

AZ-700 Designing and Implementing Microsoft Azure Networking Solutions

店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

Your company has a single on-premises datacenter in Washington DC. The East US Azure region has a peering location in Washington DC. The company only has Azure resources in the East US region. You need to implement ExpressRoute to support up to 1 Gbps. You must use only ExpressRoute Unlimited data plans. The solution must minimize costs.

Which type of ExpressRoute circuits should you create?

- A. ExpressRoute Local
- B. ExpressRoute Direct
- C. ExpressRoute Premium
- D. ExpressRoute Standard

Correct Answer: A

Reference:

<https://azure.microsoft.com/en-us/pricing/details/expressroute/>

Community vote distribution

A (90%)

10%

 **jasonsmithss** Highly Voted 2 months, 1 week ago
itexamslab.com

Answer is correct.
upvoted 59 times

 **Tightbot** Highly Voted 1 year, 1 month ago

Selected Answer: A


Expressroute Local supports this particular networking scenario for two reasons. 1) The Washington DC peering location has East US as its Local Azure region. So, you don't need access to all the Geopolitical locations in order to connect the on-prem DC to Azure. Which means you won't necessarily need Expressroute standard. 2) ExpressRoute Local is a more economical solution compared to the standard.

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-faqs#what-are-the-benefits-of-expressroute-local>
<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-locations-providers#global-commercial-azure>
upvoted 22 times


 **HoangNam2711** Most Recent 1 week, 2 days ago


Selected Answer: A


A is correct because Washing is in EastUS geopolitical
upvoted 1 times


 **Jonny_sin** 1 month, 2 weeks ago
itexamstest.com

Correct Answer
upvoted 13 times

 **_Cris** 4 months, 1 week ago
appears on exam, 19 Sept 2023
upvoted 2 times

 **Verytutos** 4 months, 2 weeks ago
Appeared on Exam 05 Sep 2023
upvoted 2 times

 **SLGUY** 5 months ago
Appeared on Exam 26 Aug 2023
upvoted 1 times

 **ESAJRR** 10 months, 1 week ago
Selected Answer: A
Correct.
upvoted 1 times

 **saurabhjsshukla** 10 months, 1 week ago

Circuit bandwidth Local Standard Premium Inbound Outbound
1 Gbps \$1,200 \$5,700 \$6,450 Unlimited Unlimited

So Answer is Expressroute Local (Option A)
upvoted 1 times

  **dani999** 1 year ago

Selected Answer: A

-Local

(if available) provides free egress data transfer and gives you access to only 1-2 Azure regions in the same metro as your circuit.

-Standard

gives you access to all Azure regions in the same geopolitical region as your circuit.

-Premium provides support for more than 4K routes, ability to connect to more than 10 virtual networks, and global connectivity. Premium also gives you access to your services deployed worldwide.

upvoted 1 times

  **TJ001** 1 year ago

will go with A - one region and unlimited data is fulfilled. It is a classic use case for local SKU

upvoted 1 times

  **Naish2006** 1 year, 1 month ago

Exam 20/12

upvoted 1 times

  **nostroner89** 1 year, 1 month ago

Correct one is A

upvoted 1 times

  **IHensch** 1 year, 1 month ago

Selected Answer: D

To minimize costs and support up to 1 Gbps, you should create ExpressRoute Standard circuits. ExpressRoute Standard circuits support up to 1 Gbps and are available with ExpressRoute Unlimited data plans, which provide a cost-effective solution for high-bandwidth connectivity. ExpressRoute Local and ExpressRoute Direct circuits are not suitable for this scenario because they do not support the required bandwidth, and ExpressRoute Premium circuits are not cost-effective for this scenario because they are more expensive than ExpressRoute Standard circuits.

upvoted 3 times

  **EdwardY** 11 months, 3 weeks ago

"Compared to a Standard ExpressRoute circuit, a Local circuit has the same set of features except:

Scope of access to Azure regions as described above

ExpressRoute Global Reach isn't available on Local"

Still A

upvoted 3 times

  **gunjant25** 1 year, 4 months ago

ExpressRoute local, standard, global offer unlimited data plans.

ExpressRoute local: access azure region locally

ExpressRoute Standard: access azure multiple regions within a geopolitical location.

ExpressRoute Global: access azure regions globally/all over the world

upvoted 4 times

  **n0t4u2c** 1 year, 4 months ago

Wouldn't the answer be ExpressRoute Premium as that allows for unlimited data on both inbound and outbound traffic? Local only allows for unlimited inbound per the Microsoft document.

upvoted 1 times

  **paweu** 1 year, 4 months ago

Selected Answer: A

so as in my previous message, A

upvoted 1 times

You are planning an Azure Point-to-Site (P2S) VPN that will use OpenVPN.
Users will authenticate by an on-premises Active Directory domain.
Which additional service should you deploy to support the VPN authentication?

- A. an Azure key vault
- B. a RADIUS server
- C. a certification authority
- D. Azure Active Directory (Azure AD) Application Proxy

Correct Answer: B

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about>

Community vote distribution

B (100%)

 **walkwolf3** Highly Voted 2 years, 2 months ago

B. a RADIUS server

AD Domain authentication allows users to connect to Azure using their organization domain credentials. It requires a RADIUS server that integrates with the AD server.

<https://docs.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about>

upvoted 15 times

 **trashbox** Most Recent 3 months, 2 weeks ago

Selected Answer: B

"AD Domain authentication allows users to connect to Azure using their organization domain credentials. It requires a RADIUS server that integrates with the AD server."

<https://learn.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about#authentication>

upvoted 1 times

 **SLGUY** 5 months ago

Appeared on Exam 26 Aug 2023

upvoted 1 times

 **sserna** 1 year ago


En examen 20/01/2023

upvoted 1 times

 **TJ001** 1 year ago

correct Answer B

upvoted 1 times

 **nostromer89** 1 year, 1 month ago

It's Radius server. Please check the Documentation it is clearly given.

upvoted 1 times

 **nostromer89** 1 year, 1 month ago

correct answer B

upvoted 1 times

 **IHensch** 1 year, 1 month ago

Selected Answer: B

The correct answer is B. a RADIUS server.

In order to support the VPN authentication for your Azure Point-to-Site (P2S) VPN using OpenVPN, you will need to deploy a RADIUS server on your on-premises network. The RADIUS server will be used to authenticate users who are trying to connect to the VPN using their Active Directory credentials. This will allow you to securely and efficiently manage user access to the VPN.

A certification authority is not necessary for this scenario, because you are not using certificates for authentication. Similarly, an Azure key vault is not needed, because you are not using keys for authentication. Azure Active Directory (Azure AD) Application Proxy is not relevant to this scenario, because it is used for publishing web applications, not for VPN authentication.

upvoted 4 times

 **jilguens** 1 year, 4 months ago

Selected Answer: B

radius server
upvoted 2 times

🗨️ **1particle** 1 year, 6 months ago

B.
AD Domain authentication allows users to connect to Azure using their organization domain credentials. It requires a RADIUS server that integrates with the AD server. Organizations can also leverage their existing RADIUS deployment.
<https://docs.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about#authenticate-using-active-directory-ad-domain-server>
upvoted 3 times

🗨️ **zerocool114** 1 year, 6 months ago

correct, on exam today
upvoted 1 times

🗨️ **wooyourdaddy** 1 year, 6 months ago

Selected Answer: B

Ref Link: <https://docs.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about>
upvoted 1 times

🗨️ **unclegrandfather** 1 year, 7 months ago

Appeared on exam 6/28/22
upvoted 1 times

🗨️ **kogunribido** 1 year, 7 months ago

This came out 6/27/2022
upvoted 1 times

🗨️ **Edward1** 1 year, 9 months ago

Selected Answer: B

I think the correct answer is B: AD Domain authentication allows users to connect to Azure using their organization domain credentials. It requires a RADIUS server that integrates with the AD server. Organizations can also leverage their existing RADIUS deployment.
<https://docs.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about>
upvoted 1 times

🗨️ **jj22222** 1 year, 10 months ago

Selected Answer: B

B. a RADIUS server
upvoted 1 times

🗨️ **rockethack** 1 year, 11 months ago

This question was on the exam on 18th Feb 2022.
upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

You plan to configure BGP for a Site-to-Site VPN connection between a datacenter and Azure.

Which two Azure resources should you configure? Each correct answer presents a part of the solution. (Choose two.)

NOTE: Each correct selection is worth one point.

- A. a virtual network gateway
- B. Azure Application Gateway
- C. Azure Firewall
- D. a local network gateway
- E. Azure Front Door

Correct Answer: AD

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/bgp-howto>

Community vote distribution

AD (100%)

 **crawfish** Highly Voted 2 years, 3 months ago

Looks like the question number got changed/updated. Now, this question is around setting up BGP for a Site-to-Site VPN .

The given answers: A)Virtual Network Gateways and D) Local Network Gateways are correct as they are the key component required to setup S2S VPN tunnel.

upvoted 19 times

 **IHensch** Highly Voted 1 year, 1 month ago

Selected Answer: AD

The correct answers are A. a virtual network gateway and D. a local network gateway.

To configure BGP for a Site-to-Site VPN connection between a datacenter and Azure, you will need to configure a virtual network gateway and a local network gateway. The virtual network gateway will be used to establish the VPN connection between your datacenter and Azure, and the local network gateway will be used to define the on-premises network that you want to connect to Azure.

Azure Application Gateway, Azure Firewall, and Azure Front Door are not relevant to this scenario, because they are not used for configuring BGP for a Site-to-Site VPN connection.

upvoted 6 times

 **trashbox** Most Recent 3 months, 2 weeks ago

Selected Answer: AD

This question is also asked on the AZ-900 exam.

upvoted 1 times

 **jakubklapka** 4 months ago

In exam Sep, 2023

upvoted 1 times

 **JennyHuang36** 11 months, 1 week ago

In exam Feb, 2023

upvoted 2 times

 **JennyHuang36** 11 months, 1 week ago

In exam Feb, 2023

upvoted 1 times

 **sserna** 1 year ago

En examen 20/01/2023

upvoted 1 times

 **TJ001** 1 year ago

Correct Answers are A and D

upvoted 2 times

 **sshera** 1 year ago

in exam 4jan23

upvoted 2 times

🗄️ 👤 **Naish2006** 1 year, 1 month ago

in exam 20/12
upvoted 1 times

🗄️ 👤 **nostroner89** 1 year, 1 month ago

Answer is AD
upvoted 1 times

🗄️ 👤 **1particle** 1 year, 6 months ago

A.
If the IPsec tunnel fails to establish, Azure will keep retrying every few seconds. For this reason, troubleshooting "VPN down" issues is very convenient on IKEDiagnosticLog because you do not have to wait for a specific time to reproduce the issue.

<https://docs.microsoft.com/en-us/azure/vpn-gateway/troubleshoot-vpn-with-azure-diagnostics#IKEDiagnosticLog>
upvoted 3 times

🗄️ 👤 **1particle** 1 year, 6 months ago

A & D
PART 1 STEP 2: Create the VPN gateway for TestVNet1 with BGP parameters
In this step, you create a VPN gateway with the corresponding BGP parameters.

In the Azure portal, navigate to the Virtual Network Gateway resource from the Marketplace, and select Create.

PART2 STEP 1: Configure BGP on the local network gateway
In this step, you configure BGP on the local network gateway.
<https://docs.microsoft.com/en-us/azure/vpn-gateway/bgp-howto>
upvoted 2 times

🗄️ 👤 **zerocool114** 1 year, 6 months ago

on exam today
upvoted 1 times

🗄️ 👤 **Edward1** 1 year, 9 months ago

Selected Answer: AD

I think the correct answer is A y D:

-To establish a cross-premises connection, you need to create a Local Network Gateway to represent your on-premises VPN device, and a Connection to connect the VPN gateway with the local network gateway.

-BGP requires a Route-Based VPN gateway, and also the addition parameter, -Asn, to set the ASN (AS Number) for VNet.

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-bgp-resource-manager-ps>
upvoted 2 times

🗄️ 👤 **milan92stankovic** 1 year, 10 months ago

Selected Answer: AD

Correct answer A & D.
upvoted 2 times

🗄️ 👤 **rockethack** 1 year, 11 months ago

This question was on the exam on 18th Feb 2022.
upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

You fail to establish a Site-to-Site VPN connection between your company's main office and an Azure virtual network. You need to troubleshoot what prevents you from establishing the IPsec tunnel. Which diagnostic log should you review?

- A. IKEDiagnosticLog
- B. RouteDiagnosticLog
- C. GatewayDiagnosticLog
- D. TunnelDiagnosticLog

Correct Answer: A

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/troubleshoot-vpn-with-azure-diagnostics>

Community vote distribution

A (100%)

 **crawfish** Highly Voted 2 years, 3 months ago

Answer is correct - IKEDiagnosticLog

IKEDiagnosticLog = The IKEDiagnosticLog table offers verbose debug logging for IKE/IPsec. This is very useful to review when troubleshooting disconnections, or failure to connect VPN scenarios.

GatewayDiagnosticLog = Configuration changes are audited in the GatewayDiagnosticLog table.

TunnelDiagnosticLog = The TunnelDiagnosticLog table is very useful to inspect the historical connectivity statuses of the tunnel.

RouteDiagnosticLog = The RouteDiagnosticLog table traces the activity for statically modified routes or routes received via BGP.

P2SDiagnosticLog = The last available table for VPN diagnostics is P2SDiagnosticLog. This table traces the activity for Point to Site.

<https://docs.microsoft.com/en-us/azure/vpn-gateway/troubleshoot-vpn-with-azure-diagnostics>

upvoted 47 times

 **anishk** Most Recent 7 months, 1 week ago

I = I for remembering

upvoted 1 times

 **TJ001** 1 year ago

correct Answer

upvoted 1 times

 **charada83** 1 year, 4 months ago

correct

upvoted 1 times


 **1particle** 1 year, 6 months ago

A.

If the IPsec tunnel fails to establish, Azure will keep retrying every few seconds. For this reason, troubleshooting "VPN down" issues is very convenient on IKEDiagnosticLog because you do not have to wait for a specific time to reproduce the issue.

<https://docs.microsoft.com/en-us/azure/vpn-gateway/troubleshoot-vpn-with-azure-diagnostics#IKEDiagnosticLog>

upvoted 1 times

 **derrrp** 1 year, 6 months ago

If you have trouble remembering this question and you start to think the answer is TunnelDiagnosticLog, then you need to remember to tunnel deeper - as the answer is IKEDiagnosticLog. Although it is very easy to immediately see the word tunnel thinking it may be the right answer.

upvoted 1 times

 **Edward1** 1 year, 9 months ago

Selected Answer: A

A.

<https://docs.microsoft.com/es-es/azure/vpn-gateway/troubleshoot-vpn-with-azure-diagnostics>

upvoted 1 times

 **d0bermannn** 1 year, 11 months ago

Selected Answer: A

A. IKEDiagnosticLog
upvoted 1 times

🗄️ 👤 **Joshalom** 1 year, 11 months ago
on exam 6/2/2022
upvoted 1 times

🗄️ 👤 **Pravda** 2 years ago
On exam 1/6/2022
upvoted 1 times

🗄️ 👤 **AidenYoukhana** 2 years ago

Selected Answer: A

IKEDiagnosticLog
upvoted 4 times

🗄️ 👤 **[Removed]** 2 years, 1 month ago
same question in whizlabs is marked gatewaydiagnosticlogs but i feel ikediagnosticlog is more accurate.
upvoted 3 times

🗄️ 👤 **Pamban** 2 years, 1 month ago
appeared on exam 5th Dec 2021
upvoted 1 times

🗄️ 👤 **chreaxa** 2 years, 3 months ago
Correct
upvoted 1 times

🗄️ 👤 **RandomUser** 2 years, 3 months ago
Yeah, that's the most detailed log. The only that would help you troubleshooting the most common issue - IKE errors.
upvoted 1 times

🗄️ 👤 **AmalMOQ** 2 years, 3 months ago
correct !
The IKEDiagnosticLog table offers verbose debug logging for IKE/IPsec. This is very useful to review when troubleshooting disconnections, or failure to connect VPN scenarios.
upvoted 3 times

店铺: IT认证考试服务

店铺: IT认证考试服务

You have an Azure virtual network and an on-premises datacenter.

You are planning a Site-to-Site VPN connection between the datacenter and the virtual network.

Which two resources should you include in your plan? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. a user-defined route
- B. a virtual network gateway
- C. Azure Firewall
- D. Azure Web Application Firewall (WAF)
- E. an on-premises data gateway
- F. an Azure application gateway
- G. a local network gateway

Correct Answer: BG

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal>

Community vote distribution

BG (100%)

 **omgMerrick** Highly Voted 11 months, 3 weeks ago

Selected Answer: BG

- B. a virtual network gateway
- G. a local network gateway

To establish a Site-to-Site VPN connection between an on-premises datacenter and an Azure virtual network, you must include two resources in your plan: a virtual network gateway in Azure and a local network gateway in the datacenter.

A virtual network gateway acts as the VPN endpoint in Azure and allows the VPN connection to be established with the datacenter.

A local network gateway represents the on-premises VPN device and its IP address. This allows Azure to establish a VPN connection with the datacenter over the public Internet.

The virtual network gateway and the local network gateway work together to create the VPN connection, allowing secure communication between the datacenter and the virtual network.

upvoted 8 times

 **trashbox** Most Recent 3 months, 2 weeks ago

Selected Answer: BG

The answers are correct.
upvoted 1 times

 **ESAJRR** 10 months, 1 week ago

Selected Answer: BG

It's corrects.
upvoted 2 times

 **sserna** 1 year ago

En examen 20/01/2023
upvoted 1 times

 **TJ001** 1 year ago

BG is correct
upvoted 1 times

 **sshera** 1 year ago

in exam 4jan23
upvoted 1 times

 **MyPractice** 1 year, 1 month ago

This came in Dec 2022
upvoted 1 times

HasanHHH 1 year, 3 months ago

Selected Answer: BG

Main Component of S2S VPN
local network gateway & virtual network gateway
upvoted 3 times

BlackZeros 1 year, 4 months ago

Selected Answer: BG

similar to another question with less options
upvoted 3 times

1particle 1 year, 6 months ago

B & G.

In Search resources, services, and docs (G+/) type virtual network gateway. Locate Virtual network gateway in the Marketplace search results and select it to open the Create virtual network gateway page.

<https://docs.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal#create-the-gateway>

The local network gateway is a specific object that represents your on-premises location (the site) for routing purposes.

<https://docs.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal#LocalNetworkGateway>

upvoted 2 times

zerocool114 1 year, 6 months ago

on exam today

upvoted 1 times

kogunribido 1 year, 7 months ago

This came out 6/27/2022

upvoted 1 times

milan92stankovic 1 year, 8 months ago

Selected Answer: BG

Correct Answer

upvoted 3 times

Whatsamattr81 1 year, 8 months ago

B and G... None of the other things on there own will do S2S

upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT -

You need to connect an on-premises network and an Azure environment. The solution must use ExpressRoute and support failing over to a Site-to-Site VPN connection if there is an ExpressRoute failure.

What should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Routing type:

	▼
Policy-based	
Route-based	
Static routing	

Number of virtual network gateways:

	▼
1	
2	
3	

Correct Answer:

Answer Area

Routing type:

	▼
Policy-based	
Route-based	
Static routing	

Number of virtual network gateways:

	▼
1	
2	
3	

Reference:

<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-howto-coexist-resource-manager>

 **nawere** Highly Voted 1 year, 8 months ago

The correct answer is route based and two virtual network gateways - one for ExpressRoute connection (ExpressRoute virtual network gateway) and the second for the VPN connection (VPN virtual network gateway).

Check the architecture and read the description at the source.

Source: <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/expressroute-vpn-failover>
upvoted 80 times

 **MightyMonarch74** 11 months, 1 week ago

all you have to do is look at the architecture diagram at <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/expressroute-vpn-failover>

This confirms 1 ER gateway and 1 VPN gateway (both in the gateway subnet)

upvoted 5 times

 **Libaax01** 10 months, 3 weeks ago

You are 100 Percent! correct, in a Virtual Network (VNET) you can have two Gateways.

- One VPN Gateway

- One Express Route Gateway
upvoted 1 times

🗨️ **Libaax01** 10 months, 3 weeks ago

in the question, they asked "The solution must use ExpressRoute(Express Route Gateway) and support failing over to a Site-to-Site VPN(VPN Gateway) so a total of two Network Virtual Gateways are required."
upvoted 1 times

🗨️ **lasmus** 1 year, 8 months ago

how about this?

