Dashboard My Courses Hands-on Labs Sandbox Support

Home / Dashboard / My Courses / Microsoft Azure Exam AZ-104 Certification / Implement and manage virtual networking / **Report**

Level: Advanced

Microsoft Azure Exam AZ-104 Certification

Back to the **Course**

Implement and manage virtual networking - **Practice Mode**

Completed on Sat, 04 Oct 2025

1st
Attempt

8/13
Marks Obtained

61.54%
Your Score

FAIL
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	Implement and manage virtual networking	13	8	5	0	0
Total	All Domains	13	8	5	0	0

Review the Answers

Filter By

Question 1

Incorrect

Domain: Implement and manage virtual networking

You have an Azure subscription that contains a storage account named TestStorage1 and the following virtual machines:

VirtualMachine1 has a public IP address of 13.68.158.24 and is connected to VirtualNetwork1/Subnet1

VirtualMachine2 has a public IP address of 52.255.145.76 and is connected to VirtualNetwork1/Subnet1

VirtualMachine3 has a public IP address of 13.68.158.50 and is connected to VirtualNetwork1/Subnet2

The subnets have the following service endpoints:

Subnet1 has a Microsoft.Storage service endpoint

Subnet2 does not have any service endpoint

TestStorage1 has a firewall configured to allow access from the 13.68.158.0/24 IP address range only. You need to identify which virtual machines can access TestStorage1. What should you identify?

○ A. VirtualMachine1 only wrong

B. VirtualMachine3 only

C. VirtualMachine1 and VirtualMachine2 only

D. VirtualMachine1 and VirtualMachine3 only right

Explanation:

Correct Answer: D

Option D is CORRECT because VirtualMachine1 meets both the criteria; first, it has a public IP address within the allowed range (13.68.158.0/24) of the firewall and second, it is connected to a subnet (Subnet1) with a Microsoft.Storage service endpoint, allowing it to access TestStorage1. Also, VirtualMachine3 has a public IP address within the allowed range (13.68.158.0/24) of the firewall, although it is not connected to a subnet with Microsoft.Storage service endpoint, TestStorage1 would still allow access from the specified IP address range, enabling VirtualMachine3 to access TestStorage1 directly.

Option A is INCORRECT because although VirtualMachine1 satisfies both the conditions to access TestStorage1, it is not the only virtual machine to access the storage account. VirtualMachine3 can also access TestStorage1.

Option B is INCORRECT because although VirtualMachine3 satisfies the condition of the IP address within the allowed range of the firewall to access TestStorage1, it is not the only virtual machine to access the storage account. VirtualMachine1 can also access TestStorage1.

Option C is INCORRECT because VirtualMachine2 cannot access TestStorage1. Although it is connected to a subnet with a Microsoft.Storage service endpoint, it has a public IP address outside the allowed range (52.255.145.76) of the firewall. Thus, in this case, the firewall would restrict access to TestStorage1 for VirtualMachine2.

Reference:

https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal#grant-access-from-a-virtual-network

https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal#grant-access-from-an-internet-ip-range

Ask our Experts

Did you like this **Question?** 👍 👎

Question 2

Correct

Domain: Implement and manage virtual networking

View Case Study

You need to suggest a solution to ensure that the storage account (TestStorage) can only be accessed from VNet2 and VNet3. The solution must meet the technical requirements. Which service should you configure?

A. Private Link

B. Azure Firewall

○ C. Service Endpoints right

D. Network Security Groups

Explanation:

