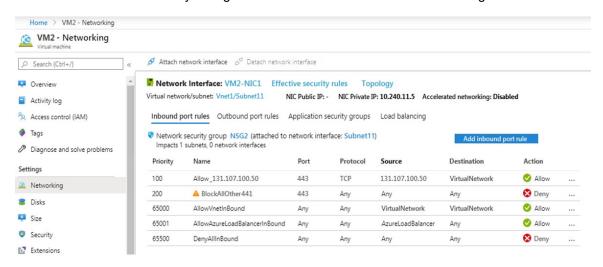
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an app named App1 that is installed on two Azure virtual machines named VM1 and VM2. Connections to App1 are managed by using an Azure Load Balancer.

The effective network security configurations for VM2 are shown in the following exhibit.



You discover that connections to App1 from 131.107.100.50 over TCP port 443 fail. You verify that the Load Balancer rules are configured correctly.

You need to ensure that connections to App1 can be established successfully from 131.107.100.50 over TCP port 443.

Solution: You create an inbound security rule that allows any traffic from the AzuteLoadBalancer source and has a cost of 150.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A Explanation:

https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

QUESTION 55

DRAG DROP

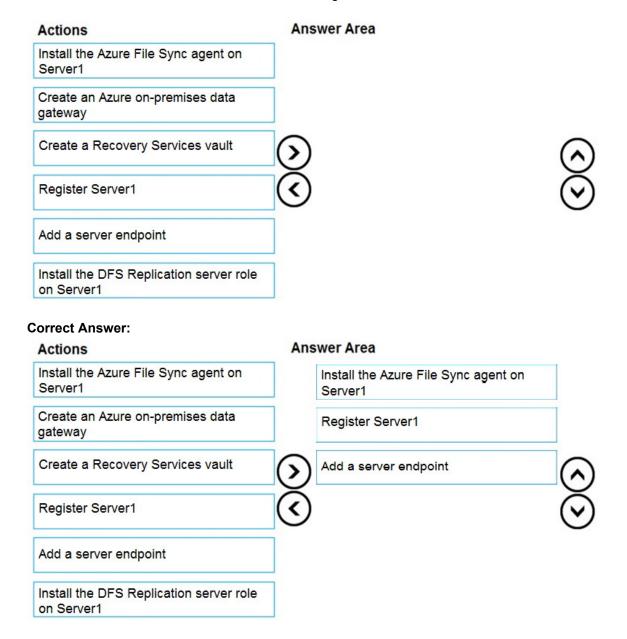
You have an on-premises file server named Server1 that runs Windows Server 2016.

You have an Azure subscription that contains an Azure file share.

You deploy an Azure File Sync Storage Sync Service, and you create a sync group.

You need to synchronize files from Server1 to Azure.

Which three 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.



QUESTION 56

You have an Azure virtual network named VNet1 that contains a subnet named Subnet1.

Subnet1 contains three Azure virtual machines. Each virtual machine has a public IP address.

The virtual machines host several applications that are accessible over port 443 to user on the Internet.

Your on-premises network has a site-to-site VPN connection to VNet1.

You discover that the virtual machines can be accessed by using the Remote Desktop Protocol (RDP) from the Internet and from the on-premises network.

You need to prevent RDP access to the virtual machines from the Internet, unless the RDP connection is established from the on-premises network. The solution must ensure that all the applications can still be accesses by the Internet users.

What should you do?

- A. Modify the address space of the local network gateway.
- B. Remove the public IP addresses from the virtual machines.
- C. Modify the address space of Subnet1.
- D. Create a deny rule in a network security group (NSG) that is linked to Subnet1.

Correct Answer: D **Explanation**:

You can filter network traffic to and from Azure resources in an Azure virtual network with a network security group. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources.

You can use a site-to-site VPN to connect your on-premises network to an Azure virtual network. Users on your on-premises network connect by using the RDP or SSH protocol over the site-to-site VPN connection. You don't have to allow direct RDP or SSH access over the internet. And this can be achieved by configuring a deny rule in a network security group (NSG) that is linked to Subnet1 for RDP / SSH protocol coming from internet.

Modify the address space of Subnet1: Incorrect choice

Modifying the address space of Subnet1 will have no impact on RDP traffic flow to the virtual network.

Modify the address space of the local network gateway: Incorrect choice

Modifying the address space of the local network gateway will have no impact on RDP traffic flow to the virtual network.

Remove the public IP addresses from the virtual machines: Incorrect choice

If you remove the public IP addresses from the virtual machines, none of the applications be accessible publicly by the Internet users.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-network/security-overview https://docs.microsoft.com/en-us/azure/security/fundamentals/network-best-practices

QUESTION 57

Your on-premises network contains an SMB share named Share1.

You have an Azure subscription that contains the following resources:

- A web app named webapp1
- A virtual network named VNET1

You need to ensure that webapp1 can connect to Share1.

What should you deploy?

- A. an Azure Application Gateway
- B. an Azure Active Directory (Azure AD) Application Proxy
- C. an Azure Virtual Network Gateway
- D. none of the above

Correct Answer: C Explanation:

A Site-to-Site VPN gateway connection can be used to connect your on-premises network to an Azure virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel.

This type of connection requires a VPN device, a VPN gateway, located on-premises that has an externally facing public IP address assigned to it.

Reference:

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal

QUESTION 58

You have an Azure Storage account named storage1.

You plan to use AzCopy to copy data to storage1.

You need to identify the storage services in storage1 to which you can copy the data.

What should you identify?

- A. blob, file, table, and queue
- B. blob and file only
- C. file and table only
- D. file only
- E. blob, table, and queue only

Correct Answer: B Explanation:

AzCopy is a command-line utility that you can use to copy blobs or files to or from a storage account.

Reference:

https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10

QUESTION 59

You have a virtual network named VNet1 as shown in the exhibit. (Click the Exhibit tab.)

Refresh	Move	Delete	
Resource group (change) Production		Address space 10.2.0.0/16	
Location West US		DNS servers Azure provided DNS service	
Subscription (cl Production subs	J .		
Subscription ID 14d26092-8e42		lcef70fb1ea	
Tags (change) Click here to add	d tags		
Connected de	evices		
Search con	nected devices		
DEVICE	TYPE	IP ADDRESS SUBNET	
No results.			

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?

- A. Configure a service endpoint on VNet2.
- B. Modify the address space of VNet1.
- C. Add a gateway subnet to VNet1.
- D. Create a subnet on VNet1 and VNet2.

Correct Answer: B 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.

References:

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering#requirements-and-constraints

QUESTION 60

You have an Azure web app named webapp1.