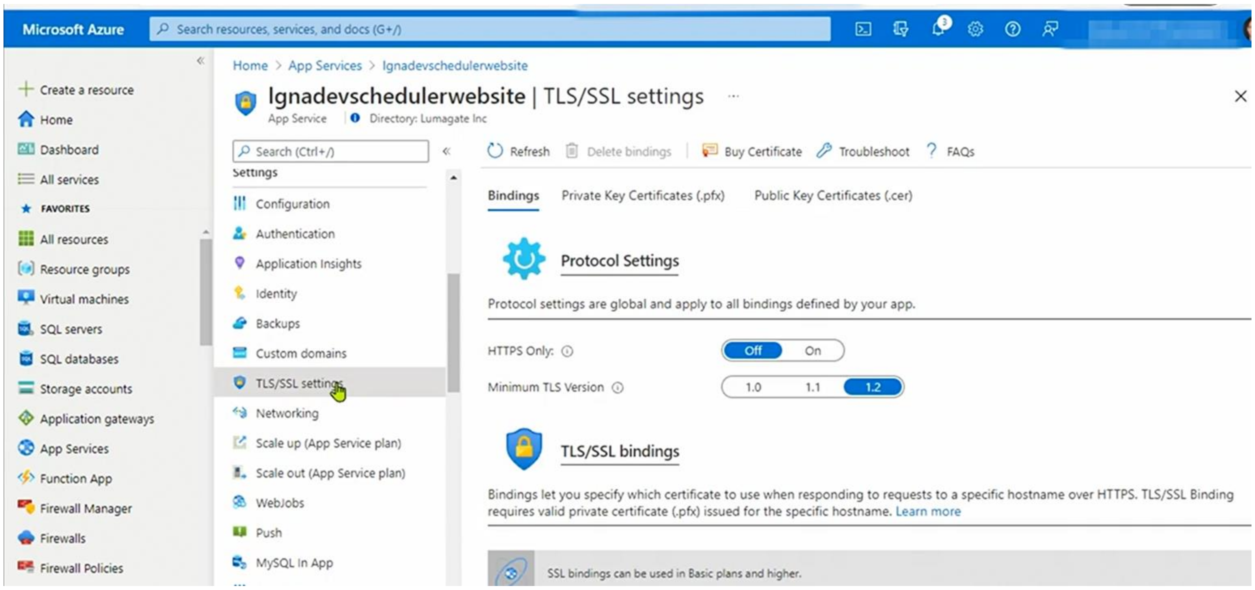
Client IP address 73.166.232.69

Rule name	Start IP	End IP

No firewall rules configured.

Virtual networks

+ Add existing virtual network + Create new virtual network



Ignadevschedulerwebsite | TLS/SSL settings

App Service | Directory: Lumagate Inc

Protocol Settings

Protocol settings are global and apply to all bindings defined by your app.

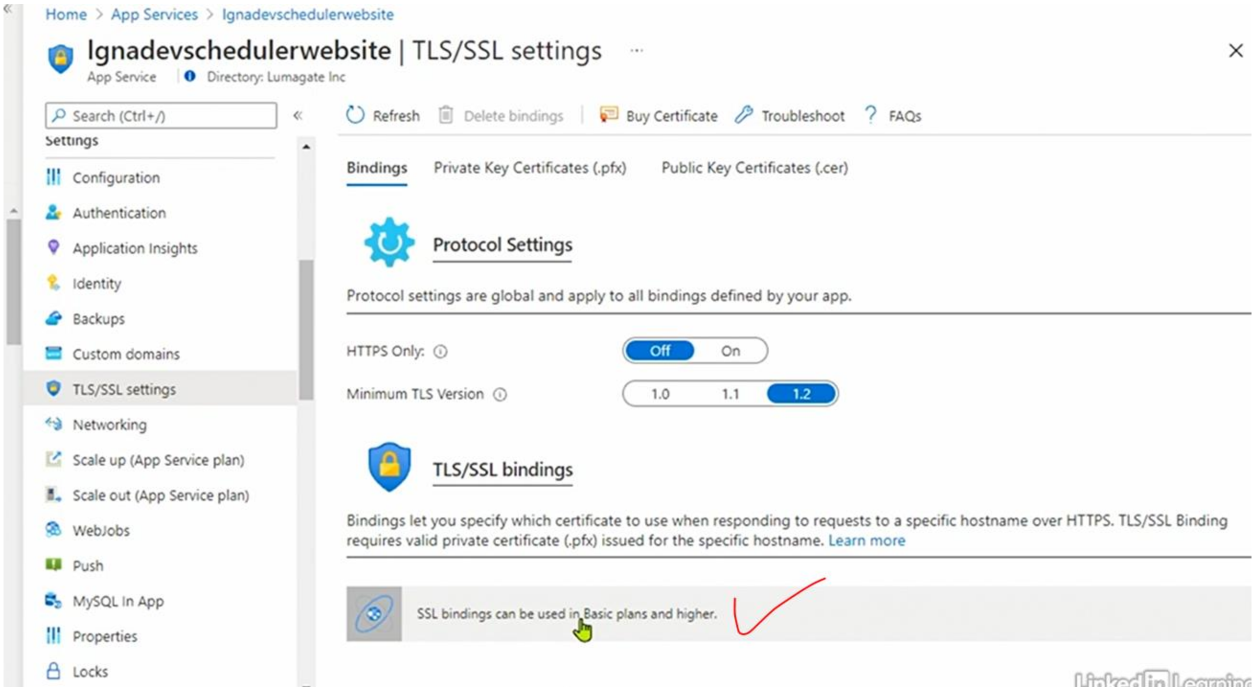
HTTPS Only: [✓ Off] On

Minimum TLS Version: 1.0 1.1 [✓ 1.2]

TLS/SSL bindings

Bindings let you specify which certificate to use when responding to requests to a specific hostname over HTTPS. TLS/SSL Binding requires valid private certificate (.pfx) issued for the specific hostname. Learn more

SSL bindings can be used in Basic plans and higher.