<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-howto-coexist-resource-manager>

maybe 1 is correct as via powershell you can do it
upvoted 1 times

🗨️ **jellybiscuit** 1 year, 4 months ago

The doc is correct. You are misreading it.

"If you have a virtual network that has only one virtual network gateway (let's say, Site-to-Site VPN gateway) and you want to add another gateway of a different type (let's say, ExpressRoute gateway),"

Another gateway of a different type. Two total.
upvoted 7 times

🗨️ **NotBillGates** 1 year, 7 months ago

No, that just means you can have an ExpressRoute gateway and a virtual network gateway in the same subnet, hence the term co-existence, they co-exist together. ExpressRoute Gateways don't provide S2S, hence, you need two.
upvoted 3 times

🗨️ **rac_sp** 1 year, 6 months ago

This is correct and I did a lab that worked really fine with this architecture
upvoted 2 times

🗨️ **voldemort123** Most Recent 4 months ago

Expressroute GW and VPN GW are types of virtual network gateways. For co existence they carved out of GatewaySubnet (min /27). So the question asks how many virtual network gateways -- which is 2 -- one ExR and one VPN.
upvoted 1 times

🗨️ **Izariqi** 5 months, 1 week ago

All Answers are incorrect. You can have Express Route and VPN on the same Virtual Network Gateway. It depends only on the SKU what you choose.
upvoted 1 times

🗨️ **skkk** 5 months, 2 weeks ago

The correct answer is need route based and two virtual network gateways
upvoted 1 times

🗨️ **Jamezz** 7 months, 1 week ago

in real life, we did route base and 2 virtual network gateways.
upvoted 1 times

🗨️ **henryhung** 9 months, 3 weeks ago

Route-based
2 virtual network gateways

From ChatGPT Plus (GPT-4)

For this scenario, the routing type that should be configured is "Route-based" because it allows for more flexibility in routing and is recommended for ExpressRoute connections.

As for the number of virtual network gateways, you should deploy 2 virtual network gateways for redundancy and failover purposes, one for the ExpressRoute connection and another for the Site-to-Site VPN connection. This is because a virtual network gateway can only be associated with one connection at a time. So, having two virtual network gateways allows you to switch between them if one of the connections fails.
upvoted 2 times

🗨️ **Nibo** 10 months, 4 weeks ago

its route based but you need two VNG
<https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/expressroute-vpn-failover>
upvoted 2 times

🗨️ **mVic** 11 months, 3 weeks ago

Route based and 2 Gateways of VPN and ExpressRoute type
upvoted 2 times

🗨️ **sserna** 1 year ago

En examen 20/01/2023

upvoted 2 times

🗨️ 👤 **TJ001** 1 year ago

Route based and 2 Gateways of VPN and ExpressRoute type

upvoted 4 times

🗨️ 👤 **NoeHdzMII** 1 year ago

Route based and 2 Gateways, as you can see in the Powershell commands to coexist

```
$gw = New-AzVirtualNetworkGateway -Name "VPNGateway" -ResourceGroupName
```

```
$gw = New-AzVirtualNetworkGateway -Name "ERGateway" -ResourceGroupName
```

upvoted 1 times

🗨️ 👤 **jozamaymen** 1 year ago

Correct answer:

You choose a Route-based when you create a VNG. Then in VNG you can add multi connection (S2S) and another one with ExpressRoute. No need to new VNG.

upvoted 1 times

🗨️ 👤 **sshera** 1 year ago

in exam 4jan23

upvoted 2 times

🗨️ 👤 **varundhiman** 1 year, 1 month ago

Correct Answer is route Based and 2 Gateway S2S gateway and ER Gateway. Though you can use the same gateway subnet for both of them.

upvoted 1 times

🗨️ 👤 **MyPractice** 1 year, 1 month ago

This came in Dec 2022

upvoted 1 times

🗨️ 👤 **Pradh** 1 year, 3 months ago

ROUTE BASED

2 VNG

This is the right answer .

upvoted 3 times

🗨️ 👤 **HasanHHH** 1 year, 3 months ago

The correct answer is route based and two virtual network gateways

ExpressRoute virtual network gateway. The ExpressRoute virtual network gateway enables the VNet to connect to the ExpressRoute circuit used for connectivity with your on-premises network.

VPN virtual network gateway. The VPN virtual network gateway enables the VNet to connect to the VPN appliance in the on-premises network.

The VPN virtual network gateway is configured to accept requests from the on-premises network only through the VPN appliance

upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

Your company has an on-premises network and three Azure subscriptions named Subscription1, Subscription2, and Subscription3. The departments at the company use the Azure subscriptions as shown in the following table.

Department	Subscription
IT	Subscription1
Research	Subscription1
Development	Subscription2
Testing	Subscription2
Distribution	Subscription3

All the resources in the subscriptions are in either the West US Azure region or the West US 2 Azure region.

You plan to connect all the subscriptions to the on-premises network by using ExpressRoute.

What is the minimum number of ExpressRoute circuits required?

- A. 1
- B. 2
- C. 3
- D. 4
- E. 5

Correct Answer: A

Reference:

<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction>

Community vote distribution

A (88%)

13%

 **Hawaii_IT** Highly Voted 1 year, 5 months ago

Answer: A - 1

Managing Authorization

The circuit owner can share a circuit with up to 10 Azure subscriptions. The circuit owner can view who has been authorized to the circuit. The owner can revoke the authorization at any time.

<https://azure.microsoft.com/en-us/blog/enable-multiple-subscription-expressroute/#:~:text=The%20circuit%20owner%20can%20share,the%20authorization%20at%20any%20time.>

upvoted 21 times

 **jellybiscuit** 1 year, 3 months ago

You are correct, though network topology can negate the ExpressRoute subscription limit anyway. For example, connect the ExpressRoute to a hub vnet and peer the subscription vnets to it.

upvoted 6 times

 **AdityaGupta** Highly Voted 1 year, 4 months ago

Selected Answer: A

1 Express Route Circuit standard sku would be good enough. With 1 er circuit you can connect upto 10 vnets and standard sku allows you to connect within same geopolitical region without additional cost.

upvoted 6 times

 **Ajdlfasudfo0** 1 year, 1 month ago

it's in the same metro, so local is fine

upvoted 3 times

 **KeZhai** Most Recent 3 weeks ago

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-faqs>

Yes. You can link up to 10 virtual networks in the same subscription as the circuit or different subscriptions using a single ExpressRoute circuit. This limit can be increased by enabling the ExpressRoute premium feature. Connectivity and bandwidth charges for the dedicated circuit gets applied to the ExpressRoute circuit owner and all virtual networks share the same bandwidth.

upvoted 1 times

🗨️ **_Cris** 4 months, 1 week ago

appears on exam, 19 Sept 2023

upvoted 3 times

🗨️ **Verytutos** 4 months, 2 weeks ago

Appeared on Exam 05 Sep 2023

upvoted 1 times

🗨️ **SLGUY** 5 months ago

Appeared on Exam 26 Aug 2023

upvoted 2 times

🗨️ **Ben_88** 7 months, 3 weeks ago

Selected Answer: A

1 Express Route Circuit standard sku would be good enough. With 1 er circuit you can connect upto 10 vnets and standard sku allows you to connect within same geopolitical region without additional cost.

upvoted 1 times

🗨️ **ESAJRR** 9 months, 1 week ago

Selected Answer: A

Answer: A - 1

upvoted 1 times

🗨️ **khanda** 9 months, 2 weeks ago

Selected Answer: A

You can link up to 10 virtual networks to a standard ExpressRoute circuit. All virtual networks must be in the same geopolitical region when using a standard ExpressRoute circuit. West US and West US 2 are in the same Azure geopolitical region, so you would need only one ER circuits.

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-howto-linkvnet-portal-resource-manager#connect-a-vnet-to-a-circuit---different-subscription>

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-locations-providers>

upvoted 3 times

🗨️ **mauchi** 10 months, 1 week ago

if the express route would be with a standard SKU, then yes, I think A - 1 express route would be enough

upvoted 1 times

🗨️ **Mo22** 11 months, 3 weeks ago

Selected Answer: B

B. 2

You need at least two ExpressRoute circuits to connect all three Azure subscriptions to the on-premises network. One circuit connects the West US Azure region and another circuit connects the West US 2 Azure region. All the resources in the subscriptions are in either the West US Azure region or the West US 2 Azure region, so you need to connect both regions.

upvoted 3 times

🗨️ **sapien45** 1 year, 4 months ago

Selected Answer: A

Not true for Local SKU though.

. With a Local SKU ExpressRoute circuit you can connect to resources in Azure regions in the same metro as the peering site. In this case, your on-premises network can access UK South Azure resources over ExpressRoute. For more information, see What is ExpressRoute Local?. When you configure a Standard SKU ExpressRoute circuit, connectivity to Azure resources will expand to all Azure regions in a geopolitical area.

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-faqs>

upvoted 1 times

🗨️ **Ajdifasudfo** 1 year, 1 month ago

same metro, so local is fine

upvoted 1 times

🗨️ **AdityaGupta** 1 year, 4 months ago

1 Express Route Circuit standard sku would be good enough. With 1 er circuit you can connect upto 10 vnets and standard sku allows you to connect within same geopolitical region without additional cost.

upvoted 1 times

🗨️ **Alessandro365** 1 year, 4 months ago

Selected Answer: A

Answer: A - 1

upvoted 1 times

🗨️ **Jamesat** 1 year, 5 months ago

Selected Answer: A

ExpressRoute circuits can be shared between subscriptions.

Correct answer is A
upvoted 4 times

 **iwikneerg** 1 year, 5 months ago

Looks like the correct answer is A

You can have an ExpressRoute Circuit going into one region and gain access to other regions from there...

Connectivity to all regions within a geopolitical region

You can connect to Microsoft in one of our peering locations and access regions within the geopolitical region.

For example, if you connect to Microsoft in Amsterdam through ExpressRoute. You'll have access to all Microsoft cloud services hosted in Northern and Western Europe. For an overview of the geopolitical regions, the associated Microsoft cloud regions, and corresponding ExpressRoute peering locations, see the ExpressRoute partners and peering locations article.

<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction#connectivity-to-all-regions-within-a-geopolitical-region>
upvoted 2 times

 **iwikneerg** 1 year, 5 months ago

<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-locations#locations>

See North America geopolitical region

upvoted 1 times

 **milan92stankovic** 1 year, 8 months ago

Selected Answer: A

Answer: A

upvoted 4 times

店铺: IT认证考试服务

店铺: IT认证考试服务

Your company has offices in New York and Amsterdam. The company has an Azure subscription. Both offices connect to Azure by using a Site-to-Site VPN connection.

The office in Amsterdam uses resources in the North Europe Azure region. The office in New York uses resources in the East US Azure region. You need to implement ExpressRoute circuits to connect each office to the nearest Azure region. Once the ExpressRoute circuits are connected, the on-premises computers in the Amsterdam office must be able to connect to the on-premises servers in the New York office by using the ExpressRoute circuits.

Which ExpressRoute option should you use?

- A. ExpressRoute FastPath
- B. ExpressRoute Global Reach
- C. ExpressRoute Direct
- D. ExpressRoute Local

Correct Answer: B

Reference:

<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-global-reach>

Community vote distribution


B (100%)

 **jakubklapka** 4 months ago

In exam Sep, 2023
upvoted 2 times

 **Verytutos** 4 months, 2 weeks ago

Appeared on Exam 05 Sep 2023
upvoted 1 times

 **ESAJRR** 9 months, 1 week ago

Selected Answer: B

Global Reach classic
upvoted 1 times

 **Mo22** 11 months, 3 weeks ago

Selected Answer: B

B. ExpressRoute Global Reach

ExpressRoute Global Reach provides the ability to connect multiple Azure regions and on-premises locations with a single ExpressRoute circuit. In this scenario, you need to connect the Amsterdam office to the North Europe Azure region and the New York office to the East US Azure region. ExpressRoute Global Reach enables the communication between the on-premises computers in the Amsterdam office and the on-premises servers in the New York office through the ExpressRoute circuits. Hence, ExpressRoute Global Reach is the most suitable option to use in this scenario.

upvoted 3 times

 **TJ001** 1 year ago

Global Reach classic use case
upvoted 3 times

 **Takloy** 1 year, 2 months ago

Selected Answer: B

ExpressRoute Global Reach is the right answer.
upvoted 1 times

 **HasanHHH** 1 year, 3 months ago

Selected Answer: B

With ExpressRoute Global Reach, you can link ExpressRoute circuits together to make a private network between your on-premises networks
upvoted 3 times

 **jellybiscuit** 1 year, 3 months ago

Selected Answer: B

I am thinking global reach is the answer they're looking for. This assumes that the two offices do not have existing connectivity to each other. I don't like having to make that assumption though.
upvoted 1 times

AdityaGupta 1 year, 4 months ago

Selected Answer: B

Express Route global reach is correct answer, since each data centre is connected to nearest Azure region by using ER circuit, you only need to enable Global Reach feature on bith ER circuit.

upvoted 1 times

Alessandro365 1 year, 4 months ago

Selected Answer: B

ExpressRoute Global Reach

upvoted 1 times

azeem0077 1 year, 5 months ago

Selected Answer: B

ExpressRoute Global Reach is the correct answer

upvoted 2 times

iwikneerg 1 year, 5 months ago

Selected Answer: B

With ExpressRoute Global Reach, you can link ExpressRoute circuits together to make a private network between your on-premises networks. In the above example, with the addition of ExpressRoute Global Reach, your San Francisco office (10.0.1.0/24) can directly exchange data with your London office (10.0.2.0/24) through the existing ExpressRoute circuits and via Microsoft's global network.

<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-global-reach>

upvoted 3 times

1particle 1 year, 6 months ago

B.

With ExpressRoute Global Reach, you can link ExpressRoute circuits together to make a private network between your on-premises networks. In the above example, with the addition of ExpressRoute Global Reach, your San Francisco office (10.0.1.0/24) can directly exchange data with your London office (10.0.2.0/24) through the existing ExpressRoute circuits and via Microsoft's global network.

<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-global-reach>

upvoted 3 times

derrrp 1 year, 6 months ago

"Once the ExpressRoute circuits are connected..." Remember that the ExpressRoute has already been established. The ExpressRoute Global Reach service option is like the delicious sauce on top of the already-existing ExpressRoute

upvoted 4 times

derrrp 1 year, 6 months ago

With ExpressRoute Global Reach, you can link ExpressRoute circuits together to make a private network between your on-premises networks.

In the Microsoft Support Documentation, we're shown a diagram of an on-prem network connected to an Azure datacenter through an express route in one geopolitical region - and another on-prem datacenter connected to Azure in another geopolitical region. Two ExpressRoutes are shown. ExpressRoute Global Reach is the peering between these two ExpressRoutes despite being in different geopolitical regions.

upvoted 2 times

milan92stankovic 1 year, 8 months ago

Selected Answer: B

Correct answer - Global Reach!

upvoted 3 times

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT -

You have an Azure subscription that contains a single virtual network and a virtual network gateway.

You need to ensure that administrators can use Point-to-Site (P2S) VPN connections to access resources in the virtual network. The connections must be authenticated by Azure Active Directory (Azure AD).

What should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area:

Azure AD configuration:

An access package
Conditional access policy
An enterprise application
A VPN certificate

P2S VPN tunnel type:

IKEv2
IKEv2 and SSTP (SSL)
OpenVPN (SSL)
SSTP (SSL)

Correct Answer:

Answer Area:

Azure AD configuration:

An access package
Conditional access policy
An enterprise application
A VPN certificate

P2S VPN tunnel type:

IKEv2
IKEv2 and SSTP (SSL)
OpenVPN (SSL)
SSTP (SSL)

Box 1: An enterprise application

Enable Azure AD authentication on the VPN gateway:

1. Locate the Directory ID of the directory that you want to use for authentication. It's listed in the properties section of the Active Directory page.
2. Under your Azure AD, in Enterprise applications, you see Azure VPN listed. Copy the Directory ID.
3. Sign in to the Azure portal as a user that is assigned the Global administrator role.
4. Next, give admin consent. Copy and paste the URL that pertains to your deployment location in the address bar of your browser.
5. Select the Global Admin account if prompted.
6. Select Accept when prompted.



Permissions requested Accept for your organization



This app would like to:

- ✓ Sign in and read user profile

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their [terms of service](#) and [privacy statement](#). You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Cancel

Accept

7. Under your Azure AD, in Enterprise applications, you see Azure VPN listed.

The screenshot shows the Azure AD portal interface for 'Enterprise applications - All applications'. The left sidebar contains navigation options like Overview, Diagnose and solve problems, Manage, Security, and Activity. The main content area shows a table of applications with columns for NAME, HOMEPAGE URL, OBJECT ID, and APPLICATION ID. One application is listed: Azure VPN with the homepage URL https://www.microsoft.com.

Box 2: Open VPN (SSL)

When you connect to your VNet using Point-to-Site, you have a choice of which protocol to use. The protocol you use determines the authentication options that are available to you. If you want to use Azure Active Directory authentication, you can do so when using the OpenVPN protocol.

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/openvpn-azure-ad-tenant>

sapien45 Highly Voted 1 year, 4 months ago

Azure AD authentication is supported only for OpenVPN® protocol connections and requires the Azure VPN Client.

<https://learn.microsoft.com/en-us/azure/vpn-gateway/openvpn-azure-ad-tenant>

upvoted 10 times

_Cris Most Recent 4 months, 1 week ago

appears on exam, 19 Sept 2023

upvoted 2 times

JennyHuang36 11 months, 1 week ago

In exam Feb,2023

upvoted 3 times

sserna 1 year ago

En examen 20/01/2023

upvoted 2 times

TJ001 1 year ago

correct answers
upvoted 1 times

🗨️ **sshera** 1 year ago
in exam 04jan23
upvoted 2 times

🗨️ **MyPractice** 1 year, 1 month ago
This came in Dec 2022
upvoted 1 times

🗨️ **Takloy** 1 year, 4 months ago
The answer is correct!
Enterprise Application and OpenVPN (SSL).
upvoted 2 times

🗨️ **BillyB2022** 1 year, 4 months ago
Correct, enterprise application
See <https://docs.microsoft.com/en-us/azure/vpn-gateway/openvpn-azure-ad-tenant>
upvoted 3 times

🗨️ **DerekKey** 1 year, 4 months ago
Correct
upvoted 2 times

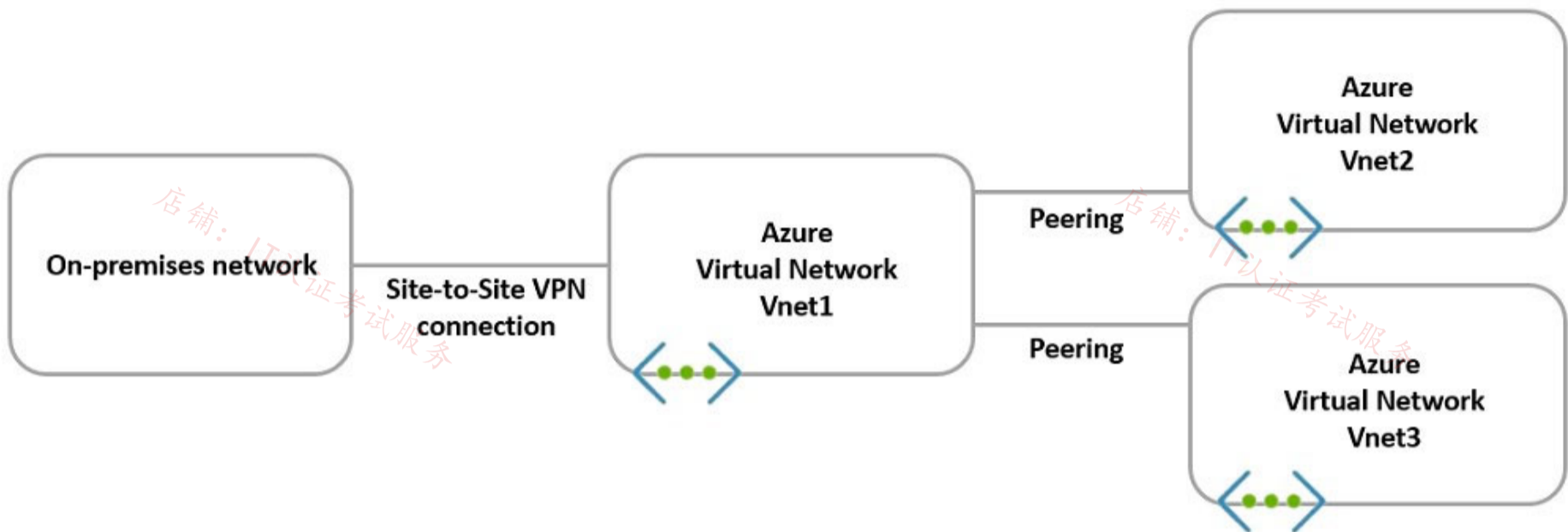
店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT -

You have the hybrid network shown in the Network Diagram exhibit.