Correct Answer: C

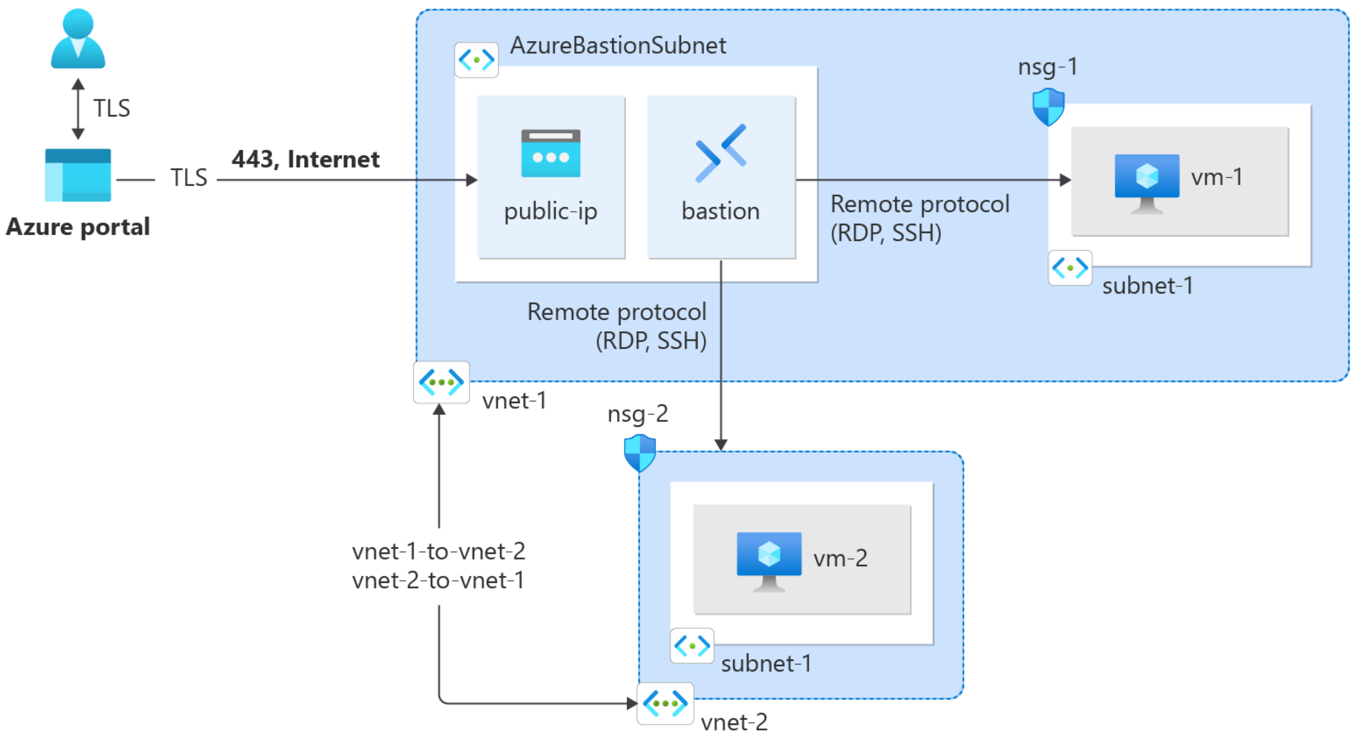
Option C is CORRECT because this solution allows you to restrict access to the Azure Storage account to specific VNets (VNet2 and VNet3), meeting the technical requirements effectively and efficiently. Service Endpoints use the Azure backbone network to optimize a direct and secure connection to Azure services. By configuring Service Endpoints, you can ensure that the Azure Storage Account (TestStorage) is only accessible from specified VNets.

Option A is INCORRECT because, although it provides a similar level of security, it is not the simplest solution for the scenario described. While Private Link could be used to restrict access to the storage account to specific VNets, it is generally more complex to set up and manage compared to Service Endpoints. Additionally, Private Link is designed for scenarios where you need to secure access from a specific set of private IP addresses, not necessarily from multiple VNets without significant configuration.

Option B is INCORRECT because Azure Firewall is primarily used for network security and traffic control rather than restricting access to Azure services from specific VNets. While it can help restrict access based on network rules, it is not specifically designed to control access to Azure PaaS services from VNets in the same way Service Endpoints are.

Option D is INCORRECT because NSGs are used for traffic filtering at the network level but do not directly control access to Azure PaaS services. NSGs can control traffic to and from VM subnets and network interfaces but do not provide the capability to secure Azure PaaS services like Azure Storage in the same manner as Service Endpoints.

Architectural Diagram/Screenshots:



[Source: Microsoft Documentation]

Reference:

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

Ask our Experts

Did you like this **Question?**

Question 3 Correct

Domain: Implement and manage virtual networking

View Case Study

You want to configure a private endpoint for the SQLDB resource in VNet1.

What is the first recommended step you need to follow?

A. Create a new virtual network for the private endpoint

B. Configure DNS settings for the SQLDB

C. Modify the network security group (NSG) settings for VNet1

○ D. Create a private endpoint resource in the Azure portal right

Explanation:

Correct Answer: D

Option D is CORRECT because the initial step in setting up a private endpoint is to create the private endpoint resource itself. This involves specifying the target resource (SQLDB in this case), the virtual network (VNet1), and the subnet where the private endpoint will be placed. This step is fundamental because it establishes the private link to the SQLDB, making it accessible via a private IP within VNet1.

Steps to Create a Private Endpoint:

Navigate to the Azure portal and select "Private endpoints."

Select "+ Create" to start the creation process.

In the Basics tab, fill in the necessary details:

Resource Group

Name of the private endpoint

Region

Select the target resource (SQLDB in VNet1) and the specific sub-resource (e.g., SQL server).

Choose the virtual network (VNet1) and subnet where the private endpoint will be deployed.

Configure DNS integration settings if required.

Review and create the private endpoint.

Option A is INCORRECT because creating a new virtual network is not required unless there are specific isolation or organizational requirements. In this scenario, the private endpoint is intended for VNet1, so a new virtual network is unnecessary.

Option B is INCORRECT because configuring DNS settings is necessary to ensure proper name resolution of the private endpoint. However, this step comes after the creation of the private endpoint. Once the private endpoint is created, the appropriate DNS configurations can be applied to resolve the SQLDB's private endpoint correctly within the virtual network.

Option C is INCORRECT because this is a subsequent step after the private endpoint is created. NSG settings might need to be adjusted to ensure that traffic to the private endpoint is allowed. This involves configuring rules to permit traffic to and from the private IP address assigned to the private endpoint.