Home > App Services > Ignadevschedulerwebsite

Ignadevschedulerwebsite | TLS/SSL settings ...

App Service | Directory: Lumagate Inc

Search (Ctrl+/)

Settings

- Configuration
- Authentication
- Application Insights
- Identity
- Backups
- Custom domains
- TLS/SSL settings
- Networking
- Scale up (App Service plan)
- Scale out (App Service plan)
- WebJobs
- Push
- MySQL In App
- Properties
- Locks

Refresh | Delete bindings | Buy Certificate | Troubleshoot | FAQs

Bindings | Private Key Certificates (.pfx) | Public Key Certificates (.cer)

Protocol Settings

Protocol settings are global and apply to all bindings defined by your app.

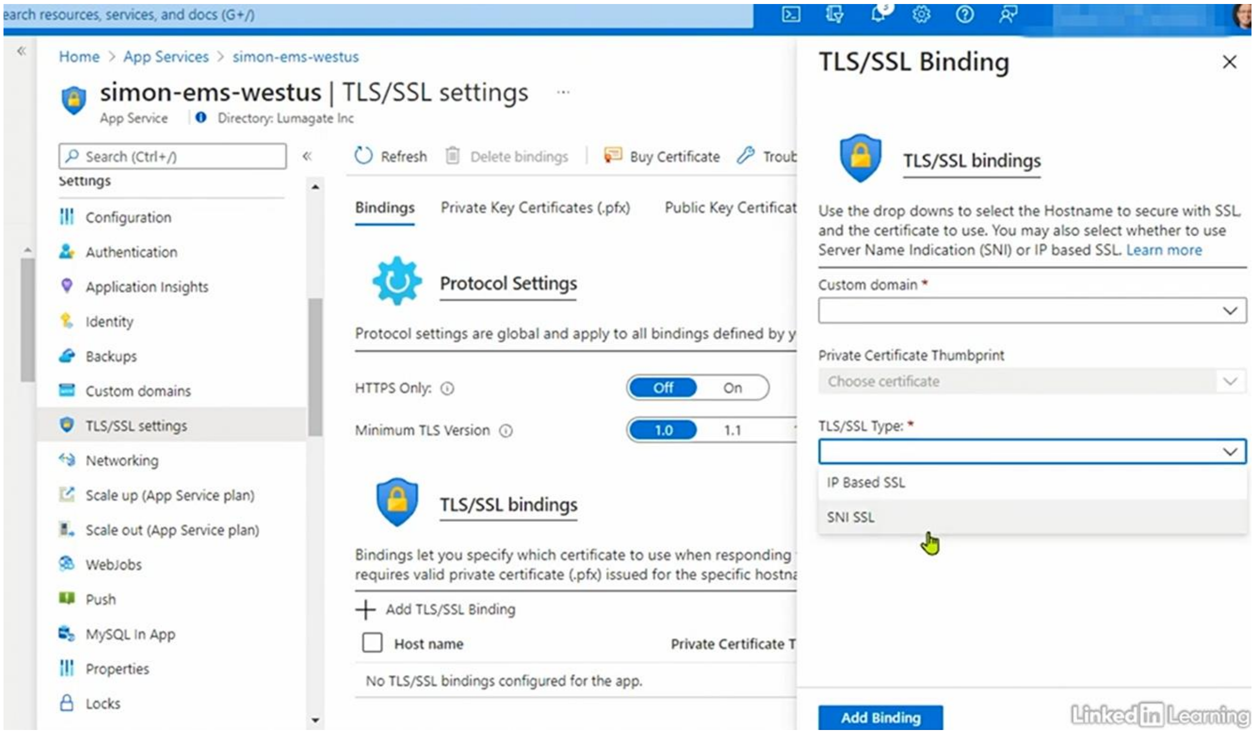
HTTPS Only: Off | On

Minimum TLS Version: 1.0 | 1.1 | 1.2

TLS/SSL bindings

Bindings let you specify which certificate to use when responding to requests to a specific hostname over HTTPS. TLS/SSL Binding requires valid private certificate (.pfx) issued for the specific hostname. Learn more

SSL bindings can be used in Basic plans and higher. ✓



earch resources, services, and docs (G+/)

Home > App Services > simon-ems-westus

simon-ems-westus | TLS/SSL settings ...

App Service | Directory: Lumagate Inc

Search (Ctrl+/)

Settings

- Configuration
- Authentication
- Application Insights
- Identity
- Backups
- Custom domains
- TLS/SSL settings
- Networking
- Scale up (App Service plan)
- Scale out (App Service plan)
- WebJobs
- Push
- MySQL In App
- Properties
- Locks

Refresh | Delete bindings | Buy Certificate | Troub

Bindings | Private Key Certificates (.pfx) | Public Key Certificat

Protocol Settings

Protocol settings are global and apply to all bindings defined by y

HTTPS Only: Off | On

Minimum TLS Version: 1.0 | 1.1

TLS/SSL bindings

Bindings let you specify which certificate to use when responding
requires valid private certificate (.pfx) issued for the specific hostna

+ Add TLS/SSL Binding

□ Host name | Private Certificate T

No TLS/SSL bindings configured for the app.