You have a peering connection between Vnet1 and Vnet2 as shown in the Peering-Vnet1-Vnet2 exhibit.

店铺: IT认证考试服务

店铺: IT认证考试服务

Add peering ...

Vnet1

This virtual network

Peering link name *

Peering-Vnet1-Vnet2 ✓

Traffic to remote virtual network ⓘ

- Allow (default)
- Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ

- Allow (default)
- Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server ⓘ

- Use this virtual network's gateway or Route Server
- Use the remote virtual network's gateway or Route Server
- None (default)

Remote virtual network

Peering link name *

Peering-Vnet1-Vnet2 ✓

Virtual network deployment model ⓘ

- Resource manager
- Classic

I know my resource ID ⓘ

Subscription* ⓘ

Subscription1 ✓

Virtual network

Vnet2 ✓

Traffic to remote virtual network ⓘ

- Allow (default)
- Block all traffic to the remote virtual network

Add

You have a peering connection between Vnet1 and Vnet3 as shown in the Peering-Vnet1-Vnet3 exhibit.

Add peering ...

Vnet3

This virtual network

Peering link name *

Peering-Vnet1-Vnet3 ✓

Traffic to remote virtual network ⓘ

- Allow (default)
 Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ

- Allow (default)
 Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server ⓘ

- Use this virtual network's gateway or Route Server
 Use the remote virtual network's gateway or Route Server
 None (default)

Remote virtual network

Peering link name *

Peering-Vnet1-Vnet3 ✓

Virtual network deployment model ⓘ

- Resource manager
 Classic

I know my resource ID ⓘ

Subscription* ⓘ

Subscription1 ✓

Virtual network

Vnet1 ✓

Traffic to remote virtual network ⓘ

- Allow (default)
 Block all traffic to the remote virtual network

Traffic to remote virtual network

- Allow (default)
 Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network

- Allow (default)
 Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server

- Use this virtual network's gateway or Route Server
 Use the remote virtual network's gateway or Route Server
 None (default)

Add

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area:

Statements	Yes	No
The resources in Vnet2 can communicate with the resources in Vnet1.	<input type="radio"/>	<input type="radio"/>
The resources in Vnet2 can communicate with the resources in Vnet3.	<input type="radio"/>	<input type="radio"/>
The resources in Vnet2 can communicate with the resources in the on-premises network.	<input type="radio"/>	<input type="radio"/>

店铺: IT认证考试服务

店铺: IT认证考试服务

Correct Answer:

Answer Area:

Statements	Yes	No
The resources in Vnet2 can communicate with the resources in Vnet1.	<input checked="" type="radio"/>	<input type="radio"/>
The resources in Vnet2 can communicate with the resources in Vnet3.	<input type="radio"/>	<input checked="" type="radio"/>
The resources in Vnet2 can communicate with the resources in the on-premises network.	<input type="radio"/>	<input checked="" type="radio"/>

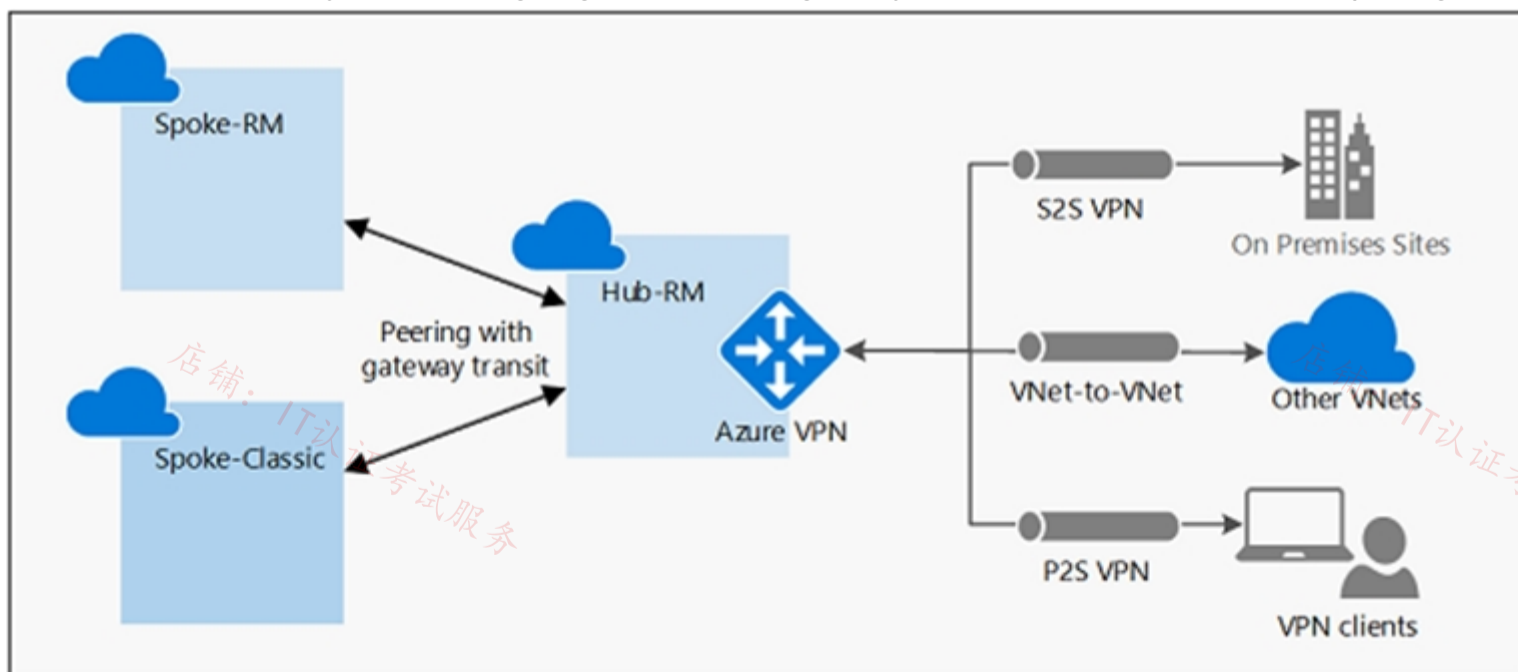
Box 1: Yes -

Virtual network peering seamlessly connects two Azure virtual networks, merging the two virtual networks into one for connectivity purposes.

Box 2: No -

No Virtual Gateway is used.

Gateway transit is a peering property that lets one virtual network use the VPN gateway in the peered virtual network for cross-premises or VNet-to-VNet connectivity. The following diagram shows how gateway transit works with virtual network peering.



店铺: IT认证考试服务

店铺: IT认证考试服务

In the diagram, gateway transit allows the peered virtual networks to use the Azure VPN gateway in Hub-RM. Connectivity available on the VPN gateway, including S2S, P2S, and VNet-to-VNet connections, applies to all three virtual networks.

Box 3: No -

No Virtual Gateway is used.

Reference:

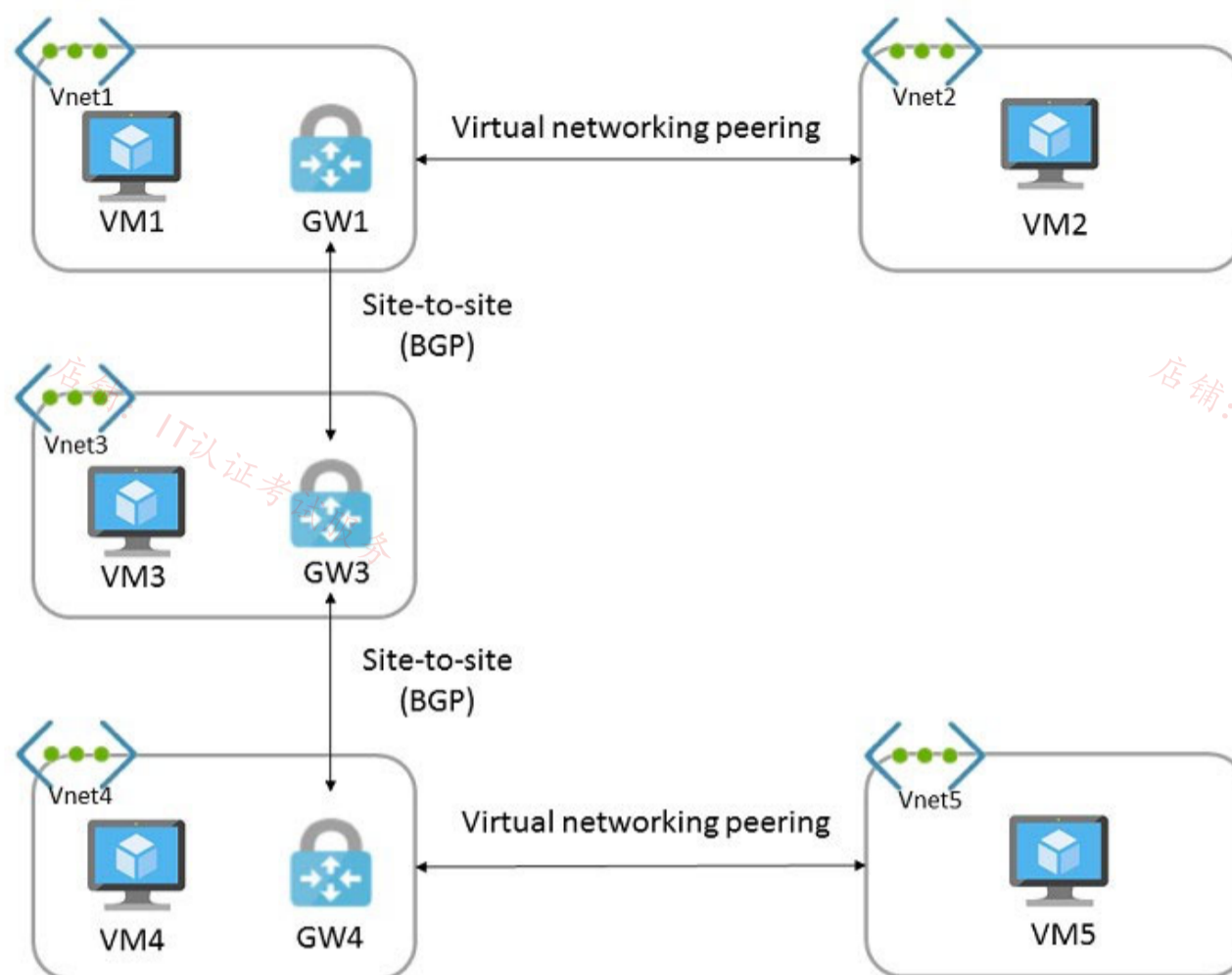
<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-peering-gateway-transit>

-  **amt2022** Highly Voted 11 months, 3 weeks ago
Correct answer Y,N,N.
Remember Azure VNET Peering is NON-Transitive. Meaning, only direct peered VNETs can talk to each other. To make it transitive you either use VNET Gateway or NVAs/Azure FireWall.
upvoted 10 times
-  **Prutser2** Highly Voted 1 year, 3 months ago
correct, vnet1 cannot be a transit between vnets2 and 3, without using the gateway as transit
upvoted 6 times
-  **vikrants31** 1 month, 1 week ago
Incorrect. Vnet2 can communicate to Vnet3 because the communication is via AZURE backbone not via Gateway, gateway is only required if Vnet2 wants to communicate to On-prem.
My take YYN
As per this MSDOC
<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview>
upvoted 1 times
-  **c2e9cb4** 1 month ago
This is not correct No transitivity by default between spokes vnets
upvoted 1 times
-  **CiscoExam** Most Recent 3 weeks, 5 days ago
The options have all changed on the actual Azure Portal UI now. It's much clearer and self-explanatory now in fact !
upvoted 1 times
-  **MARTINOV** 3 months, 2 weeks ago
I don't get it, why can't VNET1 communicate with on-prem when there is a site-to-site VPN present?
upvoted 2 times
-  **MARTINOV** 3 months, 2 weeks ago
I read the question wrong, my bad!
upvoted 1 times
-  **bp_a_user** 4 months ago
The last one should be yes: It is stated that there is a Site-to-Site VPN which implies that there is virtual network gateway.
upvoted 1 times
-  **bp_a_user** 4 months ago
I am wrong, I think it that old screenshot, the option "remote gateway or route server" should be enabled
upvoted 3 times
-  **vDreams** 5 months ago
Answer is tricky. Y/N/N is correct, because it's not mentioned the usage of NVA or VNG. If it mentioned NVA, or use of VNG, then it would be Y/Y/Y
upvoted 2 times
-  **omgMerrick** 11 months, 1 week ago
Answer is correct.

Y
N
N
upvoted 1 times
-  **TJ001** 1 year ago
yes,no,no
upvoted 1 times
-  **zukako** 1 year ago
correct vnet1 not use its gateway for vnet2
upvoted 1 times
-  **DeepMoon** 1 year, 4 months ago
Doesn't the 2nd Link name on both those peerings are wrong matter?
upvoted 1 times
-  **GetulioJr** 1 year, 4 months ago
Answer is correct, The option: "Use the remote virtual network's gateway" is not enabled
upvoted 2 times
-  **DerekKey** 1 year, 4 months ago
Correct
upvoted 3 times

HOTSPOT -

You have the Azure environment shown in the exhibit.



You have virtual network peering between Vnet1 and Vnet2. You have virtual network peering between Vnet4 and Vnet5. The virtual network peering is configured as shown in the following table.

Virtual network	Traffic to remote virtual network	Use remote gateway	Allow gateway transit
Vnet1	Allow	None	Enabled
Vnet2	Allow	Enabled	None
Vnet4	Allow	None	Enabled
Vnet5	Block	Enabled	None

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Hot Area:

Answer Area:

Statements	Yes	No
VM1 and VM4 can communicate.	<input type="radio"/>	<input type="radio"/>
VM2 and VM4 can communicate.	<input type="radio"/>	<input type="radio"/>
VM1 and VM5 can communicate.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

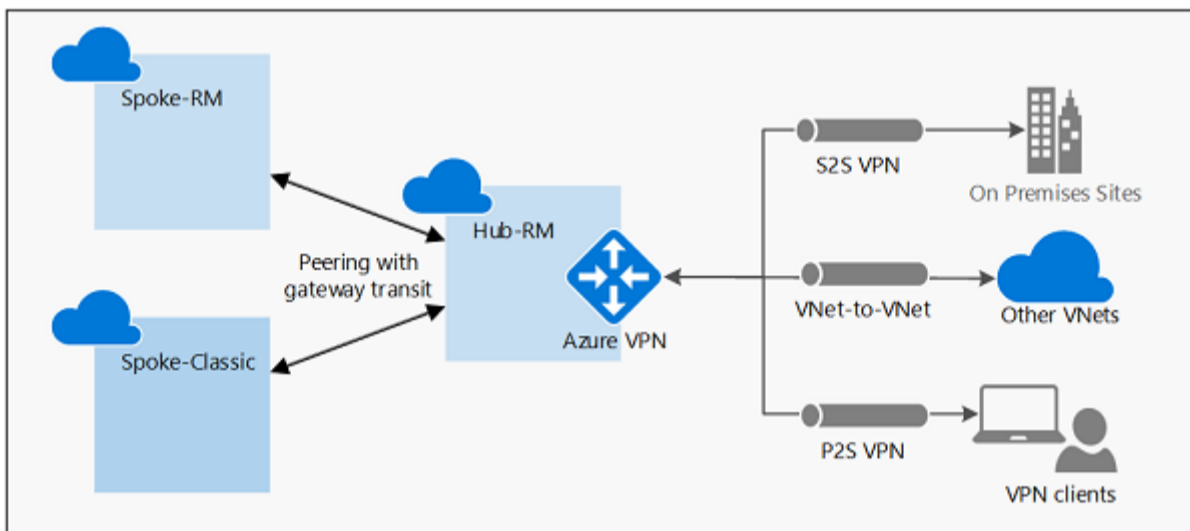
Answer Area:

Statements	Yes	No
VM1 and VM4 can communicate.	<input checked="" type="radio"/>	<input type="radio"/>
VM2 and VM4 can communicate.	<input checked="" type="radio"/>	<input type="radio"/>
VM1 and VM5 can communicate.	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: Yes -

Virtual network peering seamlessly connects two Azure virtual networks, merging the two virtual networks into one for connectivity purposes. Gateway transit is a peering property that lets one virtual network use the VPN gateway in the peered virtual network for cross-premises or VNet-to-VNet connectivity.

The following diagram shows how gateway transit works with virtual network peering.



In the diagram, gateway transit allows the peered virtual networks to use the Azure VPN gateway in Hub-RM. Connectivity available on the VPN gateway, including S2S, P2S, and VNet-to-VNet connections, applies to all three virtual networks.

In hub-and-spoke network architecture, gateway transit allows spoke virtual networks to share the VPN gateway in the hub, instead of deploying VPN gateways in every spoke virtual network.

Box 2: Yes -

VM2 uses the remote gateway GW1 to reach VM4.

Box 3: No -

VM2 can reach VM4 through GW1, but not VM5 as VNET1 does not use remote Gateways.

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-peering-gateway-transit> <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-troubleshoot-peering-issues>

zenithcsa1 Highly Voted 1 year, 4 months ago

YYY / tested in lab

VM1 and VM5 can communicate.

'Traffic to remove virtual network : Block' setting in Vnet5 does not block communication between VM5 and GW4, while it blocks communication between VM5 and VM4.

upvoted 26 times

Aiwa23 1 year, 4 months ago

it blocks communication from VNET5 to VNET4 but allows VNET4 to VNET5

upvoted 4 times

Pratheeshp 8 months, 3 weeks ago

How about the the return traffic VNET5 to VNET4 ?

upvoted 2 times

zenithcsa1 1 year, 4 months ago

That's not true. 'Block' option is about NSG's VirtualNetwork tag whether it contains network address of Vnet4 or not. When you choose 'block' and create security rules on VM5's NSG, VM5 still can communicate with resources in Vnet4.

upvoted 2 times

  **A_way** 1 year, 4 months ago

Could you pls clarify? This is referring the vnet peering settings not NSG

upvoted 6 times

  **dani999** 1 year ago

Microsoft:

NOTE: Selecting the Block all traffic to remote virtual network setting only changes the definition of the VirtualNetwork service tag. It doesn't fully prevent traffic flow across the peer connection, as explained in this setting description.

upvoted 3 times

  **Alessandro365** Highly Voted 1 year, 4 months ago

YYY, tested in lab.

vnet5 peering is disabled, but remote gateway is enabled, allowing the vm5 to be accessed from other vnets. Only VM4 cannot access VM5 (peering blocked).

Note that BGP needs to be configured, user routes does not work.

upvoted 10 times

  **sam881989** Most Recent 2 weeks, 5 days ago

The answer is correct it is YYN tested in lab!

The remote gateway and allow gateway transit only applies to Vnet peering in this case between Vnet 2 and Vnet 1, and another is between Vnet 4 and Vnet 5. Because the connection between the Vnet 1, 3, and 4 is using BGP no option to set remote gateway and transit gateway. All the routes are forwarded to Vnet 2 and Vnet 5 but because Vnet 5 is blocking the traffic to Vnet 4 VM1 can't reach VM5 but rest all can reach each other.

upvoted 1 times

  **Opala79** 1 month, 2 weeks ago


I think it would be NNN because the option "Use remote gateway" of VNET 1 is disabled, someone disagrees ?

upvoted 2 times

  **Verytutos** 4 months, 2 weeks ago

Appeared on Exam 05 Sep 2023

upvoted 3 times

  **Oklama** 8 months, 1 week ago

YYY is correct

upvoted 1 times

  **arnaudhelin** 10 months ago

Hi everyone,

I tried a lot of configuration to test the last point. With wireshark on both sides, and traffic flow always on (ping and http request), the result is quite clear even if it is not logical at the first look. When you choose the option BLOCK on one side, the entire communication is blocked. If you want to have the "expected" behavior (vm4 to vm5 ok but not the other way), you must set a NSG with an explicit rule wich allows the traffic.

upvoted 7 times

  **mm2** 12 months ago

YYY:

for 3rd:

- Select Block all traffic to the remote virtual network if you don't want traffic to flow to the peered virtual network by default. You can select this setting if you have peering between two virtual networks but occasionally want to disable default traffic flow between the two. You may find enabling/disabling is more convenient than deleting and re-creating peerings. When this setting is selected, traffic doesn't flow between the peered virtual networks by default; however, traffic may still flow if explicitly allowed through a network security group rule that includes the appropriate IP addresses or application security groups.

upvoted 2 times

  **[Removed]** 9 months, 1 week ago

When this setting is selected, traffic doesn't flow between the peered virtual networks by default; however, traffic may still flow if explicitly allowed through a network security group rule that includes the appropriate IP addresses or application security groups.

