Microsoft Azure Certification AZ-103 Exam

- **Vendor: Microsoft**
- **Exam Code: AZ-103**
- **Exam Name: Microsoft Azure Administrator**

NEW QUESTION 295
You have an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com that contains 100 user accounts. You purchase 10 Azure AD Premium P2 licenses for the tenant. You need to ensure that 10 users can use all the Azure AD Premium features. What should you do?

A. From the Directory role blade of each user, modify the directory role.
B. From the Azure AD domain, add an enterprise application.
C. From the Groups blade of each user, invite the users to a group.
D. From the Licenses blade of Azure AD, assign a license.

Answer: D
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/license-users-groups

NEW QUESTION 296
You have an Azure subscription. You have 100 Azure virtual machines. You need to quickly identify underutilized virtual machines that can have their service tier changed to a less expensive offering. Which blade should you use?

A. Metrics
B. Monitor
C. Customer insights
D. Advisor

Answer: D
Explanation:
Advisor helps you optimize and reduce your overall Azure spend by identifying idle and underutilized resources. You can get cost recommendations from the Cost tab on the Advisor dashboard.
https://docs.microsoft.com/en-us/azure/advisor/advisor-cost-recommendations

NEW QUESTION 297
You have an Azure subscription named Subscription1. Subscription1 contains a resource group named RG1. RG1 contains resources that were deployed by using templates. You need to view the date and time when the resources were created in RG1.
Solution: From the RG1 blade, you click Deployments.
Does this meet the goal?

A. Yes
B. No

Answer: A
Explanation:
From the RG1 blade, click Deployments. You see a history of deployment for the resource group.
https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/template-tutorial-create-first-template?tabs=azure-powershell

NEW QUESTION 298
You have an Azure subscription. Users access the resources in the subscription from either home or from customer sites. From home, users must establish a point-to-site VPN to access the Azure resources. The users on the customer sites access the Azure resources by using site-to-site VPNs. You have a line-of-business app named App1 that runs on several Azure virtual machine. The virtual machines run Windows Server 2016. You need to ensure that the connections to App1 are spread across all the virtual machines. What are two possible Azure services that you can use? (Each correct answer presents a complete solution. Choose two.)

A. an Azure Content Delivery Network (CDN)
B. an Azure Application Gateway
C. Traffic Manager
D. an internal load balancer
E. a public load balancer

Answer: BD

NEW QUESTION 299
You have an Azure subscription named Subscription1. You have 5 TB of data that you need to transfer to Subscription1. You plan to use an Azure Import/Export job. What can you use as the destination of the imported data?

A. Azure Data Lake Store
B. a virtual machine
C. the Azure File Sync Storage Sync Service
D. Azure Blob Storage

Answer: D
Explanation:
Azure Import/Export service is used to securely import large amounts of data to Azure Blob storage and Azure Files by shipping disk drives to an Azure datacenter. The maximum size of an Azure Files Resource of a file share is 5 TB.
https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-service

NEW QUESTION 300
You have two Azure virtual networks named VNet1 and VNet2. VNet1 contains an Azure virtual machine named VM1. VNet2 contains an Azure virtual machine named VM2. VM1 hosts a frontend application that connects to VM2 to retrieve data. Users report that the frontend application is slower than usual. You need to view the average round-trip time (RTT) of the packets from VM1 to VM2. Which Azure Network Watcher feature should you use?

