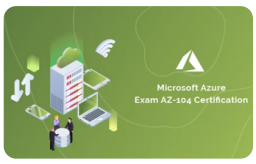


Level: Advanced

Microsoft Azure Exam AZ-104 Certification

← Back to the **Course**

Free Test - **Practice Mode**

Completed on Mon, 15 Sep 2025

1st	20/40	50.00%	FAIL
Attempt	Marks Obtained	Your Score	Result

Share this Report in Social Media Share

Download Report

Domain wise Quiz Performance Report

No.	Domain	Total Question	Correct	Incorrect	Unattempted	Marked for Review
1	Manage Azure identities and governance	5	3	2	0	0
2	Implement and manage storage	12	2	10	0	0
3	Deploy and manage Azure compute resources	12	7	4	1	3
4	Implement and manage virtual networking	6	4	2	0	1
5	Monitor and maintain Azure resources	5	4	1	0	0
Total	All Domains	40	20	19	1	4

Review the Answers

Filter By

Question 1

Incorrect

Domain: Implement and manage storage

Contoso Inc. is a multinational company having offices in multiple countries. The company is planning on moving its on-premises file servers to Azure Files.

While setting up identity-based access for Azure Files, which of the following mechanisms enforces granular access control for files and directories within a share?

A. Microsoft Entra Domain Services right

B. Role-Based Access Control (RBAC) wrong

C. Shared Key Authentication

D. Virtual Network Service Endpoints

Explanation:

Correct Answer: A

Option A is Correct This service provides managed domain services such as domain join, group policies, LDAP, and Kerberos/NTLM authentication, which are fully compatible with Active Directory Domain Services. It allows you to configure Windows access control lists (ACLs) for fine-grained permissions at the file and directory level

Option B is incorrect because While RBAC is used to manage access to Azure resources at a broader level, it does not provide the fine-grained control needed for individual files and directories within an Azure Files share. RBAC is more suitable for controlling access to Azure resources like storage accounts, virtual machines, and databases.

Option C is incorrect because Shared Key Authentication is a method to authenticate access to Azure Storage resources using an account's access key securely.

Option D is incorrect because Virtual Network Service Endpoints in Azure extend private network connectivity to Azure services, enabling secure access without public internet exposure, enhancing security, and reducing latency.

Reference:

Use Microsoft Entra Domain Services with Azure Files | Microsoft Learn

Ask our Experts

Did you like this **Question?**

Question 2

Incorrect

Domain: Implement and manage storage

View Case Study

You have been asked to transfer a 500MB set of training documents to Azure Blob Storage as part of a migration task. Which of the following is the most appropriate and efficient method to complete this task?

A. Generate a Shared Access Signature (SAS), map the storage as a network drive, and copy the files using File Explorer

B. Use the Azure Import/Export service to upload the data wrong

C. Use an access key to map an Azure File Share as a drive, then copy files using File Explorer

D. Use Azure Storage Explorer to upload the files directly to Azure Storage right

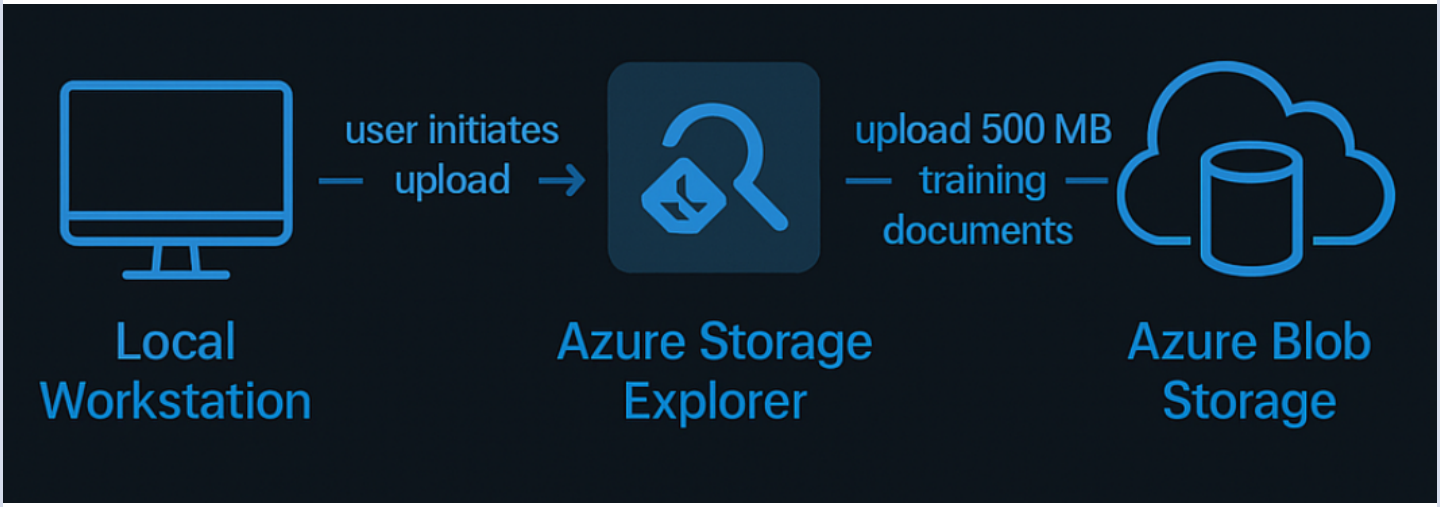
---

Explanation:

Correct Answer: D

Option D: Use Azure Storage Explorer to upload the files directly to Azure Storage. Azure Storage Explorer is a free, GUI-based tool provided by Microsoft that allows you to manage Azure Storage accounts. It supports drag-and-drop upload, file browsing, and access to blobs, file shares, queues, and tables. For transferring a small amount of data, like 500MB, it is the most **efficient, simple, and user-friendly** option.

Why it's correct: No setup complexity, no scripting required, supports direct uploads with a visual interface, ideal for small-to-medium data volumes.



Option A: Generate a Shared Access Signature (SAS), maps the storage as a network drive, and copies the files using File Explorer is incorrect because this method involves generating a SAS token, mounting Azure File Storage as a network drive, and then using File Explorer to copy files. While technically possible, it introduces unnecessary complexity for a one-time, small-volume transfer like 500MB. It's more suitable for scenarios that require temporary delegated access to users or applications, not for initial data upload tasks.

Why it's wrong: Not user-friendly for one-time use, requires multiple steps, and more setup than needed for small data transfers.

Option B: Using the Azure Import/Export service to upload the data is incorrect because the Azure Import/Export is a service designed for very large data transfers, often in the terabyte range. It involves preparing data on physical drives and shipping them to Microsoft data centers, which is time-consuming and costly.

Why it's wrong: Completely impractical for just 500MB; the overhead of physical disk preparation and shipping is overkill.

Option C: Use an access key to map an Azure File Share as a drive, then copy files using File Explorer is Incorrect because using an account key to mount an Azure File Share is useful for continuous or long-term access to Azure Files. It allows applications or users to work with Azure File Shares like regular file servers. However, it's not the most efficient or necessary method for a small, one-time data upload like 500MB.

Why it's wrong: Suitable for persistent drive mapping in hybrid scenarios—not optimal for quick, ad hoc uploads.

Final Takeaway:

For ad-hoc or small-sized data uploads to Azure Storage, Azure Storage Explorer is the best combination of simplicity, speed, and usability. Other methods are either too complex or designed for different use cases (e.g., long-term access, massive data volumes).

References:

Azure Storage Explorer – cloud storage management | Microsoft Azure

Connect Azure Storage Explorer to a storage account - Training | Microsoft Learn

Ask our Experts

Did you like this **Question?**

Question 3 Incorrect

Domain: Implement and manage virtual networking

A company has deployed the following Azure Load Balancer resources to their Azure subscription

Name	SKU
whizlabload1	Basic
whizlabload2	Standard

Each load balancer would have to load balance requests across three virtual machines.

You want to ensure that **whizlabload1** can load balance requests across the three virtual machines.

Which of the following has to be implemented?

A. Ensure the virtual machines are created in the different regions.

B. Ensure the virtual machines are created in the same resource group.

C. Ensure the virtual machines are created in the same virtual network. wrong

D. Ensure the virtual machines are created in the same availability set or virtual machine scale set. right

---

Explanation:

Answer – D

You look at the comparison between the Standard and the Basic Load Balancer in the Microsoft documentation. It clearly mentions that the virtual machines need to be part of an availability set or a virtual machine scale set.

	Standard Load Balancer	Basic Load Balancer
Scenario	Equipped for load-balancing network layer traffic when high performance and ultra-low latency is needed. Routes traffic within and across regions, and to availability zones for high resiliency.	Equipped for small-scale applications that don't need high availability or redundancy. Not compatible with availability zones.
Backend type	IP based, NIC based	NIC based
Protocol	TCP, UDP	TCP, UDP
Backend pool endpoints	Any virtual machines or virtual machine scale sets in a single virtual network	Virtual machines in a single availability set or virtual machine scale set

Since this is clearly mentioned in the documentation, all other options are incorrect.

For more information on the Azure Load Balancer, please visit the following URL-

What is Azure Load Balancer? - Azure Load Balancer | Microsoft Learn

Azure Load Balancer SKUs | Microsoft Learn

Ask our Experts

Did you like this **Question?**

Question 4 Correct

Domain: Monitor and maintain Azure resources

View Case Study

The Whizbuddy app is a critical business application. You have been tasked with implementing a backup strategy to ensure data protection and recovery capabilities. Which of the following should you create first to begin setting up Azure Backup?

A. A recovery plan

B. An Azure Backup Server

C. A backup policy

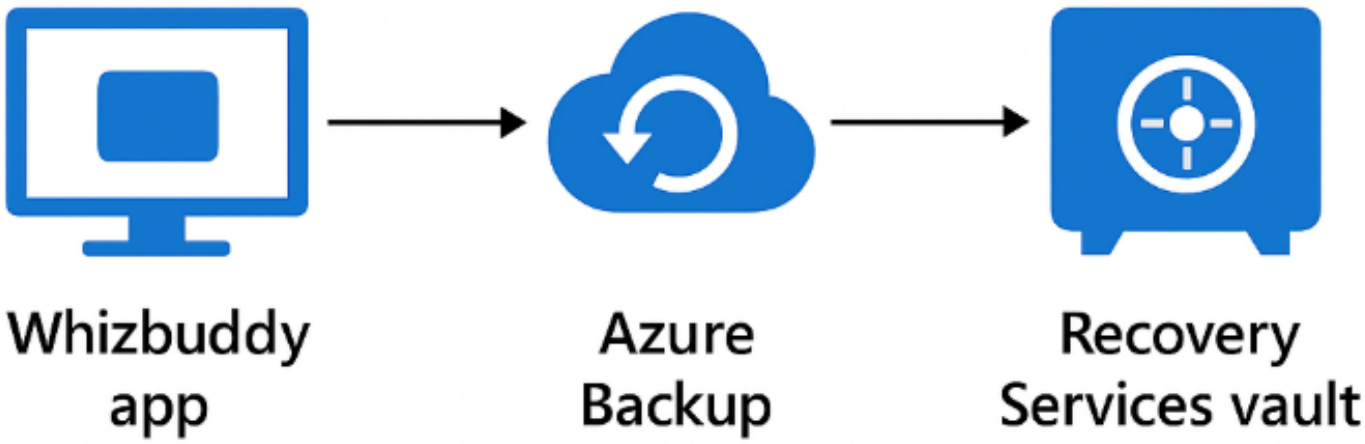
D. A Recovery Services vault right

Explanation:

Correct Answer: D

Option D is correct because A Recovery Services vault is the first and most essential component when configuring Azure Backup. It is a **storage and management container** for all backup data and configurations. You need to create a vault before you can define policies, register virtual machines, or trigger backups. The vault stores backup metadata, recovery points, and configurations. It's scoped per region and resource group.

Why it's correct: It's the prerequisite for all backup activities in Azure. Without it, no backups or policies can be created.



Option A is incorrect because A recovery plan is used in **Azure Site Recovery (ASR)** and is designed to automate **failover and failback** processes during a disaster. It helps organize the sequence and grouping of virtual machines during failover. However, this is **not a starting point for setting up backups**. Recovery plans are used **after backup infrastructure** (like the vault and backup policies) has been configured.

> Why it's wrong: It's a disaster recovery component, not a backup prerequisite. You can't define a recovery plan without having backup components already in place.

Option B is incorrect because Azure Backup Server (MABS) is a Microsoft-provided on-premises solution that allows backup of on-prem workloads (like file servers, VMs, SQL databases) to Azure. While MABS integrates with Azure Backup via a Recovery Services vault, it is not needed for protecting native Azure resources such as Azure VMs.

> Why it's wrong: MABS is part of a hybrid or on-prem backup strategy, not required for Azure-native backups. You only need this if you're backing up non-Azure infrastructure.

Option C is incorrect because a backup policy defines the schedule and retention rules for backup jobs — i.e., what to back up, how often, and how long to retain data. However, you **cannot create or apply a backup policy until a Recovery Services vault exists** to associate it with. The vault is the container where the backup policy lives.

> Why it's wrong: A backup policy is created after the Recovery Services vault. It depends on the vault for its existence and application.

Reference:

> Back up Azure VMs in a Recovery Services vault - Azure Backup | Microsoft Learn

Ask our Experts

Did you like this **Question?**

Question 5 Incorrect

Domain: Deploy and manage Azure compute resources

You need to increase the number of CPU cores and memory for running Azure Container Instance.

What steps do you take to carry out this task?

A. Stop the ACI

- [x] B. Redeploy ARM ACI deployment template right
- [x] C. In Azure portal, select the Scale up for ACI container wrong

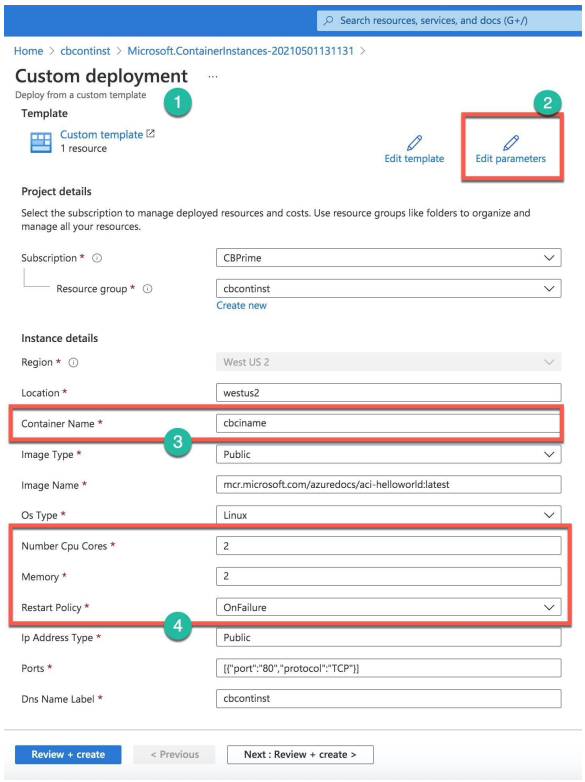
D. Update Dockerfile

E. Delete the ACI right

Explanation:

Correct Answers: B and E

Unfortunately, Azure does not allow to scale Azure Container Instances. You need to **delete the current ACI** and create a new instance with the new resource requirements. The most convenient way is to reuse and **run the ARM template from the previous ACI deployment**. You can find the template under the Deployments section on the ACI's resource group blade. When you select the deployment template and click on the Redeploy button on the top bar, the Azure portal opens the Custom deployment screen (Number 1). Here you click on the "Edit Parameters (Number 2) and can change the number of CPU cores, memory, restart policy, etc. (Number 4). If you have not deleted the previous ACI and keep the same name for the new instance (Number 3), you will get a deployment failed error when you click on the Create button after a review.



The error status message is the following.

```
{
    "status": "Failed",
    "error": {
        "code": "InvalidContainerGroupUpdate",
        "message": "The updates on container group 'cbciname' are invalid. If you are going to update
        the os type, restart policy, network profile, CPU, memory or GPU resources for a container
        group, you must delete it first and then create a new one."
    }
}
```

Therefore, you must delete the old ACI or change the name of the new ACI.

All other options are incorrect.

For more information about creating and updating the ACI using the ARM templates, please visit the below URLs:

https://docs.microsoft.com/en-us/azure/container-instances/container-instances-update#properties-that-require-container-delete

https://docs.microsoft.com/en-us/azure/container-instances/container-instances-quickstart-template

Ask our Experts

Did you like this **Question?**

Question 6 Correct

Domain: Implement and manage virtual networking

View Case Study

You are designing the network architecture for hosting the different tiers (e.g., web application, application logic, and database) of the Whizlabs-app in Azure. How many virtual networks (VNets) would you recommend for hosting the virtual machines across these tiers, considering best practices for network isolation and security?