TLS/SSL Binding

TLS/SSL bindings

Use the drop downs to select the Hostname to secure with SSL and the certificate to use. You may also select whether to use Server Name Indication (SNI) or IP based SSL. Learn more

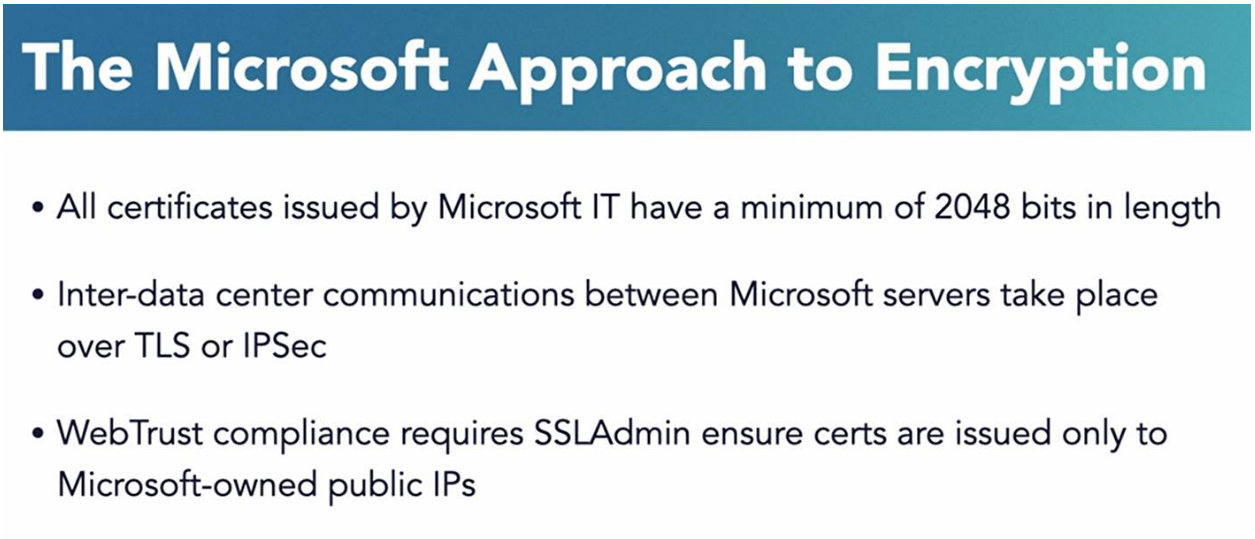
Custom domain *

Private Certificate Thumbprint: Choose certificate

TLS/SSL Type: *

- IP Based SSL
- SNI SSL

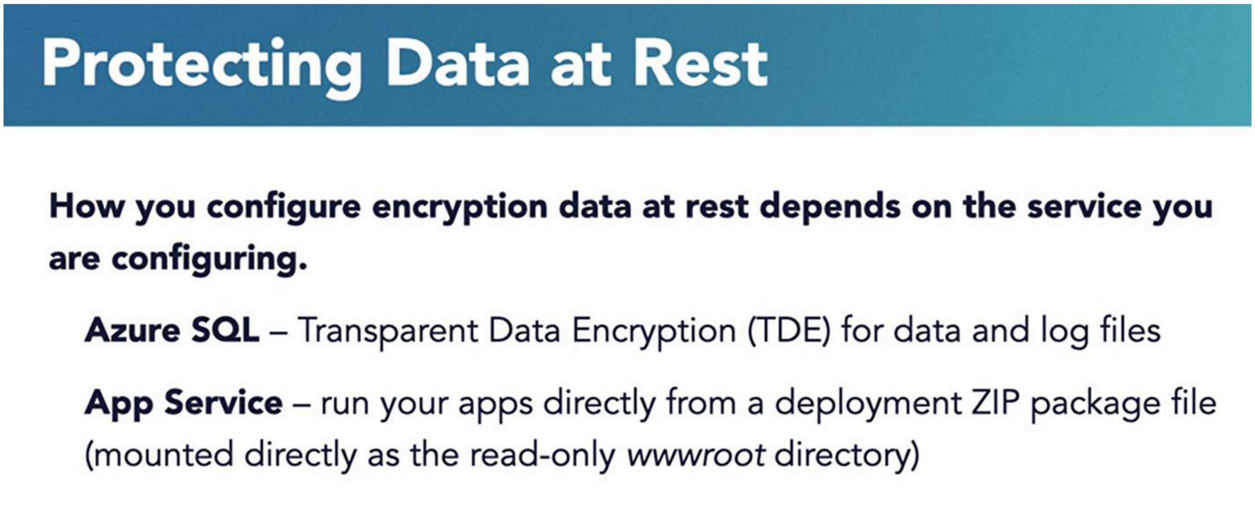
Add Binding



The Microsoft Approach to Encryption

- All certificates issued by Microsoft IT have a minimum of 2048 bits in length
- Inter-data center communications between Microsoft servers take place over TLS or IPSec
- WebTrust compliance requires SSLAdmin ensure certs are issued only to Microsoft-owned public IPs