There is no point to NSG so i think 3rd is NO

upvoted 3 times

  **tester2023** 12 months ago

YYN

To test the 'block' on the peering between vNet4 and vNet5 I did the following:

Deployed two vNets. On the second vNet, I selected the "Block all traffic to the remote virtual network" and the Portal displays "Resources in vnet-2 cannot communicate to resources in the vnet-1"

When I do a Connection Troubleshoot test, it fails with "Traffic blocked due to the following network security group rule: DefaultRule_DenyAllInBound".

When I set the peering setting to "Allow (default)", the Connection Troubleshoot is successful.

upvoted 5 times

  **asdasd123123iu** 6 months, 3 weeks ago

Agree. We don't have an information that traffic between vm5 and remote networks has been allowed on NSG so by default it will be blocked.
upvoted 1 times

🗨️ **mauchi** 1 year ago

To me YYN seems correct.

I think the last option is a NO, bc the statement says "VM1 and VM5 can communicate" to me it implies a bidirectional communication. And the table states that Vnet 5 blocks traffic going to a different vnet, such as vnet1, thus (bidirectional) communication between them is not possible.

upvoted 6 times

🗨️ **TJ001** 1 year ago

YYY seems right

upvoted 1 times

🗨️ **MyPractice** 1 year, 1 month ago

This came in Dec 2022

upvoted 1 times

🗨️ **geuser** 1 year, 1 month ago

I say YYN

No because: Select Block all traffic to the remote virtual network if you don't want traffic to flow to the peered virtual network by default. You can select this setting if you have peering between two virtual networks but occasionally want to disable default traffic flow between the two. You may find enabling/disabling is more convenient than deleting and re-creating peerings.

upvoted 4 times

🗨️ **Takloy** 1 year, 2 months ago

YYY

For the 3rd question, if you read carefully and look closely to the chart, it means Traffic to remote network from VNET5. Meaning, From VNET5 to any of the remote networks will be blocked but not inbound. This is why the answer is Yes.

upvoted 2 times

🗨️ **GokuSS** 1 year, 3 months ago

YYN, for 3rd questions, does this explanation makes sense? "VM1 can reach VM4 through GW1, but not VM5 as VNet1 does not use remote Gateways."

upvoted 1 times

🗨️ **ACSlarning1** 1 year, 3 months ago

How can "VM1 and VM5 can communicate" be yes if "use remote gateway" is set to none on vnet1?

upvoted 1 times

🗨️ **TJ001** 1 year ago

that is only for peering not for BGP

upvoted 1 times

🗨️ **mingorad** 1 year, 4 months ago

correct is YYY ; traffic to remote virtual network is blocked on Vnet5 so from Vnet5 to exterior not from Vnet4 to Vnet5

upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT -

You have on-premises datacenters in New York and Seattle.

You have an Azure subscription that contains the ExpressRoute circuits shown in the following table.

Name	Azure region	Datacenter
ERC1	East US	New York
ERC2	West US2	Seattle

You need to ensure that all the data sent between the datacenters is routed via the ExpressRoute circuits. The solution must minimize costs.

How should you configure the network? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

ExpressRoute configuration:

Direct
FastPath
Global Reach
Premium

Peering:

Microsoft
Private
Public

Answer Area

ExpressRoute configuration:

Direct
FastPath
Global Reach
Premium

Correct Answer:

Peering:

Microsoft
Private
Public

Box 1: Global Reach -

ExpressRoute Global Reach is the service where if you have two datacenters, which are located at different geo-locations and both are connected to Microsoft

Azure via Express Route then these two datacenters can also connect to each other securely via Microsoft's backbone.

Incorrect:

FastPath is designed to improve the data path performance between your on-premises network and your virtual network. When enabled, FastPath sends network traffic directly to virtual machines in the virtual network, bypassing the gateway.

Box 2: Private -

With ExpressRoute Global Reach, you can link ExpressRoute circuits together to make a private network between your on-premises networks.

Reference:

<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-global-reach>

 **jakubklapka** 4 months ago

In exam Sep, 2023

upvoted 2 times

 **[Removed]** 4 months, 1 week ago

You have to use ExpressRoute Global Reach. That is the requirement for connecting two On-Premise data centers through two different ExpressRoutes.

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-introduction>

upvoted 1 times

  **ironbornson** 5 months, 2 weeks ago

A-Global reach: that is a difficult one as WEST US and EAST US are inside the same geopolitical region as "mauchi" wrote down, actually Standard SKU might be enough for the ER to connect together, but the question is which configuration is better, so Premium is not a configuration is an SKU, from Direct, FastPath and GlobalReach, globalreach seems the only logical:

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-faqs#do-i-need-expressroute-premium-for-expressroute-global-reach>

B-Private obviously

upvoted 2 times

  **bakamon** 8 months ago

:: Global Reach

:: Private

upvoted 1 times

  **Himank20** 9 months ago

From MS Docs:-

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-faqs#what-is-expressroute-global-reach>

If a metro in a supported country/region has more than one ExpressRoute peering location, you can connect together the ExpressRoute circuits created at different peering locations in that metro.

upvoted 1 times

  **sserna** 1 year ago

En examen 20/01/2023

upvoted 2 times

  **Tightbot** 1 year, 1 month ago

Global reach


<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-faqs#what-is-expressroute-global-reach>

upvoted 2 times

  **Takloy** 1 year, 2 months ago

Global reach functions like a "Transit gateway" for on premise networks. hence, allowing them 2 different on-premise locations to communicate.

upvoted 2 times

  **sikbeats** 1 year, 3 months ago

Why is it called "Global Reach" if it is within US regions. I thought Global Reach was for different global regions like if a US provider doesn't have a locations in the other region.

upvoted 2 times

  **TJ001** 1 year ago

East US and West US does not fall in the same geopolitical,,,,East US and East US 2 may

upvoted 1 times

  **mauchi** 1 year ago

that's not right, they are indeed under the same geopolitical region - check here <https://learn.microsoft.com/en-us/azure/expressroute/expressroute-locations>

upvoted 2 times

  **Apptech** 10 months, 3 weeks ago

I agree. Geopolitical region is North America. It includes East US, West US, East US 2, West US 2, West US 3, Central US, South Central US, North Central US, West Central US, Canada Central, Canada East

upvoted 1 times

  **BlackZeros** 1 year, 4 months ago

seems like a right answer

Global Reach

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-global-reach>

Peering

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-circuit-peerings>

upvoted 4 times

  **AdityaGupta** 1 year, 4 months ago

Global Reach is a feature for connecting your On-Prem Datacenters over Express Route.

And Private Peering allows to you connect On-Prem to Azure Platform Private Networks.


upvoted 1 times

  **DerekKey** 1 year, 4 months ago

Configure ExpressRoute Global Reach -> Azure private peering is configured on your ExpressRoute circuits.

<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-howto-set-global-reach>

upvoted 1 times

 **WhiteRhino1743** 1 year, 5 months ago

Looks correct. To confirm the second question - <https://docs.microsoft.com/en-us/azure/expressroute/expressroute-howto-set-global-reach>.
upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

You have an Azure virtual network named Vnet1 and an on-premises network. The on-premises network has policy-based VPN devices. In Vnet1, you deploy a virtual network gateway named GW1 that uses a SKU of VpnGw1 and is route-based. You have a Site-to-Site VPN connection for GW1 as shown in the following exhibit.

Save Discard

Use Azure Private IP Address ⓘ
 Disabled Enabled

BGP ⓘ
 Disabled Enabled

IPsec / IKE policy ⓘ
 Default Custom

Use policy based traffic selector ⓘ
 Enable Disable

DPD timeout in seconds * ⓘ

Connection Mode ⓘ
 Default InitiatorOnly ResponderOnly

IKE Protocol ⓘ
 IKEv2

You need to ensure that the on-premises network can connect to the route-based GW1. What should you do before you create the connection?

- A. Set Connection Mode to ResponderOnly.
- B. Set BGP to Enabled.
- C. Set Use Azure Private IP Address to Enabled.
- D. Set IPsec / IKE policy to Custom.

Correct Answer: B

BGP is the standard routing protocol commonly used in the Internet to exchange routing and reachability information between two or more networks. BGP enables the Azure VPN Gateways and your on-premises VPN devices, called BGP peers or neighbors, to exchange "routes" that will inform both gateways on the availability and reachability for those prefixes to go through the gateways or routers involved. BGP can also enable transit routing among multiple networks by propagating routes a BGP gateway learns from one BGP peer to all other BGP peers.

Incorrect:

Not C: A VPN gateway must have a Public IP address. Verify that you have an externally facing public IPv4 address for your VPN device.

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-bgp-resource-manager-ps> <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-cli>

Community vote distribution

D (90%)

10%

 **mrgreat** Highly Voted 10 months ago

D. Set IPsec / IKE policy to Custom.

In order to ensure that the on-premises network can connect to the route-based virtual network gateway, you need to set the IPsec / IKE policy to Custom. The default policy settings for a virtual network gateway are not compatible with policy-based VPN devices. By setting the IPsec / IKE policy to Custom, you can configure the policy to match the requirements of the on-premises VPN devices.

Option A, "Set Connection Mode to ResponderOnly," is not a valid option for a route-based VPN gateway.

Option B, "Set BGP to Enabled," is not necessary to enable connectivity between a route-based gateway and a policy-based VPN device.

Option C, "Set Use Azure Private IP Address to Enabled," is not relevant to this scenario. This setting is used to specify whether the virtual network gateway should use a private or public IP address for the VPN connection.

upvoted 19 times

 **RageshBethapudi** Highly Voted 1 year, 5 months ago

correct answer is D.

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-connect-multiple-policybased-rm-ps>

upvoted 15 times

 **vDreams** Most Recent 5 months ago

correct answer is D.

BGP will trade routes, not the algorithm to setup the VPN. Also, as per documentation (<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-bgp-overview#why>) is an optional feature to use as Route-Based.

<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-bgp-overview#why>


upvoted 1 times

 **khanda** 9 months, 2 weeks ago

Selected Answer: D

Correct answer is D

upvoted 1 times

 **Chezzer83** 9 months, 4 weeks ago

Selected Answer: D

I assumed D for this. BGP is not required to configure a VPN connection.

upvoted 2 times

 **where2go** 10 months ago

Its D --- The configuration option is part of the custom IPsec/IKE connection policy. If you enable the policy-based traffic selector option, you must specify the complete policy (IPsec/IKE encryption and integrity algorithms, key strengths, and SA lifetimes).

The configuration option is part of the custom IPsec/IKE connection policy. If you enable the policy-based traffic selector option, you must specify the complete policy (IPsec/IKE encryption and integrity algorithms, key strengths, and SA lifetimes).

upvoted 1 times

 **bennasu** 10 months, 2 weeks ago

If you set the IPsec/IKE config to default, under most of the circumstances, azure VPN GW will automatically match the on prem Firewall's IPsec Phase 1 and phase 2 configuration(modern FW like fortigate,sonicwall). But if you are using cisco ASA then it's a different story. You would need to configure the phase manually

upvoted 1 times

 **Bbb78** 11 months, 4 weeks ago

I am not sure any of the 4 answers are correct. Mainly because this is ENABLED - "Use policy based traffic selector " ...if the onPrem device(s) is route based then this is not needed ?

upvoted 1 times

 **sserna** 1 year ago

En examen 20/01/2023

upvoted 2 times

 **mm2** 1 year ago

Selected Answer: D

route-based also mean static routes and all others routing protocols, when policy based, based on configured networks that should be routed for this specific VPN.

From network perspective route-based use ROUTING TABLE to make route decision, this includes all directly connected networks and mentioned static routes. Making an assumption that BGP=Route-based as a must - is wrong imho

however you can configure route-based to communicated with multiple policy base devices. Please notice POLICY BASE DEVICES for on prem, not DEVICE [one], there are multiple in question.

upvoted 2 times

 **mm2** 1 year ago

route-based also mean static routes and all others routing protocols, when policy based, based on configured networks that should be routed for this specific VPN.

From network perspective route-based use ROUTING TABLE to make route decision, this includes all directly connected networks and mentioned static routes. Making an assumption that BGP=Route-based as a must - is wrong imho.

upvoted 1 times

 **zukako** 1 year ago

Not have to set BGP if onpremise is act/standby

upvoted 1 times

 **Andre369** 1 year, 1 month ago

Selected Answer: D

correct answer is D.

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-connect-multiple-policybased-rm-ps>

upvoted 1 times

 **JRodJ** 1 year, 1 month ago

I don't think any of these answers is correct. In order to talk to on premises there is another button that must be enabled not visible on this screenshot. Use custom traffic selectors and it needs to be enabled. I have verified this works by configuring it at my customer's location with 3 separate sites.

upvoted 1 times

 **Libaax01** 1 year, 3 months ago

The correct answer is D, you can not have Policy based VPN one end and Route Based VPN on the other. Both ends need to match on the type of VPN being used.

upvoted 1 times

 **Prutser2** 1 year, 3 months ago

Selected Answer: D

Previously, when working with policy-based VPNs, you were limited to using the policy-based VPN gateway Basic SKU and could only connect to 1 on-premises VPN/firewall device. Now, using custom IPsec/IKE policy, you can use a route-based VPN gateway and connect to multiple policy-based VPN/firewall devices. To make a policy-based VPN connection using a route-based VPN gateway, configure the route-based VPN gateway to use prefix-based traffic selectors with the option "PolicyBasedTrafficSelectors".

as per <https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-connect-multiple-policybased-rm-ps>

upvoted 4 times

 **HasanHHH** 1 year, 3 months ago

Selected Answer: D

Previously, when working with policy-based VPNs, you were limited to using the policy-based VPN gateway Basic SKU and could only connect to 1 on-premises VPN/firewall device. Now, using custom IPsec/IKE policy, you can use a route-based VPN gateway and connect to multiple policy-based VPN/firewall devices. To make a policy-based VPN connection using a route-based VPN gateway, configure the route-based VPN gateway to use prefix-based traffic selectors with the option "PolicyBasedTrafficSelectors".

<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-connect-multiple-policybased-rm-ps>

upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT

-

Your on-premises network contains a VPN device.

You have an Azure subscription that contains a virtual network and a virtual network gateway.

You need to create a Site-to-Site VPN connection that has a custom cryptographic policy.

How should you complete the PowerShell script? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

```

...
$policy =  -IkeEncryption AES256 -IkeIntegrity SHA384 -DhGroup DHGroup24 -IpsecEncryption AES256
 New-AzIpssecPolicy
 New-AzIpssecTrafficSelectorPolicy
 New-AzServiceEndpointPolicy
 New-AzVpnClientIpssecPolicy
 -IpsecIntegrity SHA256 -PfsGroup None -SALifeTimeSeconds 14400 -SADataSizeKilobytes 102400000
...
 -Name $Connection16 -ResourceGroupName $RG1 -VirtualNetworkGateway1 $vnet1gw
 New-AzVirtualHub
 New-AzVirtualNetworkGateway
 New-AzVirtualNetworkGatewayConnection
 New-AzVirtualNetworkGatewayNatRule
 -LocalNetworkGateway2 $lng6 -Location $Location1 -ConnectionType IPsec -IpsecPolicies $policy -SharedKey 'AzureA1b2C3'

```

Answer Area

```

...
$policy =  New-AzIpssecPolicy
 New-AzIpssecTrafficSelectorPolicy
 New-AzServiceEndpointPolicy
 New-AzVpnClientIpssecPolicy
 -IpsecIntegrity SHA256 -PfsGroup None -SALifeTimeSeconds 14400 -SADataSizeKilobytes 102400000
...
 -Name $Connection16 -ResourceGroupName $RG1 -VirtualNetworkGateway1 $vnet1gw
 New-AzVirtualHub
 New-AzVirtualNetworkGateway
 New-AzVirtualNetworkGatewayConnection
 New-AzVirtualNetworkGatewayNatRule
 -LocalNetworkGateway2 $lng6 -Location $Location1 -ConnectionType IPsec -IpsecPolicies $policy -SharedKey 'AzureA1b2C3'

```

Correct Answer:

Goofer Highly Voted 1 year ago

1 = New-AzIpssecPolicy

<https://learn.microsoft.com/en-us/powershell/module/az.network/new-azipsecpolicy?view=azps-9.2.0>

2 = New-AzVirtualNetworkGatewayConnection

<https://learn.microsoft.com/en-us/powershell/module/az.network/new-azvirtualnetworkgatewayconnection?view=azps-9.2.0#example-1>

upvoted 13 times

Aunehwet79 1 year ago

Thanks - agreed

upvoted 1 times

_Cris Most Recent 4 months, 1 week ago

appears on exam, 19 Sept 2023

upvoted 3 times

SLGUY 5 months ago

Appeared on Exam 26 Aug 2023

upvoted 2 times

Billabongs 6 months, 2 weeks ago

Correct answers.

Confirm it by checking the syntax of each one here:

<https://learn.microsoft.com/en-us/powershell/module/az.network/new-azipsecpolicy?view=azps-10.1.0>
<https://learn.microsoft.com/en-us/powershell/module/az.network/new-azvirtualnetworkgatewayconnection?view=azps-10.1.0>
upvoted 1 times

🗨️ 👤 **Rajan395** 1 year ago
answer looks correct
upvoted 3 times

🗨️ 👤 **liono** 1 year ago
Given Answer is correct
upvoted 1 times

🗨️ 👤 **TJ001** 1 year ago
Given answers looks good
upvoted 1 times

🗨️ 👤 **Goofer** 1 year ago
<https://learn.microsoft.com/en-us/powershell/module/az.network/new-azvirtualnetworkgatewayconnection?view=azps-9.2.0#example-1>
upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT

-

You have an Azure virtual network and an on-premises datacenter that connect by using a Site-to-Site VPN tunnel.

You need to ensure that all traffic from the virtual network to the internet is routed through the datacenter.

How should you complete the PowerShell script to configure forced tunneling? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

```
$force1 = Get-AzLocalNetworkGateway
Get-AzNatGateway
Get-AzNetworkVirtualAppliance
Get-AzVirtualNetworkGateway -Name "HQ" -ResourceGroupName "ForcedTunneling"

$force2 = Get-AzVirtualNetworkGateway -Name "Gateway1" -ResourceGroupName "ForcedTunneling"
Set-AzVirtualNetworkGatewayConnection
Set-AzVirtualNetworkGatewayDefaultSite
Set-AzVirtualNetworkPeering
Set-AzVirtualNetworkSubnetConfig -GatewayDefaultSite $force1 -VirtualNetworkGateway $force2
```

Answer Area

```
$force1 = Get-AzLocalNetworkGateway
Get-AzNatGateway
Get-AzNetworkVirtualAppliance
Get-AzVirtualNetworkGateway -Name "HQ" -ResourceGroupName "ForcedTunneling"

$force2 = Get-AzVirtualNetworkGateway -Name "Gateway1" -ResourceGroupName "ForcedTunneling"
Set-AzVirtualNetworkGatewayConnection
Set-AzVirtualNetworkGatewayDefaultSite
Set-AzVirtualNetworkPeering
Set-AzVirtualNetworkSubnetConfig -GatewayDefaultSite $force1 -VirtualNetworkGateway $force2
```

Correct Answer:

 **DavidSapery** Highly Voted 1 year ago

Answer is correct. It's the exact example in <https://learn.microsoft.com/en-us/powershell/module/az.network/set-azvirtualnetworkgatewaydefaultsite?view=azps-9.2.0>

upvoted 11 times

 **Verytutos** Most Recent 4 months, 2 weeks ago

Appeared on Exam 05 Sep 2023

upvoted 2 times

 **dani999** 1 year ago

Correct answer :

```
$LocalGateway = Get-AzLocalNetworkGateway -Name "ContosoLocalGateway" -ResourceGroupName "ContosoResourceGroup"
```

```
$VirtualGateway = Get-AzVirtualNetworkGateway -Name "ContosoVirtualGateway"
```

```
Set-AzVirtualNetworkGatewayDefaultSite -GatewayDefaultSite $LocalGateway -VirtualNetworkGateway $VirtualGateway
```

upvoted 3 times

 **liono** 1 year ago

Correct. Local Network gateway for sending all internet traffic via on-prem DC

upvoted 2 times

You are planning an Azure deployment that will contain three virtual networks in the East US Azure region as shown in the following table.