Reference:

https://learn.microsoft.com/en-us/azure/private-link/create-private-endpoint-portal?tabs=dynamic-ip#create-a-private-endpoint

Ask our Experts

Did you like this **Question?** 👍 👎

Question 4

Incorrect

Domain: Implement and manage virtual networking

View Case Study

The IT department assigns WebAppTest with a custom user-defined domain, “www.fabriakamwebapp.net” to ensure ease of accessibility for non-tech users in the department.

You need to ensure that WebAppTest can access the SQLDB over the private endpoint.

The solution must meet the technical requirements.

What DNS configuration is required to achieve the goal?

A. Create an Azure DNS private zone and link it to VNet1 and VNet3 right

○ B. Update the SQLDB’s DNS to point to the private IP address wrong

C. Configure a public DNS zone and link it to both virtual networks

D. Enable public DNS resolution in VNet3

Explanation:

Correct Answer: A

Option A is CORRECT because Azure Private DNS provides DNS resolution for private endpoints within a virtual network, ensuring that DNS queries are resolved to private IP addresses rather than public ones. By linking the DNS private zone to both VNet1 (where the SQLDB is located) and VNet3 (where the WebAppTest is located), both VNets can resolve the DNS name of the SQLDB to its private IP address. This setup meets the security requirement of keeping the SQLDB accessible only within the virtual networks, and it allows WebAppTest to access SQLDB over the private endpoint securely.

Option B is INCORRECT because Manually updating DNS entries for SQLDB is not a standard approach and can lead to maintenance and management issues. DNS records should be managed within a DNS zone, not by directly updating the service DNS settings to a private IP. This approach does not leverage Azure's DNS capabilities and fails to provide the necessary scalability and manageability for DNS resolution within Azure VNets.

Option C is INCORRECT because linking a public DNS zone to the VNets would expose internal resources, potentially making them accessible from the public internet, which violates the security requirements. This approach does not meet the need for private, secure access to SQLDB from WebAppTest in VNet3. Private endpoints require private DNS zones for proper resolution within Azure VNets.

Option D is INCORRECT because public DNS resolution would expose SQLDB to the public internet, which contradicts the security requirements of keeping SQLDB accessible only within VNet1. Enabling public DNS resolution does not provide a secure method for WebAppTest to resolve SQLDB’s private endpoint. It fails to ensure that only internal resources can access SQLDB. The requirement is for private, internal DNS resolution, not public DNS.

Reference:

https://learn.microsoft.com/en-us/azure/private-link/private-endpoint-dns

https://learn.microsoft.com/en-us/azure/dns/private-dns-overview

Ask our Experts

Did you like this **Question?** 👍 👎

Question 5 Correct

Domain: Implement and manage virtual networking

View Case Study

You need to ensure that the traffic between VNet1 and VNet2 flows through the Network Virtual Appliance (NVA) in VNet3. How can you achieve this?

A. Create a VPN gateway in each VNet

B. Configure a peering connection between VNet1 and VNet2

○ C. Set up user-defined routes in each VNet with the NVA as the next hop right

D. Enable service endpoints for all VNets

Explanation:

Correct Answer: C

Option C is CORRECT because it effectively addresses the requirement by explicitly defining routing rules that direct traffic through the NVA in VNet3, ensuring inspection and control of inter-VNet traffic. User-defined routes allow customizing the routing behavior within Azure virtual networks. By defining routes with the NVA's private IP address as the next hop, you specify that traffic destined for other VNets should first pass through the NVA for inspection and routing. This option aligns with the requirement of ensuring traffic between VNet1 and VNet2 flows through the NVA in VNet3.

Option A is INCORRECT because while VPN gateways are useful for establishing secure connections, they do not directly address the requirement of routing traffic through the NVA in VNet3. VPN gateways are used to establish secure connections between Azure virtual networks and on-premises networks or other Azure virtual networks. However, deploying VPN gateways in each VNet does not inherently route traffic between VNet1 and VNet2 through the NVA in VNet3. It establishes secure connections but doesn't enforce traffic routing through a specific path.

Option B is INCORRECT because while peering connections facilitate direct communication between VNets, they do not ensure traffic routing through a specific network appliance like the NVA in VNet3.

Option D is INCORRECT because enabling service endpoints does not address the requirement of routing traffic through the NVA in VNet3. It focuses on providing secure access to Azure services within VNets but does not enforce specific traffic routing paths.

Reference:

https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview#user-defined

https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-create-route-table-portal

Ask our Experts

Did you like this **Question?**

Question 6

Correct

Domain: Implement and manage virtual networking

View Case Study

Which route configuration is necessary to ensure that the traffic between VNet1, VNet2, and VNet3 is inspected by the NVA in VNet3?

A. Route tables with a next-hop type of Internet

B. Route tables with a next-hop type of Virtual Network

○ C. Route tables with a next-hop type of Virtual Appliance right

D. Route tables with a next-hop type of None

Explanation:

Correct Answer: C

Option C is CORRECT because this option allows you to specify a virtual appliance, such as the Network Virtual Appliance (NVA) located in VNet3, as the next hop for the traffic between VNets. By configuring the route tables with the NVA as the next hop, you ensure that traffic between VNets is directed to the NVA for inspection and potential routing based on network policies. The NVA serves as a central point for inspecting traffic between VNets, allowing you to enforce network security policies, perform network address translation (NAT), and route traffic based on defined rules. This option aligns perfectly with the requirement to ensure that traffic between VNet1, VNet2, and VNet3 flows through the NVA in VNet3 for inspection. It enables you to optimize network security and performance by centrally managing and controlling inter-VNet traffic.