2.8 Configure encryption at rest

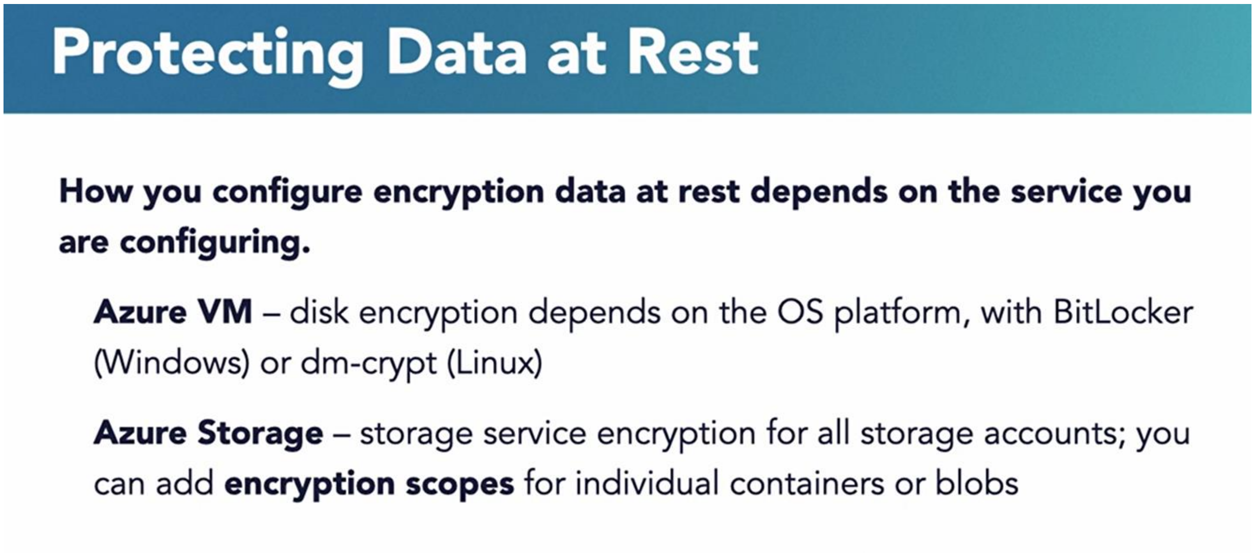


Protecting Data at Rest

How you configure encryption data at rest depends on the service you are configuring.

Azure SQL – Transparent Data Encryption (TDE) for data and log files

App Service – run your apps directly from a deployment ZIP package file (mounted directly as the read-only *wwwroot* directory)

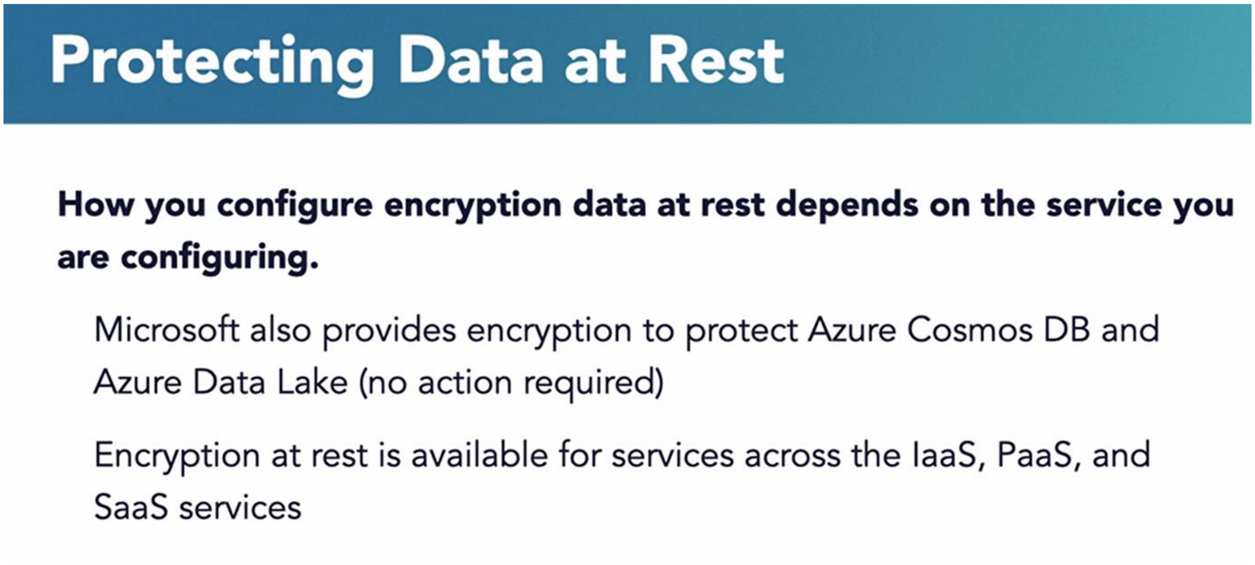


Protecting Data at Rest

How you configure encryption data at rest depends on the service you are configuring.

Azure VM – disk encryption depends on the OS platform, with BitLocker (Windows) or dm-crypt (Linux)

Azure Storage – storage service encryption for all storage accounts; you can add **encryption scopes** for individual containers or blobs

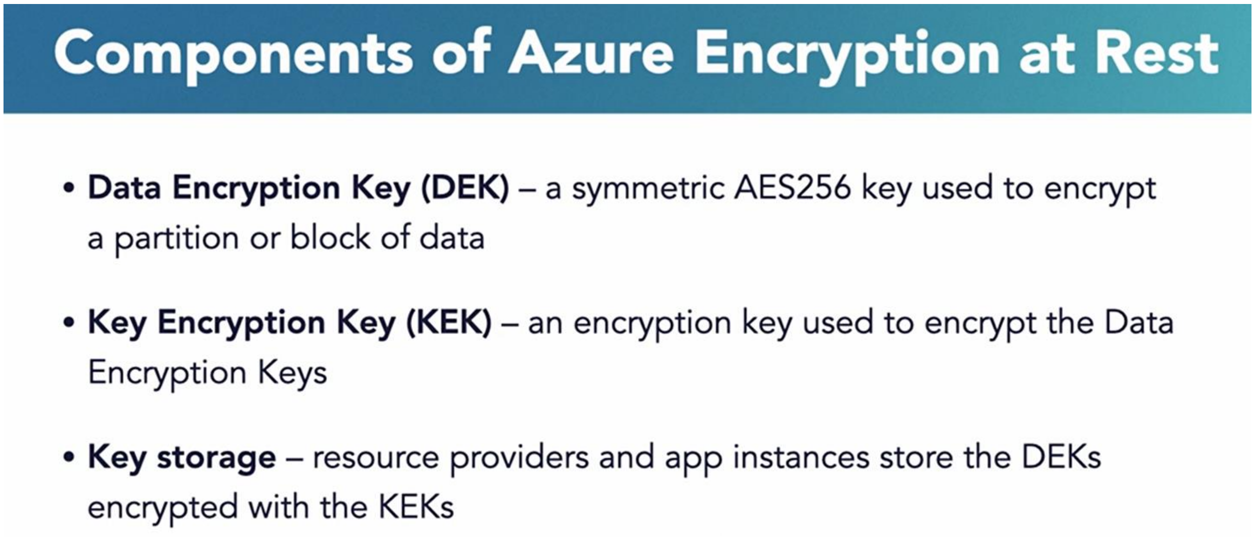


Protecting Data at Rest

How you configure encryption data at rest depends on the service you are configuring.