A. IP flow verify
B. Connection monitor
C. NSG flow logs
D. Connection troubleshoot

Answer: B
Explanation:
The connection monitor capability monitors communication at a regular interval and informs you of reachability, latency, and network topology changes between the VM and the endpoint.
Incorrect:
Not A: The IP flow verify capability enables you to specify a source and destination IPv4 address, port, protocol (TCP or UDP), and traffic direction (inbound or outbound). IP flow verify then tests the communication and informs you if the connection succeeds or fails. If the connection fails, IP flow verify tells you which security rule allowed or denied the communication, so that you can resolve the problem.
Not C: The NSG flow log capability allows you to log the source and destination IP address, port, protocol, and whether traffic was allowed or denied by an NSG.
Not D: The connection troubleshoot capability enables you to test a connection between a VM and another VM, an FQDN, a URI, or an IPv4 address. The test returns similar information returned when using the connection monitor capability, but tests the connection at a point in time, rather than monitoring it over time, as connection monitor does.
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview

NEW QUESTION 301
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?

A. Change the directory for Subscription1.
B. Configure the MFA Server setting in Tenant1.
C. Create and link a subscription to Tenant2.
D. Transfer the administration of Subscription1 to a global administrator of Tenant2.

Answer: C

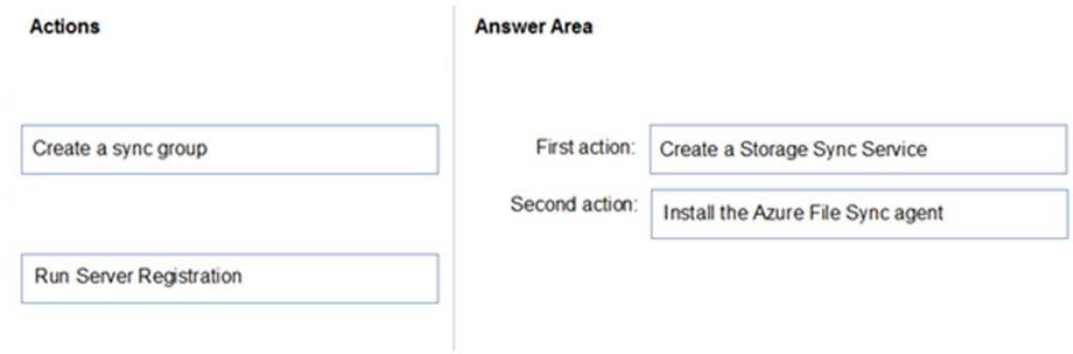
NEW QUESTION 302
You have an Azure Active Directory (Azure AD) tenant. All administrators must enter a verification code to access the Azure portal. You need to ensure that the administrators can access the Azure portal without entering a verification code when they are connecting from your on-premises network. What should you configure?

A. an Azure AD Identity Protection user risk policy
B. the multi-factor authentication service settings
C. the default for all the roles in Azure AD Privileged Identity Management
D. an Azure AD Identity Protection sign-in risk policy

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

NEW QUESTION 303
Drag and Drop
You have an Azure subscription that contains an Azure file share. You have an on-premises server named Server1 that runs Windows Server 2016. You plan to set up Azure File Sync between Server1 and the Azure file share. You need to prepare the subscription for the planned Azure File Sync. Which two actions should you perform in the Azure subscription? (To answer, drag the appropriate actions to the correct targets. Each action may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.)

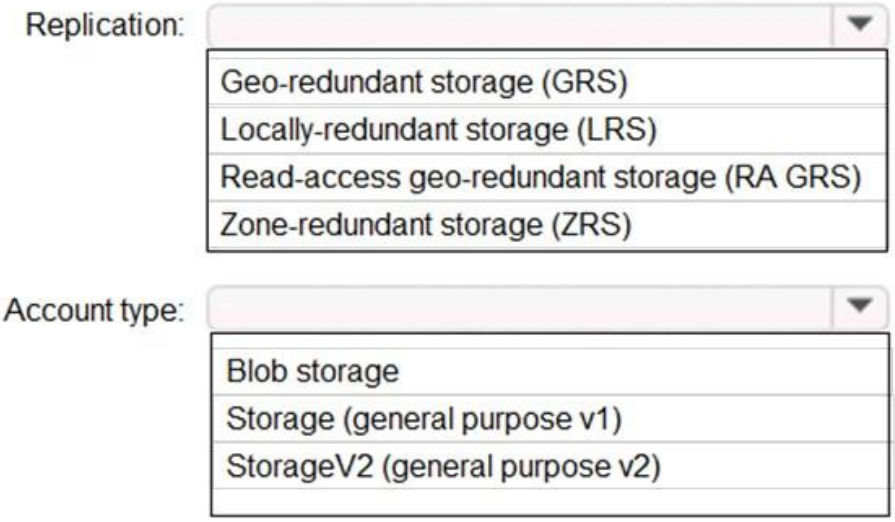
Answer:



Explanation:
Step 1: Create a Storage Sync Service. The deployment of Azure File Sync starts with placing a Storage Sync Service resource into a resource group of your selected subscription.
Step 2: Install the Azure File Sync agent. The Azure File Sync agent is a downloadable package that enables Windows Server to be synced with an Azure file share. When the Azure File Sync agent installation is finished, the Server Registration UI automatically opens. You must have a Storage Sync Service before registering.
Step 3: Run Server Registration. Registering your Windows Server with a Storage Sync Service establishes a trust relationship between your server (or cluster) and the Storage Sync Service. A server can only be registered to one Storage Sync Service and can sync with other servers and Azure file shares associated with the same Storage Sync Service.
https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-deployment-guide?tabs=azure-portal

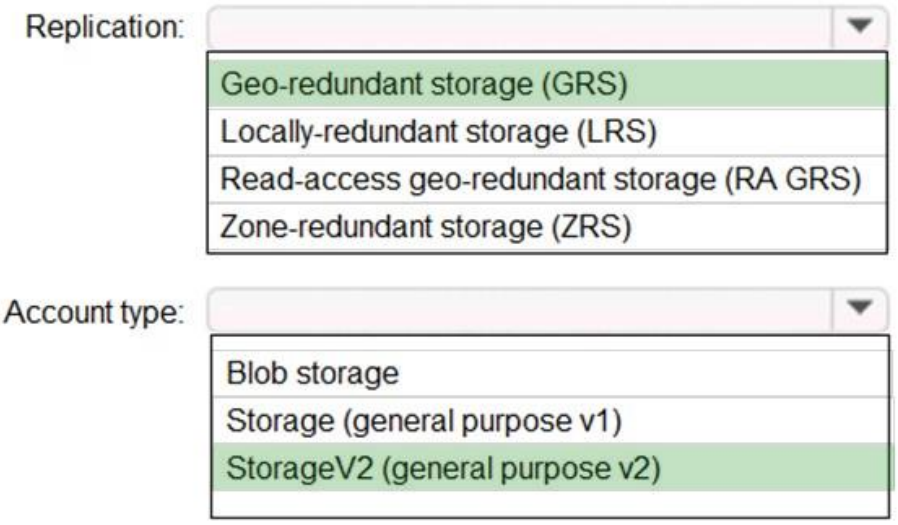
NEW QUESTION 304
Hotspot
You plan to create an Azure Storage account in the Azure region of East US 2. You need to create a storage account that meets the following requirements:
- Replicates synchronously.
- Remains available if a single data center in the region fails.
How should you configure the storage account? (To answer, select the appropriate options in the answer area.)

Answer Area



Answer:

Answer Area

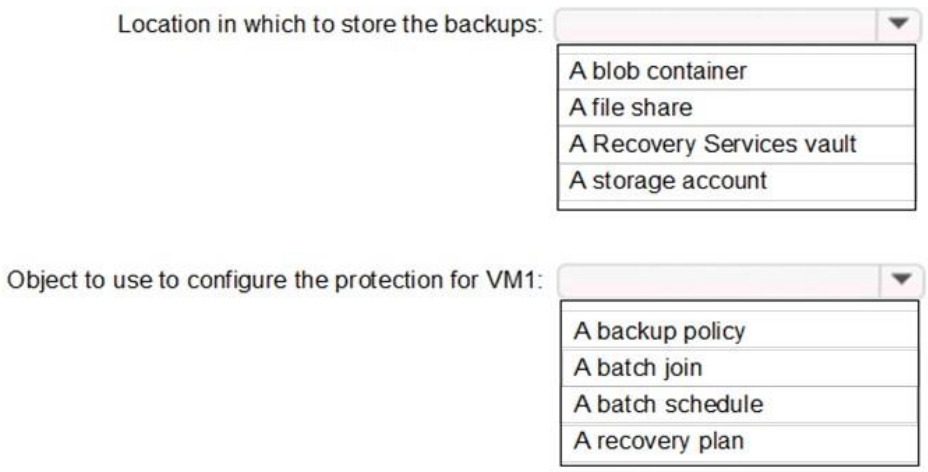


Explanation:
Box 1: Zone-redundant storage (ZRS). Zone-redundant storage (ZRS) replicates your data synchronously across three storage clusters in a single region. LRS would not remain available if a data center in the region fails GRS and RA GRS use asynchronous replication.

Box 2: StorageV2 (general purpose V2). ZRS only support GPv2.
https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy
https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy-zrs

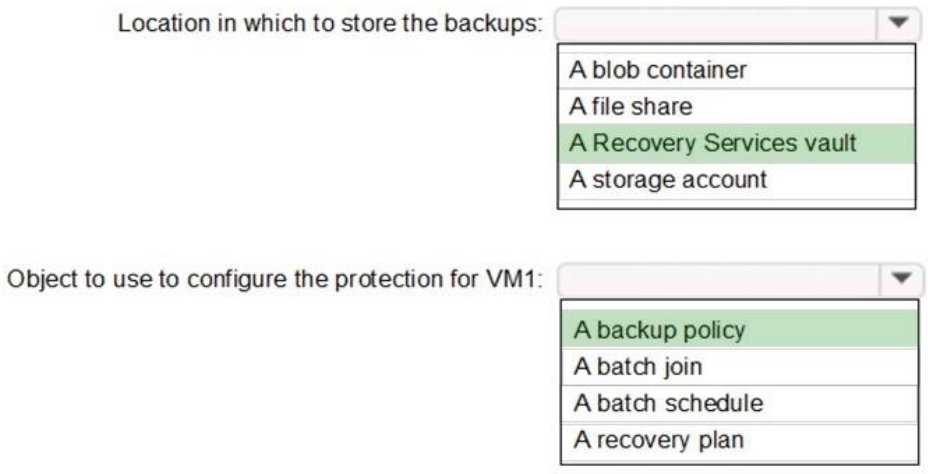
NEW QUESTION 305
Hotspot
You purchase a new Azure subscription named Subscription1. You create a virtual machine named VM1 in Subscription1. VM1 is not protected by Azure Backup. You need to protect VM1 by using Azure Backup. Backups must be created at 01:00 and stored for 30 days. What should you do? (To answer, select the appropriate options in the answer area.)

Answer Area



Answer:

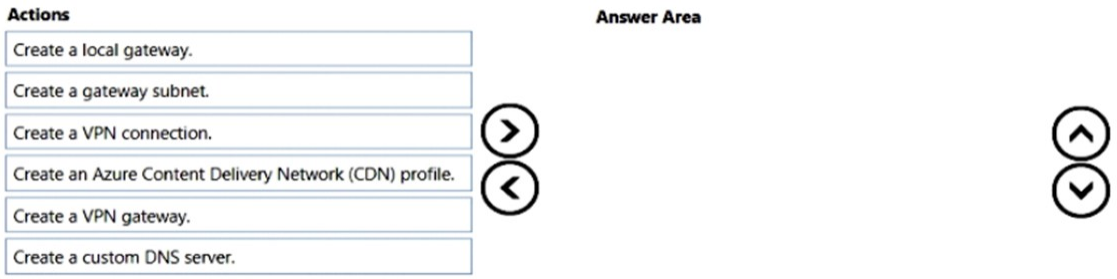
Answer Area



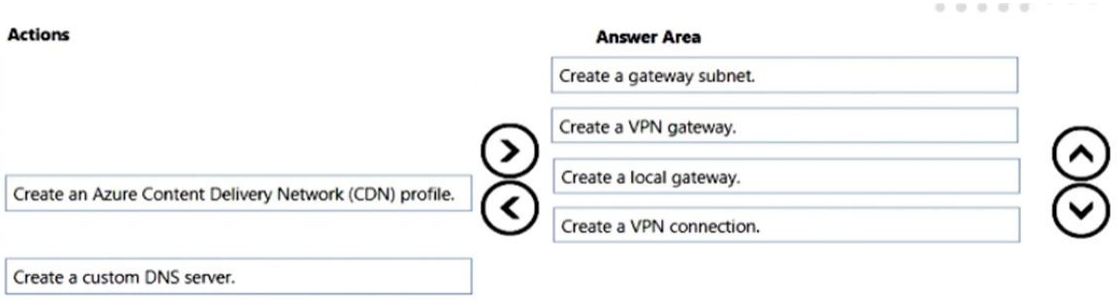
Explanation:
Box 1: A Recovery Services vault. A Recovery Services vault is an entity that stores all the backups

and recovery points you create over time.
Box 2: A backup policy. When a new policy is applied, schedule and retention of the new policy is followed.
https://docs.microsoft.com/en-us/azure/backup/backup-configure-vault
https://docs.microsoft.com/en-us/azure/backup/backup-azure-backup-faq

NEW QUESTION 306
Drag and Drop
You have an on-premises network that you plan to connect to Azure by using a site-to-site VPN. In Azure, you have an Azure virtual network named VNet1 that uses an address space of 10.0.0.0/16. VNet1 contains a subnet named Subnet1 that uses an address space of 10.0.0.0/24. You need to create a site-to-site VPN to Azure. Which four actions should you perform in sequence? (To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.)



Answer:



NEW QUESTION 307
.....

NEW QUESTION 401
You have an Azure virtual machine named VM1. You use Azure Backup to create a backup of VM1 named Backup1. After creating Backup1, you perform the following changes to VM1:
- Modify the size of VM1.
- Copy a file named Budget.xls to a folder named Data.
- Reset the password for the built-in administrator account.
- Add a data disk to VM1.
An administrator uses the Replace existing option to restore VM1 from Backup1. You need to ensure that all the changes to VM1 are restored. Which change should you perform again?

A. Modify the size of VM1.
B. Add a data disk.
C. Reset the password for the built-in administrator account.
D. Copy Budget.xls to Data.

Answer: D
Explanation:
https://docs.microsoft.com/en-us/azure/backup/backup-azure-arm-restore-vms#replace-existing-disks

NEW QUESTION 402
You have an Azure virtual machine named VM1 that runs Windows Server 2016. You need to create an alert in Azure when more than two error events are logged to the System log on VM1 within an hour.
Solution: You create an event subscription on VM1. You create an alert in Azure Monitor and specify VM1 as the source.
Does this meet the goal?

A. Yes
B. No

Answer: B
Explanation:
Instead: You create an Azure Log Analytics workspace and configure the data settings. You install the Microsoft Monitoring Agent on VM1. You create an alert in Azure Monitor and specify the Log Analytics workspace as the source.
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agents-overview

NEW QUESTION 403
You have an Azure virtual machine named VM1 that runs Windows Server 2016. You need to create an alert in Azure when more than two error events are logged to the System log on VM1 within an hour.
Solution: You create an Azure Log Analytics workspace and configure the data settings. You install the Microsoft Monitoring Agent on VM1. You create an alert in Azure Monitor and specify the Log Analytics workspace as the source.
Does this meet the goal?