Option A is INCORRECT because this option would direct traffic to the Internet, not through the NVA in VNet3. It doesn't align with the requirement to route traffic between VNets through the NVA.

Option B is INCORRECT because this option would route traffic within the same virtual network, not between different VNets. It doesn't address the requirement to route traffic between VNets through the NVA.

Option D is INCORRECT because this option would effectively drop the traffic instead of routing it through the NVA. It doesn't fulfill the requirement to route traffic between VNets through the NVA.

Reference:

https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview#user-defined

https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-create-route-table-portal

Ask our Experts

Did you like this **Question?**

Question 7

Incorrect

Domain: Implement and manage virtual networking

Your Azure subscription includes the following virtual networks:

Name	Location	No. of VMs connected
VNET1	WestUS	5
VNET2	WestUS	7
VNET3	EastUS	10
VNET4	EastUS	4

All the virtual networks are fully peered using global virtual network peering.

You want to set up Azure Bastion for all the virtual machines connected to these networks.

What is the minimum number of Azure Bastion host(s) you need to deploy?

A. 1

B. 2 right

C. 3

○ D. 4 wrong

Explanation:

Correct Answer: B

Option A is INCORRECT, While global virtual network peering allows for connectivity across regions, Azure Bastion must be deployed in each region where you want to provide secure and seamless RDP/SSH access to your VMs. Since you have virtual networks in two different regions (West US and East US), one Azure Bastion host is not sufficient.

Option B is CORRECT, Since all the virtual networks are fully peered using global virtual network peering, you only need to deploy one Azure Bastion host per region. In this case, you have virtual networks in two regions: West US and East US. Therefore, you need a minimum of two Azure Bastion hosts, one in each region.

Option C is INCORRECT because there is no need for three Azure Bastion hosts in this scenario. Global virtual network peering allows for seamless communication between virtual networks across regions, so only one Azure Bastion host is needed to provide remote access to all the virtual machines.

Option D is INCORRECT because deploying four Azure Bastion hosts would be excessive and unnecessary in this scenario. Global virtual network peering ensures connectivity between all the virtual networks across regions, so only one Azure Bastion host is required to cover all the virtual machines.

Reference:

https://learn.microsoft.com/en-us/azure/bastion/vnet-peering

Tutorial: Deploy Azure Bastion using specified settings: Azure portal | Microsoft Learn

Ask our Experts

Did you like this **Question?** 👍 👎

Question 8

Correct

Domain: Implement and manage virtual networking

You are configuring Azure Bastion to provide secure RDP access to virtual machines in Azure. Which of the following IP address allocations is required for the public IP address associated with Azure Bastion?

A. Dynamic

○ B. Static right

C. Reserved

D. Floating

Explanation:

Correct Answer: B

Option B is CORRECT because when configuring Azure Bastion to provide secure RDP access to virtual machines in Azure, the public IP address associated with Azure Bastion must be allocated statically. This ensures that the public IP address remains constant and does not change over time, providing a reliable endpoint for securely accessing virtual machines. Using a static public IP address is essential for maintaining consistent connectivity to Azure Bastion, especially in scenarios where dynamic IP addresses might change, causing disruptions in connectivity. Therefore, a static allocation is required to ensure uninterrupted access to Azure Bastion and the virtual machines it protects.

Option A is INCORRECT because dynamic IP addresses can change over time, leading to connectivity issues and interruptions when accessing virtual machines via Azure Bastion. Therefore, more than a dynamic allocation is needed to ensure consistent and reliable access to Azure Bastion.

Option C is INCORRECT because Azure Bastion requires a static allocation for its public IP address to ensure consistent and reliable connectivity. However, reserved is not a valid allocation type for Azure public IP addresses.

Option D is INCORRECT because floating is not a standard IP address allocation type in the context of Azure public IP addresses.

Reference:

https://learn.microsoft.com/en-us/azure/bastion/configuration-settings#public-ip

Ask our Experts

Did you like this **Question?** 👍 👎

Question 9 Correct

Domain: Implement and manage virtual networking

You've deployed Azure virtual machines across the three Azure regions, each with its virtual network. These networks feature multiple subnets interconnected in a full mesh topology, with each subnet equipped with a network security group (NSG) defining specific rules.