Microsoft also provides encryption to protect Azure Cosmos DB and Azure Data Lake (no action required)

Encryption at rest is available for services across the IaaS, PaaS, and SaaS services



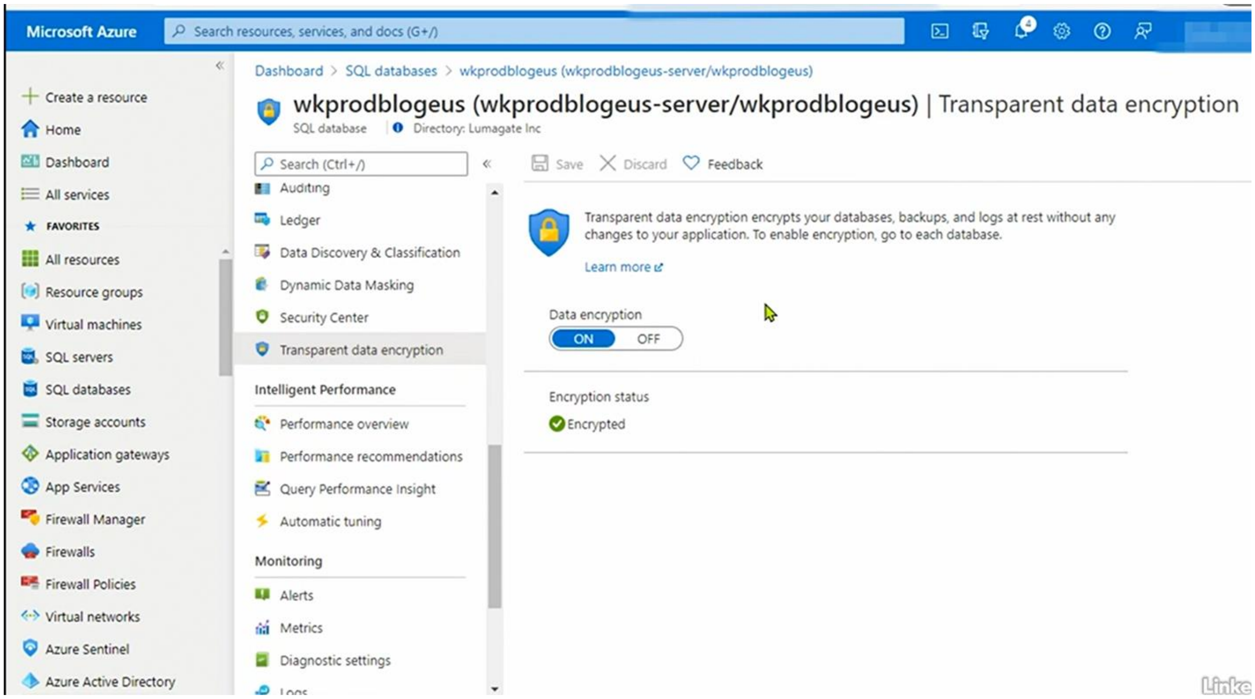
Components of Azure Encryption at Rest

- **Data Encryption Key (DEK)** – a symmetric AES256 key used to encrypt a partition or block of data
- **Key Encryption Key (KEK)** – an encryption key used to encrypt the Data Encryption Keys
- **Key storage** – resource providers and app instances store the DEKs encrypted with the KEKs

Customer-Managed Keys (CMK)

- By default, data is encrypted with Microsoft-managed keys
- For additional control over encryption keys, you can manage your own keys
- Customer-managed keys must be stored in **Azure Key Vault** or **Key Vault Managed Hardware Security Module (HSM)**

Using customer-managed keys with Azure Storage encryption requires that both soft delete and purge protection be enabled for the key vault.



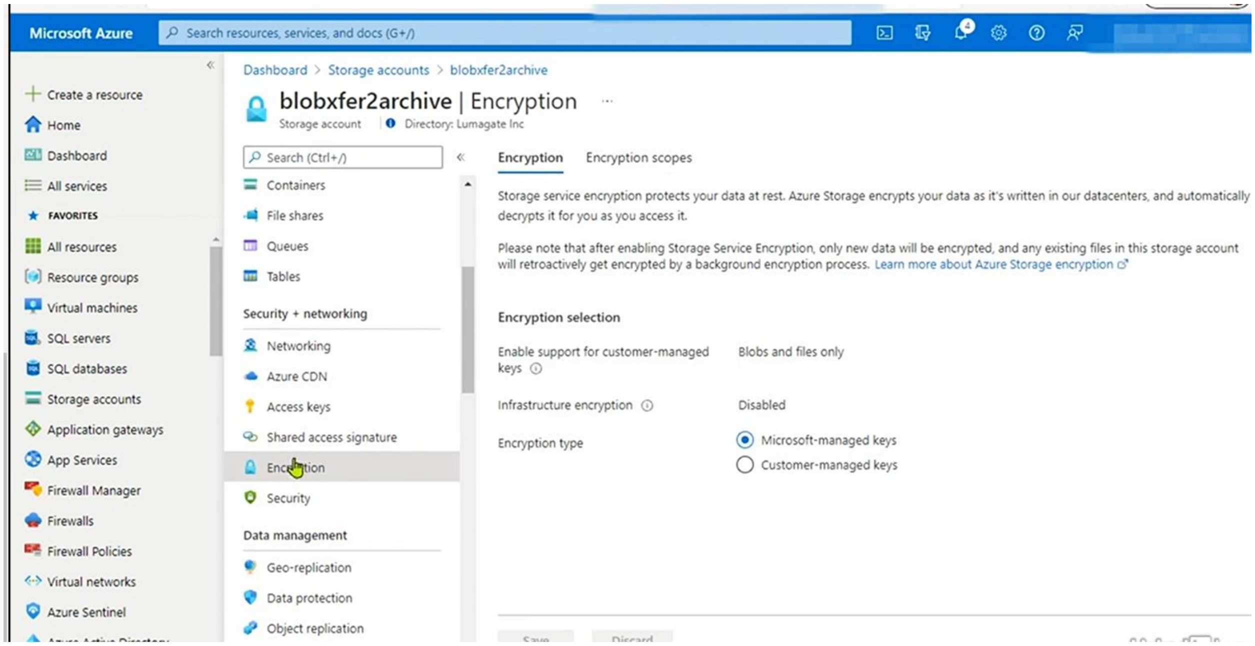
wkprodblogeus (wkprodblogeus-server/wkprodblogeus) | Transparent data encryption

