Answer Sheet

Q1) State whether the following statement is correct or incorrect -

"Azure Management Groups can be used to control policy and RBAC for multiple subscriptions. Management groups enable organizational alignment for your Azure subscriptions through custom hierarchies and groupings."

✅ Correct

Explanation:-Azure Management Groups can be used to control policy and RBAC for multiple subscriptions. Management groups enable organizational alignment for your Azure subscriptions through custom hierarchies and groupings.

⚪ Incorrect

Q2)

You have an Azure subscription that contains 10 virtual networks. The virtual networks are hosted in separate resource groups.

Another administrator plans to create several network security groups (Network Security Groupss) in the subscription.

You need to ensure that when an Network Security Groups is created, it automatically blocks TCP port 8080 between the virtual networks.

Solution: You create a resource lock, and then you assign the lock to the subscription. Does this meet the goal?

✅ Incorrect

Explanation:-Azure resource manager policies are used to control what you can and cannot do with resources called resource actions. Reference: https://blogs.msdn.microsoft.com/azureedu/2016/04/27/using-azure-resource-manager-policy-and-azure-lock-to-control-your-azure-resources/

⚪ Correct

Q3)

You have an Azure subscription that contains the resources in the following table.

Name	Type	Azure region	Resource group
VNet1	Virtual network	West US	RG2
VNet2	Virtual network	West US	RG1
VNet3	Virtual network	East US	RG1
NSG1	Network security group (NSG)	East US	RG2

To which subnets can you apply Network Security Groups1?

⚪ the subnets on VNet2 only

⚪ the subnets on VNet2 and VNet3 only

✅ the subnets on VNet3 only

Explanation:-All Azure resources are created in an Azure region and subscription. A resource can only be created in a virtual network that exists in the same region and subscription as the resource. References: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-vnet-plan-design-arm

⚪ the subnets on VNet1, VNet2, and VNet3

⚪ the subnets on VNet1 only

Q4) State whether the following statement is correct or incorrect -

"A resource is simply a single service instance in Azure. Most services in Azure can be represented as a resource. For example, a Web App instance is a resource. An App Service Plan is also a resource. Even a SQL Database instance is a resource."

✅ Correct

Explanation:-A resource is simply a single service instance in Azure. Most services in Azure can be represented as a resource. For example, a Web App instance is a resource. An App Service Plan is also a resource. Even a SQL Database instance is a resource.

⚪ Incorrect

Q5)

You have an Azure subscription that contains a virtual network named VNET1. VNET1 contains the subnets shown in the following table.

Name	Connected virtual machines
Subnet1	VM1, VM2
Subnet2	VM3, VM4
Subnet3	VM5, VM6

Each virtual machine uses a static IP address. You need to create network security groups (Network Security Groupss) to meet following requirements:

Allow web requests from the internet to VM3, VM4, VM5, and VM6.
Allow all connections between VM1 and VM2.
Allow Remote Desktop connections to VM1.

Prevent all other network traffic to VNET1. What is the minimum number of Network Security Groups you should create?

⚪ 12

✅ 4

Explanation:-A network security group (Network Security Groups) contains a list of security rules that allow or deny network traffic to resources

connected to Azure Virtual Networks (VNet). Network Security Groupss can be associated to subnets, individual VMs (classic), or individual network interfaces (NIC) attached to VMs (Resource Manager). Each network security group also contains default security rules.refer - https://docs.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works

- 3
- 1

Q6)

You set the multi-factor authentication status for a user named admin1@contoso.com to Enabled.Admin1 accesses the Azure portal by using a web browser.

Which additional security verifications can Admin1 use when accessing the Azure portal?

- ✅ A phone call, a text message that contains a verification code, and a notification or a verification code sent from the Microsoft Authenticator app

Explanation:-Verification methods:

You can choose the verification methods that are available for your users.

When your users enroll their accounts for Azure Multi-Factor Authentication, they choose their preferred verification method from the options that you have enabled. Guidance for the user enrollment process is provided in Set up my account for two-step verification.

Call to phone: Places an automated voice call. The user answers the call and presses # in the phone keypad to authenticate. The phone number is not synchronized to on-premises Active Directory.

Text message to phone: Sends a text message that contains a verification code. The user is prompted to enter the verification code into the sign-in interface. This process is called one-way SMS. Two-way SMS means that the user must text back a particular code. Two-way SMS is deprecated and not supported after November 14, 2018. Users who are configured for two-way SMS are automatically switched to call to phone verification at that time.

Notification through mobile app: Sends a push notification to your phone or registered device. The user views the notification and selects Verify to complete verification. The Microsoft Authenticator app is available for Windows Phone, Android, and iOS.