A. Deploy all VMs in a single VNet and single subnet

B. Deploy VMs across two separate VNets

C. Deploy all VMs in a single VNet with three separate subnets right

D. Deploy each tier in its own VNet

Explanation:

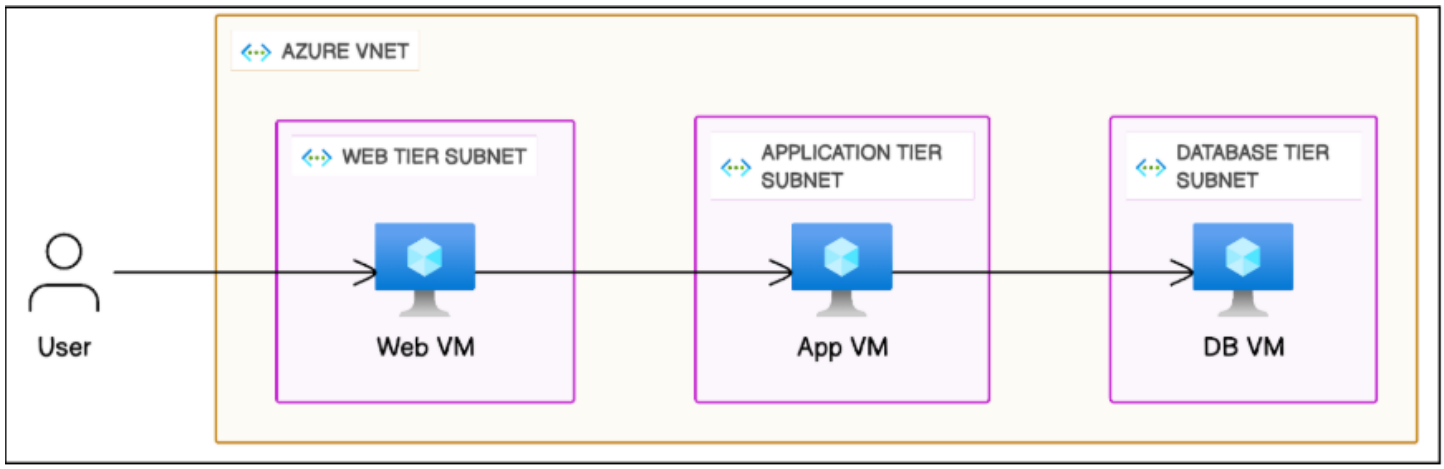
Correct Answer: C

Option C: Deploy all VMs in a single VNet with three separate subnets is correct because the best practice for network security and isolation dictates the Azure-recommended approach for a three-tier app is to use a single VNet, divided into three subnets one for each tier (Web, Application, Database).

This allows for easier routing, simpler peering setup, centralized DNS, and cost efficiency.

Network Security Groups (NSGs) can be scoped to each subnet, enforcing tier-specific access policies.

Communication across subnets remains fast, secure, and cost-free within the VNet.



Why it's correct: This design balances security, manageability, and performance while avoiding unnecessary peering overhead.

Option A Deploy all VMs in a single VNet and single subnet is incorrect because using a single VNet and a single subnet for all tiers may simplify initial deployment, but it fails to implement network segmentation. All resources are flat within the same address space, and NSG-level control becomes difficult.

Why it's wrong: Lacks isolation. Compromising one tier (e.g., web) can lead to lateral movement to more sensitive tiers (e.g., database).

Option B: Deploy VMs across two separate VNets is incorrect because separating tiers across two VNets is only partial isolation. For a three-tier application, you'd still have at least one tier sharing a VNet, which means security controls may overlap or become inconsistent.

Why it's wrong: Provides only limited segmentation and doesn't allow dedicated control for each tier.

Option D: Deploying each tier in its own VNet is incorrect because using three separate VNets (one per tier) is possible and offers strong isolation, but it introduces complexity in routing, VNet peering, and troubleshooting. For most internal-tier communication (app ↔ DB), this setup is overly complex unless you have strict regulatory boundaries between tiers.

Why it's wrong: Too complex for standard apps; adds overhead with no significant security gain compared to subnet isolation within a single VNet.

References:

Best practices for network security - Microsoft Azure

Recommendations for networking and connectivity - Microsoft Azure Well-Architected Framework

Ask our Experts

Did you like this **Question?**

Question 7 Correct

Domain: Deploy and manage Azure compute resources

Which of the following languages supports and facilitates development for deployment of all resource types and API versions available in Azure Preview and General Availability?

A. KQL

B. Java

C. Bicep right

D. SQL

Explanation:

Correct Answer: C

Bicep offers immediate compatibility with all preview and generally available (GA) versions of Azure services. Whenever a new resource type or API version is introduced by a resource provider, you can seamlessly incorporate them into your Bicep file. There's no need to delay your utilization of new services while waiting for tool updates.

Option A is incorrect because KQL [Kusto Query Lanuguage] is used for querying against the Log Analytics Workspaces.

Option B is incorrect Java JSON format files can be used for these deployments, however, supports are limited and can be complex to write the ARM templates.

Option C is correct Bicep delivers a streamlined syntax, dependable type safety, and the ability to easily reuse code. It presents an exceptional platform for creating infrastructure-as-code solutions within the Azure environment, providing a top-tier authoring experience.

Option D is incorrect SQL is a database language and is not meant for deployment of azure resources.

Reference:

Bicep language for deploying Azure resources - Azure Resource Manager | Microsoft Learn

Ask our Experts

Did you like this **Question?**

Question 8 Correct

Domain: Implement and manage virtual networking

View Case Study

You are designing the network infrastructure for the Whizlabs-App, a three-tier application consisting of a web front end, an application middle tier, and a SQL database back end. To ensure security and proper network segmentation, how many subnets would you recommend within a single Virtual Network (VNet) to host the Virtual Machines for this application?

A. Use one subnet for all tiers

B. Use two subnets for shared and isolated tiers

C. Use three subnets, one per application tier right

D. Use four subnets to further isolate each tier

Explanation:

Correct Answer: C

Option C: Use three subnets, one per application tier correct because this is the **Azure-recommended design** for a three-tier application. By using a **single VNet** divided into three subnets (Web, Application, and Database), you achieve:

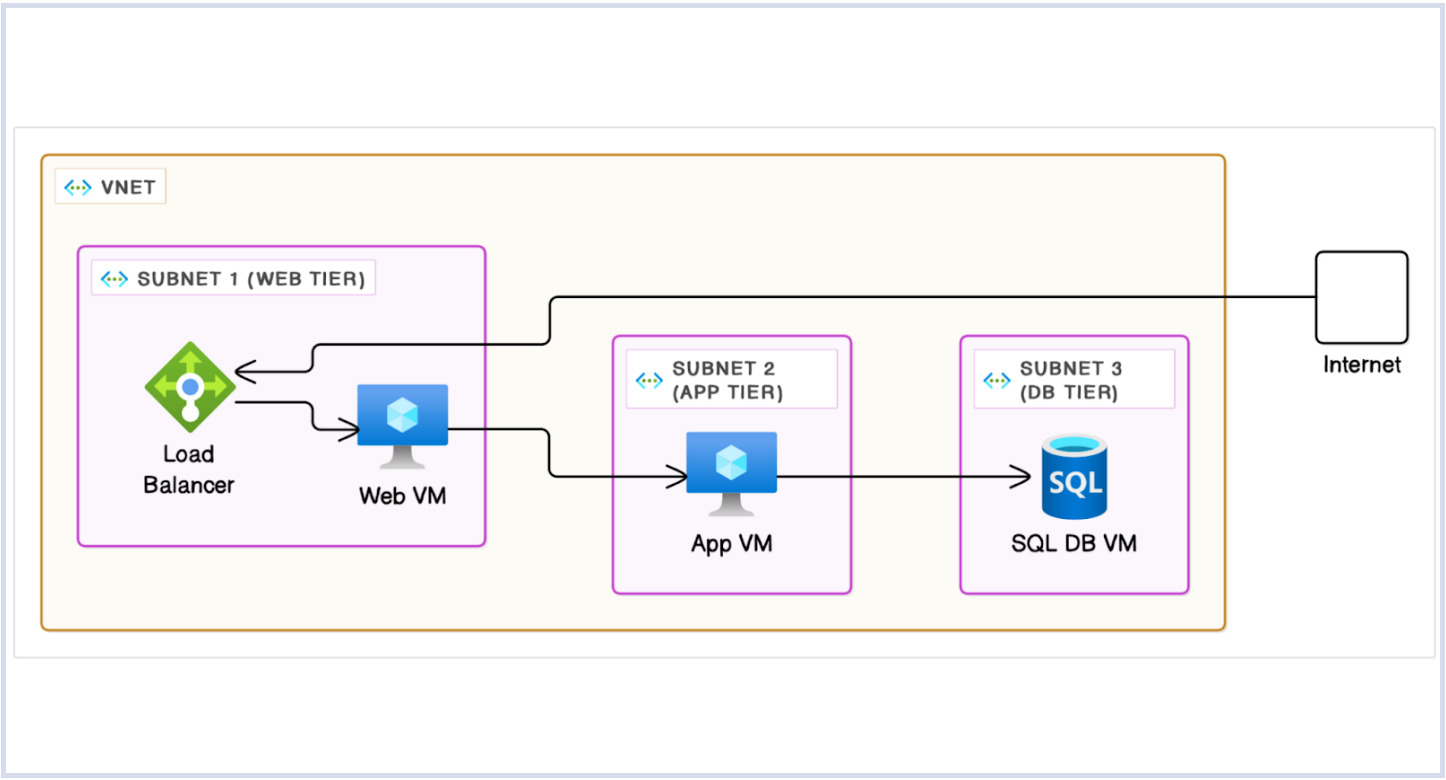
Logical isolation of each tier

Scoped NSG policies for fine-grained access control

Efficient traffic flow within the same VNet (low latency, no extra costs)

Simplified routing, centralized DNS, and easier monitoring

Why it's correct: This model balances **security, manageability, and performance.** It limits lateral movement in case of compromise, allows flexible security rules per tier, and avoids unnecessary complexity (e.g., peering).



Option A: Use one subnet for all tiers is incorrect because putting all VMs in one subnet simplifies setup but **eliminates isolation** between application tiers. All tiers share a flat address space, making **tier-specific NSG policies hard to enforce.**

Why it's wrong: One compromised tier (e.g., a vulnerable web server) could easily access others (like the database), increasing the risk of lateral movement and breach propagation.

Option B: Use two subnets for shared and isolated tiers is incorrect because this offers **some isolation** but falls short for a three-tier app. For example, combining Web + App in one subnet still exposes the middle tier to external attack surfaces.

Why it's wrong: Security rules become less granular, and you lose the ability to apply targeted NSGs for each tier.

Option D: Use four subnets to further isolate each tier is incorrect because more subnets mean more complexity. While advanced cases may justify this (e.g., regulatory needs), for a standard three-tier app, this adds overhead without real benefit.

Why it's wrong: It complicates routing, NSG management, and diagnostics, especially if there's no strict need for additional segmentation.

References:

Virtual networks and virtual machines in Azure

Multi-tier web application built for HA/DR - Azure Architecture Center

Ask our Experts

Did you like this **Question?**

Question 9 Correct

Domain: Manage Azure identities and governance

You have a Microsoft Entra ID tenant. You create a new user named Admin. You need to ensure that Admin can:

Assign Microsoft Entra licenses to groups

Reset passwords of other users in Microsoft Entra ID

Which Microsoft Entra built-in role should you assign to Admin?

A. Billing Administrator

B. Helpdesk Administrator

C. License Administrator

D. User Administrator right

Explanation:

Correct Answer: D

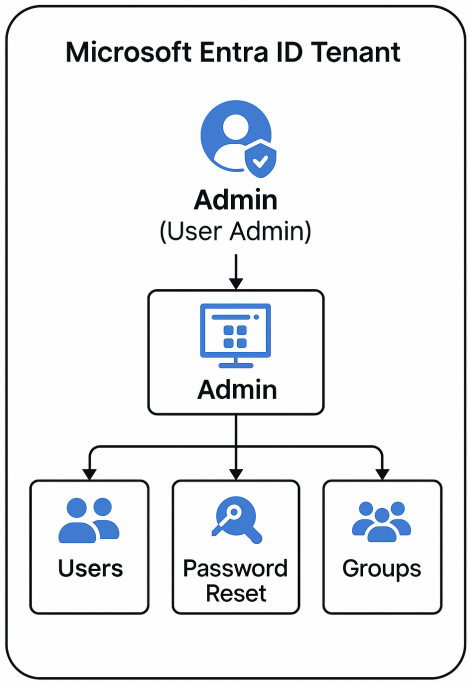
Option D: User Administrator is correct because the User Administrator role provides permissions to **manage users and groups**, including:

Resetting passwords for non-administrators

Assigning licenses to users and groups

Managing group memberships

Creating and deleting users



Why it's correct: It's the only role listed that allows both:

Assigning licenses to Microsoft Entra groups

Resetting user passwords (for non-admin users)

This role is commonly used for **IT helpdesk staff or user management administrators** who need broad control over identity objects but don't require full admin access.

Option A: Billing Administrator is incorrect because this role is focused solely on managing subscriptions, invoices, and payment methods in Microsoft 365 or Azure. It does not have rights to reset passwords or assign licenses.

Why it's wrong: Limited to financial tasks, not user or group management.

Option B: Helpdesk Administrator is incorrect because this role allows **password resets**, but only for **non-admin users**. It does **not** allow license assignment or group management.

Why it's wrong: Meets only one requirement, resetting passwords -but not license assignment to groups.

Option C: License Administrator is incorrect because this role allows assigning/removing licenses to users, but not to groups. It also does not allow resetting user passwords.

Why it's wrong: Provides partial capability — license management for individual users, but not for groups, and lacks password reset permissions

Role	Reset Passwords	Assign Licenses to Users	Assign Licenses to Groups	Manage Users/Groups
User Administrator	✅ Yes	✅ Yes	✅ Yes	✅ Yes
Helpdesk Administrator	✅ Yes (users only)	❌ No	❌ No	❌ No
License Administrator	❌ No	✅ Yes	❌ No	❌ No
Billing Administrator	❌ No	❌ No	❌ No	❌ No

References:

https://learn.microsoft.com/en-us/entra/fundamentals/licensing

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#user-administrator

Ask our Experts

Did you like this **Question?**

Question 10 Incorrect

Domain: Implement and manage storage

Version-level immutability can be enabled or disabled on the storage account any point of time. Is the above statement true or false?

A. True wrong

B. False right

Explanation:

Correct Answer: B

Version-level immutability cannot be disabled after it is enabled on the storage account, although locked policies can be deleted.

Option A is incorrect because version level immutability can be only enabled once and once enabled it cannot be disabled.

Option B is correct because the statement is incorrect. Version level immutability can be only enabled once and once enabled it cannot be disabled.

Reference:

Configure immutability policies for blob versions - Azure Storage | Microsoft Learn

Ask our Experts

Did you like this **Question?**

Question 11 Correct

Domain: Manage Azure identities and governance

You have an Azure subscription that includes a virtual network named VNetW in the West US region. You plan to deploy the following container instances:

instance1, running a Windows container image in West US

instance2, running a Linux container image in West US

instance3, running a Windows container image in East US

Which container instances can be deployed to VNetW?

A. instance1

B. instance1, instance2 and instance3

C. instance1 and instance3

D. instance1 and instance2 right

E. instance2

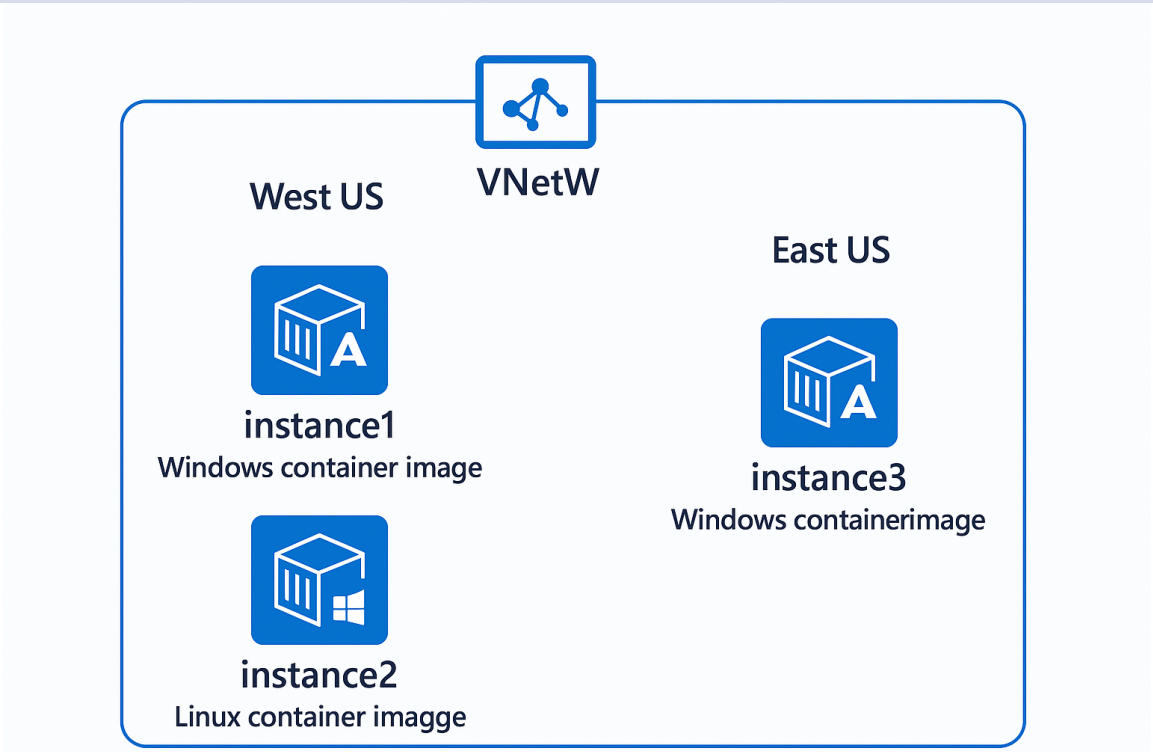
Explanation:

Correct Answer: D

Option D: instance1 and instance2 is correct because Azure Container Instances (ACI) can be deployed into a virtual network (**VNet**) only if the container and the VNet are in the **same region**. In this scenario:

instance1 (Windows, West US)

instance2 (Linux, West US)



Both container instances are in the West US, which matches the region of VNetW. Azure supports VNet injection for both Windows and Linux containers in most regions, including the West US.

Why it's correct:

Both containers are in the same region as VNetW.