A. Yes
B. No

Answer: A
Explanation:
Alerts in Azure Monitor can identify important information in your Log Analytics repository. They are created by alert rules that automatically run log searches at regular intervals, and if results of the log search match particular criteria, then an alert record is created and it can be configured to perform an automated response. The Log Analytics agent collects monitoring data from the guest operating system and workloads of virtual machines in Azure, other cloud providers, and on-premises. It collects data into a Log Analytics workspace.
https://docs.microsoft.com/en-us/azure/azure-monitor/learn/tutorial-response
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agents-overview

NEW QUESTION 404
You have an Azure virtual machine named VM1. The network interface for VM1 is configured as shown in the exhibit.
.....
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?

A. Change the priority of Rule6 to 100.

B. Change the priority of Rule3 to 450.
C. Delete Rule1.
D. Modify the action of Rule1.

Answer: B
Explanation:
Rule 2 is blocking HTTPS access (port 443) and has a priority of 500. Changing Rule 3 (ports 60-500) 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.
Incorrect:
Not A: HTTPS uses port 443. Rule6 only applies to ports 150 to 300.
Not C and D: Rule 1 blocks access to port 80, which is used for HTTP, not HTTPS.
https://docs.microsoft.com/en-us/azure/virtual-network/security-overview

NEW QUESTION 405
You have a Microsoft 365 tenant and an Azure Active Directory (Azure AD) tenant named contoso.com. You plan to grant three users named User1, User2, and User3 access to a temporary Microsoft SharePoint document library named Library1. You need to create groups for the users. The solution must ensure that the groups are deleted automatically after 180 days. Which two groups should you create? (Each correct answer presents a complete solution. Choose two.)

A. a Security group that uses the Assigned membership type
B. an Office 365 group that uses the Assigned membership type
C. an Office 365 group that uses the Dynamic User membership type
D. a Security group that uses the Dynamic User membership type
E. a Security group that uses the Dynamic Device membership type

Answer: BC
Explanation:
You can set expiration policy only for Office 365 groups in Azure Active Directory (Azure AD). Note: With the increase in usage of Office 365 Groups, administrators and users need a way to clean up unused groups. Expiration policies can help remove inactive groups from the system and make things cleaner. When a group expires, all of its associated services (the mailbox, Planner, SharePoint site, etc.) are also deleted. You can set up a rule for dynamic membership on security groups or Office 365 groups.
Incorrect:
Not A and D and E: You can set expiration policy only for Office 365 groups in Azure Active Directory (Azure AD).
https://docs.microsoft.com/en-us/office365/admin/create-groups/office-365-groups-expiration-policy?view=o365-worldwide

NEW QUESTION 406
You have an Azure subscription. You enable multi-factor authentication for all users. Some users report that the email applications on their mobile device cannot connect to their Microsoft Exchange Online mailbox. The users can access Exchange Online by using a web browser and from Microsoft Outlook 2016 on their computer. You need to ensure that the users can use the email applications on their mobile device. What should you instruct the users to do?

A. Reinstall the Microsoft Authenticator app.
B. Create an app password.
C. Enable self-service password reset.
D. Reset the Azure Active Directory (Azure AD) password.

Answer: B

Explanation:
If you're enabled for multi-factor authentication, make sure that you have set up app passwords. Note: During your initial two-factor verification registration process, you're provided with a single app password. If you require more than one, you'll have to create them yourself. Go to the Additional security verification page.
https://docs.microsoft.com/en-us/office365/troubleshoot/sign-in/sign-in-to-office-365-azure-intune
https://docs.microsoft.com/sv-se/azure/active-directory/user-help/multi-factor-authentication-end-user-app-passwords

