Azure VNet, ASG, NSG, VMSS & Storage Account MCQs

20 Scenario-Based Multiple Choice Questions

Question 1: VNet Peering Scenario

Your company has two VNets: VNet-A (10.0.0.0/16) in East US and VNet-B (10.1.0.0/16) in West US. You've configured VNet peering between them. VMs in VNet-A cannot communicate with VMs in VNet-B. What is the most likely cause?

A) VNet peering doesn't support cross-region communication
B) The peering status is "Initiated" on one side but not connected on the other
C) You need to create a VPN Gateway for cross-region communication
D) The address spaces are incompatible

Answer: B - VNet peering must be configured bidirectionally and both sides must show "Connected" status.

Question 2: NSG Rule Priority

You have an NSG with the following rules:

- Priority 100: Allow port 443 from Internet
- Priority 200: Deny port 443 from Internet
- Priority 300: Allow all traffic from Internet

A user tries to access your web app on port 443. What happens?

A) Access is denied because deny rules always take precedence
B) Access is allowed because of priority 300
C) Access is allowed because priority 100 is evaluated first
D) Access is denied because Azure blocks port 443 by default

Answer: C - NSG rules are processed by priority number (lowest first). Priority 100 allows the traffic before other rules are evaluated.

Question 3: ASG Implementation

You need to allow database traffic (port 1433) from all web servers to all database servers without using IP addresses. You have 15 web VMs and 8 database VMs that may scale up or down. What's the best approach?

A) Create NSG rules with all individual VM IP addresses
B) Create two ASGs (WebServers-ASG and DBServers-ASG) and create NSG rule allowing 1433 from

WebServers-ASG to DBServers-ASG
C) Use service tags in NSG rules
D) Create a separate NSG for each VM

Answer: B - ASGs allow you to group VMs logically and apply security rules based on workload, making management easier as VMs scale.

Question 4: Storage Account Redundancy

Your application requires data to be replicated across multiple Azure regions to survive regional failures, with read access to the secondary region. Which redundancy option should you choose?

A) Locally Redundant Storage (LRS)
B) Zone-Redundant Storage (ZRS)
C) Geo-Redundant Storage (GRS)
D) Read-Access Geo-Redundant Storage (RA-GRS)

Answer: D - RA-GRS provides geo-replication with read access to the secondary region. GRS also replicates to secondary region but doesn't provide read access.

Question 5: VMSS Auto-scaling

You configure a VMSS with minimum 2 instances, maximum 10 instances, and an auto-scale rule to add 1 instance when CPU > 75%. Currently, you have 5 instances and CPU is at 80% sustained for 15 minutes. What happens?

A) Nothing, manual intervention is required
B) 1 new instance is added, bringing total to 6
C) 5 new instances are added to reach maximum
D) All instances are restarted

Answer: B - Auto-scale rules trigger based on defined conditions. When CPU exceeds the threshold, it adds the specified increment (1 instance).

Question 6: NSG Association

You have a VNet with 3 subnets. You want to apply different security rules to each subnet. What's the best practice?

A) Create one NSG and associate it with the VNet
B) Create three separate NSGs and associate each with its respective subnet
C) NSGs cannot be applied to subnets, only to NICs
D) Create one NSG with all rules and associate it with all subnets

Answer: B - Each subnet can have its own NSG with specific rules. This provides granular control over traffic for different tiers (web, app, database).

Question 7: Storage Account Access Tier

Your application generates logs that need to be retained for 7 years for compliance but are rarely accessed after 90 days. Which storage solution is most cost-effective?

A) Premium SSD with LRS
B) Hot tier blob storage
C) Cool tier blob storage with lifecycle management to Archive tier after 90 days
D) Standard HDD with GRS

Answer: C - Cool tier for initial storage and Archive tier for long-term retention provides the most cost-effective solution for infrequently accessed data.

Question 8: VNet Service Endpoints

You want to secure your Azure Storage Account so it's only accessible from VMs in a specific subnet, not from the internet. What should you implement?

A) Configure firewall rules with VM IP addresses
B) Enable VNet service endpoint for Storage on the subnet and configure storage firewall
C) Use Azure Firewall
D) Place storage account in the VNet

Answer: B - Service endpoints provide secure connectivity from VNet to Azure services over the Azure backbone network, and you can restrict storage access to specific VNets/subnets.

Question 9: VMSS Update Policy

Your VMSS hosts a production application. You need to update the VM image with zero downtime. Which upgrade policy should you use?

A) Automatic upgrade policy
B) Manual upgrade policy
C) Rolling upgrade policy
D) All instances upgrade simultaneously

Answer: C - Rolling upgrades update instances in batches, ensuring some instances remain available during the update, providing zero downtime.

Question 10: NSG Flow Logs

You need to troubleshoot network connectivity issues and analyze traffic patterns for security auditing. What Azure feature should you enable?

A) Azure Monitor Metrics
B) NSG Flow Logs with Traffic Analytics
C) Azure Security Center
D) Application Insights

Answer: B - NSG Flow Logs capture information about IP traffic and Traffic Analytics provides visualization and insights for security and optimization.