Azure now supports VNet integration for Linux and Windows containers

These two instances can be deployed to VNetW without issue

Option A: instance1 is incorrect because this option includes **only instance1**, which is valid, but **excludes instance2**, which is also valid.

Why it's wrong: It's partially correct, but not the best answer. instance2 should also be included.

Option B: instance1, instance2 and instance3 are incorrect because instance3 is in **East US**, while VNetW is in the **West US**. Azure **does not support cross-region VNet deployment** for ACI.

Why it's wrong: Includes instance3, which is not in the same region, making this choice invalid.

Option C: instance1 and instance3 are incorrect because only instance1 is in the same region as VNetW. instance3 is in East US, so it cannot be deployed to a West US VNet.

Why it's wrong: Includes a container from a different region, which breaks Azure's regional VNet constraint for ACI.

Option E: instance2 is incorrect because while instance2 is valid and deployable to VNetW, instance1 is also valid and should be included.

Why it's wrong: It's incomplete, ignoring a valid Windows container in the same region.

Final Key Takeaway:

Instance	OS Type	Region	Same as VNetW?	VNet-Compatible?	Deployable to VNetW
instance1	Windows	West US	✅ Yes	✅ Yes	✅ Yes
instance2	Linux	West US	✅ Yes	✅ Yes (now supported)	✅ Yes
instance3	Windows	East US	❌ No	✅ OS, ❌ region	❌ No

Reference:

https://learn.microsoft.com/en-us/azure/container-instances/container-instances-vnet

Ask our Experts

Did you like this **Question?**

Question 12 Correct

Domain: Deploy and manage Azure compute resources

You are tasked with deploying Azure resources for a web application using an infrastructure-as-code approach. You have the following code snippet from an Azure Bicep file:

```
param location string = 'East US'
resource appServicePlan 'Microsoft.Web/serverfarms@2022-03-01' = {
  name: 'myAppServicePlan'
  location: location
  sku: {
    name: 'P1V2'
    tier: 'PremiumV2'
  }
}
```

```
resource webApp 'Microsoft.Web/sites@2022-06-01' = {
  name: 'WhizApp'
  location: location
  properties: {
    serverFarmId: appServicePlan.id
    siteConfig: {
      alwaysOn: true
      nodeVersion: '14'
    }
  }
}
```

What will the execution of this Bicep file result in?

A. Creation of an Azure Storage Account in the specified location

B. Deployment of a virtual machine instance with premium storage

C. Provisioning of an Azure App Service Plan and a related web app right

D. Configuration of a network security group to restrict incoming traffic

---

Explanation:

Correct Answer: C

This block of code creates an Azure Web App with the following details:

```
resource webApp 'Microsoft.Web/sites@2022-06-01' = {
  name: 'WhizApp'
  location: location
  properties: {
    serverFarmId: appServicePlan.id
    siteConfig: {
      alwaysOn: true
      nodeVersion: '14'
    }
  }
}
```

name: The name of the Web App is set to 'WhizApp'.

location: The location is set to the value of the location parameter, which is 'East US'.

serverFarmId: This specifies the App Service Plan that the Web App should be associated with. It uses the id property of the appServicePlan resource, which is the unique identifier of the previously created App Service Plan.

siteConfig: Configures settings for the Web App, including enabling 'alwaysOn' (keeping the app always running) and setting the Node.js version to '14'.

In summary, this ARM template (or Bicep file) creates an App Service Plan and an associated Web App in the 'East US' region with specific configuration settings. Parameters like location are used to make the template more flexible, allowing you to specify different regions and configurations when deploying the resources.

Option A is incorrect because no mention of the storage account configuration in the code.

Option B is incorrect because a serverless WebApp is being deployed in the configuration.

Option C is correct because the code defines a webapp along with its service plan.

Option D is incorrect because no network security group or azure firewall policies are being created by the code.

Reference:

https://learn.microsoft.com/en-us/azure/app-service/provision-resource-bicep

Ask our Experts

Did you like this **Question?**

Question 13 Incorrect Marked for review

Domain: Implement and manage virtual networking

A company has set up an external load balancer that load balances traffic on port 80 and 443 across 3 virtual machines. You have to ensure that all traffic is directed towards a VM named *demovm*. How would you achieve this?

A. By creating a new public load balancer for demovm

B. By creating a new internal load balancer for demovm wrong

C. By creating an inbound NAT rule right

D. By creating a new IP configuration

Explanation:

Answer – C

Inbound NAT rule: This rule allows you to specify that traffic on certain ports should be directed to a specific backend resource, in this case, the demovm VM. This setup ensures that all traffic on ports 80 and 443 is routed directly to demovm, bypassing the load balancing across the other VMs

Options A and B are incorrect since we don't need to recreate an entire load balancer just for this scenario.

Option D is incorrect because this option does not address the requirement of directing traffic specifically to demovm through the existing load balancer setup.

For more information on port forwarding for the load balancer, please go to the below URL-

https://docs.microsoft.com/en-us/azure/load-balancer/tutorial-load-balancer-port-forwarding-portal

Ask our Experts

Did you like this **Question?**

Question 14 Correct

Domain: Manage Azure identities and governance

You have an Azure subscription that contains the following resources:

A storage account named **storage123**

A container instance named **container1**

The subscription contains a virtual network named **VirtualNet4** with the following subnets:

SubnetA: Has a Microsoft.Storage service endpoint

SubnetB: **container1** is deployed to this subnet

SubnetC: No resources are currently deployed here

You plan to deploy another Azure container instance named **container5** into **VirtualNet4**. To which subnets can you deploy **container5**?

A. SubnetA, SubnetB, and SubnetC

B. SubnetB and SubnetC only right

C. SubnetB only

D. SubnetC only

Explanation:

Correct Answer: B

Option B: SubnetB and SubnetC are correct ones because Azure Container Instances (ACI) **can be deployed** into a subnet within a virtual network **as long as that subnet is not restricted by service endpoint limitations**. In this case:

SubnetA has a Microsoft.Storage service endpoint, which restricts it to only accept traffic related to Azure Storage services. This subnet is not valid for container instance deployment.

SubnetB already hosts a container instance (**container1**), so it's correctly configured and available for container deployment.

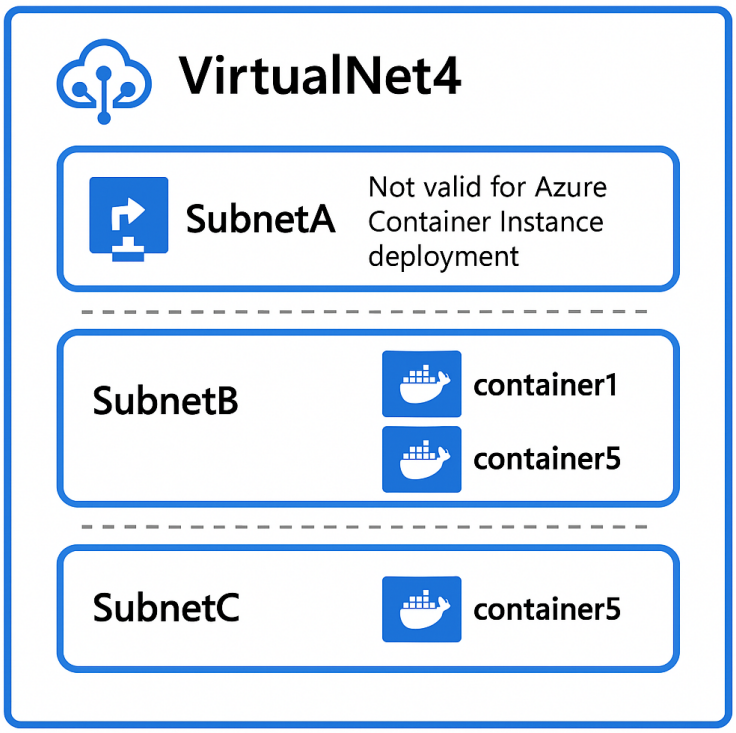
SubnetC is empty and has no restrictions — it is also a valid target for ACI deployment.

Why it's correct:

ACI requires unrestricted subnets.

Subnets with service endpoints for specific services (like Microsoft.Storage) can block non-storage resources, such as container instances

SubnetB and SubnetC do not have such restrictions and are both valid for deploying container5.



Option A: SubnetA, SubnetB, and SubnetC is incorrect because SubnetA has a **Microsoft.Storage service endpoint**, which may cause ACI deployment to fail unless additional configuration (e.g., NSG and route table exceptions) is applied.

Why it's wrong: Service endpoints can restrict subnet usage to specific Azure services. It's not a general-purpose subnet unless explicitly configured otherwise.

Option C: SubnetB only is incorrect because while SubnetB is valid, **SubnetC is also available and unrestricted**, making this answer **incomplete.**

Why it's wrong: Misses another valid option — SubnetC.

Option D: SubnetC only is incorrect because while SubnetC is valid, **SubnetB already hosts an ACI** and is correctly configured, so it should also be included.

Why it's wrong: Ignore an active subnet already used by container instances.

References:

https://learn.microsoft.com/en-us/azure/container-instances/container-instances-vnet#deploy-to-new-virtual-network

https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview

Ask our Experts

Did you like this **Question?**

Question 15 Correct Marked for review

Domain: Deploy and manage Azure compute resources

View Case Study

To meet the technical requirements of migrating all websites and app services from App and Web servers to Azure. Which of the following services must be required for websites and applications to work in an optimized and secured manner? [Select Two]

A. Network Security Groups

B. Azure Firewall

- [x] C. Azure App Services right
- [x] D. Azure Application Gateway right

Explanation:

Correct Answers: C and D

Option A is incorrect because network security groups are used for managing security on virtual machines and subnets.

Option B is incorrect because Azure firewall is not a required service, it is good to have, however, not required as app services have their own web application firewall features.

Option C is correct because Azure App Services is a fully managed platform for building, deploying, and scaling web apps. It provides high availability, auto-scaling, and built-in security features, making it ideal for hosting your websites and applications

Option D is correct because Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications. It includes a Web Application Firewall (WAF) that helps protect your applications from common web vulnerabilities and attacks

References:

https://learn.microsoft.com/en-us/azure/application-gateway/overview

https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overview

https://learn.microsoft.com/en-us/azure/app-service/overview

Ask our Experts

Did you like this **Question?**

Question 16 Correct Marked for review

Domain: Deploy and manage Azure compute resources

You plan to deploy an Azure Web App with the following settings:

Name: WebApp1

Publish: Docker Container

Operating System: Windows

Region: West US

App Service Plan (Windows, West US): ASP-RG1-8bcf

You need to ensure that WebApp1 uses the ASP.NET V4.8 runtime stack. Which setting should you modify?

A. Publish right

B. Operating system

C. Region

D. Windows Plan

Explanation:

Correct Answer: A

Option A: Publish is correct becuase

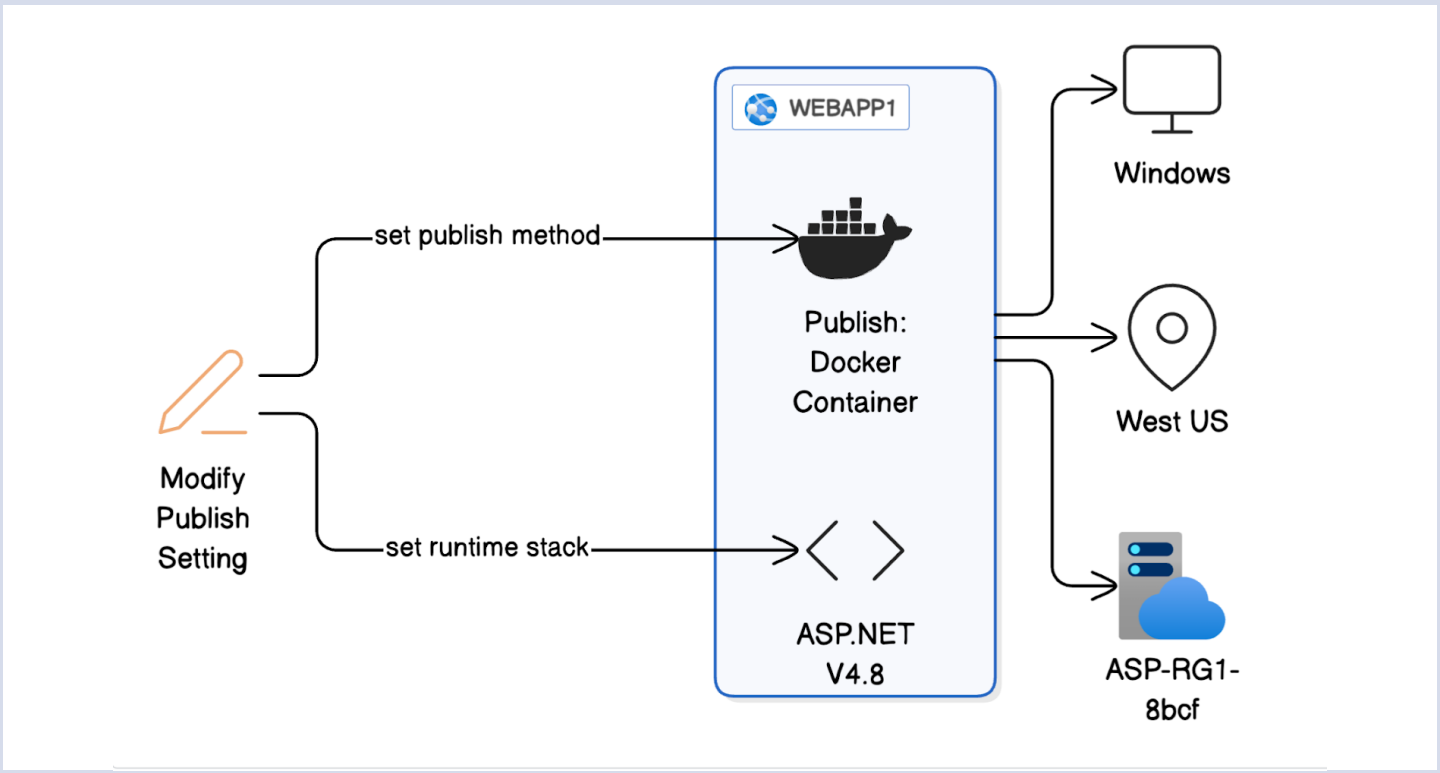
Currently, the app is set to "Publish: Docker Container", which means you're deploying a custom container image — not using built-in runtime stacks such as ASP.NET v4.8.

To use ASP.NET V4.8, you must select "Code" as the publish method instead of Docker. This tells Azure App Service to use a pre-configured runtime environment, including ASP.NET frameworks like v4.8, instead of expecting a user-defined container.

Why it's correct: The Publish option defines how the app is delivered and run.

Selecting "Code" allows you to choose ASP.NET runtime stacks (e.g., .NET Framework 4.8).

Selecting "Docker Container" means you must provide a container image that includes everything — including the framework — and Azure won't give you a runtime stack option.



Option B: Operating system is incorrect because Windows is the correct OS because **ASP.NET 4.8 only** runs on **Windows** App Service — it's not supported on Linux.

Why it's wrong: This setting is already correctly configured.

Option C: Region is incorrect because the region (West US) has no impact on the runtime stack or framework availability

Why it's wrong: Changing the region won't make ASP.NET 4.8 appear unless Publish is set to "Code".

Option D: Windows Plan is incorrect because the App Service Plan is already a valid Windows-based plan in the same region. It doesn't affect the available **runtime stack**, only the **hosting resources** (e.g., compute, pricing tier).

Why it's wrong: The issue isn't with the plan but with how the app is being published.

References:

https://learn.microsoft.com/en-us/azure/app-service/overview

https://learn.microsoft.com/en-us/azure/app-service/quickstart-dotnetcore?tabs=net80&pivots=development-environment-vs

Ask our Experts

Did you like this **Question?**

Question 17 Incorrect Marked for review

Domain: Deploy and manage Azure compute resources

You plan to deploy the following Azure web apps:

WebApp1 – uses the .NET 8 runtime stack

WebApp2 – uses the ASP.NET V4.8 runtime stack

WebApp3 – uses the Java 21 runtime stack

WebApp4 – uses the PHP 8.3 runtime stack

You need to create the App Service Plans to support these apps. What is the minimum number of App Service Plans that should be created?

A. 1

B. 2 right

C. 3 wrong

D. 4

Explanation:

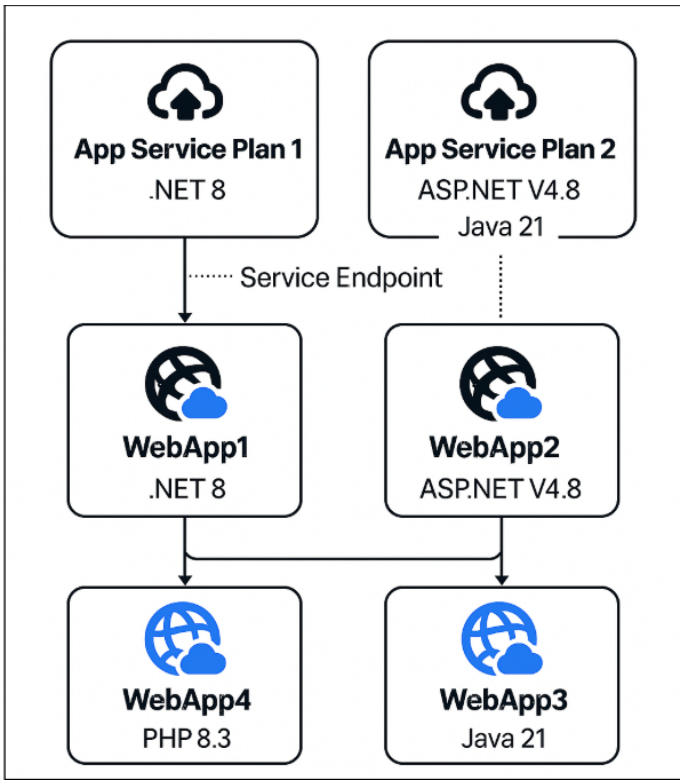
Correct Answer: B

Option B: 2 Correct because Azure App Service Plans can be shared by multiple web apps, if those apps use the same operating system (OS platform). The runtime stack determines whether the app needs to run on Windows or Linux:

So, we have:

One Windows plan needed for WebApp2 (.NET Framework 4.8 is Windows-only)

One Linux plan for WebApp1, WebApp3, and WebApp4 (all supported on Linux)



Why it's correct: You can host multiple apps on the same plan as long as they share the same OS platform. Since the Windows vs. Linux boundary is strict, we need 2 separate plans:

One Windows App Service Plan

One Linux App Service Plan

Option A: 1 incorrect because

You cannot run both Windows and Linux apps on the same App Service Plan.