Verification code from mobile app or hardware token: The Microsoft Authenticator app generates a new OATH verification code every 30 seconds. The user enters the verification code into the sign-in interface. The Microsoft Authenticator app is available for Windows Phone, Android, and iOS.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings

- An app password, a text message that contains a verification code, and a verification code sent from the Microsoft Authenticator app
- A phone call, an email message that contains a verification code, and a text message that contains an app password
- An app password, a text message that contains a verification code, and a notification sent from the Microsoft Authenticator app

---

Q7)

You have five Azure virtual machines that run Windows Server 2016.

The virtual machines are configured as web servers.

You have an Azure load balancer named LB1 that provides load balancing services for the virtual machines.

You need to ensure that visitors are serviced by the same web server for each request.

What should you configure?

- Session persistence to None
- Idle Time-out (minutes) to 20
- Protocol to UDP
- ✅ Session persistence to Client IP

Explanation:-You can set the sticky session in load balancer rules with setting the session persistence as the client IP.

Q8)

You have an Azure subscription that contains a virtual network named VNet1.

VNet1 contains four subnets named Gateway, Perimeter, NVA, and Production.

The NVA subnet contains two network virtual appliances (NVAs) that will perform network traffic inspection between the Perimeter subnet and the Production subnet.

You need to implement an Azure load balancer for the NVAs. The solution must meet the following requirements:
The NVAs must run in an active-active configuration that uses automatic failover.
The NVAs must load balance traffic to two services on the Production subnet.

The services have different IP addresses.

Which three actions should you perform? Each correct answer presents part of the solution.

- Deploy a basic load balancer.
- ✅ Add two load balancing rules that have HA Ports and Floating IP enabled.

Explanation:-A standard load balancer is required for the HA ports. Two backend pools are needed as there are two services with different IP addresses. Floating IP rule is used where backend ports are reused. Incorrect Answers:F: HA Ports are not available for the basic load balancer. References: https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-standard-overview https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-multivip-overview

- ✅ Add a frontend IP configuration, two backend pools, and a health probe.

Explanation:-A standard load balancer is required for the HA ports. Two backend pools are needed as there are two services with different IP addresses. Floating IP rule is used where backend ports are reused. Incorrect Answers:F: HA Ports are not available for the basic load balancer. References: https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-standard-overview https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-multivip-overview

- Add two load balancing rules that have HA Ports enabled and Floating IP disabled.
- ✅ Deploy a standard load balancer.

Explanation:-A standard load balancer is required for the HA ports. Two backend pools are needed as there are two services with different IP addresses. Floating IP rule is used where backend ports are reused. Incorrect Answers:F: HA Ports are not available for the basic load balancer. References: https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-standard-overview https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-multivip-overview

---

Q9)

You configure Azure AD Connect for Azure Active Directory Seamless Single Sign-On (Azure AD Seamless SSO) for an on-premises network. Users report that when they attempt to access myapps.microsoft.com, they are prompted multiple times to sign in and are forced to use an account name that ends with onmicrosoft.com.

You discover that there is a UPN mismatch between Azure AD and the on-premises Active Directory.

You need to ensure that the users can use single-sign-on (SSO) to access Azure resources.

What should you do first?

✔ From Azure AD, add and verify a custom domain name.

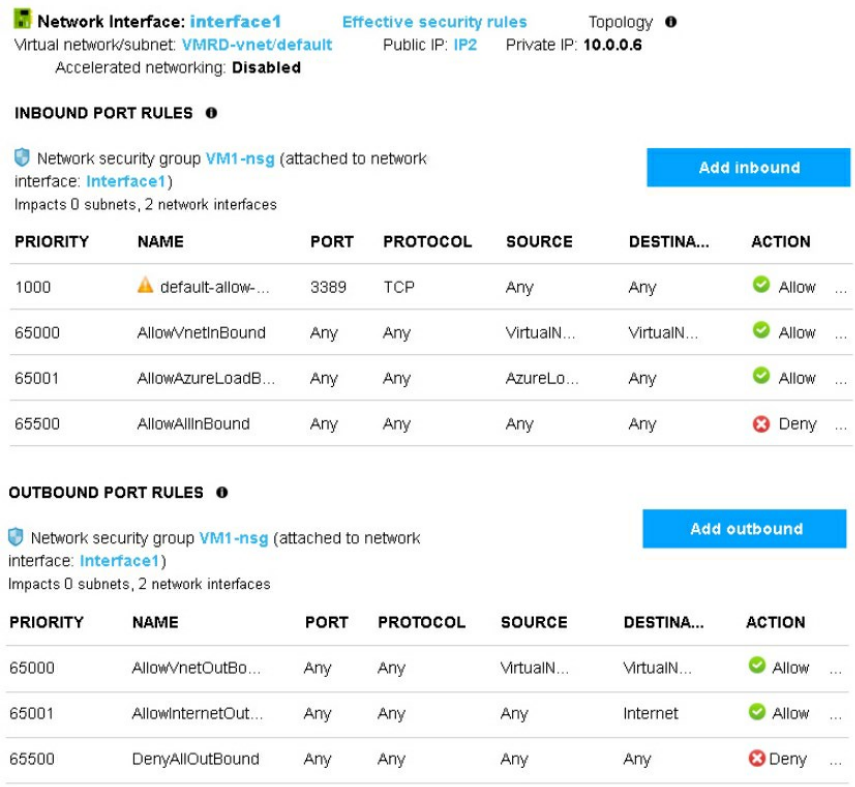
Explanation:-Every new Azure AD tenant comes with an initial domain name, domainname.onmicrosoft.com. You can't change or delete the initial domain name, but you can add your organization's names to the list. Adding custom domain names helps you to create user names that are familiar to your users, such as alain@contoso.com.