Name	Description
Vnet1	Hub virtual network for shared services
Vnet2	Virtual machines for the IT department
Vnet3	Virtual machines for the research department

A Site-to-Site VPN will connect Vnet1 to your company's on-premises network.

You need to recommend a solution that ensures that the virtual machines on all the virtual networks can communicate with the on-premises network. The solution must minimize costs.

What should you recommend for Vnet2 and Vnet3?

- A. VNet-to-VNet VPN connections
- B. peering
- C. service endpoints
- D. route tables

Correct Answer: B

Community vote distribution


B (100%)

 **unciax** 5 months ago

Appeared on Exam 28 Aug 2023
upvoted 3 times

 **ronin201** 7 months, 1 week ago

Pls be noticed for peering in description of question must be at least 1 Azure VPN gateway and transitive routes for peerings, "vpn connection" can be built via NVA for example
upvoted 2 times

 **Rick0304** 8 months, 1 week ago

Peering is the correct answer!
upvoted 2 times

 **ESAJRR** 10 months, 1 week ago

Selected Answer: B

Peering is correct!
upvoted 1 times

 **mVic** 11 months, 3 weeks ago

Selected Answer: B

Peering is correct.
upvoted 4 times

 **Rajan395** 1 year ago

Correct. VNET peering is the answer.
upvoted 3 times

 **liono** 1 year ago

VNET Peering!
upvoted 1 times

 **krishnadasns96** 1 year ago

Selected Answer: B

Correct, Peering
upvoted 3 times

Your company has an office in New York.

The company has an Azure subscription that contains the virtual networks shown in the following table.

Name	Location
Vnet1	East US
Vnet2	North Europe
Vnet3	West US
Vnet4	West Europe

You need to connect the virtual networks to the office by using ExpressRoute. The solution must meet the following requirements:

- The connection must have up to 1 Gbps of bandwidth.
- The office must have access to all the virtual networks.
- Costs must be minimized.

How many ExpressRoute circuits should be provisioned, and which ExpressRoute SKU should you enable?

- A. one ExpressRoute Premium circuit
- B. two ExpressRoute Premium circuits
- C. four ExpressRoute Standard circuits
- D. one ExpressRoute Standard circuit

Correct Answer: A

Community vote distribution

A (100%)

 **sumandev** Highly Voted 1 year ago

Express Route Premium SKU provides ability to connect from on-premises to any of the Azure regions across the globe.
upvoted 8 times

 **SLGUY** Highly Voted 5 months ago

Appeared on Exam 26 Aug 2023
upvoted 6 times

 **OrangeSG** Most Recent 2 months, 3 weeks ago

Selected Answer: A

ExpressRoute SKU scope access:

- With a Local SKU ExpressRoute circuit, you can connect to resources in Azure regions in the same metro as the peering site.
- When you configure a Standard SKU ExpressRoute circuit, connectivity to Azure resources expand to all Azure regions in a geopolitical area.
- To allow your on-premises network to access resources globally across all Azure regions, you need to configure an ExpressRoute premium SKU circuit.

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-faqs#what-is-the-connectivity-scope-for-different-expressroute-circuit-skus>
upvoted 1 times

 **jakubklapka** 4 months ago

In exam Sep, 2023
upvoted 1 times

 **_Cris** 4 months, 1 week ago

appears on exam, 19 Sept 2023
upvoted 3 times

 **charrua86** 6 months ago

I understand that in terms of cost reduction we could configure a standard and peering between Vnets from different regions. BUT... ^^, the question has a "banana peel", because the statement communicates that "The office must have access to all the virtual networks.", and that changes everything, because only the Premium SKU has the ability to have full access to all services and resources of a geopolitical region other

than the ER peering. Something that helps us is the diagram and explanation in this link: <https://learn.microsoft.com/en-us/azure/expressroute/expressroute-faqs#what-is-the-connectivity-scope-for-different-expressroute-circuit-skus>

upvoted 3 times

🗨️ 👤 **Pratheeshp** 8 months, 3 weeks ago

4 x Local SKU ER is cheaper than 1 x Premium SKU ER. However since it is not an option, i would go with Answer A

upvoted 1 times

🗨️ 👤 **[Removed]** 9 months ago

Answer is A

If there was 2x standard ExpressRoute circuits available, that would be the most cost-effective answer.

upvoted 1 times

🗨️ 👤 **Rafael1984** 10 months ago

I think is D because you must be minimized cost

upvoted 1 times

🗨️ 👤 **ryswick7** 9 months, 4 weeks ago

ER Standard SKU doesn't allow you to connect across a geopolitical area. Hence, it is A

ref: <https://eighty20solutions.com.au/azure-expressroute/>

upvoted 4 times

🗨️ 👤 **jarz** 9 months, 1 week ago

This is a much better explanation compared to MS garble!

upvoted 1 times

🗨️ 👤 **ESAJRR** 10 months, 1 week ago

Selected Answer: A

An ExpressRoute Premium circuit is a higher-end offering for Azure ExpressRoute that provides increased resiliency and higher bandwidth capabilities compared to the standard ExpressRoute circuits.

upvoted 2 times

🗨️ 👤 **blah1234_5** 11 months, 1 week ago

Express route premium allows 4 circuits - <https://learn.microsoft.com/en-us/azure/expressroute/expressroute-faqs>

upvoted 1 times

🗨️ 👤 **SeanPan** 11 months, 3 weeks ago

A is correct

upvoted 2 times

🗨️ 👤 **dani999** 12 months ago

Selected Answer: A

A is correct

upvoted 4 times

🗨️ 👤 **liono** 1 year ago

One ExpressRoute circuit is required for the office with premium SKU

upvoted 1 times

🗨️ 👤 **DeepMoon** 1 year ago

If you need to connect to multiple geo's then you need express route premium sku. If it is only a single region, then you can use a standard sku.

upvoted 4 times

店铺: IT认证考试服务

店铺: IT认证考试服务

You have an Azure subscription that contains a virtual network.

You plan to deploy an Azure VPN gateway and 90 Site-to-Site VPN connections. The solution must meet the following requirements:

- Ensure that the Site-to-Site VPN connections remain available if an Azure datacenter fails.
- Minimize costs.

Which gateway SKU should you specify?

- A. VpnGw1AZ
- B. VpnGw2AZ
- C. VpnGw4AZ
- D. VpnGw5AZ

Correct Answer: C

Community vote distribution

C (100%)

 **DavidSapery** Highly Voted 1 year ago

Basic SKU supports max 10 S2S connections. SKUs 1, 2, and 3 support max 30 S2S connections. SKUs 4 & 5 support max 100 S2S. Of those 2, SKU4 minimizes the cost.

Answer C

upvoted 32 times

 **DeepMoon** 1 year ago

Ditto.

upvoted 1 times

 **ESAJRR** Highly Voted 10 months, 1 week ago

Selected Answer: C

VPN GTW SKU S2S V2V PS2 P2S THROUGHPUT BGP

Generation2 VpnGw2AZ Max. 30 Max. 128 Max. 500 1.25 Gbps Supported

Generation2 VpnGw3AZ Max. 30 Max. 128 Max. 1000 2.5 Gbps Supported Yes

Generation2 VpnGw4AZ Max. 100* Max. 128 Max. 5000 5 Gbps Supported

Generation2 VpnGw5AZ Max. 100* Max. 128 Max. 10000 10 Gbps Supported

upvoted 5 times

 **Pixan** Most Recent 2 months, 3 weeks ago

Hi Everyone!!

Join ET and get actual and valid study material: <https://examstopics.quora.com/> and pass your exam in first attempt. Study Smart Not Hard

upvoted 1 times

 **Lazylinux** 2 months, 3 weeks ago


Selected Answer: C

I C

as per

<https://azure.microsoft.com/en-au/pricing/details/vpn-gateway/>

upvoted 1 times

 **Rick0304** 8 months, 1 week ago

Generation2 VpnGw4AZ Max. 100* Max. 128 Max. 5000 5 Gbps Supported

upvoted 1 times

 **wooyourdaddy** 10 months, 3 weeks ago

Selected Answer: C

Answer can be derived from the table at:

<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings#benchmark>

In the columns marked "S2S/Vnet-to-Vnet Tunnels" and "Zone-Redundant".

All SKUs that end in AZ are zone-redundant, which covers the datacenter failure scenario, so all 4 answers are still valid at this point.

From the chart, we see the following max connections:

- A. VpnGw1AZ - Max 30 connections
- B. VpnGw2AZ - Max 30 connections
- C. VpnGw4AZ - Max 100 connections
- D. VpnGw5AZ - Max 100 connections

So while VpnGw4AZ and VpnGw5AZ can both handle the 90 connections, the final deciding criteria is cost. So C, VpnGw4AZ would be the correct answer.

upvoted 3 times

 **dani999** 12 months ago

Selected Answer: C

VpnGw4AZ Max. 100 s2s
Zone-redundant is support

upvoted 4 times

 **sserna** 1 year ago

En examen 20/01/2023

upvoted 2 times

 **liono** 1 year ago

Correct! SKU4

upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

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

Name	Type	Description
Vnet1	Virtual network	In the US East Azure region
LB1	Load balancer	Basic SKU
VM1	Virtual machine	Connected to Vnet1 Member of the backend pool of LB1
VM2	Virtual machine	Connected to Vnet1 Member of the backend pool of LB1

You create a virtual network named Vnet2 in the West US region.

You plan to enable peering between Vnet1 and Vnet2.

You need to ensure that the virtual machines connected to Vnet2 can connect to VM1 and VM2 via LB1.

What should you do?

- A. From the Peerings settings of Vnet2, set Traffic forwarded from remote virtual network to Allow.
- B. Change the Floating IP configurations of LB1.
- C. From the Peerings settings of Vnet1, set Traffic forwarded from remote virtual network to Allow.
- D. Change the SKU of LB1.

Correct Answer: D

Community vote distribution

D (100%)

 **DeepMoon** Highly Voted 1 year ago

Basic sku won't support cross-region traffic.

<https://learn.microsoft.com/en-us/azure/load-balancer/skus>

<https://learn.microsoft.com/en-us/azure/load-balancer/cross-region-overview>

upvoted 12 times

 **ConanBarb** 3 months, 3 weeks ago

you may be right, but it is not about cross-region load balancing as the vms of the backend pool (vm1 and vm2) both reside in the same vnet (vnet1)

cross-region load-balancing is used when you have backend pools in different regions, as can be read in the second link you provided

upvoted 4 times


 **daemon101** Highly Voted 6 months, 1 week ago

Vnet1 and Vnet2 reside in different regions.

Global VNet Peering now supports Standard Load Balancer. Previously, resources in one virtual network could not communicate with the front-end IP address of an internal load balancer over a globally peered connection.

<https://azure.microsoft.com/en-us/updates/global-vnet-peering-now-supports-standard-load-balancer/>

upvoted 5 times

 **ConanBarb** 3 months, 3 weeks ago

this, IMHO, is the right reasoning behind D - Standard SKU, not Basic

upvoted 1 times

 **ConanBarb** Most Recent 3 months, 3 weeks ago

Selected Answer: D

Global VNet Peering now supports Standard Load Balancer

upvoted 2 times

 **khanda** 9 months, 2 weeks ago

Selected Answer: D

Azure Standard Load Balancer supports cross-region load balancing.

upvoted 4 times

🗨️ **ESAJRR** 10 months, 1 week ago

Selected Answer: D

SCENARIO Standard Load Balancer Basic Load Balancer
Global VNet Peering Support Standard ILB is supported via Global VNet Peering Not supported
upvoted 2 times

🗨️ **liono** 1 year ago

Correct. Change SKU to Standard.
upvoted 3 times

🗨️ **Stevy_nash** 1 year ago

Selected Answer: D

we should also change the SKU of VMs' IP addresses to standard or remove them
upvoted 4 times

🗨️ **Neostar** 10 months, 2 weeks ago

The question didn't mention that the VMs have public IP addresses.
upvoted 1 times

🗨️ **TT924** 1 year ago

Selected Answer: D

Standard ILB is supported via Global VNet Peering

Standard ILB is supported via Global VNet Peering
upvoted 2 times

🗨️ **TT924** 1 year ago

<https://learn.microsoft.com/en-us/azure/load-balancer/skus#skus>
upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

DRAG DROP

-

Your on-premises network contains an Active Directory Domain Services (AD DS) domain named contoso.com that has an internal certification authority (CA).

You have an Azure subscription.

You deploy an Azure application gateway named AppGwy1 and perform the following actions:

- Configure an HTTP listener
- Associate a routing rule with the listener

You need to configure AppGwy1 to perform mutual authentication for requests from domain-joined computers to contoso.com.

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.

Actions

- From AppGwy1, create a frontend IP configuration.
- From AppGwy1, create an SSL profile.
- From AppGwy1, add an HTTP listener and associate the listener to the SSL profile.
- From AppGwy1, create a routing rule.
- From an on-premises computer, upload a certificate to AppGwy1.

Answer Area



Correct Answer:

- Answer Area**
- From AppGwy1, create a frontend IP configuration.
 - From AppGwy1, create an SSL profile.
 - From an on-premises computer, upload a certificate to AppGwy1.
 - From AppGwy1, add an HTTP listener and associate the listener to the SSL profile.

aklas Highly Voted 8 months, 2 weeks ago

Given answer and all the discussions are incorrect.

1. Create an SSL profile
2. Upload a certificate
3. Add an HTTP listener and associate the listener to the profile
4. Create a routing rule

The question says you already deploy an App Gateway and configure a listener and a routing rule. You can't deploy a listener without a frontend IP so that assumes you already have one.

Listener needs a routing rule otherwise it's useless.

upvoted 22 times

asdasd123123iu 6 months, 3 weeks ago

Agree. However must be some mistake in answer related with listener, because there is no possibility to sign SSL profile to HTTP, only HTTPS.

upvoted 3 times

DCor2022 5 months ago

Agree. In this link is added the routing rule: <https://learn.microsoft.com/en-us/azure/application-gateway/mutual-authentication-powershell>

upvoted 2 times

harshit101 Highly Voted 11 months, 3 weeks ago

what is going on here?

upvoted 7 times

Pixan Most Recent 2 months, 3 weeks ago

Hi Everyone!!

Join ET and get actual and valid study material: <https://examsttopics.quora.com/> and pass your exam in first attempt. Study Smart Not Hard

upvoted 1 times

🗨️ **Lazylinux** 2 months, 3 weeks ago

Based on the URL below and fact the existing listener is http and NOT https and fact the fronted IP is created part of the Listener creation the the correct answer is as per below and mentioned by others

1. Create an SSL profile
2. Upload a certificate
3. Add an HTTP listener and associate the listener to the profile
4. Create a routing rule

<https://learn.microsoft.com/en-us/azure/application-gateway/mutual-authentication-portal>

upvoted 1 times

🗨️ **ConanBarb** 3 months, 3 weeks ago

trick question. anything with HTTP (missing S as in HTTPS) is there to lure, disturb and distract.

Hence the option with HTTP listener is out of question, leaving:

- 1 create frontend ip
- 2 create ssl profile
- 3 upload cert
- 4 create routing rule

(even though some steps are taken in the beginning, nothing says that you must use that specific configuraton)

upvoted 1 times

🗨️ **voldemort123** 4 months ago

such discussions, much confusion

upvoted 1 times

🗨️ **_Cris** 4 months, 1 week ago

appears on exam, 19 Sept 2023

upvoted 1 times

🗨️ **SLGUY** 5 months ago

Appeared on Exam 26 Aug 2023

upvoted 3 times

🗨️ **pijp** 5 months ago

thanks for the feedback

upvoted 1 times

🗨️ **[Removed]** 9 months ago

The given answer is correct!

1. From AppGwy1, create a frontend IP configuration.
2. From AppGwy1, create an SSL profile.
3. From an on-premises computer, upload a certificate to AppGwy1.
4. From AppGwy1, add an HTTP listener and associate the listener to the SSL Profile.

<https://learn.microsoft.com/en-us/azure/application-gateway/mutual-authentication-portal>

upvoted 4 times

🗨️ **khanda** 9 months, 2 weeks ago

Answer is correct: <https://learn.microsoft.com/en-us/azure/application-gateway/mutual-authentication-portal>

upvoted 1 times

🗨️ **rj_289** 10 months ago

Given answer is correct!

upvoted 2 times

🗨️ **Aziza_Adam** 11 months, 2 weeks ago

The given answer is correct

upvoted 3 times

🗨️ **kienvu** 11 months, 2 weeks ago

1. From AppGwy1, create a frontend IP configuration
2. From AppGwy1, create a routing rule
3. From an on-premises computer, upload a certificate to AppGwy1
4. From AppGwy1, add an HTTP listener and associate the listener to the SSL Profile

upvoted 6 times

🗨️ **omgMerrick** 11 months, 1 week ago

This is incorrect! There is no need to create a routing rule.

The given answer is correct.

<https://learn.microsoft.com/en-us/azure/application-gateway/mutual-authentication-portal>

upvoted 7 times

🗨️ **TedSund69543** 11 months, 2 weeks ago

<https://learn.microsoft.com/en-us/azure/application-gateway/mutual-authentication-portal>

店铺: IT认证考试服务

店铺: IT认证考试服务

upvoted 5 times

 **tryhard97** 11 months, 3 weeks ago

help answer plz

upvoted 1 times

店铺：IT认证考试服务

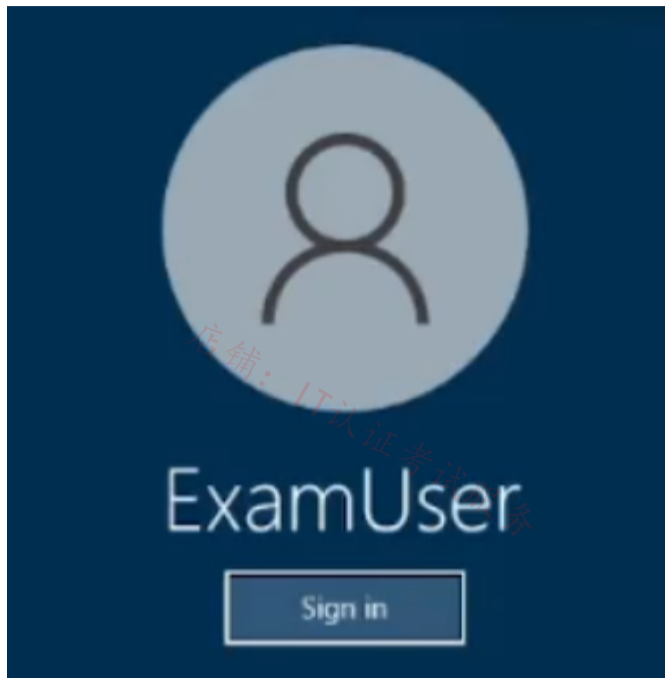
店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You are preparing to connect your on-premises network to VNET4 by using a Site-to-Site VPN. The on-premises endpoint of the VPN will be created on a firewall named Firewall1.

The on-premises network has the following configuration:

- internal address range: 10.10.0.0/16
- Firewall1 internal IP address: 10.10.1.1
- Firewall public IP address: 131.107.50.60

BGP is NOT used.

You need to create the object that will provide the IP addressing configuration of the on-premises network to the Site-to-Site VPN. You do NOT need to create a virtual network gateway to complete this task.

To complete this task, sign in to the Azure portal.

Correct Answer:

Create a site-to-site VPN connection in the Azure portal
We only create a local network gateway

The local network gateway is a specific object that represents your on-premises location (the site) for routing purposes. You give the site a name by which Azure can refer to it, then specify the IP address of the on-premises VPN device to which you'll create a connection. You also specify the IP address prefixes that will be routed through the VPN gateway to the VPN device. The address prefixes you specify are the prefixes located on your on-premises network. If your on-premises network changes or you need to change the public IP address for the VPN device, you can easily update the values later.

Step 1: From the Azure portal, in Search resources, services, and docs (G+) type local network gateway. Locate local network gateway under Marketplace in the search results and select it. This opens the Create local network gateway page.

Step 2: On the Create local network gateway page, on the Basics tab, specify the values for your local network gateway.

* Select Endpoint type: IP address

* Endpoint: Enter 131.107.50.60 (The Firewall public IP address)

(IP address: If you have a static public IP address allocated from your Internet service provider for your VPN device, select the IP address option and fill in the IP address as shown in the example. This is the public IP address of the VPN device that you want Azure VPN gateway to connect to. If you don't have the IP address right now, you can use the values shown in the example, but you'll need to go back and replace your placeholder IP address with the public IP address of your VPN device. Otherwise, Azure won't be able to connect.)