Since ASP.NET V4.8 (WebApp2) requires Windows, and the rest require Linux, at least two plans are mandatory.

Azure does not support mixed-platform app plans.

Option C: 3 incorrect because

This overestimates the number of plans needed.

Some may think Java or PHP requires separate plans, but Azure supports hosting different Linux runtimes together in the same Linux plan.

WebApp1 (.NET 8), WebApp3 (Java), and WebApp4 (PHP) can all run on a single Linux plan, so a third plan isn't needed.

Option D: 4 incorrect because

You do not need one App Service Plan per web app unless you're intentionally isolating for scaling or billing.

Azure App Service Plans are multi-tenant capable — you can deploy multiple apps on one plan, as long as they use the same OS.

This option ignores the resource-sharing capabilities of Azure App Service.

References:

https://learn.microsoft.com/en-us/azure/app-service/overview-hosting-plans

https://learn.microsoft.com/en-us/azure/app-service/configure-common?tabs=portal

Ask our Experts

Did you like this **Question?**

Question 18 Unattempted

Domain: Deploy and manage Azure compute resources

Whizlabs Inc. is planning on deploying Azure container registry. What is the correct order in the process of creating and managing an Azure container registry.

Correct Answer

1. D. Create an Azure container registry
2. B. Choose a pricing tier
3. A. Configure container registry settings
4. E. Set up authentication and security
5. C. Access and manage container images

Explanation:

Correct Answer: D, B, A, E and C

The correct order of steps as follows:

D. Create an Azure container registry.

B. Choose a pricing tier.

A. Configure container registry settings.

E. Set up authentication and security.

C. Access and manage container images.

Create an Azure Container Registry: This is the first step in the process. You need to create the actual container registry in Azure before you can perform any other actions related to it.

Choose a Pricing Tier: After creating the container registry, you need to select a pricing tier that aligns with your requirements. The pricing tier determines the features and capacity of the registry.

Configure Container Registry Settings: Once the pricing tier is selected, you should configure various settings for the container registry,

such as network settings, repository names, and more. This step ensures the registry is properly configured for your use case.

Set up Authentication and Security: Before you start using the container registry, it's important to set up authentication and security measures. This includes configuring user roles, permissions, and authentication mechanisms to ensure secure access to the registry.

Access and Manage Container Images: After all the setup steps are complete, you can start uploading, managing, and accessing container images within the registry. This step involves tasks like pushing images, pulling images, and managing repository versions.

Reference:

Tutorial - Create geo-replicated registry - Azure Container Registry | Microsoft Learn

Ask our Experts

Did you like this **Question?**

Question 19 Incorrect

Domain: Implement and manage storage

A company needs to create a storage account that must follow the requirements below.

Copies your data synchronously three times within a single physical location

Durability for storage resources of at least 99.99999999999999% over a given year.

Ability to store archive data.

Users should be able to have Azure files in place and accessible across multiple VMs.

The solution needs to be cost-effective.

What is the type of replication they need to implement for the storage account?

A. Locally redundant storage (LRS) right

B. Zone-redundant storage (ZRS) wrong

C. Geo-redundant storage (GRS)

D. Read-access geo-redundant storage (RA-GRS)

Explanation:

Answer: **A**

Copies your data synchronously three times within a single physical location: LRS replicates data three times within a single data center.
Durability for storage resources of at least 99.99999999999999% over a given year: LRS provides high durability by keeping multiple copies of the data.

Ability to store archive data: LRS supports different storage tiers, including archive.
Users should be able to have Azure files in place and accessible across multiple VMs: LRS supports Azure Files, which multiple VMs can access.
The solution needs to be cost-effective: LRS is the most cost-effective option compared to other replication strategies like ZRS, GRS, and RA-GRS.

Option B is incorrect because ZRS copies your data synchronously across three Azure availability zones within the same region. This provides high availability and durability but does not meet the requirement of copying data within a single physical location (data center). ZRS is generally more expensive than LRS due to the additional redundancy across availability zones.

Option C is incorrect because GRS copies your data synchronously three times within one or more availability zones in the primary region using LRS, and then copies your data asynchronously to a secondary region. This protects against regional disasters but does not meet the requirement of copying data within a single physical location. GRS is more expensive than LRS due to the additional geo-replication

Option D is incorrect because it does not provide GRS durability for storage resources of at least 99.99999999999999% (16 9's) over a given year and is not supported for Azure Files.

Reference: Data redundancy - Azure Storage | Microsoft Learn

Ask our Experts

Did you like this **Question?**

Question 20

Correct

Domain: Deploy and manage Azure compute resources

You have an Azure subscription. You plan to create a storage account with the following settings:

Name: storage1

Performance: Standard

Redundancy: Zone-redundant storage (ZRS)

What is the minimum number of copies of storage1 data stored in Azure?

A. 2

B. 9

C. 6

D. 3 right

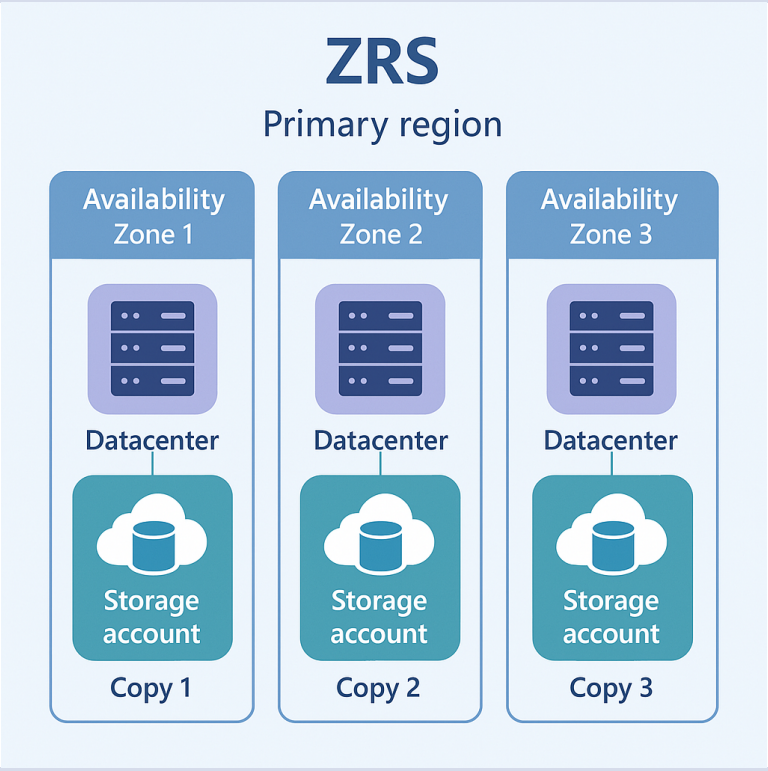
Explanation:

Correct Answer: D

Option D: 3 is correct because When you use **Zone-Redundant Storage (ZRS)**, Azure stores **three copies** of your data **across three availability zones within a single Azure region.**

Each availability zone is a physically separate location with independent power, cooling, and networking.

ZRS ensures high availability and durability even if one entire zone becomes unavailable.



Why it's correct: ZRS replicates your data synchronously across three zones, maintaining three distinct copies at all times.

Option A: 2 is incorrect because Azure **does not use 2 copies** for any standard redundancy option. Two copies would not meet Azure's durability SLA or protect against zone failure.

Why it's wrong: This would create a single point of failure and is not supported in Azure's redundancy models.

Option B: 9 is incorrect because no Azure storage redundancy tier uses **9 copies**. This number might arise if someone assumes ZRS in 3 zones × 3 local copies each, but that is not how Azure ZRS operates.

Why it's wrong: This is a misunderstanding of the ZRS architecture. It uses 1 copy per zone, not 3 per zone.

Option C: 6 is incorrect because Azure does not store **6 copies for ZRS**. This might be confused with **RA-GRS (Read-Access Geo-Redundant Storage)** which stores 3 local copies in the primary region and 3 geo-replicated copies in a secondary region, totaling **6**, but that's **not ZRS**.

Why it's wrong: ZRS is zone-level, not geo-level replication. Only 3 copies are made across zones in a single region.

Reference:

Azure Storage redundancy options

Ask our Experts

Did you like this **Question?**

Question 21 Incorrect

Domain: Implement and manage storage

Version-level immutability can be enabled or disabled on the storage account at any point of time. Is this statement correct? (Select Yes or No)

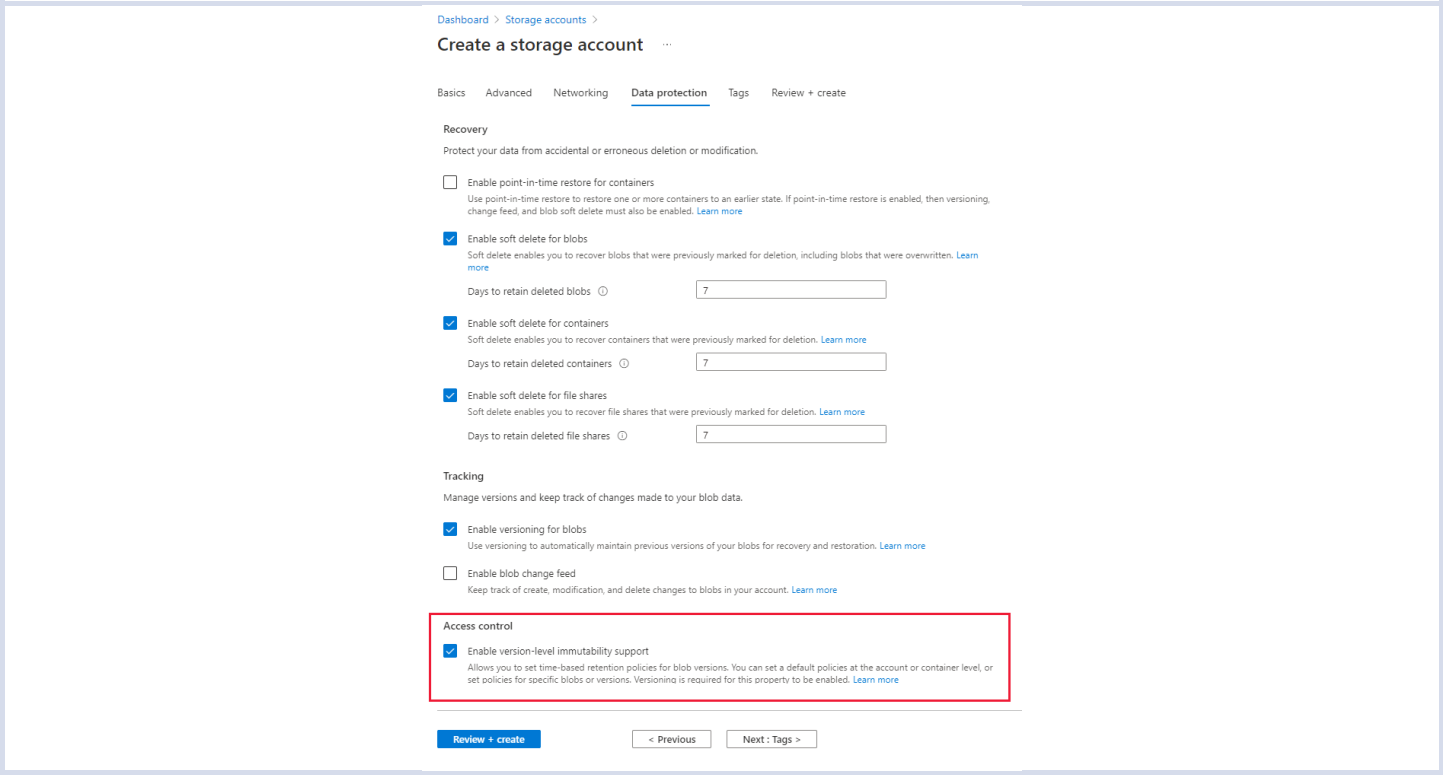
A. Yes wrong

B. No right

Explanation:

Correct Answer: B

Version-level immutability is a **storage account–level setting** that allows individual blob versions to be protected from deletion or modification using immutability policies.



[Source: Microsoft Documentation]

Once version-level immutability is enabled, it cannot be disabled — the setting becomes permanent for the storage account. This ensures that versioned blobs can always be protected using policies, even if future policy enforcement is removed or changed.

> **Note**
>
> Version-level immutability cannot be disabled after it is enabled on the storage account, although locked policies can be deleted.

This setting is **used for regulatory compliance** and **data protection** scenarios where blob data must remain tamper-proof.

Why it's correct: The original statement says that version-level immutability can be disabled at any time, but this is incorrect. Once enabled, it stays enabled permanently, even if you remove individual policies.

Reference:

https://learn.microsoft.com/en-us/azure/storage/blobs/immutable-policy-configure-version-scope?tabs=azure-portal

Ask our Experts

Did you like this **Question?**

Question 22 Incorrect

Domain: Implement and manage storage

You have a storage account named **whizlabstore**. You have created a file share named **demo** using the file service. You need to ensure that users can connect to the file share from their home computers. Which of the following port should be open to provide the connectivity?

- A. 80 wrong
- B. 443
- C. 445 right

D. 3389

Explanation:

Answer – C

To access files from home computers, users have to use SMB protocol that expects port 445 to be open.

This is clearly given in the Microsoft documentation.

Prerequisites

Ensure port 445 is open: The SMB protocol requires TCP port 445 to be open; connections will fail if port 445 is blocked. You can check if your firewall is blocking port 445 with the `Test-NetConnection` cmdlet. To learn about ways to work around a blocked 445 port, see the Cause 1: Port 445 is blocked section of our Windows troubleshooting guide.

For more information on using file shares in Azure, please visit the below URL-

https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows

Ask our Experts

Did you like this **Question?**

Question 23 Incorrect

Domain: Implement and manage storage

Contoso Inc., a multinational company, is migrating its on-premises file servers to Azure Files. The IT team wants to enforce granular access control for users accessing files and directories within a file share, using identity-based access. Which of the following mechanisms supports this capability?

A. Microsoft Entra Domain Services right

B. Role-Based Access Control (RBAC) wrong

C. Shared Key Authentication

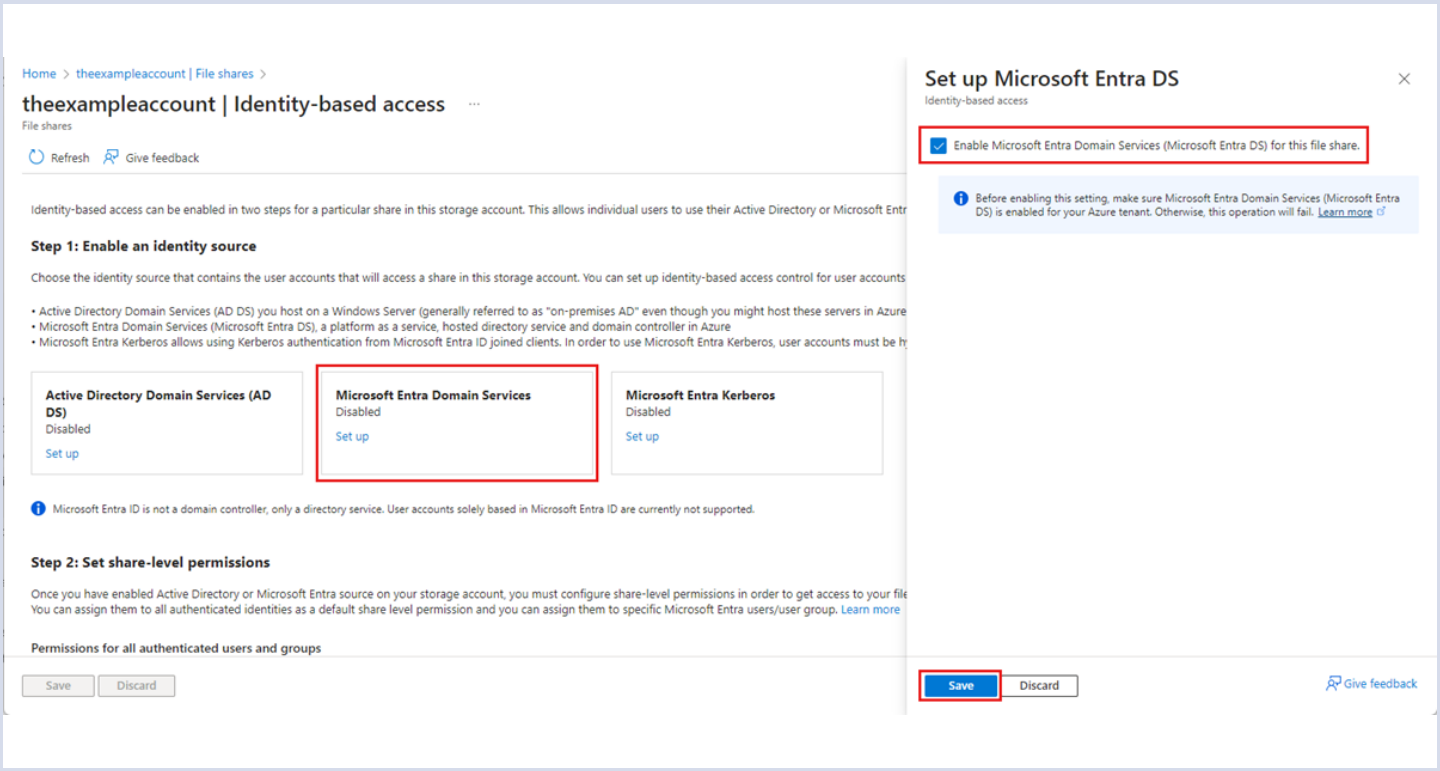
D. Virtual Network Service Endpoints

Explanation:

Correct Answer: A

Option A: Microsoft Entra Domain Services is correct because Microsoft Entra Domain Services provides domain-join, LDAP, Kerberos/NTLM authentication, and is fully compatible with Windows ACLs (Access Control Lists). It allows file shares to be integrated with a managed domain, enabling fine-grained NTFS permissions at both the file and folder level.