- From the on-premises network, deploy Active Directory Federation Services (AD FS).
- From the on-premises network, request a new certificate that contains the Active Directory domain name.
- From the server that runs Azure AD Connect, modify the filtering options.

Q10)

You have an Azure subscription named Subscription1. Subscription1 contains a virtual machine named VM1.You have a computer named Computer1 that runs Windows 10. Computer1 is connected to the Internet.

You add a network interface named Interface1 to VM1 as shown in the picture.



From Computer1, you attempt to connect to VM1 by using Remote Desktop, but the connection fails.

You need to establish a Remote Desktop connection to VM1.

What should you do first?

✔ Start VM1.

- Change the priority of the RDP rule.
- Delete the DenyAllInBound rule.
- Attach a network interface.

Q11)

You have an Azure Active Directory (Azure AD) tenant. All administrators must enter a verification code to access the Azure portal. You need to ensure that the administrators can access the Azure portal only from your on-premises network.

What should you configure?

✔ The multi-factor authentication service settings.

Explanation:-The security of two-step verification lies in its layered approach. Compromising multiple authentication factors presents a significant challenge for attackers. Even if an attacker manages to learn the user's password, it is useless without also having possession of the additional authentication method. It works by requiring two or more of the following authentication methods:

Something you know (typically a password).

Something you have (a trusted device that is not easily duplicated, like a phone).

Something you are (biometrics)

Reference: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks

If you don't want to use Conditional Access policies to enable trusted IPs, you can configure the service settings for Azure Multi-Factor Authentication using the following steps:

We don't have conditional access available as option to MFA service settings seems to be right.
Refer: https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#trusted-ips

- An Azure AD Identity Protection user risk policy.
- The default for all the roles in Azure AD Privileged Identity Management
- An Azure AD Identity Protection sign-in risk policy.

Q12)

You sign up for Azure Active Directory (Azure AD) Premium. You need to add a user named admin1@contoso.com as an administrator on all the computers that will be joined to the Azure AD domain.

What should you configure in Azure AD?

- User settings from the Users blade
- ✅ Device settings from the Devices blade

Explanation:-Device Administrators role is available for assignment only as an additional local administrator in Device settings. refer - https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

- General settings from the Groups blade
- Providers from the MFA Server blade

Q13)

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com that is configured for hybrid coexistence with the on-premises ActiveDirectory domain. The tenant contains the users shown in the following table.

Name	User Type	Source	Sign-in
User1	Member	Azure AD	User1@contoso.com
User2	Member	Windows Server Active Directory	User2@contoso.com
User3	Guest	Multiple	User3@outlook.com
User4	Guest	Multiple	User4@gmail.com

Whenever possible, you need to enable Azure Multi-Factor Authentication (MFA) for the users in contoso.com.

Which users should you enable for Azure MFA?

- ✅ User1, User2, User3, and User4

Explanation:-Guests can have MFA enabled, since Azure User is a given and AD user is also available so if you have the MFA server installed and configured on-prem.