A user encounters connectivity issues, particularly with port 33000, when attempting to connect from a virtual machine in one region to another in a different region. Which of the following approaches can you employ to diagnose the problem? (Select Two)

□ A. IP flow verify right

B. Azure Virtual Network Manager

□ C. Connection troubleshoot right

D. Azure Monitor Network Insights

Explanation:

Correct Answers: A and C

Option A is CORRECT because IP flow verify is a feature within Azure Network Watcher designed to assist in diagnosing connectivity issues by assessing if a packet adheres to the configured security and administrative rules. It scrutinizes the rules of all network security groups (NSGs) assigned to a virtual machine's network interface, encompassing those linked with subnets or network interfaces. This evaluation extends to rules governing traffic on specified ports, such as port 33000 in this scenario. Through IP flow verify, one can ascertain whether traffic destined for port 33000 is permitted or denied by the NSG rules, thereby offering insights into potential connectivity problems. IP flow verify assesses various parameters, including traffic direction, protocol, local and remote IPs, as well as local and remote ports, to validate security and administrative rules. It provides feedback on whether access is granted or denied, alongside the identification of the security rule and its associated NSG, facilitating pinpointing and potential adjustment of any rules obstructing the traffic.

Option C is CORRECT because connection troubleshoot is another feature of Azure Network Watcher specifically designed to diagnose and troubleshoot network connectivity issues. It performs comprehensive checks to detect issues related to network security groups, user-defined routes, and blocked ports, which are all relevant to diagnosing connectivity problems between virtual machines in different regions. Connection troubleshoot can detect issues such as misconfigured or missing routes, network security group (NSG) rules blocking traffic (including traffic on port 33000), and other factors that may be causing connectivity problems. It provides detailed results, including insights into the root cause of the connectivity problem and actionable steps for resolution, which can help in identifying and addressing any issues preventing communication between virtual machines in different regions.

Option B is INCORRECT because while Azure Virtual Network Manager is useful for managing and configuring virtual networks, it does not provide direct diagnostic capabilities for troubleshooting connectivity issues between virtual machines in different regions, such as those related to port 33000. Azure Virtual Network Manager does not offer specific tools or features for diagnosing connectivity issues or troubleshooting network problems like IP flow verify or Connection troubleshoot.

Option D is INCORRECT because while Azure Monitor Network Insights offers valuable insights into network performance and health, it is primarily focused on monitoring and analyzing network data rather than diagnosing specific connectivity issues between virtual machines in different regions. Azure Monitor Network Insights may not provide the detailed information needed to identify and troubleshoot issues related to port 33000 connectivity between virtual machines in different regions, which require more specific diagnostic tools like IP flow verify and Connection troubleshoot.

References:

https://learn.microsoft.com/en-us/azure/network-watcher/ip-flow-verify-overview

https://learn.microsoft.com/en-us/azure/network-watcher/connection-troubleshoot-overview#issues-detected-by-connection-troubleshoot

Ask our Experts

Did you like this **Question?** 👍 👎

Question 10 Incorrect

Domain: Implement and manage virtual networking

You are working as an Azure Administrator for Contoso where your job role is to maintain and supervise all Azure resources deployed on Contoso's infrastructure.

During a routine monitoring session, while troubleshooting an inbound connectivity issue with a standard external load balancer (ELB) on Azure, you identify that external clients are unable to establish a connection to the backend virtual machines. You need to investigate further to resolve the issue.

What recommended action should you take to address this issue?

A. Adjust the backend port configuration for the existing load balancer rule

○ B. Verify the provisioning state of the load balancer in Azure Resource Explorer to ensure it is operational wrong

C. Update the Virtual Machine Scale Set by removing the health probe and reconfiguring it to allow inbound traffic to the backend VMs

D. Implement network security group (NSG) rules to permit inbound traffic on the appropriate ports for the backend VMs right

Explanation:

Correct Answer: D

Option D is CORRECT because network security groups control traffic flow to and from network interfaces, including those associated with VMs. By configuring NSG rules to permit inbound traffic on the appropriate ports, external clients should be able to establish connections to the backend VMs through the load balancer. This action directly addresses the issue of inbound connectivity by ensuring that the necessary ports are open for external traffic to reach the backend VMs.

Option A is INCORRECT because while this might be necessary in some cases, such as if the backend VMs are listening on a different port, it's unlikely to resolve an inbound connectivity issue. Backend port configuration typically affects how traffic is routed to the VMs, not whether external clients can connect to them.

Option B is INCORRECT because while it's always good practice to verify the status of resources, including load balancers, it doesn't directly address the issue of inbound connectivity. Even if the load balancer is provisioned and operational, there could still be configuration issues preventing external clients from connecting to the backend VMs.

Option C is INCORRECT because while health probes play a role in load balancing and ensuring the availability of backend VMs, removing the health probe altogether is not recommended. Additionally, reconfiguring the health probe may not directly address the issue of inbound connectivity.
Reference:

https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-troubleshoot#problem-no-inbound-connectivity-to-standard-external-load-balancers-elb

Ask our Experts

Did you like this **Question?** 👍 👎

Question 11

Incorrect

Domain: Implement and manage virtual networking

You have two virtual machines, ***VM1*** and ***VM2,*** running in the same resource group ***vmRG*** and on the same virtual network ***VNetVM*** in different subnets: ***vm1subnet*** and ***vm2subnet***. You add two NSG outbound rules. The first rule allows access to Azure Storage from both virtual machines. The second rule — denies internet access. You provision a new storage account ***vmstracc28*** in the ***vmRG*** and add a file share ***vmfiles*** to the account.

What steps should you take to give access to ***vmfiles*** only from ***VM2***?