* Address Space: Enter 10.10.0.0/16 (The internal address range)

Select the endpoint type for the on-premises VPN device - IP address or FQDN (Fully Qualified Domain Name).

IP address: If you have a static public IP address allocated from your Internet service provider for your VPN device.

[Home](#) >

Create local network gateway

Basics Advanced Review + create

A local network gateway is a specific object that represents an on-premises location (the site) for routing purposes. [Learn more.](#)

Project details

Subscription * Content Development

Resource group * TestRG1
[Create new](#)

Instance details

Region * East US

Name * Site1

Endpoint IP address FQDN

IP address * 4.3.2.1

Address space

10.0.0.0/24

20.0.0.0/24

[Review + create](#)

[Previous](#)

[Next : Advanced >](#)

Step 3: On the Advanced tab, you can configure BGP settings if needed. Skip this.

Step 4: When you have finished specifying the values, select Review + create at the bottom of the page to validate the page.

Step 5: Select Create to create the local network gateway object.

Reference:

<https://learn.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal>

MrBlueSky Highly Voted 10 months ago

Given answer is correct, you would need to create a Local Network Gateway, which will represent the on-prem IP address upvoted 5 times

Pixan Most Recent 2 months, 3 weeks ago

Hi Everyone!!
Join ET and get actual and valid study material: <https://examstopics.quora.com/> and pass your exam in first attempt. Study Smart Not Hard upvoted 1 times

Lazylinux 2 months, 3 weeks ago

Yep Given answer is correct

upvoted 1 times

 **jakubklapka** 4 months ago

In exam Sep, 2023

upvoted 2 times

店铺：IT认证考试服务

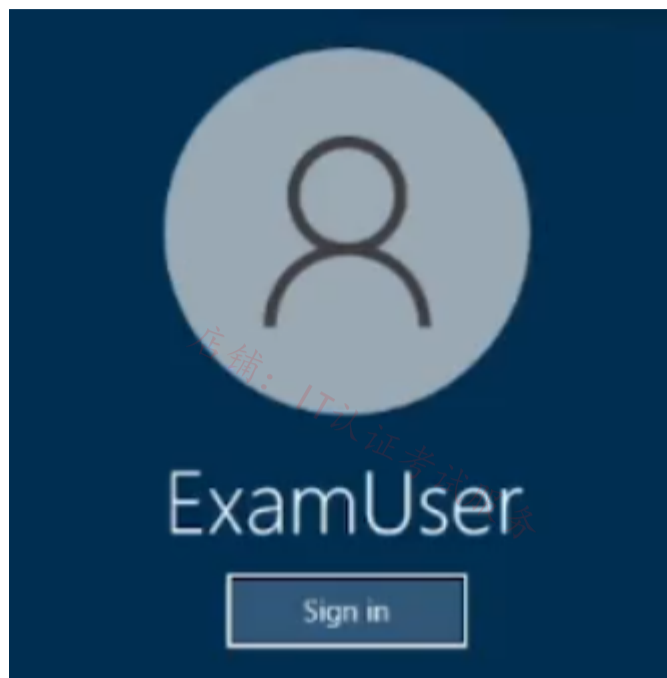
店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You need to ensure that hosts on VNET2 can access hosts on both VNET1 and VNET3. The solution must prevent hosts on VNET1 and VNET3 from communicating through VNET2.

To complete this task, sign in to the Azure portal.

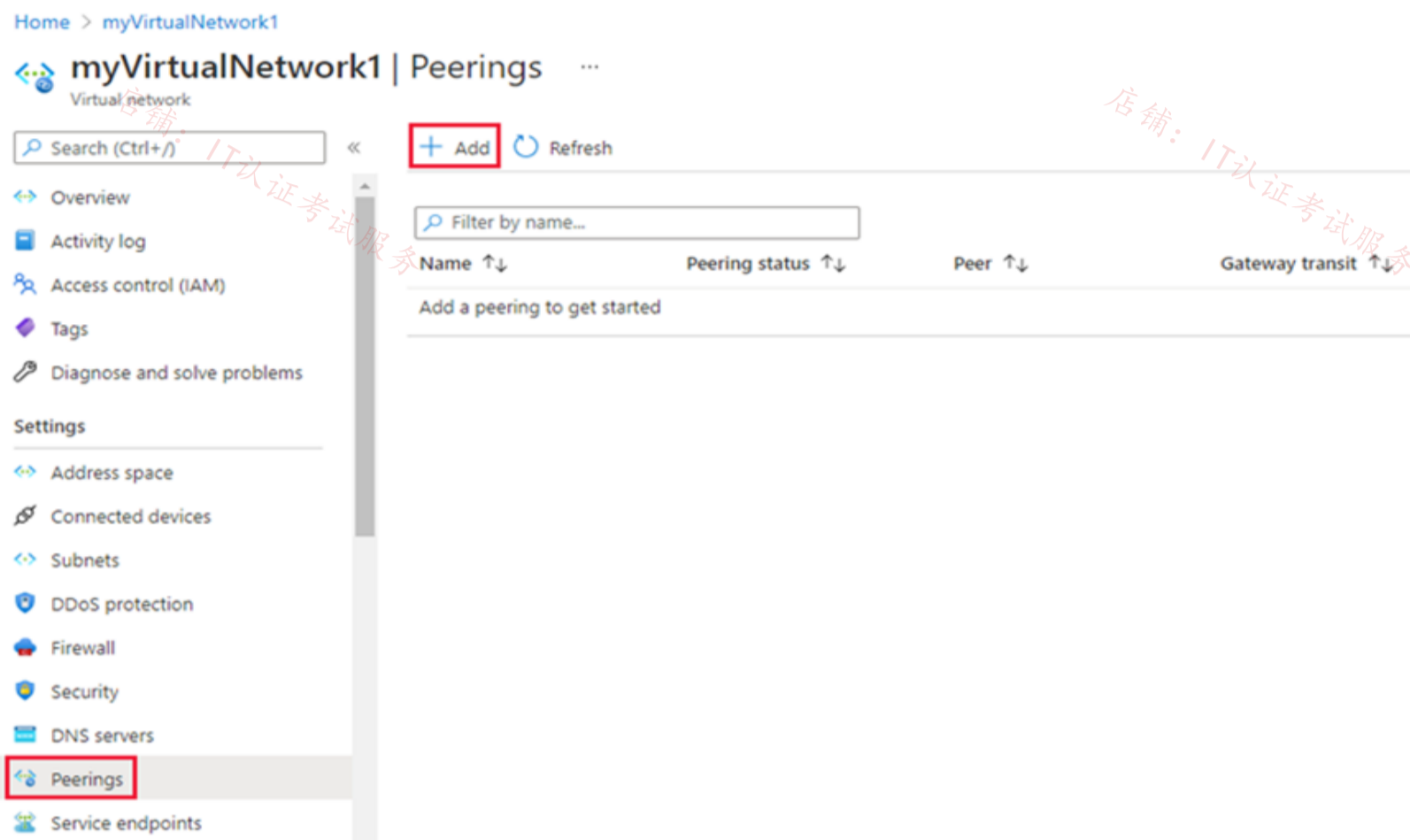
Correct Answer:

We use VNET2 as hub, and VNET1 and VNET3 as spokes.
The spoke virtual networks peer with the hub and can be used to isolate workloads.
A hub-spoke topology can be used without a gateway if you don't need cross-premises network connectivity.

Peer virtual networks

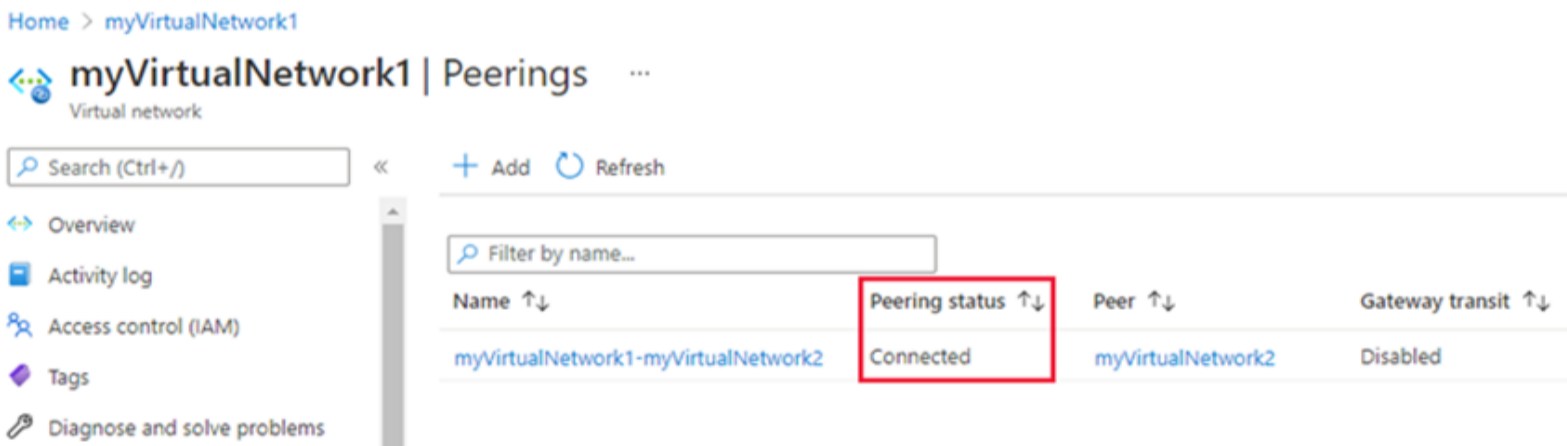
Step 1: In the search box at the top of the Azure portal, look for VNET2. When VNET2 appears in the search results, select it.

Step 2: Under Settings, select Peerings, and then select + Add, as shown in the following picture:



Step 3: Enter or select the following information, accept the defaults for the remaining settings, and then select Add.
* Virtual network - Select VNET1 for the name of the remote virtual network.

Step 4: In the Peerings page, the Peering status is Connected, as shown in the following picture:



Step 5: Repeat steps 1 to 4, but in Step 3 add VNET3 instead of VNET1.

Reference:

<https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke>

jakubklapka 4 months ago

In exam Sep, 2023
upvoted 2 times

DGUI 6 months, 3 weeks ago

Hello, ca?n you specify the url for this lab please
upvoted 1 times

Lazylinux 7 months ago

The answer is correct but should be clearer..YES it is kind of HUB-Spoke setup mainly using vNET peering, you configure it from vNET2 and allow traffic both ways i.e. i.e. vms on both peered vNET2 and vNET1 can communicate with each other or you could just configure to ONLY allow communication for vms in vNET2 to vNET1 but not otherway round. Now to prevent vNET1 and vNET3 from accessing other resources such as internet or vms in vNET1 able to communicate with vms in vNET3 is to DISABLE GATEWAY TRANSIT.

I believe some inform is missing in this question like address space, if vNETs in same region or not and in same subscription of not but assume simple scenario it is easier to create peering (Global reach Peering is also possible) than S2S for vNETS. For me when not routes or different Geo i would use S2S for vNETs

See my next comments

upvoted 1 times

  **Lazylinux** 7 months ago

Following on

Here snippet for S2S for vNETs from MS

following reasons:

****Cross region geo-redundancy and geo-presence**

You can set up your own geo-replication or synchronization with secure connectivity without going over Internet-facing endpoints.

With Azure Traffic Manager and Load Balancer, you can set up highly available workload with geo-redundancy across multiple Azure regions.



One important example is to set up SQL Always On with Availability Groups spreading across multiple Azure regions.

****Regional multi-tier applications with isolation or administrative boundary**

Within the same region, you can set up multi-tier applications with multiple virtual networks connected together due to isolation or administrative requirements.

<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-vnet-vnet-rm-ps>

upvoted 1 times

  **thor04** 7 months, 2 weeks ago

Do we need to create the connection for VPN site-to-site ?

upvoted 1 times

  **Lazylinux** 7 months ago

No we dont, see my comments

upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT

-

You have an Azure subscription that contains a virtual network gateway named VNetGwy1. VNetGwy1 has a public IP address of 20.25.32.214.

You need to query the health probe of VNetGwy1.

How should you complete the URI? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

://20.25.32.214: /healthprobe

http	80
https	443
snmp	8081

Answer Area**Correct Answer:**

://20.25.32.214: /healthprobe

http	80
https	443
snmp	8081

 **ckyap** Highly Voted 9 months, 3 weeks ago

Correct. See <https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-troubleshoot-site-to-site-cannot-connect#step-7-verify-the-azure-gateway-health-probe>

upvoted 9 times

 **[Removed]** Most Recent 9 months ago

It was on 24/04/2023. The answer is correct.

Active/Passive: <https://<YourVirtualNetworkGatewayIP>:8081/healthprobe>

Active/Active: <https://<YourVirtualNetworkGatewayIP2>:8083/healthprobe> (Second IP)

<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-troubleshoot-site-to-site-cannot-connect#step-7-verify-the-azure-gateway-health-probe>

upvoted 4 times

HOTSPOT

-

You have an on-premises datacenter.

You have an Azure subscription that contains 10 virtual machines and a virtual network named VNet1 in the East US Azure region. The virtual machines are connected to VNet1 and replicate across three availability zones.

You need to connect the datacenter to VNet1 by using ExpressRoute. The solution must meet the following requirements:

- Maintain connectivity to the virtual machines if two availability zones fail.
- Support 1000-Mbps connections.
- Minimize costs.

What should you include in the solution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Minimum number of ExpressRoute circuits:

- One ExpressRoute Standard circuit
- One ExpressRoute Premium circuit
- Two ExpressRoute Standard circuits
- Two ExpressRoute Premium circuits
- Three ExpressRoute Standard circuits
- Three ExpressRoute Premium circuits

Minimum number of ExpressRoute gateways:

- One ExpressRoute gateway of the ErGw1AZ SKU
- One ExpressRoute gateway of the High performance SKU
- Two ExpressRoute gateway of the ErGw1AZ SKU
- Two ExpressRoute gateway of the High performance SKU
- Three ExpressRoute gateway of the ErGw1AZ SKU
- Three ExpressRoute gateway of the High performance SKU

Answer Area

Minimum number of ExpressRoute circuits:

Minimum number of ExpressRoute gateways:

Correct Answer:

- Three ExpressRoute Standard circuits
- Two ExpressRoute gateway of the ErGw1AZ SKU

 **bakamon** Highly Voted 8 months ago

Answer :

--> One ExpressRoute Standard circuit

--> One ExpressRoute gateway of the ErGw1AZ SKU

upvoted 20 times

 **CiscoTerminator** 5 months, 4 weeks ago

You need zone-redundant gateways so 1 Standard circuit won't do.

upvoted 3 times

 **thekhijir** 1 week, 5 days ago

When deploying an ErGw1AZ, it is possible to define its zone availability as "Zone-Redundant"?

upvoted 2 times

 **charrua86** Highly Voted 6 months ago

As I researched here in these 3 reference documentations:

1. <https://learn.microsoft.com/en-us/azure/reliability/availability-zones-overview>;
2. <https://learn.microsoft.com/en-us/azure/vpn-gateway/create-zone-redundant-vnet-gateway>
3. <https://learn.microsoft.com/en-us/azure/expressroute/expressroute-about-virtual-network-gateways#gwsku>

When deploying an ErGw1AZ, it is possible to define its zone availability as "Zone-Redundant", in addition it is also essential that the ip used by the ER Gateway be "Standard", because at the time of provisioning this ip will become redundant between the availability zones. Regarding the ER Circuit, it can be "Local", but in this scenario it would be unlimited and more expensive than the "Standard" Limited in 1Gbps. In my opinion the best answer would be:


1. One ExpressRoute Standard circuit
2. One ExpressRoute gateway of the ErGw1AZ SKU

upvoted 16 times

 **erreyesarroyo** Most Recent 1 week ago

Guess one and one....

upvoted 1 times

 **MCCC454** 1 week ago

These kind of questions really baffle my mind. How we suppose to memorize all the sku's and differences?

upvoted 3 times

 **Redrum702** 1 week, 6 days ago

ExpressRoute Premium Circuits offer Zone-redundant Gateway (ZRG) functionality, which means that even if one Availability Zone fails, traffic can be redirected to another Zone without interruption. However, if two Availability Zones fail simultaneously, there might be an impact on connectivity.

Answer:

- One ExressRoute Premium circuit
- One ExpressRoute gateway ErGw1AZ SKU

upvoted 1 times

 **_Cris** 4 months, 1 week ago

appears on exam, 19 Sept 2023

upvoted 3 times

 **mabalon** 5 months ago

For the Gateway, you need only one, the new SKU are zone redundant:

"you can deploy your gateways with zone-redundancy. This means that all instances of the gateways will be deployed across Azure Availability Zones"

<https://learn.microsoft.com/en-us/azure/vpn-gateway/create-zone-redundant-vnet-gateway#what-will-change-when-i-deploy-these-new-skus>

upvoted 2 times

 **SLGUY** 5 months ago

Appeared on Exam 26 Aug 2023

upvoted 4 times

 **aklas** 8 months, 2 weeks ago

For number of GW's, correct answer should be 1 ErGw1AZ:

"For a VPN gateway, the two gateway instances will be deployed in any 2 out of these three zones to provide zone-redundancy. For an ExpressRoute gateway, since there can be more than two instances, the gateway can span across all the three zones."

<https://learn.microsoft.com/en-us/azure/vpn-gateway/about-zone-redundant-vnet-gateways#pipzrg>

upvoted 4 times

 **[Removed]** 9 months ago

1. Maintain connectivity to the virtual machines if two availability zones fail - Needs two VPN gateways to tolerate two AV zones.

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-about-virtual-network-gateways#zrgw>


2. Support 1000-Mbps connections - Standard/ERGw1Az supports up to 1Gbps and support across geopolitical areas, which is more than enough.

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-about-virtual-network-gateways#testing-conditions>

Therefore, the most cost-effective solution is;


- One ExpressRoute Standard circuit
- 2x ExpressRoute gateways (ErGw1AZ)

upvoted 5 times

 **headspace** 8 months, 2 weeks ago

It never mentioned a VPN connection, so I'm thinking 1 ER Standard, SKU 1 ErGw1AZ

upvoted 2 times

 **henryhung** 9 months, 3 weeks ago

Update: Answer from ChatGPT Plus(GPT 4.0)

To meet the requirements, you need to have the following:



Minimum number of ExpressRoute circuits:
Two ExpressRoute Standard circuits

This is because ExpressRoute Standard circuits do not provide connectivity across multiple regions, and you need to maintain connectivity if two availability zones fail. Therefore, you will need two ExpressRoute Standard circuits to ensure connectivity in case of failure.

Minimum number of ExpressRoute gateways:
Two ExpressRoute gateways of the ErGw1AZ SKU



The ErGw1AZ SKU supports up to 2,000 Mbps, which meets the 1,000 Mbps requirement, and it also provides Zone Redundant Gateway for increased reliability. Having two ExpressRoute gateways of the ErGw1AZ SKU ensures that connectivity is maintained even if two availability zones fail, meeting the requirement.

upvoted 1 times

  **zman_83** 6 months ago

Stop using Chat GPT for this, it doesn't work that way...please!!!
It fails delux...!

upvoted 7 times

  **[Removed]** 9 months, 2 weeks ago



I don't think ChatGPT is correct here.

First of all, connectivity across multiple regions doesn't matter in terms of availability zones because they are usually located in the same region. This would only matter for services with cross-regional replication such as storage accounts. Not entirely sure if two circuits are necessary - I think one would be enough.

For ExpressRoute gateways you should only need one because it spans across three availability zones if you configure the public IP with standard SKU and zone redundancy. Regular VPN Gateways only span two availability zones. In that case you would probably need two Gateways.

<https://learn.microsoft.com/en-us/azure/vpn-gateway/about-zone-redundant-vnet-gateways#pipzrg>

upvoted 4 times

  **henryhung** 9 months, 3 weeks ago

Answer from ChatGPT:

To maintain connectivity to the virtual machines if two availability zones fail, at least two ExpressRoute circuits are required for redundancy, one of which must be in a different availability zone.

For supporting a 1000-Mbps connection, ExpressRoute Premium is required. Therefore, the minimum number of circuits needed is two ExpressRoute Premium circuits.

Regarding the minimum number of ExpressRoute gateways, at least one ExpressRoute gateway is required for each circuit. Therefore, two ExpressRoute gateways are required, one in each availability zone.