When collaborating with external B2B guest users, it's a good idea to protect your apps with multi-factor authentication (MFA) policies. Then external users will need more than just a user name and password to access your resources. In Azure Active Directory (Azure AD), you can accomplish this goal with a Conditional Access policy that requires MFA for access. MFA policies can be enforced at the tenant, app, or individual guest user level, the same way that they are enabled for members of your own organization. https://docs.microsoft.com/en-us/azure/active-directory/b2b/b2b-tutorial-require-mfa

- User2 only
- User1 only
- User1 and User2 only
- User1, User2, and User3 only

Q14)

You have an Azure subscription that contains a policy-based virtual network gateway named GW1 and a virtual network named VNet1.You need to ensure that you can configure a point-to-site connection from VNet1 to an on-premises computer.

Which two actions should you perform?

Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- Add a public IP address space to VNet1.
- ✅ Delete GW1.

Explanation:-A VPN gateway is used when creating a VPN connection to your on-premises network. Route-based VPN devices use any-to-any (wildcard) traffic selectors, and let routing/forwarding tables direct traffic to different IPsec tunnels. It is typically built on router platforms where each IPsec tunnel is modeled as a network interface or VTI (virtual tunnel interface). Policy-based VPN devices use the combinations of prefixes from both networks to define how traffic is encrypted/decrypted through IPsec tunnels. It is typically built on firewall devices that perform packet filtering. IPsec tunnel encryption and decryption are added to the packet filtering and processing engine.

- Add a connection to GW1.
- ✅ Create a route-based virtual network gateway.

Explanation:-A VPN gateway is used when creating a VPN connection to your on-premises network. Route-based VPN devices use any-to-any

(wildcard) traffic selectors, and let routing/forwarding tables direct traffic to different IPsec tunnels. It is typically built on router platforms where each IPsec tunnel is modeled as a network interface or VTI (virtual tunnel interface). Policy-based VPN devices use the combinations of prefixes from both networks to define how traffic is encrypted/decrypted through IPsec tunnels. It is typically built on firewall devices that perform packet filtering. IPsec tunnel encryption and decryption are added to the packet filtering and processing engine.

- Reset GW1.

Q15) From the MFA Server blade, you open the Block/unblock users blade as shown in the exhibit. What caused AlexW to be blocked?

- The user reported a fraud alert when prompted for additional authentication.
- The user account password expired.
- ✅ An administrator manually blocked the user.

Explanation:-Only an admin can block users and not a reason and complaints in terms of the software way of working. An Administrator can block a user:

1. Sign in to the Azure portal as an administrator.
2. Browse to Azure Active Directory > MFA > Block/unblock users.
3. Select Add to block a user.
4. Select the Replication Group. Enter the username for the blocked user as username@domain.com. Enter a comment in the Reason field, for example: Lost phone.
5. Select Add to finish blocking the user.

- The user entered an incorrect PIN four times within 10 minutes.

Q16) State whether the following statement is correct or incorrect -

"You can configure alerts based on metric alerts (captured from Azure Metrics) to Activity Log alerts that can notify only with an Azure Automation Runbook (and not by email)."

- ✅ Incorrect

Explanation:-You can configure alerts based on metric alerts (captured from Azure Metrics) to Activity Log alerts that can notify by email, web hook, SMS, Logic Apps, or even an Azure Automation Runbook.

- Correct

Q17)

You have an Azure subscription named Subscription1 that contains an Azure virtual network named VM1. VM1 is in a resource group named RG1.VM1 runs services that will be used to deploy resources to RG1.

You need to ensure that a service running on VM1 can manage the resources in RG1 by using the identity of VM1.

What should you do first?

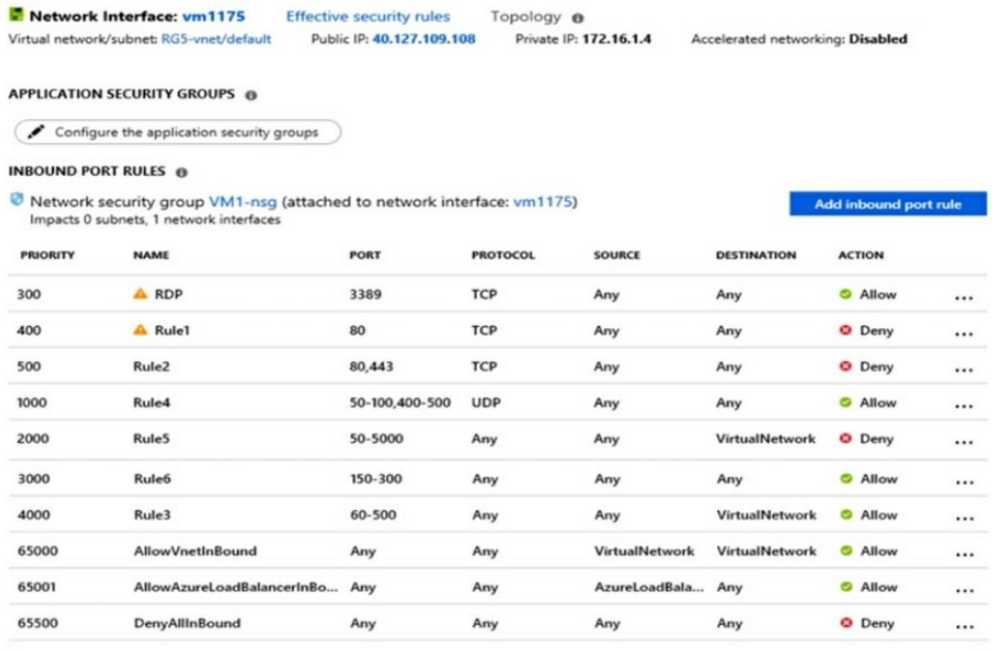
- From the Azure portal, modify the Access control (IAM) settings of RG1.
- From the Azure portal, modify the Policies settings of RG1.
- From the Azure portal, modify the Access control (IAM) settings of VM1.
- ✅ From the Azure portal, modify the value of the Managed Service Identity option for VM1.