□ A. Add a service endpoint for Microsoft.Storage in vm2subnet right

□ B. Create an NSG rule to access the storage account only from VM2 wrong

C. Enable access to the storage account only from vm1subnet

D. Deny all traffic to the storage account right

E. Add a service endpoint for Microsoft.Storage in vm1subnet

F. Enable all traffic to the storage account

□ G. Enable access to the storage account only from vm2subnet right

H. Create an NSG rule to deny the storage account access from VM1

Explanation:

Correct Answers: A, D and G

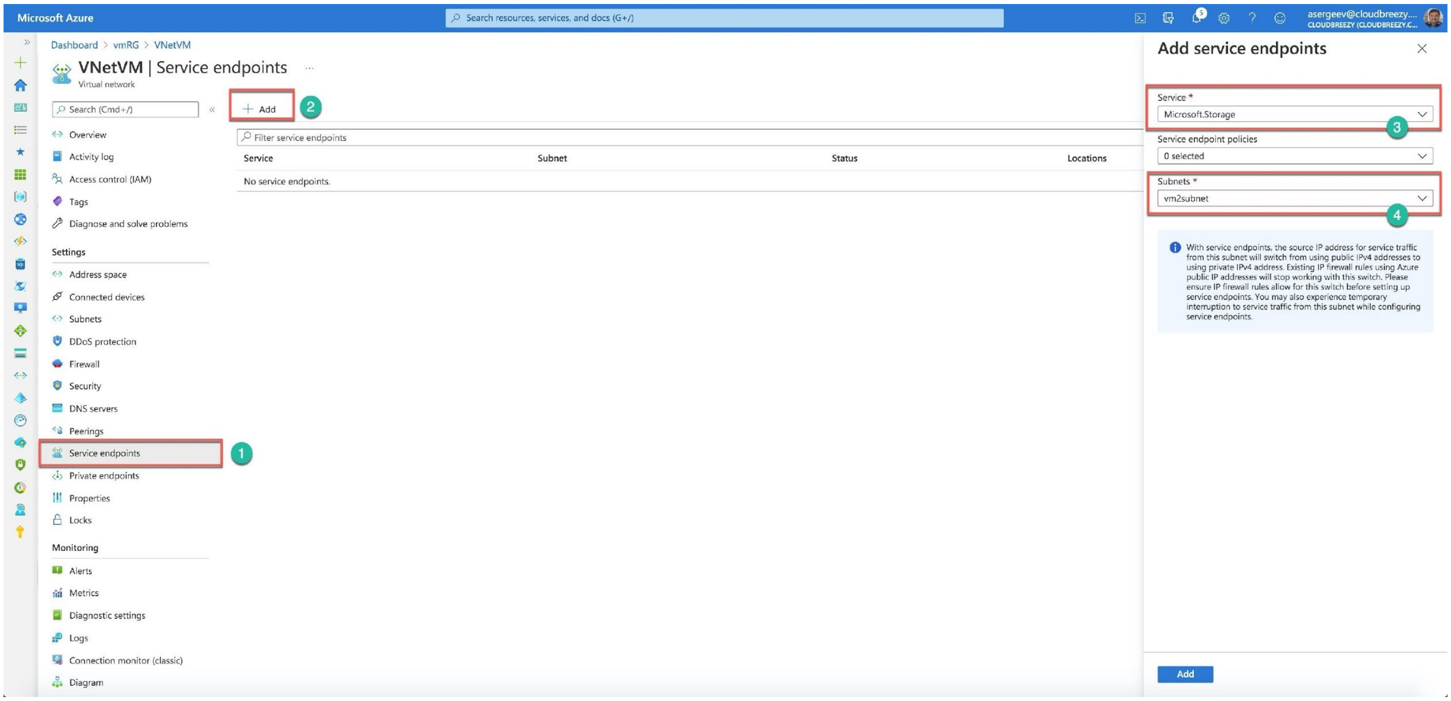
For secure and direct connection to the Azure services, you need to use virtual network endpoints. The endpoints allow you to connect Azure resources without using a public IP address on your VNet. You can access all major Azure services using the service endpoints.

To connect securely and selectively VM2 to the storage account, you need to create a service endpoint, deny all access to the storage account, and enable access only to the subnet where VM2 is running.

First, create a service endpoint for the Microsoft Storage service in your vm2subnet subnet. Here is the Azure CLI command:

```
az network vnet subnet update --vnet-name VNetVM --resource-group vmRG \
            --name vm2subnet --service-endpoints Microsoft.Storage
```

Or you can use the Azure portal. One the Virtual Network blade, select the Service endpoints (Number 1) and then the Add button (Number 2). On the new panel to the right, select Services (Number 3) and your subnet (Number 4).



Service	Subnet	Status	Locations
No service endpoints.			

Service *
Microsoft.Storage

Service endpoint policies
0 selected

Subnets *
vm2subnet

With service endpoints, the source IP address for service traffic from this subnet will switch from using public IPv4 addresses to using private IPv4 address. Existing IP firewall rules using Azure public IP addresses will stop working with this switch. Please ensure IP firewall rules allow for this switch before setting up service endpoints. You may also experience temporary interruption to service traffic from this subnet while configuring service endpoints.