Why it's correct: It is the only option that enables directory- and file-level granular permissions using Microsoft Entra (formerly Azure AD) identities through identity-based authentication with Azure Files.



[Source: Microsoft Documentation]

Option B: Role-Based Access Control (RBAC) is incorrect because it is used to control access at the Azure resource level, such as who can manage storage accounts, virtual machines, or networking — not at the file/folder level inside Azure Files.

Why it's wrong: RBAC does not support granular control over individual files and directories. It cannot enforce NTFS-level access permissions inside a file share.

Option C: Shared Key Authentication is incorrect because it grants access using a storage account key, giving broad access to the entire file share. It does not support per-user access control or directory-level restrictions.

Why it's wrong: It bypasses identity-based control. Any user with the shared key can access all files, without restrictions or auditing.

Option D: Virtual Network Service Endpoints is incorrect because Service endpoints secure traffic between your VNet and Azure Storage by keeping traffic on Microsoft's backbone network. They protect at the network level, not the file system level.

Why it's wrong: While they increase network security, they don't control file or directory access based on user identity or permissions.

Reference:

Enable Microsoft Entra Domain Services authentication on Azure Files

Ask our Experts

Did you like this **Question?**

Question 24

Correct

Domain: Implement and manage virtual networking

A company has set up a Virtual Machine in Azure. A web server listening on port 80 and a DNS server has been installed on the Virtual machine. A network security group is attached to the network interface for the virtual machine. The rules for the NSG are given below.

Inbound Rules

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	RuleA	50-60	Any	Any	Any	Deny
110	Allow_rdp	3389	Any	Any	Any	Allow
120	RuleB	50-500	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Outbound Rules

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	RuleC	80	Any	Any	Any	Deny
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

If RuleB is deleted/omitted, please select the service through which Internet users connect to the virtual machine.

A. Through the web server

B. Through the DNS server

C. both Web and DNS servers

D. Through RDP right

E. Through RDP, Web, and DNS servers

Explanation:

Answer – D

If RuleB is deleted, users won't be able to access port 80 and the web server.

There is a Deny rule of RuleA for ports 50-60. Since DNS listens on port 53, you will not be able to access the DNS server. But you will still be able to connect to the virtual machine using Remote Desktop Protocol (RDP) under the Allow_rdp rule.

Because of this logic, all other options are incorrect.

For more information on network security, please visit the below URL-

Azure network security groups overview | Microsoft Docs

Ask our Experts

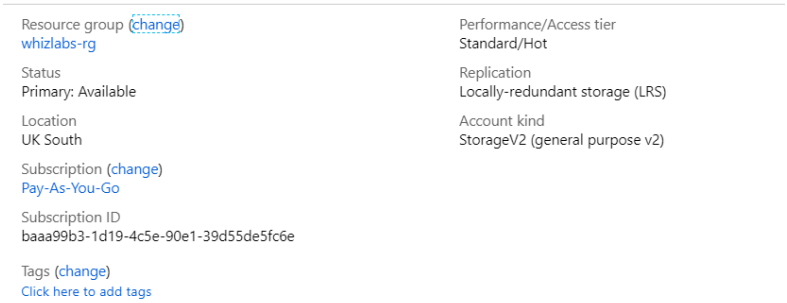
Did you like this **Question?**

Question 25

Correct

Domain: Implement and manage storage

Your company has set up a storage account in Azure, as shown below.



There is a requirement to retain any blob data that might accidentally be deleted. The deleted data needs to be retained for 14 days.

From which of the following option of the storage account would you modify to fulfill this requirement?

A. Firewall and virtual networks

B. Advanced security

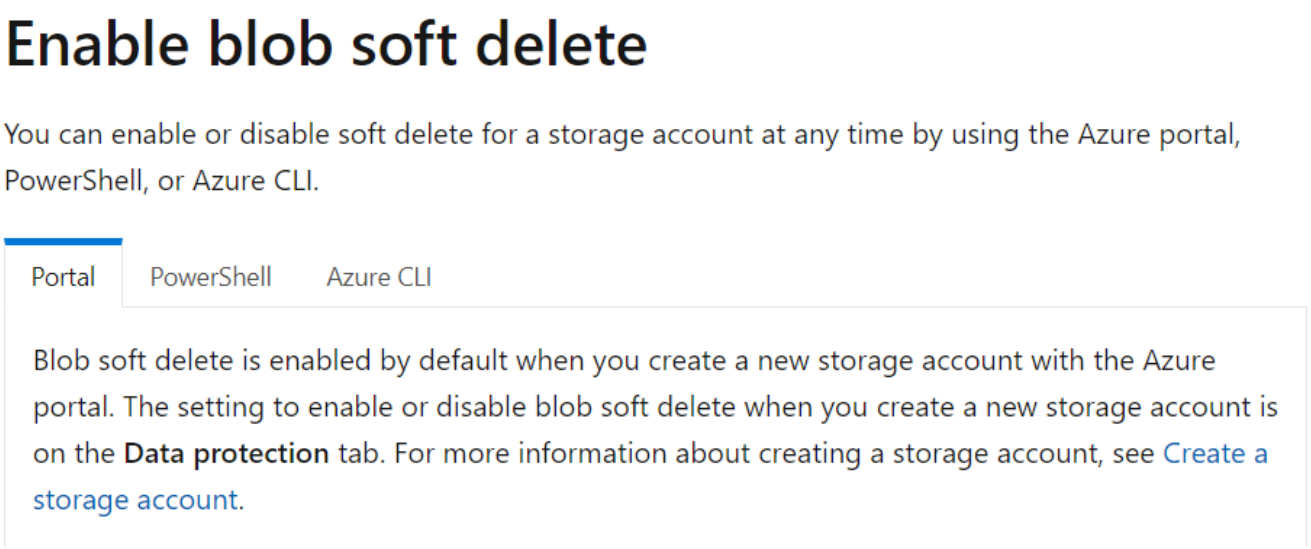
C. Data Protection(Soft Delete) right

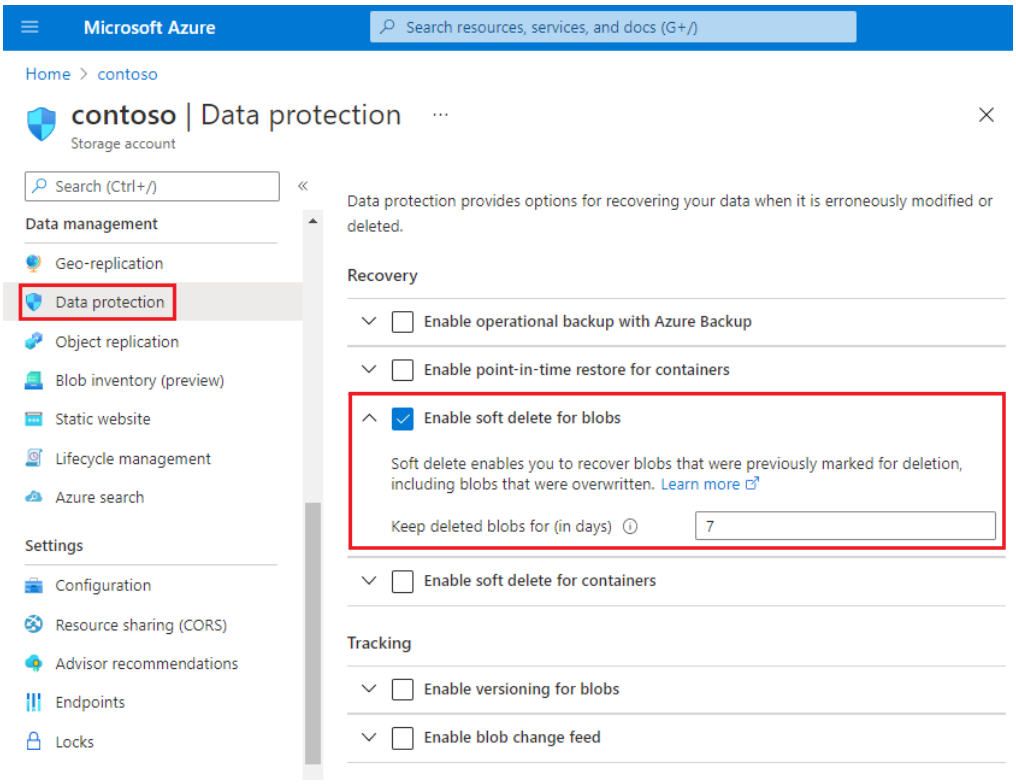
D. Lifecycle Management

Explanation:

Answer – C

This can be done from the **Data Protection** option/tab from the storage account at any time by using the Azure portal, PowerShell, or Azure CLI.





Blob soft delete **protects an individual blob, snapshot, or version from accidental deletes or overwrites by maintaining the deleted data in the system for a specified period of time.** During the retention period, you can restore a soft-deleted object to its state at the time it was deleted.

Since this is clear from the implementation, all other options are incorrect.

Reference: **Enable soft delete for blobs - Azure Storage | Microsoft Learn**

Ask our Experts

Did you like this **Question?**

Question 26 Incorrect

Domain: Monitor and maintain Azure resources

Match each Azure Monitor feature with its correct description in the context of VM Insights. Each feature is used to monitor and analyze virtual machines and their performance metrics at scale.

Note: Drag the appropriate feature name and drop them to the correct description

Your Answers

A. Activity log

Analyze performance indicators like CPU usage or disk IOPS across machines without pre-scoping a single VM

B. Alerts

Review threshold-based or dynamic warnings and incidents generated by rules across multiple VMs

C. Metrics

Access prebuilt dashboards and visualizations for multiple VMs, including performance trends and guest OS details

D. Logs

Use powerful query-based investigation into system events, boot diagnostics, and application logs across all connected machines

E. Workbooks

See recent operational events, such as VM creation, updates, or deletions, across all virtual machines by applying resource-type filters

Correct Answers

A. Activity log

See recent operational events, such as VM creation, updates, or deletions, across all virtual machines by applying resource-type filters

B. Alerts

Review threshold-based or dynamic warnings and incidents generated by rules across multiple VMs

C. Metrics

Analyze performance indicators like CPU usage or disk IOPS across machines without pre-scoping a single VM

D. Logs

Use powerful query-based investigation into system events, boot diagnostics, and application logs across all connected machines

E. Workbooks

Access prebuilt dashboards and visualizations for multiple VMs, including performance trends and guest OS details

Correct Answers [Matching]: A-1, B-3, C-2, D-4, E-5

Option A: Activity log (Correct Match: 1)

The **activity log** provides insight into Azure Resource Manager-level events, such as who started or stopped a VM, created a disk, or modified configurations. It is not VM-specific but can be filtered by VM resource types.

Why it's correct: Filtering by Virtual Machine or VMSS lets you narrow down log entries specific to compute resources — useful for auditing and troubleshooting.

Option B: Alerts (Correct Match: 3)

Alerts notify you when a monitored condition is met — such as CPU usage > 80% for 5 minutes. These rules apply across resources and can be viewed centrally for all machines.

Why it's correct: Alerts support both metric- and log-based rules, and VM alerts can be viewed in aggregate by filtering on resource types.

Option C: Metrics (Correct Match: 2)

The Metrics Explorer allows real-time charting and trend analysis of performance counters like CPU, memory, and network. By default, it's unscoped, enabling multi-VM comparison by selecting a group or subscription.

Why it's correct: Unlike Logs, Metrics are pre-aggregated and offer a near real-time view of performance across many VMs.

Option D: Logs (Correct Match: 4)

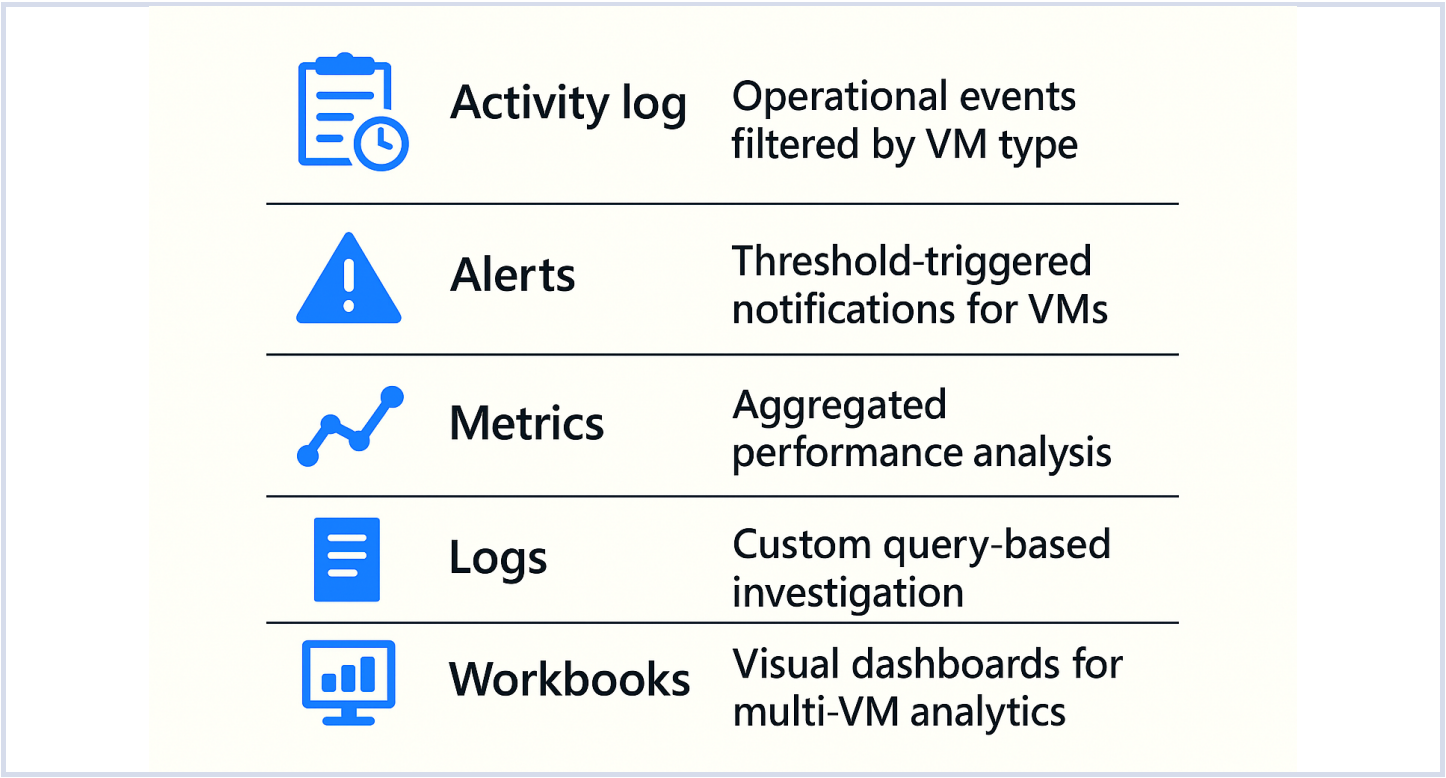
This refers to **Log Analytics**, where you can run **Kusto Query Language (KQL)** queries to analyze logs from connected machines — including boot times, update status, agent health, and custom events.