Explanation:-The managed identities for Azure resources feature in Azure Active Directory (Azure AD) solves this problem. The feature provides Azure services with an automatically managed identity in Azure AD. You can use the identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without any credentials in your code. References: https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

---

Q18)

You have an Azure virtual machine named VM1. The network interface for VM1 is configured as shown in the picture.



You deploy a web server on VM1, and then create a secure website that is accessible by using the HTTPS protocol.

VM1 is used as a web server only.

You need to ensure that users can connect to the website from the internet. What should you do?

- Create a new inbound rule that allows TCP protocol 443 and configure the protocol to have a priority of 501.
- ✓ For Rule5, change the Action to Allow and change the priority to 401.

Explanation:-HTTPS is on Port 443 inbound. This is the only port needed to be open for secure connections to the web server.
Rule 2 is blocking HTTPS access (port 443) and has a priority of 500.
Changing Rule 5 (ports 50-5000) and giving it a lower priority number will allow access on port 443.
Note: Rules are processed in priority order, with lower numbers processed before higher numbers, because lower numbers have higher priority.
Once traffic matches a rule, processing stops.
Rule 2 is blocking HTTPS access (port 443) and has a priority of 500. Creating a rule for the same protocol (443) with a higher priority number will not help.
Rule 1 blocks access to port 80, which is used for HTTP, not HTTPS.
Rule 2 is blocking HTTPS access (port 443).
Changing Rule 4 allows access on UDP but is a higher priority number than Rule.
Changing the protocol on Rule4 to TCP will not help if we don't also change the priority to a lower number.

- Modify the protocol of Rule4.
- Delete Rule1.

Q19)

You manage a virtual network named VNet1 that is hosted in the West US Azure region.VNet1 hosts two virtual machines named VM1 and VM2 that run Windows Server. You need to inspect all the network traffic from VM1 to VM2 for a period of three hours.

Solution: From Azure Network Watcher, you create a packet capture.

Does this meet the goal?

- ✓ Incorrect

Explanation:-Use the Connection Monitor feature of Azure Network Watcher. References: https://azure.microsoft.com/en-us/updates/general-availability-azure-network-watcher-connection-monitor-in-all-public-regions/

- Correct

Q20)

You have an Azure Active Directory (Azure AD) tenant named contosocloud.onmicrosoft.com.Your company has a public DNS zone for contoso.com.

You add contoso.com as a custom domain name to Azure AD. You need to ensure that Azure can verify the domain name. Which type of DNS record should you create?

- ✓ TXT

Explanation:-You can configure Azure DNS to host a custom domain for your web apps. For example, you can create an Azure web app and have your users access it using either www.contoso.com or contoso.com as a fully qualified domain name (FQDN).

To do this, you have to create three records:

* A root "A" record pointing to contoso.com

A root "TXT" record for verification

A "CNAME" record for the www name that points to the A record

Refer: https://docs.microsoft.com/en-us/azure/dns/dns-web-sites-custom-domain

- NSEC
- DNSKEY
- SRV

Q21) Azure storage accounts provide _____ .

- ✓ All of these

Explanation:-Azure storage accounts provide 4 separate services: blobs, tables, queues and files. Understand the usage scenarios of each service.

- files
- blobs
- tables
- queues

Q22)

You have an Azure Active Directory (Azure AD) tenant.

All administrators must enter a verification code to access the Azure portal.

You need to ensure that the administrators can access the Azure portal without entering a verification code when they are connecting from your on-premises network.