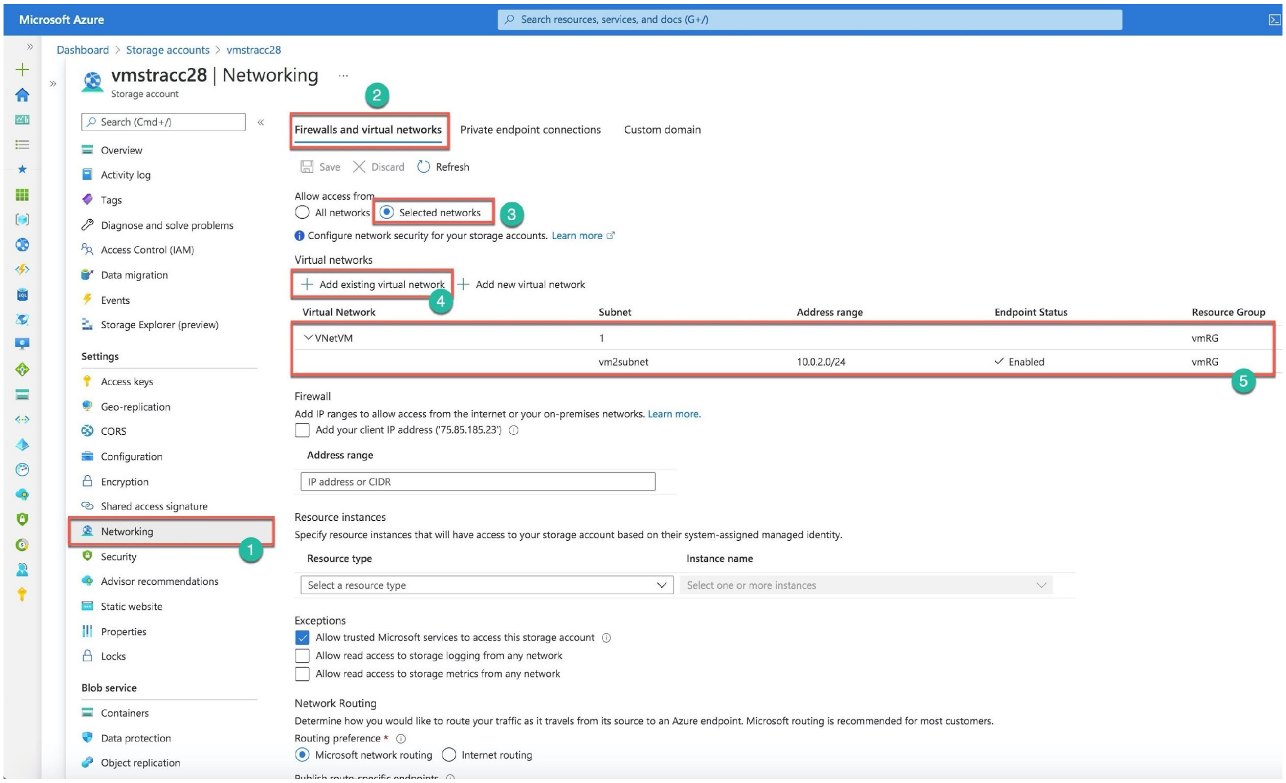
Then, you need to deny all network access to the storage account. Here is the Azure CLI command:

```
az storage account update --resource-group vmRG --name vmstracc28 --default-action Deny
```

And finally, you need to enable access to a storage account from the subnet that has a service endpoint:

```
    az storage account network-rule add --resource-group vmRG \
    --account-name vmstracc28 --vnet VNetVM --subnet vm2subnet
```

You can execute the last two steps in the portal by limiting access to storage account only to VNetVM virtual network and vm2subnet subnet and denying any other access. Select the Networking (Number 1) on the Storage account blade. Under the "Firewalls and virtual networks" tab (Number 2), select the "Selected networks" option (Number 3). Then, you can add an existing virtual network (Number 4). On the new panel, you select the network and a subnet. After you confirm your selection, the portal creates the rule for a storage account access (Number 5) with the Endpoint status "Enabled."



Allow access from

○ All networks ● Selected networks

Configure network security for your storage accounts. Learn more

Virtual networks

+ Add existing virtual network + Add new virtual network

Virtual Network	Subnet	Address range	Endpoint Status	Resource Group
VNetVM	1			vmRG
	vm2subnet	10.0.2.0/24	✓ Enabled	vmRG

Firewall

Add IP ranges to allow access from the internet or your on-premises networks. Learn more.

□ Add your client IP address ('75.85.185.23')

Address range

IP address or CIDR

Resource instances

Specify resource instances that will have access to your storage account based on their system-assigned managed identity.

Resource type	Instance name
Select a resource type	Select one or more instances

Exceptions

☑ Allow trusted Microsoft services to access this storage account

□ Allow read access to storage logging from any network

□ Allow read access to storage metrics from any network

Network Routing

Determine how you would like to route your traffic as it travels from its source to an Azure endpoint. Microsoft routing is recommended for most customers.

Routing preference *

● Microsoft network routing ○ Internet routing

Publish route-specific endpoints

All other options are incorrect.