SQL database | Directory: Lumagate Inc

Transparent data encryption encrypts your databases, backups, and logs at rest without any changes to your application. To enable encryption, go to each database.

Data encryption: ON

Encryption status: ✓ Encrypted



blobxfer2archive | Encryption

Storage account | Directory: Lumagate Inc

Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically decrypts it for you as you access it.

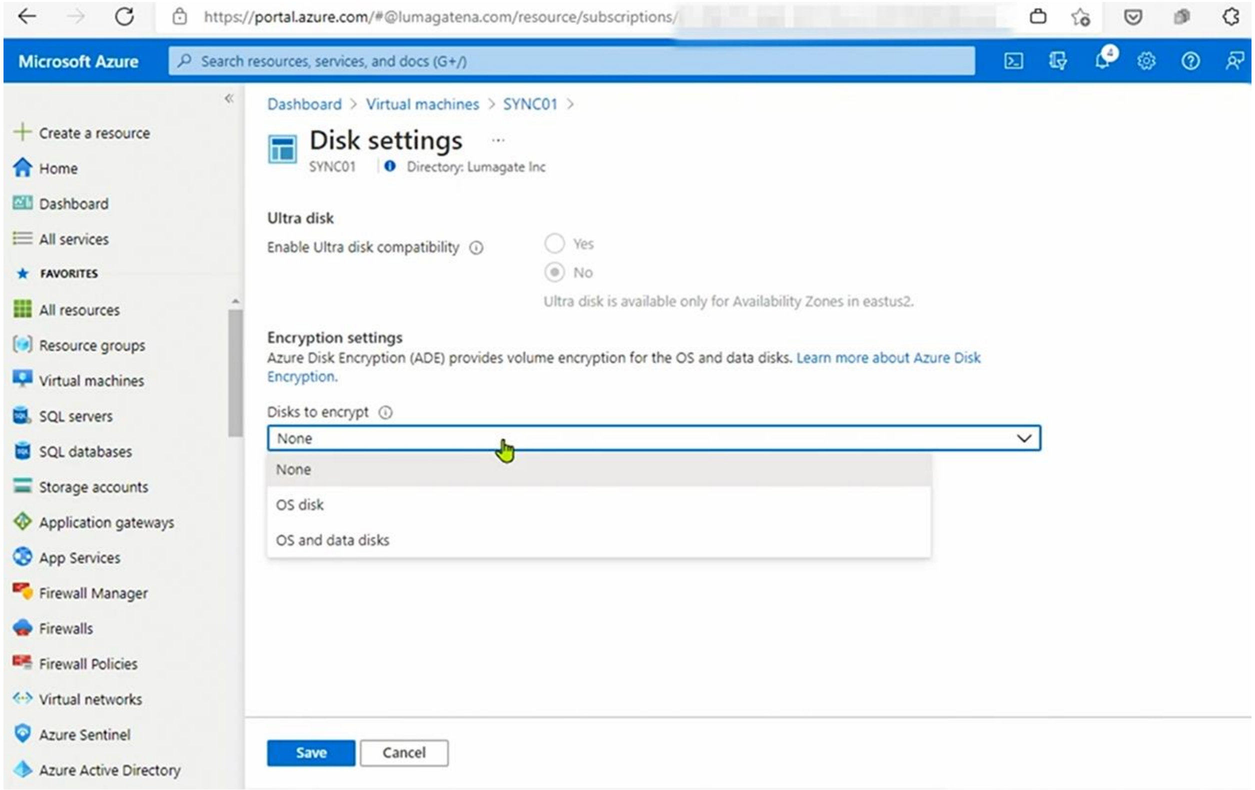
Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in this storage account will retroactively get encrypted by a background encryption process. Learn more about Azure Storage encryption

Encryption selection

Enable support for customer-managed keys: Blobs and files only

Infrastructure encryption: Disabled

Encryption type: ● Microsoft-managed keys ○ Customer-managed keys



Disk settings

SYNC01 | Directory: Lumagate Inc

Ultra disk

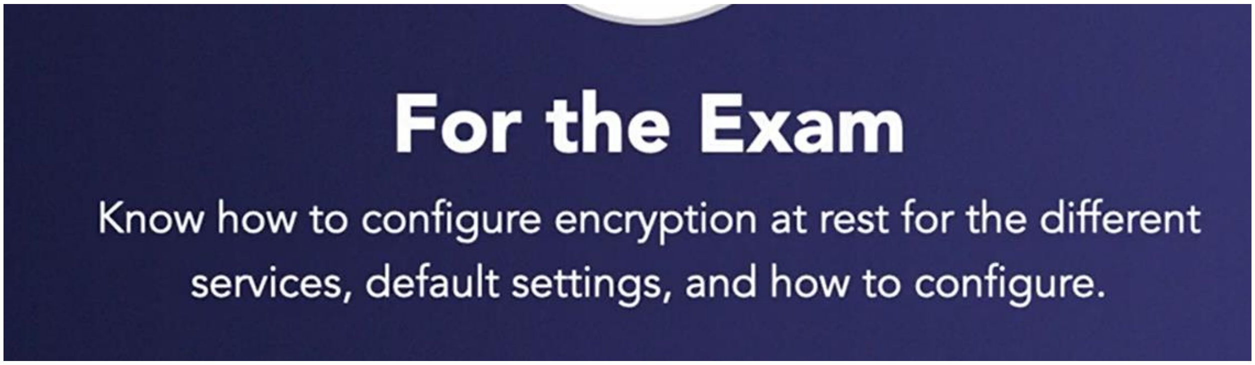
Enable Ultra disk compatibility: ○ Yes ● No

Ultra disk is available only for Availability Zones in eastus2.