Question 11: Storage Account Networking

You have a storage account that should only be accessible from your company's on-premises network (IP range 203.0.113.0/24) and from Azure VMs in a specific VNet. How should you configure this?

A) Disable public access completely
B) Enable public access from all networks
C) Enable public access from selected networks, add the VNet and the IP range to allowed list
D) Use Azure AD authentication only

Answer: C - Storage account firewall allows you to specify which VNets and public IP ranges can access the storage account.

Question 12: ASG with Multiple NSGs

You have an ASG named "WebServers-ASG" with 10 VMs. Each VM's NIC has an NSG, and the subnet also has an NSG. Traffic on port 80 is allowed in the ASG rule but denied in the subnet NSG. What happens?

A) Traffic is allowed because ASG rules override subnet NSG
B) Traffic is denied because subnet NSG is evaluated first
C) Traffic is allowed because ASG rules have higher priority
D) Traffic is denied because both NSGs must allow it

Answer: D - NSG rules are cumulative. Traffic must be allowed by both subnet NSG and NIC NSG (or any NSG in the path) to flow.

Question 13: VMSS Load Balancer

Your VMSS is behind an Azure Load Balancer. You need to ensure user sessions stick to the same VM instance. What should you configure?

A) Round-robin distribution mode
B) Session persistence (Client IP)
C) Source NAT
D) Backend pool priority

Answer: B - Session persistence (also called session affinity) uses client IP or client IP and protocol to direct requests from the same client to the same backend VM.

Question 14: VNet Address Space Conflict

You need to peer VNet-A (10.0.0.0/16) with VNet-B (10.0.0.0/24). What will happen?

A) Peering will work fine
B) Peering will fail due to overlapping address spaces
C) Only non-overlapping subnets can communicate
D) Azure will automatically renumber one VNet

Answer: B - VNet peering requires non-overlapping address spaces. 10.0.0.0/24 is a subset of 10.0.0.0/16, creating an overlap.

Question 15: Storage Account Blob Versioning

You need to protect against accidental deletion or modification of blobs while keeping costs reasonable. Users should be able to recover previous versions within 30 days. What should you enable?

A) Soft delete for blobs (30-day retention)
B) Blob versioning only
C) Blob snapshots manually
D) Immutable storage

Answer: A - Soft delete allows recovery of deleted or overwritten blobs within the retention period. It's more cost-effective than versioning for this use case.

Question 16: NSG Service Tags

You need to allow outbound traffic from your VMs to Azure SQL Database only, blocking all other internet traffic. What's the most efficient NSG rule?

A) Allow outbound to SQL PaaS service using "Sql" service tag
B) Manually add all Azure SQL IP ranges
C) Allow all outbound traffic
D) Create a rule for each SQL database IP address

Answer: A - Service tags represent a group of IP address prefixes for Azure services, automatically maintained by Azure. The "Sql" tag covers Azure SQL Database.

Question 17: VMSS Health Monitoring

Your VMSS runs a web application. You want unhealthy instances to be automatically replaced. What should you configure?

A) Azure Monitor alerts only
B) Application Health Extension or Load Balancer health probes with automatic repair policy
C) Manual health checks
D) Azure Backup

Answer: B - VMSS automatic instance repairs require health monitoring through Application Health Extension or Load Balancer probes, combined with an automatic repair policy.

Question 18: Storage Account Shared Access Signature (SAS)

You need to give a third-party vendor temporary access to upload files to a specific container for 7 days, without sharing account keys. What should you use?

A) Account access keys
B) Service SAS token with container-level permissions and 7-day expiry
C) Azure AD authentication
D) Storage account public access

Answer: B - Service SAS provides delegated access with specific permissions, to specific resources, for a defined time period, without exposing account keys.

Question 19: VNet DNS Configuration

Your VMs in Azure VNet need to resolve both Azure resource names and your on-premises private DNS names. What's the recommended DNS configuration?

A) Use Azure-provided DNS only
B) Configure custom DNS servers (your on-premises DNS or Azure DNS Private Resolver)
C) Use public DNS servers
D) Configure DNS settings on each VM individually

Answer: B - Custom DNS servers allow resolution of both Azure and on-premises resources. Azure DNS Private Resolver can forward queries between Azure and on-premises.

Question 20: VMSS with Multiple ASGs

You have a VMSS where instances need to belong to multiple application security groups (WebServers-ASG and PaymentProcessing-ASG) to receive traffic on different ports. Is this possible?

A) No, each instance can only belong to one ASG
B) Yes, you can associate multiple ASGs with each NIC in the VMSS
C) Yes, but only through PowerShell, not portal
D) No, you need to create separate VMSS instances

Answer: B - A network interface can be associated with multiple ASGs, allowing you to create flexible security rules based on different application roles.

Answer Key

1. B | 2. C | 3. B | 4. D | 5. B | 6. B | 7. C | 8. B | 9. C | 10. B
2. C | 12. D | 13. B | 14. B | 15. A | 16. A | 17. B | 18. B | 19. B | 20. B