Consider that some IP restrictions are included inside the sign in risk policy.

What should you configure?

- The default for all the roles in Azure AD Privileged Identity Management
- ✓ An Azure AD Identity Protection sign-in risk policy

- An Azure AD Identity Protection user risk policy

Q23)

You have an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.You hire a temporary vendor. The vendor uses a Microsoft account that has a sign-in of user1@outlook.com.You need to ensure that the vendor can authenticate to the tenant by using user1@outlook.com.

What should you do?

- ✅ From the Azure portal, add a new guest user, and then specify user1@outlook.com as the email address.

Explanation:-You hire a temporary vendor. The vendor has to login to your tenant using the @outlook.com. So you invite the vendor as a guest user.

- From Azure Cloud Shell, run the New-AzureADUser cmdlet and specify the "UserPrincipalName user1@outlook.com parameter.
- From Windows PowerShell, run the New-AzureADUser cmdlet and specify the "UserPrincipalName user1@outlook.com parameter.
- From the Azure portal, add a custom domain name, create a new Azure AD user, and then specify user1@outlook.com as the username.

Q24)

You have an Azure subscription that contains 10 virtual networks. The virtual networks are hosted in separate resource groups.

Another administrator plans to create several network security groups (Network Security Groupss) in the subscription.

You need to ensure that when an Network Security Groups is created, it automatically blocks TCP port 8080 between the virtual networks.

Solution: From the Resource providers blade, you unregister the Microsoft.ClassicNetwork provider.

Does this meet the goal?

- ✅ Incorrect

Explanation:-You should use a policy definition. Reference: https://docs.microsoft.com/en-us/azure/azure-policy/policy-definition

- Correct

Q25) State whether the following statement is correct or incorrect -

"Azure Policy is a service that lets you create, manage, and apply policy to Azure resources at a subscription, resource group, or resource level. Policies enforce different rules over your Azure resources, so those resources remain compliant with your organization's standards."

- ✅ Correct

Explanation:-Azure Policy is a service that lets you create, manage, and apply policy to Azure resources at a subscription, resource group, or resource level. Policies enforce different rules over your Azure resources, so those resources remain compliant with your organization's standards.

- Incorrect

Q26) State whether the following statement is correct or incorrect -

"Tags in Azure can be used to logically organize resources by categories. Each tag is a name and a value pair. However, tags can be shared across multiple resources."

- The statement is Incorrect
- ✅ The statement is Correct

Explanation:-Tags in Azure can be used to logically organize resources by categories. Each tag is a name and a value pair. Tags can be shared across multiple resources and enforced with Azure Policy.

Q27) Blob storage supports _____ types of blobs, and _____ access tiers.

- ✅ 3;3

Explanation:-Microsoft has all three access tiers for the Blob Storage – Hot Tier, Cool Tier and Archive. You cannot change access tier for Page Blobs. Access tier is applicable only for Append Blobs and Block Blobs. The limitation relates to the purpose and architecture of these storage types.

Azure Storage supports three types of blobs:
1. Block blobs store text and binary data. Block blobs are made up of blocks of data that can be managed individually.
2. Append blobs are made up of blocks like block blobs, but are optimized for append operations.
3. Page blobs store random access files up to 8 TiB in size.

Refer: https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blobs-introduction

- 4;2
- 2;3
- 1;2

Q28) State whether the following statement is correct or incorrect -

"Azure does not offer a rich ecosystem of governance controls with user-level and platform-level controls in the form of role-based access control (RBAC) and Azure Policy."

- ✅ Incorrect

Explanation:-Azure offers a rich ecosystem of governance controls with user-level and platform-level controls in the form of role-based access control (RBAC) and Azure Policy.

- Correct

Q29)

You have a computer named Computer1 that has a point-to-site VPN connection to an Azure virtual network named VNet1. The point-to-site connection uses a self-signed certificate.

From Azure, you download and install the VPN client configuration package on a computer named Computer2.

You need to ensure that you can establish a point-to-site VPN connection to VNet1 from Computer2.

Solution: You export the client certificate from Computer1 and install the certificate on Computer2.

Does this meet the goal?

✅ Correct

Explanation:-Each client computer that connects to a VNet using Point-to-Site must have a client certificate installed. You generate a client certificate from the self-signed root certificate, and then export and install the client certificate. If the client certificate is not installed, authentication fails. References: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-certificates-point-to-site

⚪ Incorrect

Q30)

You have an Azure subscription named Subscription1 that contains two Azure virtual networks named VNet1 and VNet2. VNet1 contains a VPN gateway namedVPNGW1 that uses static routing. There is a site-to-site VPN connection between your on-premises network and VNet1.On a computer named Client1 that runs Windows 10, you configure a point-to-site VPN connection to VNet1.