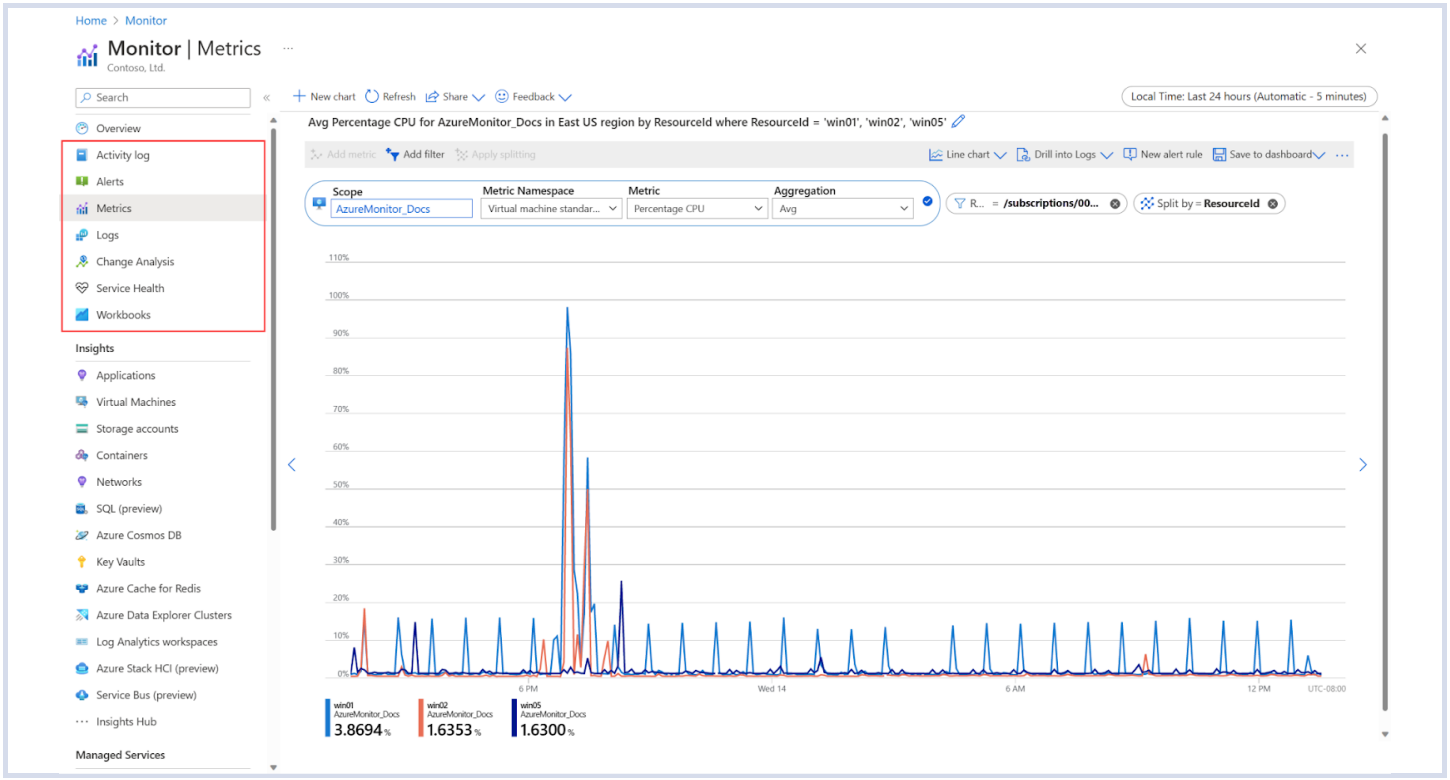
Why it's correct: Log Analytics supports deep inspection and correlation of data at the workspace level, not limited to one VM.

Option E: Workbooks (Correct Match: 5)

Workbooks are interactive, visual reports that help you track and correlate data across your infrastructure. The VM insights workbooks come prebuilt for monitoring groups of VMs together.

Why it's correct: They provide dashboard-like experiences using log and metric data for CPU, memory, disk, and health analysis.





[Source: Microsoft Documentation]

Reference:

Monitor virtual machines with Azure Monitor: Analyze monitoring data - Azure Monitor | Microsoft Learn

Ask our Experts

Did you like this **Question?**

Question 27

Incorrect

Domain: Deploy and manage Azure compute resources

A virtual machine (VM) called "myVM" is connected to the key vault to run Azure Disk Encryption. Now you need to move that virtual machine to a different resource group, subscription, and region. Identify the correct sequence of steps to achieve this using the Azure CLI.

Drag the steps into the correct order by selecting the appropriate options below and Drop them in the answer space.

Your Answer

1. az group create --name newResourceGroup --location newRegion
2. az vm deallocate --name myVM --resource-group oldResourceGroup
3. az vm wait --name myVM --resource-group oldResourceGroup --deleted
4. az vm create --name myVM --resource-group newResourceGroup --location newRegion --source oldResourceGroup

Correct Answer

1. az vm deallocate --name myVM --resource-group oldResourceGroup
2. az group create --name newResourceGroup --location newRegion
3. az vm create --name myVM --resource-group newResourceGroup --location newRegion --source oldResourceGroup
4. az vm wait --name myVM --resource-group oldResourceGroup --deleted

Explanation:

Correct Answer: B, D, C and, A

A virtual machine that is integrated with a key vault to implement Azure Disk Encryption for Linux VMs or Azure Disk Encryption for Windows VMs can be moved to another resource group when it is in a deallocated state.

However, to move such a virtual machine to another subscription, you must disable encryption.

To move a virtual machine (VM) named "myVM" to a different resource group, subscription, and region using the Azure CLI, here is the correct order of steps:

The correct order of steps is B, D, C & A.

B. az vm deallocate --name myVM --resource-group oldResourceGroup : Stop the VM in the old resource group.

D. az group create --name newResourceGroup --location newRegion: Create a new resource group in the desired region.

C. az vm create --name myVM --resource-group newResourceGroup --location newRegion --source oldResourceGroup : Move the VM to the new resource group and region.

A. az vm wait --name myVM --resource-group oldResourceGroup --deleted: Wait for the VM to be deleted from the old resource group.

Reference:

Move Azure VMs to new subscription or resource group - Azure Resource Manager | Microsoft Learn

Ask our Experts

Did you like this **Question?**

Question 28

Correct

Domain: Implement and manage virtual networking

You are managing a Virtual Machine (VM) in Azure that hosts both a web server (listening on port 80) and a DNS server (on port 53). The VM is protected using a Network Security Group (NSG) with the following rule configuration:

RuleB currently allows inbound TCP traffic on ports 50–500 (priority 120).

RuleA denies all traffic on ports 50–60 (priority 100).

An explicit rule exists to allow RDP traffic on port 3389 (priority 110).

Outbound rules allow internet access, but inbound rules control public connectivity. If RuleB is deleted, through which service can Internet users still successfully connect to the virtual machine?

A. Through the web server

B. Through the DNS server

C. Both web and DNS servers

D. Through RDP right

Explanation:

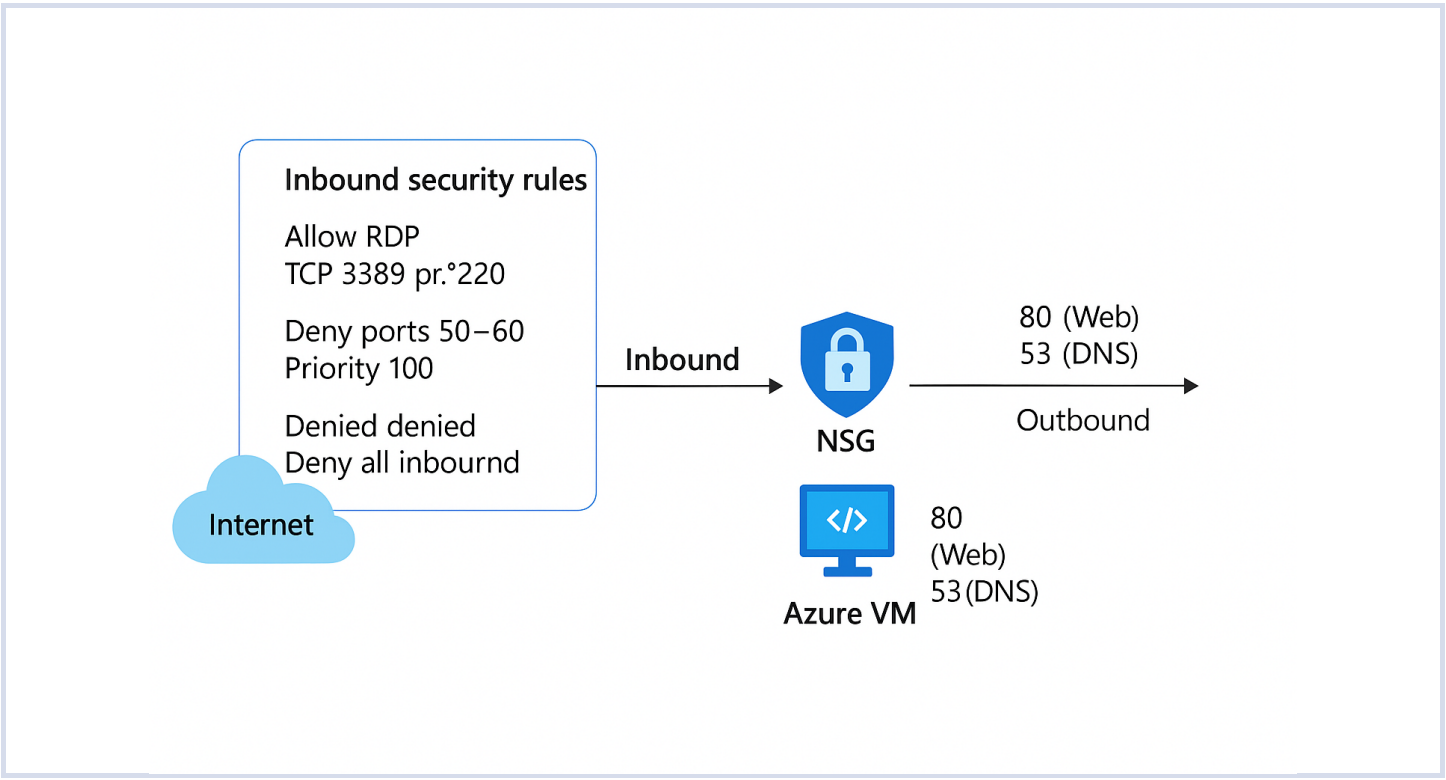
Correct Answer: D

Option D: Through RDP is correct because Even after deleting RuleB, RDP access remains allowed via the “Allow_rdp” rule. This means internet users can still remotely access the VM using RDP.

RDP uses TCP port 3389.

There is an explicit inbound allow rule for RDP in "Allow_rdp" (priority 110).

RuleA (priority 100) applies only to ports 50–60 and does not affect port 3389



Option A: Through the web server is incorrect because without RuleB, port 80 is not allowed inbound. So, internet users cannot access the web server.

The web server typically listens on port 80. While outbound traffic on port 80 is explicitly denied via RuleC (priority 100, Action: Deny), it's important to also look at the inbound rules:

RuleA denies traffic on ports 50–60

RuleB (deleted in this case) was allowing TCP traffic on ports 50–500

If RuleB is removed:

No explicit inbound allow rule exists for port 80, and

As per Azure NSG rules, the default behavior is to deny unless explicitly allowed.

Option B: Through the DNS server is incorrect because port 53 falls within the denied range (RuleA: 50–60 Deny), DNS access is also blocked.

A DNS server typically uses UDP or TCP port 53.

No inbound rule allows port 53.

RuleA only denies ports 50–60, which includes 53.

With RuleB removed, there's no explicit allow for port 53 either.

Option C: Both Web and DNS servers is incorrect because both ports are denied, so internet users cannot access either service.

As explained in A and B: Web server (port 80) and DNS server (port 53) are both blocked due to RuleA and the deletion of RuleB.

Reference:

Create and configure network security groups (NSGs)

Ask our Experts

Did you like this **Question?**

Question 29 Correct

Domain: Deploy and manage Azure compute resources

Whizlabs Corporation is looking to deploy containerized applications in Azure and needs a container registry to store their Docker images. Which of the following Azure service provides a private and secure repository for storing Docker container images?

A. Azure Kubernetes Service (AKS)

B. Azure Container Instances (ACI)

C. Azure Container Registry (ACR) right

D. Azure Container Service (ACS)

Explanation:

Correct Answer: C

Azure Container Registry (ACR) is a private and secure repository for storing Docker container images. It allows organizations to manage and distribute container images securely, making it an essential service for containerized applications in Azure.

Option A is incorrect because Azure Kubernetes Service (AKS) is a managed Kubernetes container orchestration service, not a container registry.

Option B is incorrect Azure Container Instances (ACI) is a serverless container service for running containers, but it does not provide container image storage.

Option C is correct because Azure Container Registry (ACR) is a private and secure repository for storing Docker container images. It allows organizations to manage and distribute container images securely, making it an essential service for containerized applications in Azure.

Option D is incorrect because Azure Container Service (ACS) is an older service that has been deprecated in favor of Azure Kubernetes Service (AKS) for managing Kubernetes clusters.

References:

Azure Container Registry | Microsoft Azure

Managed container registries - Azure Container Registry | Microsoft Learn

Ask our Experts

Did you like this **Question?**

Question 30 Incorrect

Domain: Implement and manage storage

You are configuring Microsoft Entra Domain Services (Entra DS) authentication for Azure Files in a hybrid environment. Your organization uses on-premises Active Directory and wants to provide identity-based access to Azure file shares for users.

Drag and drop the following steps into the correct order to enable Entra DS-based authentication for Azure Files.

Your Answer	Correct Answer
1. A. Domain join your virtual machines to Microsoft Entra Domain Services	1. C. Sync on-prem AD to Microsoft Entra ID using Entra Connect
2. C. Sync on-prem AD to Microsoft Entra ID using Entra Connect	2. A. Domain join your virtual machines to Microsoft Entra Domain Services
3. D. Configure directory/file-level NTFS permissions	3. B. Enable Azure Files Microsoft Entra DS authentication
4. B. Enable Azure Files Microsoft Entra DS authentication	4. D. Configure directory/file-level NTFS permissions

Explanation:

Correct Answers [Sequence]: C - A - B - D

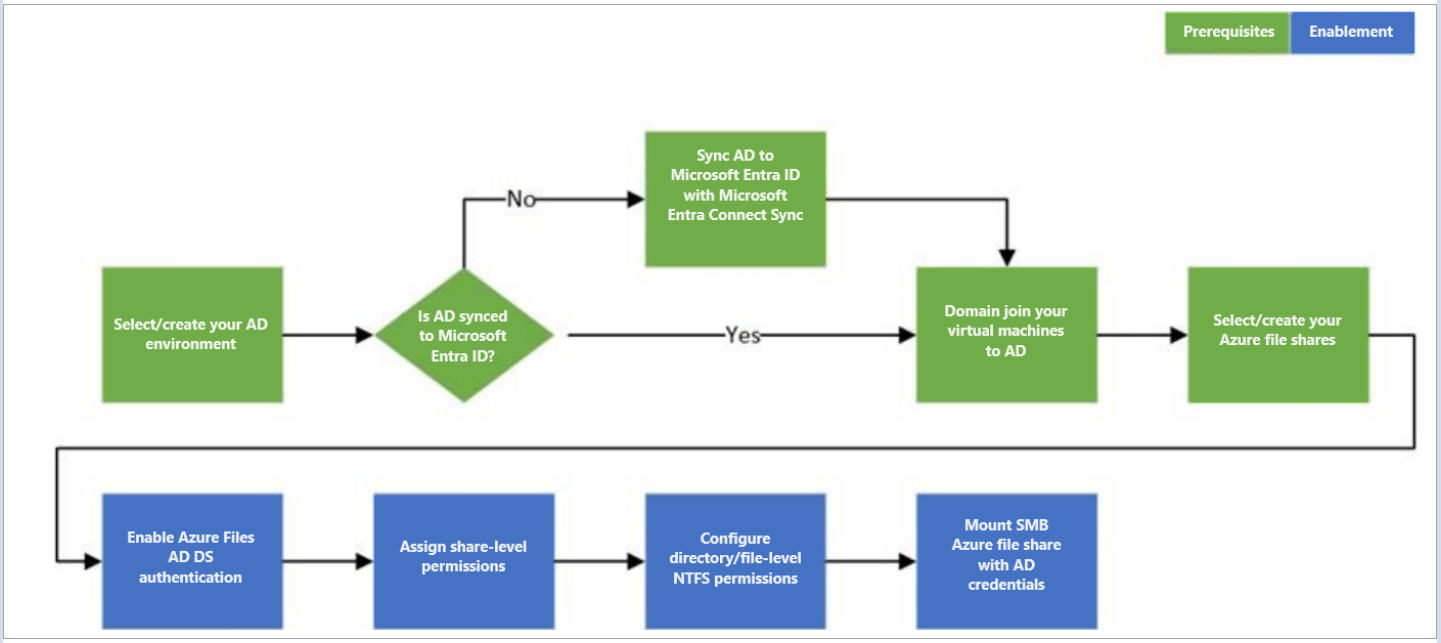
C. Sync on-prem AD to Microsoft Entra ID using Entra Connect

A. Domain join your virtual machines to Microsoft Entra Domain Services

B. Enable Azure Files Microsoft Entra DS authentication

D. Configure directory/file-level NTFS permissions

Summary Flow (Simplified): Sync identities → Join VMs to Entra DS → Enable File Share Auth → Set Permissions



[Source: Microsoft Documentation]

Option C: Sync on-prem AD to Microsoft Entra ID using Entra Connect (Step 1)

This is the **first and foundational step** in enabling Microsoft Entra DS-based authentication. You must sync your **on-premises Active Directory users and groups** to Entra ID using **Microsoft Entra Connect Sync**. This hybrid identity setup allows those users to be recognized and authenticated within Azure services, including Microsoft Entra Domain Services.

> Why it's correct: Without syncing AD identities to Entra ID, you can't proceed with domain services in Azure. Entra DS requires cloud visibility of your on-prem directory.

Option A: Domain join your virtual machines to Microsoft Entra Domain Services (Step 2)

Once Entra DS is provisioned and identity sync is in place, your VMs in Azure must be **domain joined to Microsoft Entra DS**. This allows them to communicate securely with the domain and apply access controls using NTFS and ACLs for Azure Files.

> Why it's correct: Joining VMs to the domain ensures they can authenticate users and set permissions correctly, just like a traditional Windows domain environment.

Option B: Enable Azure Files Microsoft Entra DS authentication (Step 3)

After the VM is domain-joined, you can **enable identity-based access to Azure Files** by activating Microsoft Entra DS authentication for the file share. This integrates SMB (Server Message Block) file share access with Entra DS accounts.

> Why it's correct: This setting is what binds the Azure file share to your domain-based identity provider, allowing granular access management using synced user accounts.