Since the solution must minimize costs, the recommended SKU for the ExpressRoute gateway is the ErGw1AZ SKU, which is less expensive than the High performance SKU.

Therefore, the answers are:

Minimum number of ExpressRoute circuits: Two ExpressRoute Premium circuits

Minimum number of ExpressRoute gateways: Two ExpressRoute gateways of the ErGw1AZ SKU

upvoted 1 times

  **henryhung** 9 months, 3 weeks ago

Please ignore this ChatGPT 3.5 answer.

upvoted 6 times

  **_fvt** 9 months, 4 weeks ago

Express Route Zone redundant gateways can span to three AZ.

I am not sure there, but I think the active ER GW only use the circuit so even if it would have been better to have one primary and one secondary circuit, you may have one ExpressRoute Standard circuit only, with 3 instances of Zone Redundant ER GW.

<https://learn.microsoft.com/en-us/azure/vpn-gateway/about-zone-redundant-vnet-gateways>

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-about-virtual-network-gateways#gwsku>

Zone-redundant gateways

When you create a public IP address using the Standard public IP SKU without specifying a zone, the behavior differs depending on whether the gateway is a VPN gateway, or an ExpressRoute gateway.

For a VPN gateway, the two gateway instances will be deployed in any 2 out of these three zones to provide zone-redundancy.

For an ExpressRoute gateway, since there can be more than two instances, the gateway can span across all the three zones.

upvoted 1 times

  **_fvt** 9 months, 4 weeks ago

I tested in lab, deployed an ErGw1AZ in a Region (France Central) with 3AZ and I will have 3 Instances of the Public IP and ER Gateway.
So the Answer is:

- one ErGw1AZ
- one Circuit.

upvoted 18 times

🗨️ 👤 **jarz** 9 months, 1 week ago

Standard or Premium ER CCT?
upvoted 2 times

🗨️ 👤 **JohnnyChimpo** 9 months, 1 week ago

Standard. Premium is viable when it spans over several regions and that is not the case here
upvoted 2 times

🗨️ 👤 **khanda** 9 months, 2 weeks ago

This correct.
upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

You have an Azure subscription that contains a virtual network named VNet1 and the virtual machines shown in the following table.

Name	IP address	Hosted application protocol
VM1	10.1.1.11	HTTPS (TCP port 443)
VM2	10.1.1.21	SMTP (TCP port 25)
VM3	10.1.1.31	SFTP (TCP port 22)

All the virtual machines are connected to Vnet1.

You need to ensure that the applications hosted on the virtual machines can be accessed from the internet. The solution must ensure that the virtual machines share a single public IP address.

What should you use?

- A. an internal load balancer
- B. Azure Application Gateway
- C. a NAT gateway
- D. a public load balancer

Correct Answer: D

Community vote distribution

D (100%)

 **KeZhai** 2 weeks, 4 days ago

Azure NAT Gateway is a fully managed and highly resilient Network Address Translation (NAT) service. You can use Azure NAT Gateway to let all instances in a private subnet connect outbound to the internet while remaining fully private. Unsolicited inbound connections from the internet aren't permitted through a NAT gateway. Only packets arriving as response packets to an outbound connection can pass through a NAT gateway.

upvoted 1 times

 **toto74500** 3 weeks, 4 days ago

Selected Answer: D

LB can route non HTTP traffic instead of App Gw that HTTP based.

Nat Gw handle outbound traffic .

Answer is D LB

upvoted 1 times

 **Pixan** 2 months, 3 weeks ago

Hi Everyone!!

Join ET and get actual and valid study material: <https://examstopics.quora.com/> and pass your exam in first attempt. Study Smart Not Hard

upvoted 1 times

 **Lazylinux** 2 months, 3 weeks ago

Selected Answer: D

D is correct, would almost think NAT Gateway but it allows only Internet traffic that is in RESPONSE to traffic originated from Azure vNets i.e. in response ONLY

upvoted 1 times

 **VinceWho** 3 months, 3 weeks ago


D seems the best answer, although I have been given to understand that traffic on port 25 is not allowed at all in Azure (because they want you to use Exchange online, obviously)

upvoted 1 times

 **Ben_88** 7 months, 2 weeks ago

why not a nat gateway ?

upvoted 1 times

 **Ben_88** 7 months, 2 weeks ago

bad idea , just realized that nat gateway can only handle outbound traffic . so it can only be D

upvoted 6 times

 **Oklama** 8 months, 1 week ago

Selected Answer: D

Given answer is correct
upvoted 3 times

🗨️ **james** 8 months, 1 week ago

Why not Azure Application Gateway with different listeners?
upvoted 1 times

🗨️ **GiorgioLDN** 7 months, 1 week ago

Because Application Gateway is a layer 7 load balancer, which means it works only with web traffic (HTTP, HTTPS)!
upvoted 11 times

🗨️ **DCor2022** 5 months ago

Agree, see Notes in: <https://learn.microsoft.com/en-us/azure/application-gateway/overview>
upvoted 2 times

🗨️ **ubdubdoo** 8 months, 2 weeks ago

an Azure NAT Gateway is a dedicated network appliance that provides outbound NAT functionality for virtual networks in Azure. It allows resources within a virtual network to access the internet or other resources outside of the virtual network using a single or a pool of public IP addresses.
upvoted 2 times

🗨️ **crypto700** 8 months, 3 weeks ago

Selected Answer: D

Given answer is correct
upvoted 4 times

店铺: IT认证考试服务

店铺: IT认证考试服务

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a financial company that has a main datacenter in Boston and 20 branch offices across the United States. Users have Android, iOS, and Windows 10 devices.

Existing Environment -

Hybrid Environment -

The on-premises network contains an Active Directory forest named litwareinc.com that syncs to an Azure Active Directory (Azure AD) tenant named litwareinc.com by using Azure AD Connect.

All offices connect to a virtual network named Vnet1 by using a Site-to-Site VPN connection.

Azure Environment -

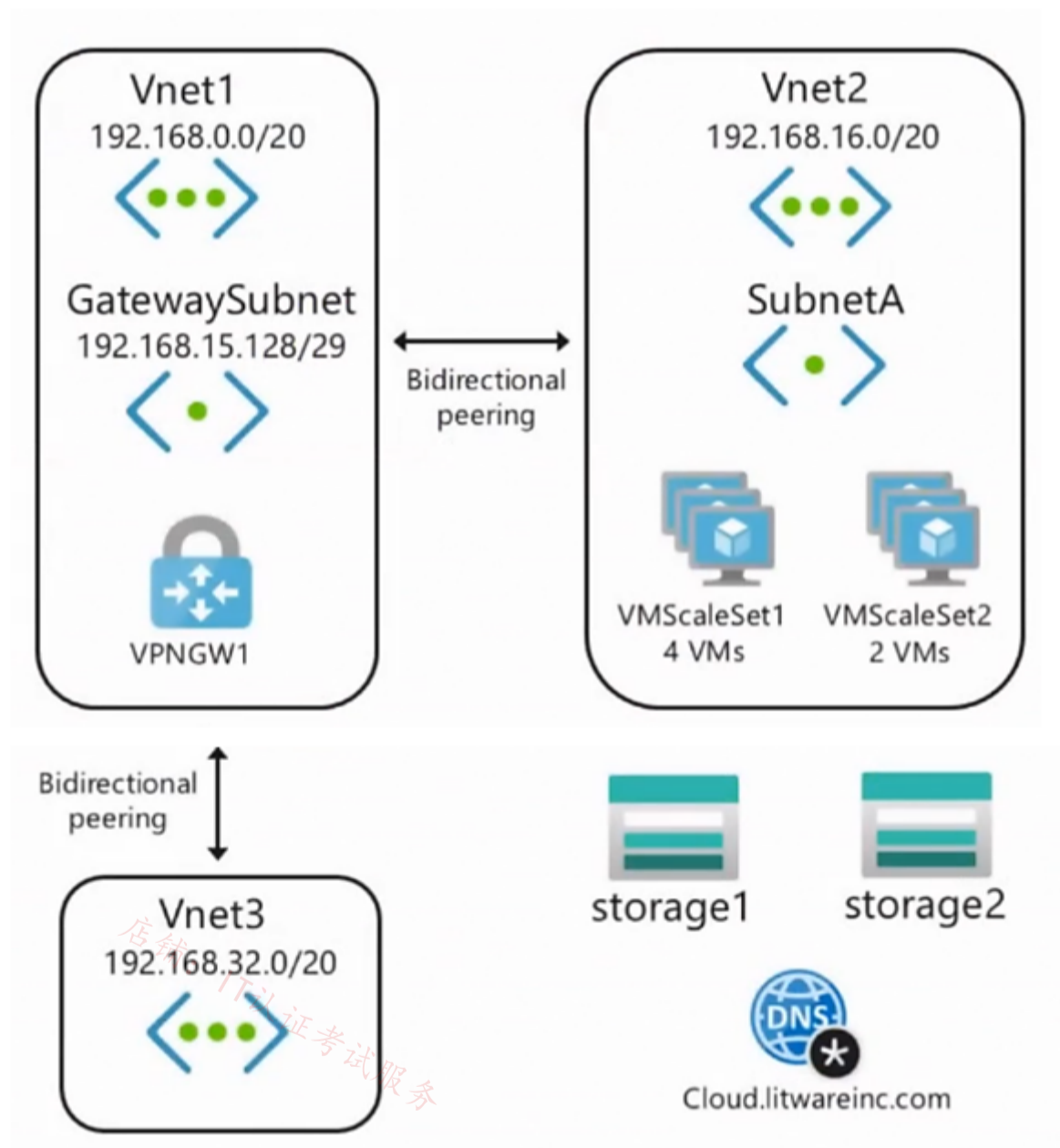
Litware has an Azure subscription named Sub1 that is linked to the litwareinc.com Azure AD tenant. Sub1 contains resources in the East US Azure region as shown in the following table.

Name	Type	Description
Vnet1	Virtual network	Uses an IP address space of 192.168.0.0/20
GatewaySubnet	Virtual network subnet	Located in Vnet1 and uses an IP address space of 192.168.15.128/29
VPNGW1	VPN gateway	Deployed to Vnet1
Vnet2	Virtual network	Uses an IP address space of 192.168.16.0/20
SubnetA	Virtual network subnet	Located in Vnet2 and uses an IP address space of 192.168.16.0/24
Vnet3	Virtual network	Uses an IP address space of 192.168.32.0/20
cloud.litwareinc.com	Private DNS zone	None
VMScaleSet1	Virtual machine scale set	Contains four virtual machines deployed to SubnetA
VMScaleSet2	Virtual machine scale set	Contains two virtual machines deployed to SubnetA
storage1	Storage account	Has the public endpoint blocked
storage2	Storage account	Has the public endpoint blocked

A diagram of the resource in the East US Azure region is shown in the Azure Network Diagram exhibit.

There is bidirectional peering between Vnet1 and Vnet2. There is bidirectional peering between Vnet1 and Vnet3. Currently, Vnet2 and Vnet3 cannot communicate directly.

Azure Network Diagram -



Requirements -

Business Requirements -

Litware wants to minimize costs whenever possible, as long as all other requirements are met.

Virtual Networking Requirements -

Litware identifies the following virtual networking requirements:

- Direct the default route of 0.0.0.0/0 on Vnet2 and Vnet3 to the Boston datacenter over an ExpressRoute circuit.
- Ensure that the records in the cloud.litwareinc.com can be resolved from the on-premises locations.
- Automatically register the DNS names of Azure virtual machines to the cloud.litwareinc.com zone.
- Minimize the size of the subnets allocated to platform-managed services.
- Allow traffic from VMScaleSet1 to VMScaleSet2 on the TCP port 443 only.

Hybrid Networking Requirements -

Litware identifies the following hybrid networking requirements:

- Users must be able to connect to Vnet1 by using a Point-to-Site (P2S) VPN when working remotely. Connections must be authenticated by Azure AD.
- Latency of the traffic between the Boston datacenter and all the virtual networks must be minimized.
- The Boston datacenter must connect to the Azure virtual networks by using an ExpressRoute FastPath connection.
- Traffic between Vnet2 and Vnet3 must be routed through Vnet1.

PaaS Networking Requirements -

Litware identifies the following networking requirements for platform as a service (PaaS):

- The storage1 account must be accessible from all on-premises locations without exposing the public endpoint of storage1.
- The storage2 account must be accessible from Vnet2 and Vnet3 without exposing the public endpoint of storage2.

You need to connect Vnet2 and Vnet3. The solution must meet the virtual networking requirements and the business requirements.

Which two actions should you include in the solution? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. On the peering from Vnet1, select Allow for Traffic forwarded from remote virtual network.
- B. On the peerings from Vnet2 and Vnet3, select Allow for Traffic forwarded from remote virtual network.
- C. On the peering from Vnet1, select Use the remote virtual network's gateway or Route Server.
- D. On the peering from Vnet1, select Allow for Traffic to remote virtual network.
- E. On the peerings from Vnet2 and Vnet3, select Use the remote virtual network's gateway or Route Server.

Correct Answer: AE

Community vote distribution

BE (89%)

11%

 **azure_dori** Highly Voted 5 months, 2 weeks ago

Selected Answer: BE

Here are my 2 cents about this question:

1. The correct answer is: BE.

2. The justification is as follows:

- E IS obviously an answer because without it the requirements cannot be met.

- D is NOT an answer, because: The case study says that "There is bidirectional peering between Vnet1 and Vnet2. There is bidirectional peering between Vnet1 and Vnet3." This means that "Traffic to remote virtual network" is already allowed for Vnet1<...>Vnet2 and Vnet1<...>.

- C is a total nonsense.

- B IS an answer, because Vnet1 contains the VPN gateway that forwards the traffic between Vnet2 and Vnet3.

- A is NOT an answer, because Vnet2 and Vnet3 don't have VPN gateways so they cannot forward traffic to Vnet1.

Documentation: <https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering?tabs=peering-portal#create-a-peering>

<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways>

upvoted 7 times

 **SKachroo** Most Recent 1 month, 1 week ago

Selected Answer: AE

A: will allow vnet 2 and 3 to send data to vent 1

upvoted 1 times

 **Lazylinux** 2 months, 3 weeks ago

Selected Answer: BE

Agreed BE

What we need is traffic to go from vnet2&3 to on-prem and come from on-prem to vnet2&3 hence

B address allowing traffic from on-prem to reach vnet 2 and 3

E address allowing traffic to flow from vnet2&3 to on-prem

upvoted 1 times

 **hogehegohoge** 2 months, 4 weeks ago

I think this answer is correct. Because vnet1 transfer the traffic from vnet2 and vnet3 to Datacenter.

upvoted 2 times

 **bp_a_user** 4 months ago

The correct answer ist DE.

" Select Allow gateway in 'vnet-1' to forward traffic to 'vnet-2' if you want vnet-2 to receive traffic from vnet-1's gateway/Route Server. vnet-1 must contain a gateway in order for this option to be enabled."

" Select Enable 'vnet-1' to use 'vnet-2' remote gateway if you want vnet-1 to use vnet-2's gateway or Route Server. vnet-1 can only use a remote gateway or Route Server from one peering connection. vnet-2 has to have a gateway or Route Server in order for you to select this option. "

from here

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering?tabs=peering-portal>

upvoted 2 times

 **bp_a_user** 4 months ago

...and here a concrete example:


<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-peering-gateway-transit>

upvoted 1 times

 **bp_a_user** 4 months ago

BE i mean

upvoted 3 times

 **bp_a_user** 4 months, 1 week ago


we have here a hub-spoke topology: why is no NAV/Firewall required?

upvoted 2 times

 **bp_a_user** 4 months, 1 week ago

I mean NVA

upvoted 2 times

 **derp12352** 5 months, 2 weeks ago

BE

E is obvious. Vnet 2 and 3 need to use Vnet 1's virtual network gateway.

A would allow Vnet1 to receive traffic from Vnet2 & Vnet3 that don't originate from those VNETs. Review the tooltips on the vnet peering page. It would read "This setting allows forwarded traffic from Vnet2/Vnet3 (traffic not originating from Vnet2/Vnet3) into Vnet1." You don't need that.

What you do need to allow is the other way so we need B. Vnet2 and Vnet3 need to allow on premise traffic that comes over the peering connection from Vnet1.

upvoted 3 times

HOTSPOT

-

You have an Azure subscription.

You plan to use Azure Virtual WAN.

You need to deploy a virtual WAN hub that meets the following requirements:

- Supports 4 Gbps of Site-to-Site (S2S) VPN traffic
- Supports 8 Gbps of ExpressRoute traffic
- Minimizes costs

How many scale units should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

For the S2S VPN gateway:

▼
2
4
8
16

For the ExpressRoute gateway:

▼
2
4
8
16**Answer Area**

For the S2S VPN gateway:

▼
2
4
8
16

Correct Answer:

For the ExpressRoute gateway:

▼
2
4
8
16

 **Acaer** Highly Voted 4 months, 3 weeks ago

8 S2S
4 ExpressRoute

For S2S 1 scale unit = 500 Mbps
4000/500 = 8 scale units

<https://learn.microsoft.com/en-us/azure/virtual-wan/gateway-settings#s2s>

For ExpressRoute 1 scale unit = 2Gbps

$8/2 = 4$

<https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-expressroute-about#expressroute-performance>

upvoted 11 times

 **ConanBarb** 3 months, 3 weeks ago

I dont get it. It says


- Supports 4 Gbps of Site-to-Site (S2S) VPN traffic
- Supports 8 Gbps of ExpressRoute traffic

You seem to assume

8 S2S

4 ER

upvoted 1 times

 **Bigfatdavey** 4 months, 3 weeks ago

did you have this in your exam

upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

DRAG DROP

-

You have an on-premises network.

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

You need to connect VNet1 to the on-premises network by using an ExpressRoute circuit.

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.

Actions

Configure Azure public peering.

Create a connection from VNet1 to the ExpressRoute circuit.

Create the ExpressRoute circuit.

Configure Azure private peering.

Send a service key to your connectivity provider.

Answer Area

1

2

3

4

Correct Answer:

Answer Area

- 1 Create the ExpressRoute circuit.
- 2 Send a service key to your connectivity provider.
- 3 Configure Azure private peering.
- 4 Create a connection from VNet1 to the ExpressRoute circuit.

Acaer Highly Voted 4 months, 3 weeks ago

Seems correct.

1. Create the ExpressRoute circuit

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-howto-circuit-portal-resource-manager#create-a-new-expressroute-circuit>

2. Send a service key to your connectivity provider.

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-howto-circuit-portal-resource-manager#send-the-service-key-to-your-connectivity-provider-for-provisioning>

3. Configure Azure private peering

4. Create a connection from Vnet1 to the ExpressRoute circuit

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-howto-linkvnet-portal-resource-manager#prerequisites>

upvoted 6 times

3fd1c62 Most Recent 6 days ago

These - do in order - questions are dumb AF. Never seen an exam make you order things like this.

upvoted 1 times

Lazylinux 2 months, 3 weeks ago

Given answer is correct as per

<https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/expressroute>

upvoted 1 times

Opiate 3 months ago

The answer provided is correct:

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-howto-linkvnet-portal-resource-manager>

Connect a virtual network to an ExpressRoute circuit using the Azure portal:

Step1: Ensure that your ExpressRoute circuit and Azure private peering have been configured successfully. Follow the instructions in Create an ExpressRoute circuit and Create and modify peering for an ExpressRoute circuit.

upvoted 2 times

Techbiz 4 months ago

The answer provided is correct, when you deploy an expressroute circuit, you need to ensure that the circuit status is enabled and peering status is provision before you go ahead with vnet peering to the expressroute circuit using the gateway deployed at the vnet

upvoted 1 times

🗄️ 👤 **_Cris** 4 months, 1 week ago
appears on exam, 19 Sept 2023
upvoted 2 times

🗄️ 👤 **jmt97** 4 months, 2 weeks ago
Correct.
"You can view the properties of the circuit by selecting it. On the Overview page for your circuit, you find the Service Key. Provide the service key to the service provider to complete the provisioning process. The service key is unique to your circuit."
<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-howto-circuit-portal-resource-manager>
upvoted 2 times

🗄️ 👤 **Tyler** 4 months, 3 weeks ago
should step3 switch with step 4? first you have to have the connection, then you can have peering
upvoted 1 times

Question #29

Topic 1

You have three on-premises networks.

You have an Azure subscription that contains a Basic Azure virtual WAN. The virtual WAN contains a single virtual hub and a virtual network gateway that is limited to a throughput of 1 Gbps.

The on-premises networks connect to the virtual WAN by using Site-to-Site (S2S) VPN connections.

You need to increase the throughput of the virtual WAN to 3 Gbps. The solution must minimize administrative effort.