You configure virtual network peering between VNet1 and VNet2.

You verify that you can connect to VNet2 from the on-premises network. Client1 is unable to connect to VNet2.You need to ensure that you can connect Client1 to VNet2.

What should you do?

⚪ Select Allow gateway transit on VNet1.

✅ Download and re-install the VPN client configuration package on Client1.

Explanation:-The problem states that you have created the point-to-site VPN before you configured peering.
Clients using Windows can access directly peered VNets, but the VPN client must be downloaded again if any changes are made to VNet peering or the network topology.
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-point-to-site-routing

⚪ Enable BGP on VPNGW1.

⚪ Select Allow gateway transit on VNet2.

Q31)

You manage a virtual network named VNet1 that is hosted in the West US Azure region.VNet1 hosts two virtual machines named VM1 and VM2 that run Windows Server. You need to inspect all the network traffic from VM1 to VM2 for a period of three hours. Solution: From Performance Monitor, you create a Data Collector Set (DCS).

Does this meet the goal?

✅ Incorrect

Explanation:-Use the Connection Monitor feature of Azure Network Watcher. References: https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview

⚪ Correct

Q32)

You have an Azure subscription named Subscription1 that contains the resource groups shown in the following table.

Name	Region
RG1	East Asia
RG2	East US

In RG1, you create a virtual machine named VM1 in the East Asia location.

You plan to create a virtual network named VNET1.

You need to create VNET1, and then connect VM1 to VNET1.

What are two possible ways to achieve this goal?

⚪ Create VNET1 in a new resource group in the West US location, and then set West US as the location.

⚪ Create VNET1 in RG2, and then set East US as the location.

⚪ Create VNET1 in RG1, and then set East US as the location.

✅ Create VNET1 in RG2, and then set East Asia as the location.

Explanation:-Resource group - A container that holds related resources for an Azure solution. The resource group includes those resources that you want to manage as a group. You decide which resources belong in a resource group based on what makes the most sense for your organization. There are some important factors to consider when defining your resource group:

* A resource group can contain resources that are located in different regions.
* All the resources in your group should share the same lifecycle. You deploy, update, and delete them together. If one resource, such as a database server, needs to exist on a different deployment cycle it should be in another resource group.
* Each resource can only exist in one resource group.
* You can add or remove a resource to a resource group at any time.
* You can move a resource from one resource group to another group.

* A resource group can be used to scope access control for administrative actions.
* A resource can interact with resources in other resource groups. This interaction is common when the two resources are related but don't share the same lifecycle (for example, web apps connecting to a database).

✅ Create VNET1 in RG1, and then set East Asia as the location.

Explanation:-RG is a logical grouping of resources, nothing is physically tied to it. So one of the possible choices is to create the VNET in the other RG even if it's in another region, and then set whatever region you want for the VNET. As long as the VNET is in the same region as the VM the resource group location doesn't matter.

Q33)

You have two Azure Active Directory (Azure AD) tenants named contoso.com and fabrikam.com.You have a Microsoft account that you use to sign in to both tenants. You need to configure the default sign-in tenant for the Azure portal.

What should you do?

⚪ From the Azure portal, change the directory.
⚪ From the Azure portal, configure the portal settings.
✅ From Azure Cloud Shell, run Set-AzureRmContext.

Explanation:-Let's analyze the answers
- From Azure Cloud Shell, run Set-AzureRmSubscription.
R: Allows you to configure the subscription to connect to by default.
This does not solve the requested
From Azure Cloud Shell, run Set-AzureRmContext.
It allows you to configure the directory and subscription to which you want to connect by default. This meets the request.
From the Azure portal, configure the portal settings.
From the portal settings you cannot define the default directory to which you want to connect. It does not comply with what is required.
From the Azure portal, change the directory.
It refers to changing the directory, but not specific in which option of the entire portal the change can be made.
The Set-AzureRmContext cmdlet sets authentication information for cmdlets that you run in the current session. The context includes tenant, subscription, and environment information. References: https://docs.microsoft.com/en-us/powershell/module/azurerm.profile/set-azurermcontext

⚪ From Azure Cloud Shell, run Set-AzureRmSubscription.

Q34)

You manage a virtual network named VNet1 that is hosted in the West US Azure region.VNet1 hosts two virtual machines named VM1 and VM2 that run Windows Server.

You need to inspect all the network traffic from VM1 to VM2 for a period of three hours. Solution: From Azure Network Watcher, you create a connection monitor.

Does this meet the goal?