Option D: Configure directory/file-level NTFS permissions (Step 4)

After enabling Entra DS authentication, the final step is to apply NTFS-level permissions from a **domain-joined VM.** This includes using Windows File Explorer or command-line tools to **assign folder- and file-level access** for specific Entra DS users or groups.

> Why it's correct: This is the final configuration step that secures access at the granular level, just like in traditional file server

environments — using ACLs (Access Control Lists).

Reference:

On-premises AD Domain Services authentication over SMB for Azure file shares

Ask our Experts

Did you like this **Question?**

Question 31 Incorrect

Domain: Manage Azure identities and governance

Your organization has several offices. You need to reflect the organization structure in Microsoft Entra ID by creating administrative units.

Please select the tools you can use to create administrative units.

- [ ] A. Power Platform Admin center wrong
- B. Microsoft Graph/PowerShell right
- [ ] C. Microsoft Entra admin center right
- D. Azure CLI

Explanation:

Correct Answers: B and C

Option A is incorrect, This tool is primarily used for managing Power Platform environments and resources. It does not support the creation or management of administrative units in Microsoft Entra ID, so this option is not applicable.

Option B is Correct, These provide powerful scripting capabilities to automate and manage Microsoft Entra ID resources, including administrative units. Ideal for automation and bulk operations.

Option C is Correct, This is a user-friendly interface specifically designed for managing Microsoft Entra ID, including creating and managing administrative units. It's convenient for those who prefer a graphical interface.

Option D is incorrect, The Azure CLI is a command-line tool for managing Azure resources. However, it does not support the creation or management of administrative units in Microsoft Entra ID, so this option is not applicable.

Reference: For more information about Microsoft Entra ID administrative units, please visit the below URLs:

Administrative units in Microsoft Entra ID | Microsoft Learn

Create or delete administrative units - Microsoft Entra ID | Microsoft Learn

Ask our Experts

Did you like this **Question?**

Question 32 Correct

Domain: Implement and manage storage

You are managing an Azure Storage account configured with container soft delete. Which of the following statements about container soft delete are true? (Select 3)

Your Answer

B. Updating the retention period affects only containers deleted after the change is made

D. Soft delete protects containers within a storage account but not the storage account itself

E. Container soft delete supports both general-purpose v2 accounts and accounts with hierarchical namespace

Correct Answer

B. Updating the retention period affects only containers deleted after the change is made

D. Soft delete protects containers within a storage account but not the storage account itself

E. Container soft delete supports both general-purpose v2 accounts and accounts with hierarchical namespace

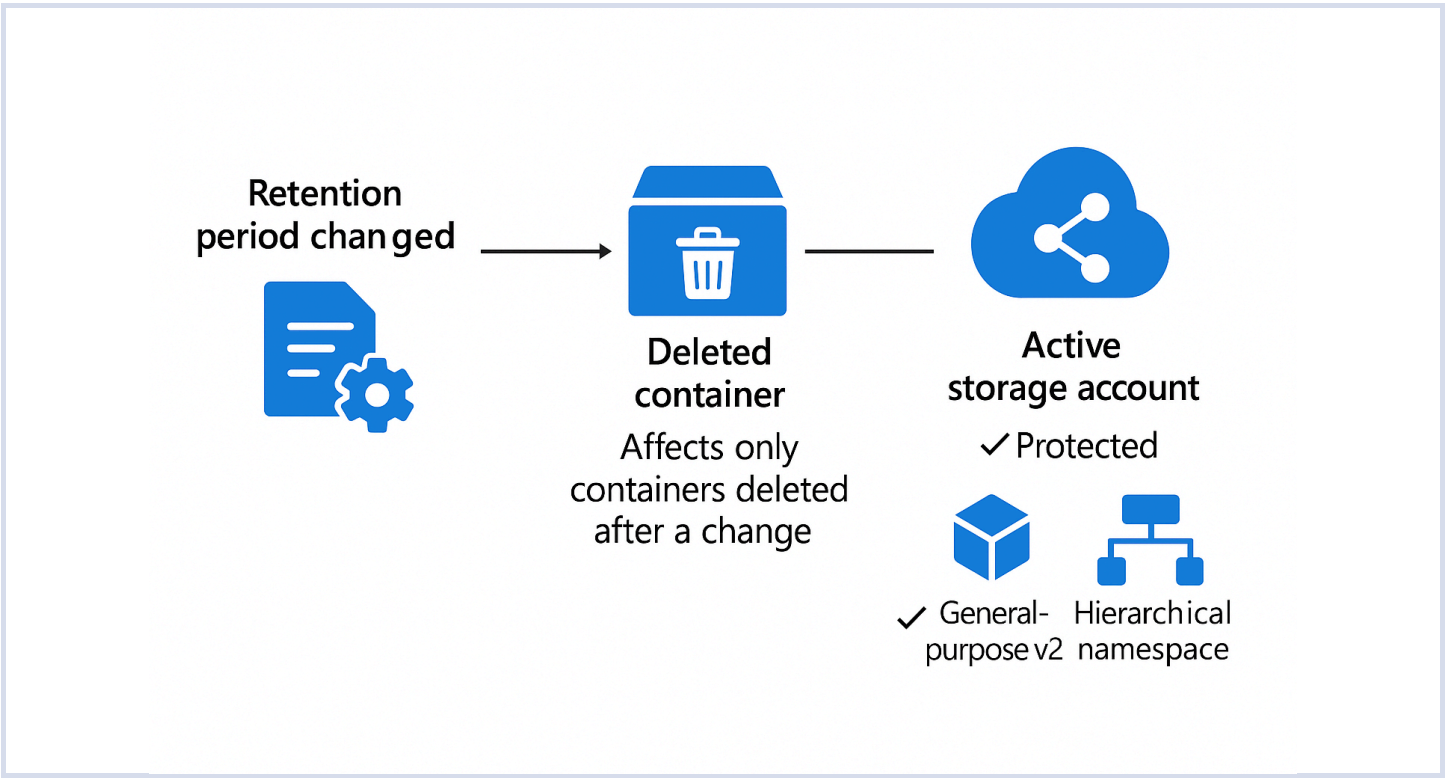
Explanation:

Correct Answers: B, D and E

Updating the retention period affects only containers deleted after the change is made.

Soft delete protects containers within a storage account but not the storage account itself.

Container soft delete supports both general-purpose v2 accounts and accounts with hierarchical namespace.



Option B: Updating the retention period affects only containers deleted after the change is made is correct because when you change the retention period, the new duration only applies to containers deleted going forward. Existing soft-deleted containers still follow the policy that was active at the time of deletion.

Why it's correct: Retention is timestamp-bound. Soft-deleted containers "lock in" the retention period at deletion time.

Option D: Soft delete protects containers within a storage account but not the storage account itself is correct because the container soft delete setting only applies to containers. If the entire storage account is deleted, no soft delete mechanism exists for its contents unless a resource lock is configured.

Why it's correct: You need to set a resource lock to prevent unintended storage account deletion.

Option E: Container soft delete supports both general-purpose v2 accounts and accounts with hierarchical namespace is correct because It's broadly supported across storage account types including Azure Data Lake Storage Gen2 (when HNS is enabled).

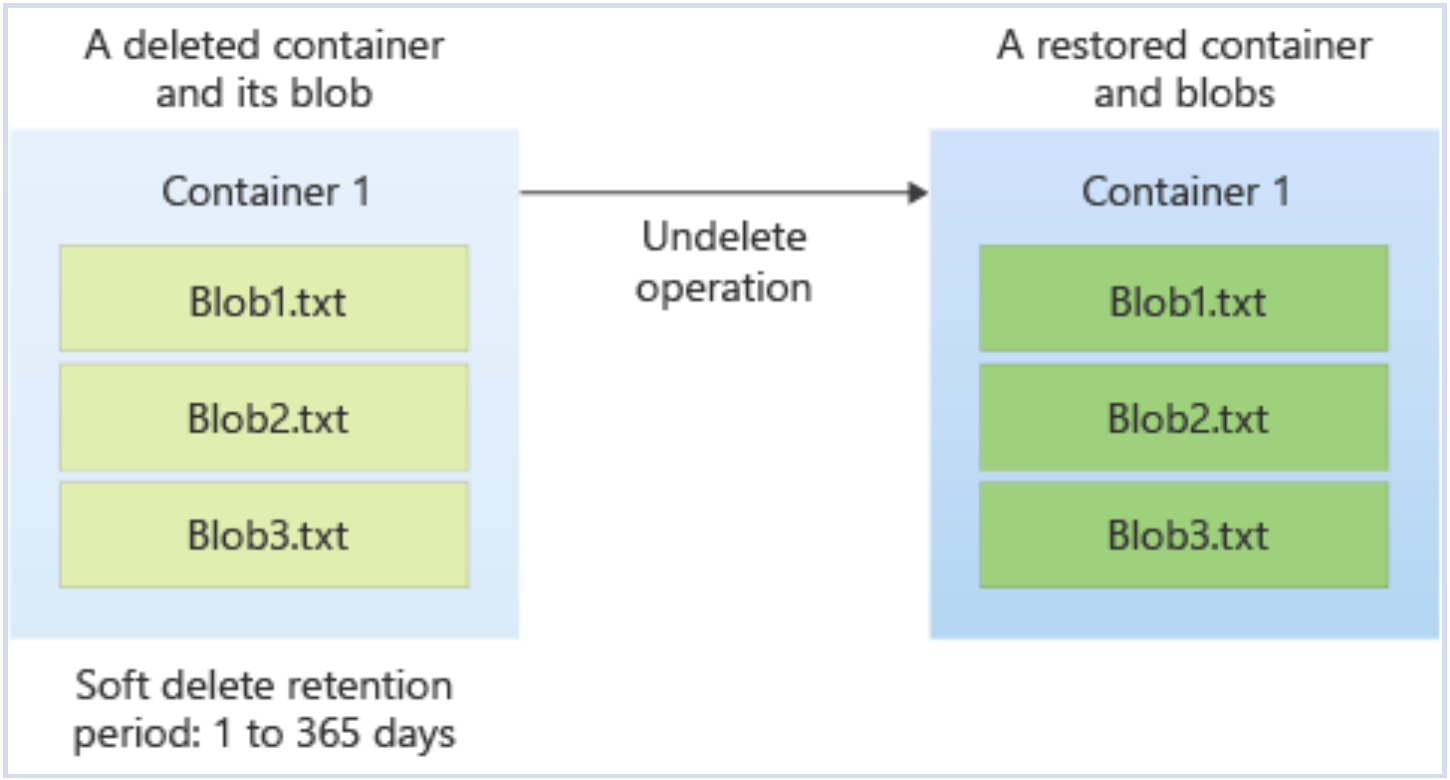
Container soft delete is supported in:

General-purpose v1 & v2 accounts

Block blob storage accounts

Blob storage accounts

Storage accounts with hierarchical namespace (used for Data Lake Gen2)



[Source: Microsoft Documentation]

Option A: A soft-deleted container can be recovered even after its retention period ends, provided soft delete is still enabled is incorrect because once the retention period expires, the container is permanently deleted, regardless of whether soft delete is still enabled.

Why it's wrong: The soft delete setting only retains the container within the retention period (1-365 days). After that, the container is unrecoverable.

Option C: Soft-deleted blobs can be restored using container soft delete even if the container wasn't deleted is incorrect because container soft delete only works when the entire container was deleted. If a blob is deleted individually and the container remains, blob soft delete or versioning is required to restore the blob.

Why it's wrong: Blob recovery without container deletion is outside the scope of container soft delete.

Reference: Soft delete for containers

Ask our Experts

Did you like this **Question?**

Question 33 Incorrect

Domain: Deploy and manage Azure compute resources

View Case Study

To ensure that all the virtual machines for WhizApp1 in Azure are protected by backups, which Azure service or feature should Whizlabs use?

A. Azure Backup right

B. Azure Site Recovery wrong

C. Azure Blob Storage

D. Azure File Sync

Explanation:

Correct Answer: A

Azure Backup is the service that allows Whizlabs to protect virtual machines and data in Azure by creating backups. It ensures that all virtual machines for WhizApp1 are backed up as per the technical requirements. The backups are stored in the **Recovery Services Vault**, which uses Azure Blob Storage for that purpose.

Option B: Incorrect. Azure Site Recovery is used for disaster recovery and does not directly address backup needs.

Option C: Incorrect. Azure Blob Storage is for storing data, not for creating backups.

Option D: Incorrect. Azure File Sync is used for file synchronization between on-premises and Azure storage, but it doesn't provide full virtual machine backup capabilities.

Reference:

Quickstart - Back up a VM with the Azure portal - Azure Backup | Microsoft Learn

Ask our Experts

Did you like this **Question?**

Question 34

Incorrect

Domain: Implement and manage storage

You are managing a virtual machine named "myVM", which is currently using Azure Disk Encryption and is tied to a key vault. You need to move this VM to a different resource group, subscription, and region using the Azure CLI.

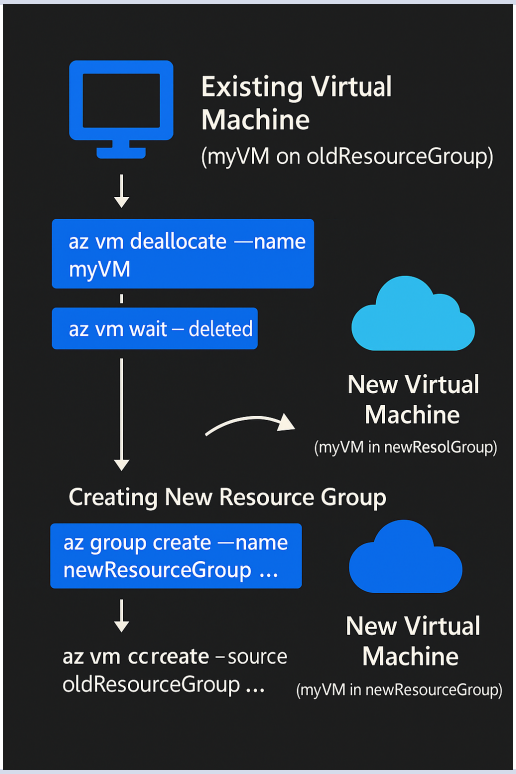
You need to drag and drop the steps in the correct order to achieve the migration successfully.

Your Answer	Correct Answer
1. D. az group create --name newResourceGroup --location newRegion	1. B. az vm deallocate --name myVM --resource-group oldResourceGroup
2. B. az vm deallocate --name myVM --resource-group oldResourceGroup	2. A. az vm wait --name myVM --resource-group oldResourceGroup --deleted
3. A. az vm wait --name myVM --resource-group oldResourceGroup --deleted	3. D. az group create --name newResourceGroup --location newRegion
4. C. az vm create --name myVM --resource-group newResourceGroup --location newRegion --source oldResourceGroup	4. C. az vm create --name myVM --resource-group newResourceGroup --location newRegion --source oldResourceGroup

Explanation:

Correct Answers [Sequence]: B - A - D - C

1. az vm deallocate --name myVM --resource-group oldResourceGroup
2. az vm wait --name myVM --resource-group oldResourceGroup --deleted
3. az group create --name newResourceGroup --location newRegion
4. az vm create --name myVM --resource-group newResourceGroup --location newRegion --source oldResourceGroup



Step 1: Deallocate the VM [az vm deallocate --name myVM --resource-group oldResourceGroup]

Why it's first: Before moving or replicating a VM across regions, the VM must be stopped and deallocated to detach resources and prepare it for export.

Step 2: Wait for deletion confirmation [az vm wait --name myVM --resource-group oldResourceGroup --deleted]

Why it's next: The operation confirms that the VM and its related metadata are in a safe, deletable state. This ensures Azure doesn't try to create a duplicate VM or conflict with name/ID references during the new deployment.

Step 3: Create a new resource group [az group create --name newResourceGroup --location newRegion]

Why it's here: Before you deploy the VM in a new region, you must have a target resource group available in that region.

Step 4: Create the VM in the new region [az vm create --name myVM --resource-group newResourceGroup --location newRegion --source oldResourceGroup]

Why it's last: This command recreates the VM in the new location using the previously stored source settings. It's the final step to reinstantiate the VM in a new region and resource group.

Reference:

Special cases to move Azure VMs to new subscription or resource group - Azure Resource Manager | Microsoft Learn

Ask our Experts

Did you like this **Question?**

Question 35 Correct

Domain: Monitor and maintain Azure resources

Whizlabs International is a Europe based company. Due to new GDPR requirements, the company is planning to reorganize their Azure resources and needs to perform various resource management tasks.

Drag the appropriate Azure services with respect to their definitions.

Note: This is a Drag and Drop Matching Type Question.

Your Answers

Azure Resource Group

This component acts as a logical container for resources, making it easier to manage and organize them

Azure Virtual Machine

This service is used to host virtual servers in the cloud and can be moved between resource groups or regions

Azure Region

When you need to change the physical location of resources, you can move them to a different one of these

Correct Answers

Azure Resource Group

This component acts as a logical container for resources, making it easier to manage and organize them

Azure Virtual Machine

This service is used to host virtual servers in the cloud and can be moved between resource groups or regions

Azure Region

When you need to change the physical location of resources, you can move them to a different one of these

Explanation:

Correct Answer: 1-C, 2-A and 3-B

Azure Virtual Machine: This service is used to host virtual servers in the cloud and can be moved between resource groups or regions

Azure Resource Group: This component acts as a logical container for resources, making it easier to manage and organize them

Azure Region: When you need to change the physical location of resources, you can move them to a different one of these

Detailed Explanation:-

Azure Resource Group: Resource groups are logical containers for resources, and they help with managing and organizing resources within Azure. This is essential for efficient resource management.

Azure Virtual Machine: Azure Virtual Machines can indeed be moved between resource groups or regions, allowing for flexibility in resource management and optimization.