Encryption settings

Azure Disk Encryption (ADE) provides volume encryption for the OS and data disks. Learn more about Azure Disk Encryption.

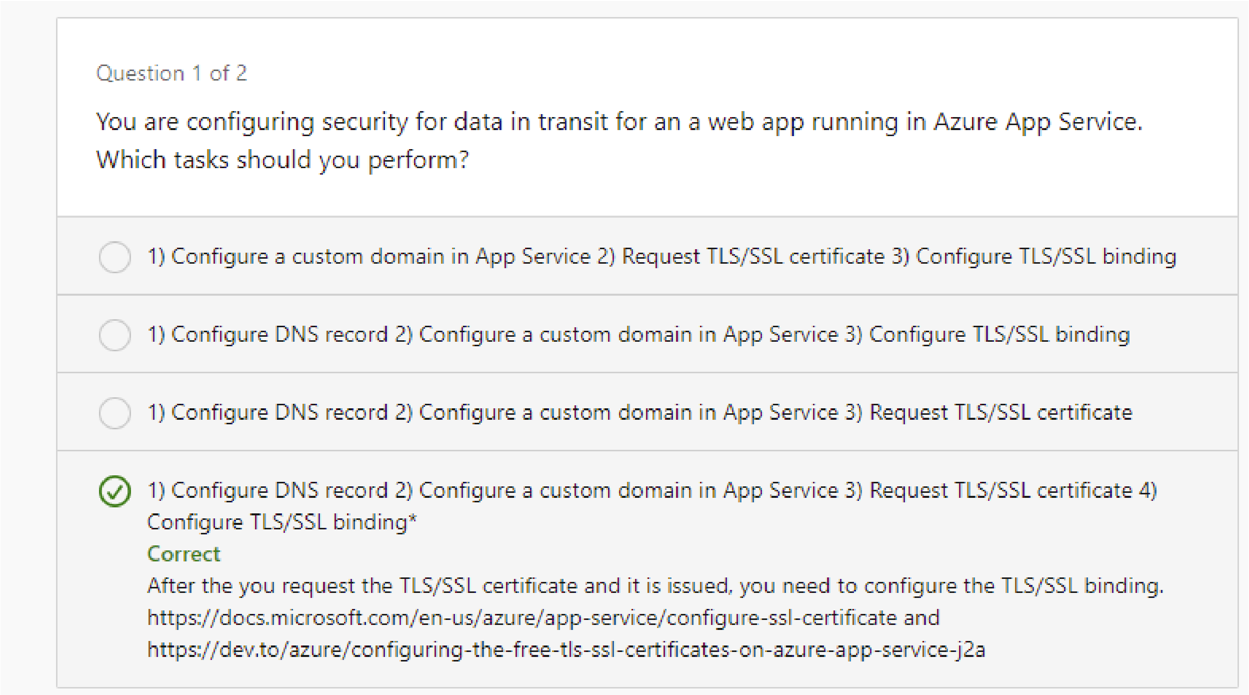
Disks to encrypt: None



For the Exam

Know how to configure encryption at rest for the different services, default settings, and how to configure.

2.9 Quiz



Question 1 of 2

You are configuring security for data in transit for an a web app running in Azure App Service. Which tasks should you perform?

○ 1) Configure a custom domain in App Service 2) Request TLS/SSL certificate 3) Configure TLS/SSL binding

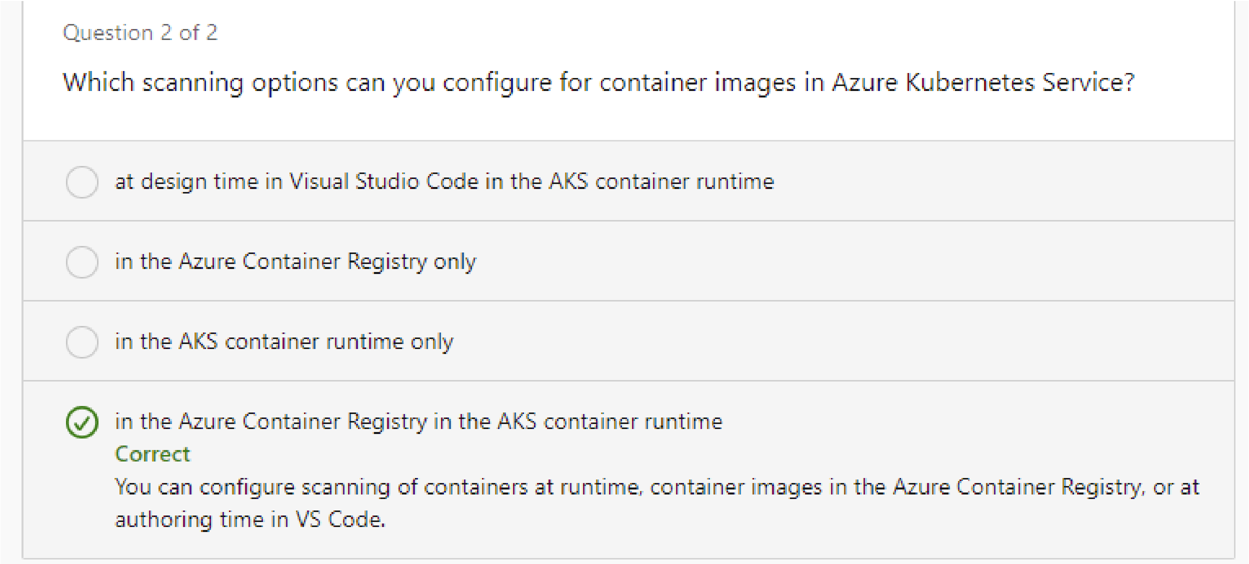
○ 1) Configure DNS record 2) Configure a custom domain in App Service 3) Configure TLS/SSL binding