✅ Correct

Explanation:-Azure Network Watcher provides tools to monitor, diagnose, view metrics, and enable or disable logs for resources in an Azure virtual network. Refer - https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview

⚪ Incorrect

Q35)

You have an Azure subscription named Subscription1 and two Azure Active Directory (Azure AD) tenants named Tenant1 and Tenant2.

Subscription1 is associated to Tenant1. Multi-factor authentication (MFA) is enabled for all the users in Tenant1.

You need to enable MFA for the users in Tenant2. The solution must maintain MFA for Tenant1.

What should you do first?

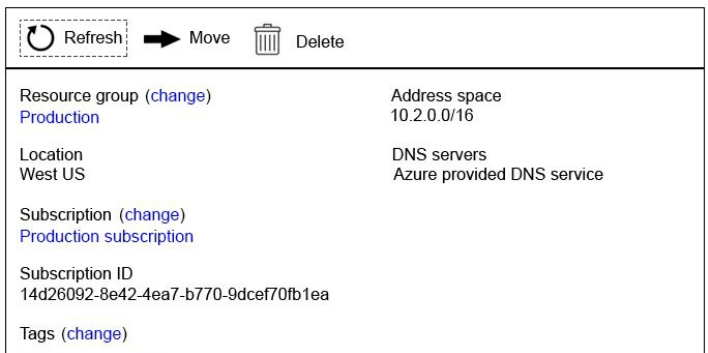
⚪ Change the directory for Subscription1.
⚪ Transfer the administration of Subscription1 to a global administrator of Tenant2.
✅ Create and link a subscription to Tenant2.

Explanation:-Azure AD Tenants can be associated with multiple Subscriptions (typically in larger organisations), but a Subscription can only ever be associated with a single Azure AD Tenant at any time. Therefore correct answer as we need another subscription to be able to connect with Tenant2. Refer: https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings

⚪ Configure the MFA Server setting in Tenant1.

Q36)

You have a virtual network named VNet1 as shown in the picture.



No devices are connected to VNet1.

You plan to peer VNet1 to another virtual network named VNet2 in the same region.

VNet2 has an address space of 10.2.0.0/16.

You need to create the peering.

What should you do first?

- Create a subnet on VNet1 and VNet2.
- ✓ Modify the address space of VNet1.

Explanation:-The virtual networks you peer must have non-overlapping IP address spaces. The exhibit indicates that VNet1 has an address space of 10.2.0.0/16, which is the same as VNet2, and thus overlaps. We need to change the address space for VNet1.

- Configure a service endpoint on VNet2.
- Add a gateway subnet to VNet1.

Q37)

You have an Azure subscription that contains 10 virtual networks. The virtual networks are hosted in separate resource groups.

Another administrator plans to create several network security groups (Network Security Groupss) in the subscription.

You need to ensure that when an Network Security Groups is created, it automatically blocks TCP port 8080 between the virtual networks.

Solution: You configure a custom policy definition, and then you assign the policy to the subscription.

Does this meet the goal?

- ✓ Correct

Explanation:-Resource policy definition used by Azure Policy enables you to establish conventions for resources in your organization by describing when the policy is enforced and what effect to take. By defining conventions, you can control costs and more easily manage your resources.
Reference: https://docs.microsoft.com/en-us/azure/azure-policy/policy-definition

- Incorrect

Q38) State whether the following statement is correct or incorrect -

"Azure Log Analytics has many management solutions that help administrators gain value out of complex machine data. These solutions contain pre-built visualizations and queries that help surface insights quickly."

- Incorrect
- ✓ Correct

Explanation:-Azure Log Analytics has many management solutions that help administrators gain value out of complex machine data. These solutions contain pre-built visualizations and queries that help surface insights quickly.

Q39)

You have an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

The User administrator role is assigned to a user named Admin1.

An external partner has a Microsoft account that uses the user1@outlook.com sign in.Admin1 attempts to invite the external partner to sign in to the

Azure AD tenant and receives the following error message: "Unable to invite user user1@outlook.com " Generic authorization exception."

You need to ensure that Admin1 can invite the external partner to sign in to the Azure AD tenant.

What should you do?

- From the Organizational relationships blade, add an identity provider.
- From the Custom domain names blade, add a custom domain.
- ✓ From the Users blade, modify the External collaboration settings.

Explanation:-By default, the person who signs up for an Azure subscription is assigned the Global administrator role for the Azure AD organization. Only Global administrators and Privileged Role administrators can delegate administrator roles. Refer: https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/user-account-management

- From the Roles and administrators blade, assign the Security administrator role to Admin1.