Azure Region: Azure regions represent the physical location of data centers. When you need to change the physical location of resources, you can indeed move them to a different Azure region. This can be helpful for disaster recovery or optimization.

Reference: Move resources to a new subscription or resource group - Azure Resource Manager | Microsoft Learn

Ask our Experts

Did you like this **Question?**

Question 36 Correct

Domain: Deploy and manage Azure compute resources

You are tasked with deploying Azure resources for a Node.js-based web application called WhizApp using an Infrastructure-as-Code (IaC) approach via Azure Bicep.

Your goal is to ensure the following:

- The application is deployed to the East US region.
- It uses App Service Plan PremiumV2 (P1V2 SKU) to support production-grade features like high performance and autoscaling.
- The app requires Node.js version 14, and it must remain always running to avoid cold starts.

You review the Bicep configuration below:

```
param location string = 'East US'
resource appServicePlan 'Microsoft.Web/serverfarms@2022-03-01' = {
  name: 'myAppServicePlan'
  location: location
  sku: {
    name: 'P1V2'
    tier: 'PremiumV2'
  }
}
resource webApp 'Microsoft.Web/sites@2022-06-01' = {
  name: 'WhizApp'
  location: location
  properties: {
    serverFarmId: appServicePlan.id
    siteConfig: {
      alwaysOn: true
      nodeVersion: '14'
    }
  }
}
```

Which of the following statements are true about this Bicep deployment? [Select three]

Your Answer

A. The web app will be deployed to the PremiumV2 App Service Plan, which supports Always On and autoscaling

B. The alwaysOn property ensures that WhizApp does not enter idle state, reducing latency for first-time requests.

D. The serverFarmId property links the web app to the App Service Plan, enabling shared scaling and pricing

Correct Answer

A. The web app will be deployed to the PremiumV2 App Service Plan, which supports Always On and autoscaling

B. The alwaysOn property ensures that WhizApp does not enter idle state, reducing latency for first-time requests.

D. The serverFarmId property links the web app to the App Service Plan, enabling shared scaling and pricing

Explanation:

Correct Answers: A, B and D

Option A is correct because - The App Service Plan specified is **PremiumV2 (P1V2)**, a high-performance tier that supports **Always On, custom domains, SSL, autoscaling**, and more — all of which are essential for production workloads.

Why it's correct: PremiumV2 offers all required production-grade features like Always On and autoscaling.

Option B is correct because - The alwaysOn: true setting ensures the app doesn't idle due to inactivity. It keeps the web app's worker process running even when there are no HTTP requests — ideal for background tasks and cold-start prevention.

Why it's correct: Prevents cold start, ensuring better responsiveness for users.

Option D is correct because -The serverFarmId property directly links the web app to the App Service Plan (myAppServicePlan). This ensures the app shares the same compute, billing, and scaling resources as other apps in the plan.

Why it's correct: Enables compute sharing, resource scaling, and centralized billing.

Option C is incorrect because - Although Node.js 18 is supported on Azure, the Bicep configuration explicitly sets nodeVersion: '14'. This is a common mismatch trap.

Why it's wrong: The app is set to use Node.js v14, not v18.

Option E is incorrect because - The app is deployed using the PremiumV2 plan, not the Free tier. Free tiers don't support features like Always On or Node.js version customization.

Why it's wrong: This deployment is explicitly configured to use PremiumV2, not the Free tier.

Reference:

https://learn.microsoft.com/en-us/azure/app-service/provision-resource-bicep?pivots=app-service-bicep-linux

Ask our Experts

Did you like this **Question?**

Question 37

Correct

Domain: Monitor and maintain Azure resources

You are tasked with monitoring Azure virtual machines across multiple environments. Virtual machines have several components, each requiring its own level of monitoring. Match each VM layer to its most appropriate monitoring description.

Note: Drag the appropriate feature name and drop them to the correct description

Your Answers

A. Virtual machine host

Underlying Azure Service Fabric that runs your virtual machine. Useful for tracking platform events like host failures or redeployments

B. Guest operating system

Installed OS (Windows/Linux) inside the VM. Monitor using agents to track logs, resource usage, and system health

C. Workloads

Critical background services (e.g., web servers, databases) that support application functions. Require telemetry for performance and uptime

D. Applications

Frontend or business apps hosted on VMs, accessed by users. Requires monitoring for responsiveness, errors, and user experience

Correct Answers

A. Virtual machine host

Underlying Azure Service Fabric that runs your virtual machine. Useful for tracking platform events like host failures or redeployments

B. Guest operating system

Installed OS (Windows/Linux) inside the VM. Monitor using agents to track logs, resource usage, and system health

C. Workloads

Critical background services (e.g., web servers, databases) that support application functions. Require telemetry for performance and uptime

D. Applications

Frontend or business apps hosted on VMs, accessed by users. Requires monitoring for responsiveness, errors, and user experience

Explanation:

Correct Answers: A-1, B-2, C-3 and D-4

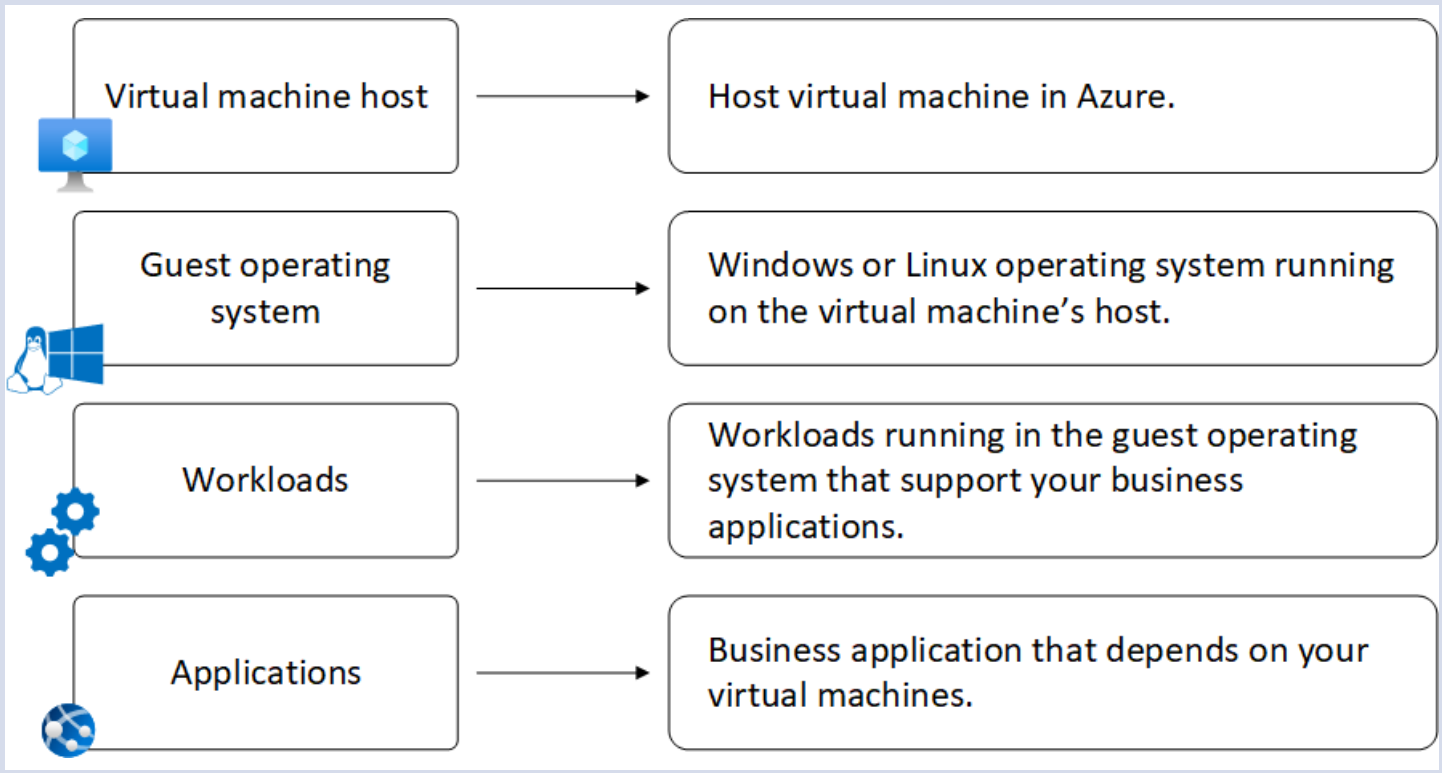
Virtual machine host: Underlying Azure Service Fabric that runs your virtual machine. Useful for tracking platform events like host failures or redeployments

Guest operating system: Installed OS (Windows/Linux) inside the VM. Monitor using agents to track logs, resource usage, and system health

Workloads: Critical background services (e.g., web servers, databases) that support application functions. Require telemetry for

performance and uptime

Applications: Frontend or business apps hosted on VMs, accessed by users. Requires monitoring for responsiveness, errors, and user experience.



[Source: Microsoft Documentation]

Option A: Virtual machine host → Azure Service Fabric Monitoring is correct match: The VM host is the Azure-managed infrastructure where your VM runs. Monitoring this layer helps detect platform-level disruptions.

> Why it's correct: Focuses on host-level reliability. Azure sends signals when the physical machine or hypervisor undergoes planned or unplanned events.

Option B: Guest operating system → OS-Level Insights is correct match: This is the Windows or Linux OS installed inside the VM. It's your responsibility to monitor its health, patches, and resource usage.

> Why it's correct: Use diagnostics and performance counters to watch CPU, memory, and system event logs — helpful for capacity planning and troubleshooting.

Option C: Workloads → Backend Services Monitoring is correct match: Workloads refer to application support layers — such as databases, APIs, or middleware — that your actual apps rely on.

> Why it's correct: These often drive the core logic or data layer of your app and need dedicated alerting for downtime or failures.

Option D: Applications → End-User App Monitoring is correct match: These are the business-critical applications accessed by end users, like ERP systems, customer portals, etc.

> Why it's correct: Requires Application Performance Management (APM) tools like Application Insights to detect performance issues and usage trends.

Reference: Monitor virtual machines with Azure Monitor - Azure Monitor | Microsoft Learn

Ask our Experts

Did you like this **Question?**

Question 38 Incorrect

Domain: Implement and manage storage

View Case Study

To copy the blueprint files to Azure over the Internet and ensure that they are stored in the archive storage tier, which Azure storage type should Whizlabs use?

- A. Azure File Storage wrong
- B. Azure Queue Storage
- C. Azure Table Storage
- D. Azure Blob Storage right

Explanation:

Correct Answer: D

Azure Blob Storage is suitable for storing unstructured data like the blueprint files, and it allows Whizlabs to copy files to Azure over the Internet. Additionally, Azure Blob Storage provides different storage tiers, including the archive storage tier, which can be used for long-term storage with cost savings.

Options A, B and C are incorrect because File Storage, queues and table are not designed for storing files like blueprint files and do not offer storage tiers like the archive storage tier.

Reference:

Access tiers for blob data - Azure Storage | Microsoft Learn

Ask our Experts

Did you like this **Question?**

Question 39 Incorrect

Domain: Manage Azure identities and governance

You're configuring external collaboration settings in Microsoft Entra ID for your organization. The security team provides two specific security requirements:

Guest users should not be able to view other users, groups, or memberships - they should only see their own profile and related info.

Only administrators with specific roles (like “User Administrator” or “Guest Inviter”) should be able to invite external guest users to the directory.

Given these requirements, which two settings should you configure? (Select Two)

A. Set "Guest user access is restricted to properties and memberships of their own directory objects" under Guest user access right

B. Set "Guest users have the same access as members" under Guest user access

C. Set "Anyone in the organization can invite guest users including guests and non-admins" under Guest invite settings

- [x] D. Set "Guest users have limited access to properties and memberships of directory objects" under Guest user access wrong
- [x] E. Set "Only users assigned to specific admin roles can invite guest users" under Guest invite settings right

---

Explanation:

Correct Answers: A and E

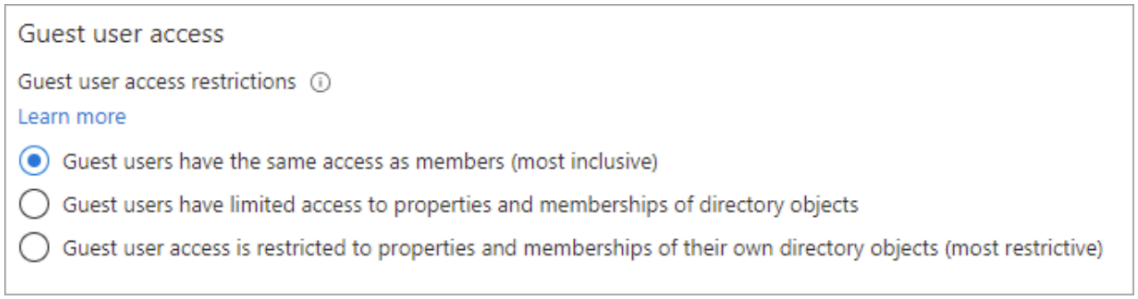
Option A: "Guest user access is restricted to properties and memberships of their own directory objects" is correct beacuse - This directly meets the security team's requirement that guest users must only see their own directory data, helping to protect sensitive user and group information from external visibility.

This is the most restrictive setting available for guest access in Microsoft Entra ID.

When this setting is enabled: Guest users can only view their own profile, groups they belong to, and nothing else. They cannot browse the full user directory, view other group memberships, or access other users’ data.

To configure guest user access

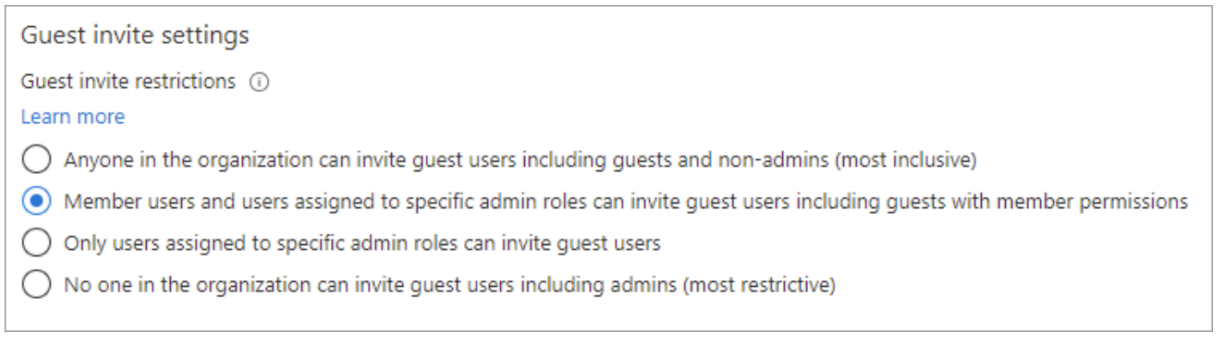
1. Sign in to the Microsoft Entra admin center.
2. Browse to **Entra ID** > **External Identities** > **External collaboration settings**.
3. Under **Guest user access**, choose the level of access you want guest users to have:



- **Guest users have the same access as members (most inclusive)**: This option gives guests the same access to Microsoft Entra resources and directory data as member users.

Option E: "Only users assigned to specific admin roles can invite guest users" is correct because – This aligns with the need for strict control over guest onboarding and ensures that only authorized personnel can extend access to external users, which minimizes the risk of unauthorized sharing.

By enabling this setting: You restrict the ability to invite external users only to admins with specific roles like User Administrator, Global Administrator, or Guest Inviter. It prevents regular employees (and existing guests) from sending out invitations.



- **Anyone in the organization can invite guest users including guests and non-admins (most inclusive)**: To allow guests in the organization to invite other guests including users who aren't members of an organization, select this radio button.
- **Member users and users assigned to specific admin roles can invite guest users including guests with member permissions**: To allow member users and users who have specific administrator roles to invite guests, select this radio button.
- **Only users assigned to specific admin roles can invite guest users**: To allow only those users with User Administrator or Guest Inviter roles to invite guests, select this radio button.
- **No one in the organization can invite guest users including admins (most restrictive)**: To deny

Option B: "Guest users have the same access as members" is incorrect because if you choose this setting: Guests can view all directory information available to member users, including other users, group details, and organizational structure. It's meant for collaborative environments where external users need full directory access — not secure environments.

Why it's wrong: This violates the first requirement, as guest users will gain too much visibility, putting internal information at risk.

Option C: "Anyone in the organization can invite guest users including guests and non-admins" is incorrect because - Enabling this means: Any user including guests can invite more external users.There's no control over who adds external identities, which is a major governance issue.

Why it's wrong: It directly conflicts with the second requirement. You lose control of who can bring in external collaborators, increasing the risk of unwanted access.

Option D: "Guest users have limited access to properties and memberships of directory objects" is incorrect because - This setting does partially limit access, but: Guests can still see certain directory objects, such as non-hidden groups and their members.It doesn't fully prevent them from seeing some directory-wide data.

Why it's wrong: While it sounds secure, it does not completely fulfill the first requirement. Guest users may still view other objects besides their own, which the security team wants to avoid.

Reference:

Configure external collaboration settings in Microsoft Entra ID

Ask our Experts

Did you like this **Question?**

Question 40

Correct

Domain: Monitor and maintain Azure resources

View Case Study

Can you send the security events of the virtual machines to the Log Analytics workspace?

A. Yes right

B. No

Explanation:

Answer – A

Yes, you can. Even though the virtual machines and the Log Analytics workspace are in separate locations, you can still connect the virtual machines to the workspace.

For more information on collecting data into a Log Analytics workspace, please visit the following URL-

https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-azurevm

Ask our Experts

Did you like this **Question?**

Finish Review