For more information about virtual network service endpoints, please visit the below URLs:

https://docs.microsoft.com/en-us/learn/modules/secure-and-isolate-with-nsg-and-service-endpoints/4-vnet-service-endpoints

https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal

https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal#grant-access-from-a-virtual-network

https://docs.microsoft.com/en-us/learn/modules/secure-and-isolate-with-nsg-and-service-endpoints/5-exercise-vnet-service-endpoints

Ask our Experts

Did you like this **Question?** 👍 👎

Question 12 Correct

Domain: Implement and manage virtual networking

Microsoft Azure provides a number of solutions for load balancing and secure network connections in the cloud. Below are some of the networking solutions and their definitions, matching the correct solution with their definition.

Your Answers

Load balancer

Load-balance internet and private network traffic with high performance and low latency

Network Security Groups

Filter network traffic to and from Azure resources in an Azure virtual network

Application Security Groups

Network security as a natural extension of an application's structure

Azure Application Gateway

Application-level routing and load balancing services that let you build a scalable and highly available web front end in Azure

Correct Answers

Load balancer

Load-balance internet and private network traffic with high performance and low latency

Network Security Groups

Filter network traffic to and from Azure resources in an Azure virtual network

Application Security Groups

Network security as a natural extension of an application's structure

Azure Application Gateway

Application-level routing and load balancing services that let you build a scalable and highly available web front end in Azure

Explanation:

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

1. Load balancer	**D. Load-balance internet and private network traffic with high performance and low latency**

2. Network Security Groups	A. Filter network traffic to and from Azure resources in an Azure virtual network
3. Application Security Groups	B. Network security as a natural extension of an application's structure
4. Azure Application Gateway	C. Application-level routing and load balancing services that let you build a scalable and highly available web front end in Azure

Load balancer: Load-balance internet and private network traffic with high performance and low latency. Instantly add scale to your applications and enable high availability. Load Balancer works across virtual machines, virtual machine scale sets, and IP addresses.

Network Security Groups: You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network. 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. For each rule, you can specify source and destination, port, and protocol.

Application Security Groups: Application security groups enable you to configure network security as a natural extension of an application's structure, allowing you to group virtual machines and define network security policies based on those groups. You can reuse your security policy at scale without manual maintenance of explicit IP addresses. The platform handles the complexity of explicit IP addresses and multiple rule sets, allowing you to focus on your business logic.

Azure Application Gateway: Azure Application Gateway gives you application-level routing and load balancing services that let you build a scalable and highly-available web front end in Azure. You control the size of the gateway and scale your deployment based on your needs.

References:

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

https://azure.microsoft.com/en-us/services/load-balancer/

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

https://docs.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works

Ask our Experts

Did you like this **Question?** 👍 👎

Question 13 Correct

Domain: Implement and manage virtual networking

A small corporation has 50 VMs (Virtual Machines) on-premises and 20 VMs in Azure. On-premises is connected to Azure using site to site connectivity. 5 Azure VMs are having network connectivity issues. Which of the following solutions would you utilize to examine the connectivity issues?

A. Microsoft Management Agent

B. Dependency Agent

○ C. Azure Network Watcher right

D. Azure Log Analytics

Explanation:

Correct Answer: C

Azure Network Watcher provides tools to monitor, diagnose, view metrics, and enable or disable logs for resources in an Azure virtual network. Network Watcher is designed to monitor and repair the network health of IaaS (Infrastructure-as-a-Service) products which includes Virtual Machines, Virtual Networks, Application Gateways, Load balancers, etc.

Option A is incorrect because the Microsoft Monitoring Agent is a service used to watch and report on application and system health on a Windows computer.

Option B is incorrect because the Dependency Agent discovers data about processes running on the VM and external process dependencies.

Option C is correct because Network Watcher provides the ability to diagnose the most common VPN Gateway and Connections issues.

Option D is incorrect because Log Analytics is a tool in the Azure portal to edit and run log queries from data collected by Azure Monitor logs and interactively analyze their results.

Reference:

https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview

Ask our Experts

Did you like this **Question?**

Finish Review

Hands-on Labs Sandbox Subscription For Business Library

Categories

- Cloud Computing Certifications
- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud
- DevOps
- Cyber Security
- Microsoft Power Platform
- Microsoft 365 Certifications
- Java Certifications

Popular Courses

- AWS Certified Solutions Architect Associate
- AWS Certified Cloud Practitioner
- Microsoft Azure Exam AZ-204 Certification
- Microsoft Azure Exam AZ-900 Certification
- Google Cloud Certified Associate Cloud Engineer
- Microsoft Power Platform Fundamentals (PL-900)
- HashiCorp Certified Terraform Associate Certific…
- Snowflake SnowPro Core Certification
- Docker Certified Associate

Company

- About Us
- Blog
- Reviews
- Careers
- Team Account

Legal

- Privacy Policy
- Terms of Use
- EULA
- Refund Policy
- Programs Guarantee

Support

- Contact Us
- FAQs

Need help? Please ☎ or ☎ +91 6364678444

Download on the App Store

GET IT ON Google Play