NEW QUESTION 407
You have an Azure subscription that contains the following resources:
- A virtual network that has a subnet named Subnet1.
- Two network security groups (NSGs) named NSG-VM1 and NSG-Subnet1.
- A virtual machine named VM1 that has the required Windows Server configurations to allow Remote Desktop connections.
NSG-Subnet1 has the default inbound security rules only. NSG-VM1 has the default inbound security rules and the following custom inbound security rule:
- Priority: 100
- Source: Any
- Source port range: *
- Destination: *
- Destination port range: 3389
- Protocol: UDP
- Action: Allow
VM1 connects to Subnet1. NSG1-VM1 is associated to the network interface of VM1. NSG-Subnet1 is associated to Subnet1. You need to be able to establish Remote Desktop connections from the internet to VM1.
Solution: You modify the custom rule for NSG-VM1 to use the internet as a source and TCP as a protocol.
Does this meet the goal?

A. Yes
B. No

Answer: A
Explanation:
The default port for RDP is TCP port 3389. A rule to permit RDP traffic must be created automatically when you create your VM. Note on NSG-Subnet1: Azure routes network traffic between all subnets in a virtual network, by default.
https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-rdp-connection

NEW QUESTION 408
You have an Azure subscription that contains the following resources:
- A virtual network that has a subnet named Subnet1.
- Two network security groups (NSGs) named NSG-VM1 and NSG-Subnet1.
- A virtual machine named VM1 that has the required Windows Server configurations to allow Remote Desktop connections.
NSG-Subnet1 has the default inbound security rules only. NSG-VM1 has the default inbound security rules and the following custom inbound security rule:
- Priority: 100
- Source: Any
- Source port range: *
- Destination: *
- Destination port range: 3389

- Protocol: UDP
- Action: Allow

VM1 connects to Subnet1. NSG1-VM1 is associated to the network interface of VM1. NSG-Subnet1 is associated to Subnet1. You need to be able to establish Remote Desktop connections from the internet to VM1.
Solution: You add an inbound security rule to NSG-Subnet1 that allows connections from the Any source to the * destination for port range 3389 and uses the TCP protocol. You remove NSG-VM1 from the network interface of VM1.
Does this meet the goal?

A. Yes
B. No

Answer: B
Explanation:
The default port for RDP is TCP port 3389. A rule to permit RDP traffic must be created automatically when you create your VM. Note on NSG-Subnet1: Azure routes network traffic between all subnets in a virtual network, by default.
https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-rdp-connection

NEW QUESTION 409
You have an Azure Active Directory (Azure AD) tenant named contoso.com. Multi-factor authentication (MFA) is enabled for all users. You need to provide users with the ability to bypass MFA for 10 days on devices to which they have successfully signed in by using MFA. What should you do?

A. From the multi-factor authentication page, configure the users' settings.
B. From Azure AD, create a conditional access policy.
C. From the multi-factor authentication page, configure the service settings.
D. From the MFA blade in Azure AD, configure the MFA Server settings.

Answer: C
Explanation:
Enable remember Multi-Factor Authentication steps:
1. Sign in to the Azure portal.
2. On the left, select Azure Active Directory -> Users.
3. Select Multi-Factor Authentication.
4. Under Multi-Factor Authentication, select service settings.
5. On the Service Settings page, manage remember multi-factor authentication, select the Allow users to remember multi-factor authentication on devices they trust option.
6. Set the number of days to allow trusted devices to bypass two-step verification. The default is 14 days.
7. Select Save.
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings

NEW QUESTION 410
You have an Azure subscription. All users are enabled for multi-factor authentication (MFA). You need to ensure that the users can lock out their own account if they receive an unsolicited MFA request from Azure. Which MFA settings should you configure?

A. Block/unblock users
B. Providers
C. Notifications
D. Fraud alert

Answer: D
Explanation:
Configure the fraud alert feature so that your users can report fraudulent attempts to access their resources. Users can report fraud attempts by using the mobile app or through their phone.
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#fraud-alert

NEW QUESTION 411
.....