○ 1) Configure DNS record 2) Configure a custom domain in App Service 3) Request TLS/SSL certificate

✓ 1) Configure DNS record 2) Configure a custom domain in App Service 3) Request TLS/SSL certificate 4) Configure TLS/SSL binding*

Correct

After the you request the TLS/SSL certificate and it is issued, you need to configure the TLS/SSL binding. https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate and https://dev.to/azure/configuring-the-free-tls-ssl-certificates-on-azure-app-service-j2a



Question 2 of 2

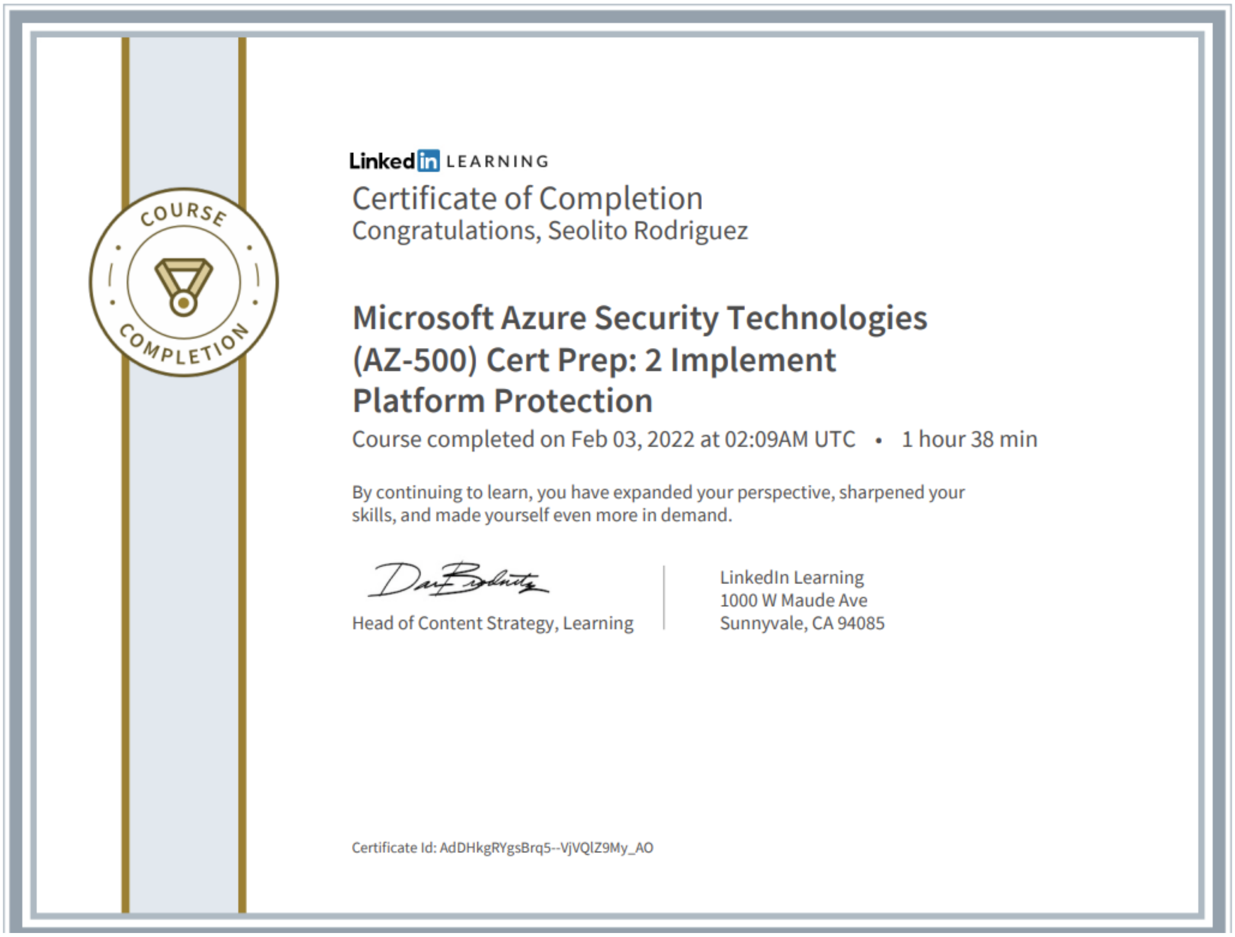
Which scanning options can you configure for container images in Azure Kubernetes Service?

○ at design time in Visual Studio Code in the AKS container runtime

○ in the Azure Container Registry only

○ in the AKS container runtime only

✓ in the Azure Container Registry in the AKS container runtime
Correct
You can configure scanning of containers at runtime, container images in the Azure Container Registry, or at authoring time in VS Code.



COURSE COMPLETION

Linked in LEARNING

Certificate of Completion
Congratulations, Seolito Rodriguez

Microsoft Azure Security Technologies (AZ-500) Cert Prep: 2 Implement Platform Protection

Course completed on Feb 03, 2022 at 02:09AM UTC • 1 hour 38 min

By continuing to learn, you have expanded your perspective, sharpened your skills, and made yourself even more in demand.

Head of Content Strategy, Learning

LinkedIn Learning
1000 W Maude Ave
Sunnyvale, CA 94085

Certificate Id: AdDHkgRYgsBrq5--VjVQlZ9My_AO

References

Configure Azure Endpoint Protection for virtual machines (linkedin.com)

Become an Azure Security Engineer (linkedin.com)