What should you do?

- A. Upgrade the virtual WAN to the Standard SKU.
- B. Add an additional VPN gateway to the Azure subscription.
- C. Create an additional virtual hub.
- D. Increase the number of gateway scale units.

Correct Answer: D

Community vote distribution

D (100%)

🗄️ 👤 **Acaer** Highly Voted 4 months, 3 weeks ago

Selected Answer: D

We want to minimize administrative effort
D. Increase the number of scale units
<https://learn.microsoft.com/en-us/azure/virtual-wan/gateway-settings#s2s>
upvoted 6 times

🗄️ 👤 **UR** Most Recent 3 months, 3 weeks ago

Selected Answer: D

<https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-faq#what-are-virtual-wan-gateway-scale-units>
upvoted 1 times

You have 10 on-premises networks that are connected by using a 3rd party Software Defined Wide Area Network (SD-WAN) solution. You have an Azure subscription that contains five virtual networks.

You plan to connect the Azure virtual networks and the on-premises networks by using an Azure Virtual WAN with a single virtual WAN hub.

You need to ensure that the Azure Virtual WAN can act as a node in the 3rd party SD-WAN solution.

What should you include in the solution?

- A. An Azure Virtual WAN ExpressRoute gateway
- B. A Network Virtual Appliance (NVA)
- C. A Site to site gateway (VPN gateway)
- D. A Point to site gateway (User VPN gateway)

Correct Answer: B

Community vote distribution

B (100%)

 **trashbox** 3 months, 1 week ago

Selected Answer: B

"Customers can deploy select Network Virtual Appliances (NVAs) directly into a Virtual WAN hub in a solution that is jointly managed by Microsoft Azure and third-party Network Virtual Appliance vendors."

<https://learn.microsoft.com/en-us/azure/virtual-wan/about-nva-hub>

upvoted 1 times

 **Acaer** 4 months, 3 weeks ago

B seems correct as shown in the documentation

<https://learn.microsoft.com/en-us/azure/virtual-wan/sd-wan-connectivity-architecture#direct-nva>

upvoted 4 times

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT

-

You have the Azure resources shown in the following table.

Name	Type	Location	Description
Sub1	Azure subscription	West Europe	None
Sub2	Azure subscription	West Europe	None
VNet1	Virtual network	West Europe	Created in Sub1
VNet2	Virtual network	West Europe	Created in Sub2
Circuit1	ExpressRoute circuit	West Europe	Linked to VNet1
Gateway1	ExpressRoute gateway	West Europe	Created in VNet1
Gateway2	ExpressRoute gateway	West Europe	Created in VNet2

You need to link VNet2 to Circuit1.

What should you create in each subscription? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Sub1:

- A new ExpressRoute circuit
- An ExpressRoute circuit connection
- An ExpressRoute circuit connection authorization


Sub2:

- A new ExpressRoute circuit
- An ExpressRoute circuit connection
- An ExpressRoute circuit connection authorization

店铺: IT认证考试服务


店铺: IT认证考试服务

Answer Area

Sub1: 

- A new ExpressRoute circuit
- An ExpressRoute circuit connection
- An ExpressRoute circuit connection authorization**

Correct Answer:

Sub2: 

- A new ExpressRoute circuit
- An ExpressRoute circuit connection**
- An ExpressRoute circuit connection authorization

店铺: IT认证考试服务

店铺: IT认证考试服务

 **Acaer** Highly Voted 4 months, 3 weeks ago

You can share an ExpressRoute circuit across multiple subscriptions.

The circuit owner is the administrator/coadministrator of the subscription in which the ExpressRoute circuit is created. The circuit owner can authorize administrators/coadministrators of other subscriptions, referred to as circuit users, to use the dedicated circuit that they own. Circuit users who are authorized to use the organization's ExpressRoute circuit can link the virtual network in their subscription to the ExpressRoute circuit after they're authorized.

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-howto-linkvnet-classic#administration>

Sub1 : An ExpressRoute circuit connection authorization

Sub2 : An ExpressRoute circuit connection

upvoted 5 times

 **Verytutos** Highly Voted 4 months, 2 weeks ago

Appeared on Exam 05 Sep 2023

upvoted 5 times

 **Lazylinux** Most Recent 2 months, 3 weeks ago

Given answer is correct - the Circuit owner creates the authorization code and provides it to the the circuit user (sub2), circuit user uses the authorization code and resource ID during the create connection process to be able to successfully connect via express route circuit

Here is more info

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-howto-linkvnet-portal-resource-manager>

<https://azureis.fun/posts/Adding-new-Connection-to-Azure-ExpressRoute-circuit/>

upvoted 1 times

 **gabrielcor** 4 months, 3 weeks ago

Correct

upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

You have an on-premises datacenter and an Azure subscription.

You plan to implement ExpressRoute FastPath.

You need to create an ExpressRoute gateway. The solution must minimize downtime if a single Azure datacenter fails.


Which SKU should you use?

- A. ErGw1AZ
- B. High performance
- C. Ultra performance
- D. ErGw3AZ
- E. ErGw2AZ

Correct Answer: D

 **karthickG** 2 months, 3 weeks ago

D is correct.
ErGw3Az and Ultra Performance SKU supports FastPath.
ErGw3Az is Zone-redundant, but not Ultra Performance SKU.
upvoted 4 times

 **Neffo** 3 weeks, 4 days ago

Correct

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-about-virtual-network-gateways#zrgw>

<https://learn.microsoft.com/en-us/azure/expressroute/about-fastpath#gateways>

upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT

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

Name	Type	Description
VWAN1	Azure Virtual WAN	Standard Virtual WAN
Hub1	Azure Virtual WAN hub	Hub for VWAN1
VNet1	Virtual network	Connected to Hub1
VNet2	Virtual network	Connected to Hub1
VNet3	Virtual network	Peered with VNet2
NVA1	Virtual machine	Hosts a routing appliance deployed to VNet2

You establish BGP peering between NVA1 and Hub1.

You need to implement transit connectivity between VNet1 and VNet3 via Hub1 by using BGP peering. The solution must minimize costs.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

On Hub1, propagate routes from connections to VNet1 and VNet2 to:

▼

A custom route table and associate the routes with the defaultRouteTable
 A custom route table and associate the routes with the same custom route table
 The defaultRouteTable and associate the routes with the defaultRouteTable

On VNet3, implement:

▼

Azure Route Server on a dedicated subnet
 Azure VPN Gateway on a dedicated subnet
 User-defined routes

Answer Area

On Hub1, propagate routes from connections to VNet1 and VNet2 to:

Correct Answer:

On VNet3, implement:

▼

A custom route table and associate the routes with the defaultRouteTable
 A custom route table and associate the routes with the same custom route table
The defaultRouteTable and associate the routes with the defaultRouteTable

▼

Azure Route Server on a dedicated subnet
 Azure VPN Gateway on a dedicated subnet
User-defined routes

ieboaix 1 week, 3 days ago

the given answer is correct refer to <https://learn.microsoft.com/en-us/azure/virtual-wan/scenario-bgp-peering-hub>
 upvoted 1 times

MostafaNawar 1 week, 3 days ago

On Hub1, propagate routes from connections to VNet1 and VNet2 to:
 1. A custom route table and associate the routes with the defaultRouteTable:

Cost: Minimal. Custom route tables are free if you don't use peering policies. Associating with the default route table avoids managing a separate table for each VNet.

2. A custom route table and associate the routes with the same custom route table:

Cost: Minimal. Similar to option 1, but creates a separate table for all routes. This introduces some management overhead but might be preferred if you need more granular control over routing in the future.

3. The defaultRouteTable and associate the routes with the defaultRouteTable:

Cost: Potentially higher. Adding routes to the default route table might trigger Azure Virtual WAN charges for route aggregation if you have many networks connected to the hub.

upvoted 1 times

You have an Azure subscription that contains an ExpressRoute Standard gateway named GW1.

You need to upgrade GW1 to support ExpressRoute FastPath. The solution must minimize downtime.

Which SKU should you use?

- A. Ultra performance
- B. ErGw3AZ
- C. ErGw2AZ
- D. High performance

Correct Answer: B

 **Jackdisuin** 1 day, 15 hours ago

Correct Answer is A. Ultra performance.

The following upgrades are supported:

Standard to High Performance
Standard to Ultra Performance
High Performance to Ultra Performance
ErGw1Az to ErGw2Az

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-about-virtual-network-gateways>
upvoted 2 times

 **MCCC454** 17 hours, 28 minutes ago

Could be both

To configure FastPath, the virtual network gateway must be either:

Ultra Performance
ErGw3AZ

<https://learn.microsoft.com/en-us/azure/expressroute/about-fastpath>
upvoted 1 times

HOTSPOT

-

Your on-premises network uses an IP address range of 10.1.0.0 to 10.1.255.255.

You plan to deploy a new Azure virtual network solution that will include the following elements:

- A virtual network named VNet1
- A Site-to-Site (S2S) VPN connection between VNet1 and the on-premises network
- GatewaySubnet in VNet1, which will be used as a route-based virtual network gateway

You need to recommend which subnet masks to assign to VNet1 and GatewaySubnet. The solution must meet the following requirements:

- Maximize the number of available IP addresses on VNet1.
- Minimize the number of available IP addresses on GatewaySubnet.

Which address spaces should you assign to VNet1 and GatewaySubnet? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

VNet1:

10.0.0.0/8
10.0.0.0/16
10.0.0.0/24
10.0.0.0/27

GatewaySubnet:

10.0.0.0/16
10.0.0.0/24
10.0.0.0/27
10.0.0.0/29

Answer Area

Correct Answer: VNet1:

10.0.0.0/8
10.0.0.0/16
10.0.0.0/24
10.0.0.0/27

GatewaySubnet:

10.0.0.0/16
10.0.0.0/24
10.0.0.0/27
10.0.0.0/29

 **Jackdisuin** 1 day, 15 hours ago

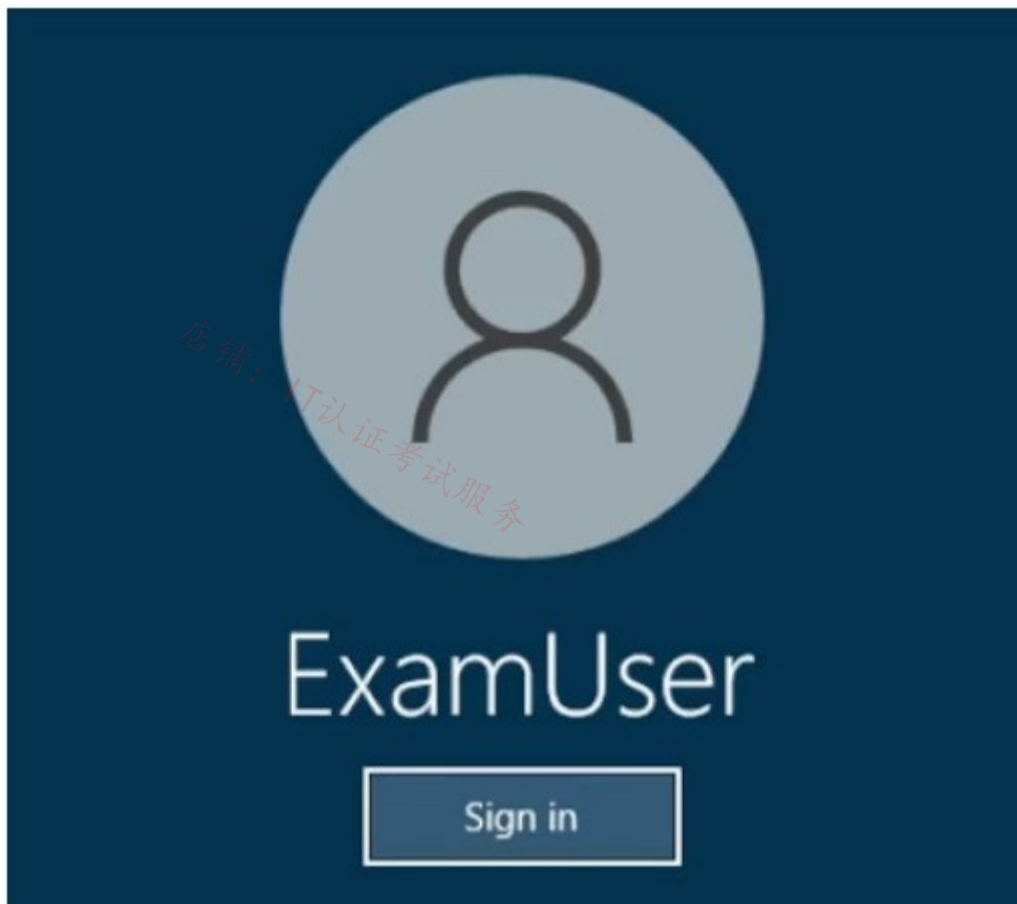
Maximize the number of available IP addresses on VNet1 10.0.0.0/16
Minimize the number of available IP addresses on GatewaySubnet 10.0.0.0/27
upvoted 3 times

 **UncleBenzz** 3 days, 5 hours ago

Correct answer should be /16 since it doesn't overlap with the on-premise address space 10.1.0.0/16
upvoted 3 times

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You have two servers that are each hosted by a separate service provider in New York and California. The server hosted in New York is accessible by using a host name of ny.contoso.com. The server hosted in California is accessible by using a host name of ca.contoso.com.

You need to implement an Azure solution to route users to the server that has the lowest latency. The solution must minimize costs.

To complete this task, sign in to the Azure portal.

Correct Answer:

Azure front Door route lowest latency

Set up Azure Front Door to route user traffic based on the lowest latency between the two web app servers. Start by adding a frontend host for Azure Front Door.

If there is already an Azure Front Door available, select it and skip phase 1. Start with phase 2.

If there is already an Azure Front Door and a backend available, select them and skip phase 1 and phase 2. Start with phase 3.

If there is already an Azure Front Door and a backend available, select them and skip phase 1 and phase 2. Start with phase 3.

Phase 1: Setup an Azure Front Door.

Step 1: From the home page or the Azure menu, select + Create a resource. Select Networking > Front Door and CDN profiles.

Step 2: On the Compare offerings page, select Explore other offerings. Then select Azure Front Door (classic). Then select Continue.

Step 3: In the Basics tab of Create a Front Door page, provide or select the following information, and then select Next: Configuration.

Example:

Subscription - Select your subscription.

Resource group - Select Create new and type FrontDoorQS_rg0 in the text box.

Resource group location - Select Central US.

Step 4: In Frontends/domains, select + to open Add a frontend host page.

Step 5: For Host name, type a globally unique hostname. For example, contoso-frontend. Select Add

The screenshot shows the 'Create a Front Door' configuration page in the 'Configuration' tab. A 'Frontends/domains' pane on the left shows a progress indicator for 'Step 1: Get started by adding a frontend host.' An 'Add a frontend host' dialog is open on the right. The dialog has a 'Host name' field containing 'contoso-frontend' and a '.azurefd.net' domain dropdown. Below this are sections for 'SESSION AFFINITY' (Status: Disabled) and 'WEB APPLICATION FIREWALL' (Status: Disabled). At the bottom of the dialog is an 'Add' button.

Next, set up a backend pool.

Step 1: Still in Create a Front Door, in Backend pools, select + to open the Add a backend pool page.

Step 2: For Name, type myBackendPool, then select Add a backend.

The screenshot shows the 'Create a Front Door' configuration page in the 'Configuration' tab. The 'Frontends/domains' pane shows 'contoso-frontend.azurefd.net'. The 'Backend pools' pane shows a progress indicator for 'Step 2'. An 'Add a backend pool' dialog is open on the right. The dialog has a 'Name' field containing 'myBackendPool'. Below this is a table for 'BACKENDS' with columns for 'Backend host name', 'Status', 'Priority', and 'Weight'. A '+ Add a backend' button is highlighted. Below the table are sections for 'HEALTH PROBES' (Status: Enabled), 'Path' (containing '/'), 'Protocol' (containing 'HTTPS'), 'Probe method' (containing 'HEAD'), and 'Interval (seconds)' (containing '30'). At the bottom of the dialog is an 'Add' button.

Step 3: Provide or select the following information in the Add a backend pane and select Add.

Example:

Backend host type - Select App service.

Subscription - Select your subscription.

Backend host name - Select the first web app you created. For example, WebAppContoso-1.

The screenshot shows the 'Create a Front Door' configuration page in the 'Configuration' tab. An 'Add a backend' dialog is open on the right. The dialog has a 'Backend host type' field. At the top left of the dialog is a link to 'Go back to backend pool'. Below the field is a description: 'Backends are your application servers where Front Door will route your client requests to. You can assign weights to your backends to define proportion of traffic to be sent and set priority for the backends to define active/stand-by kind of architectures. Learn more'. At the bottom of the dialog is an 'Add' button.

Step 4: Select Add a backend again. Provide or select the following information and select Add.

Step 5: Select Add on the Add a backend pool page to finish the configuration of the backend pool.

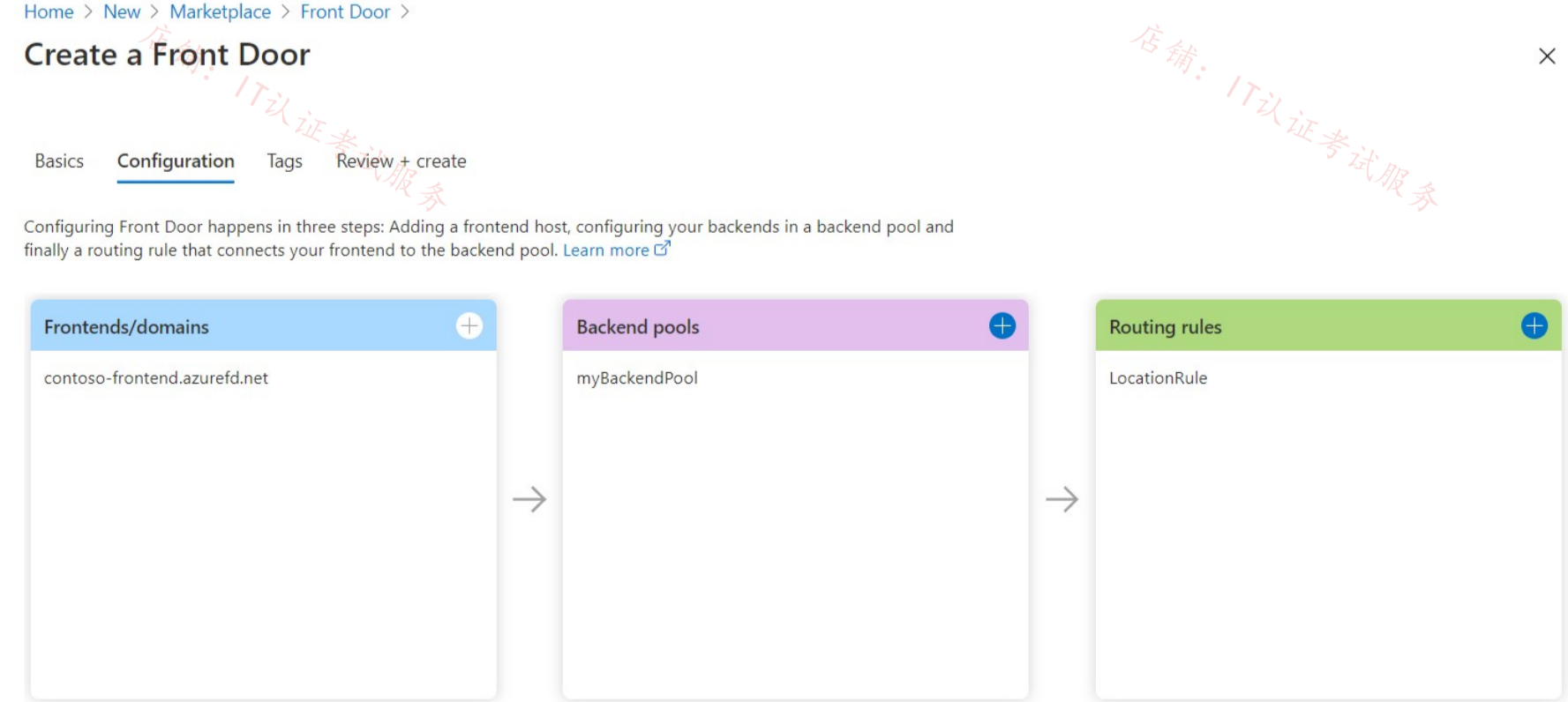
Phase 3: Create a routing rule

Lastly, create a routing rule. A routing rule links your frontend host to the backend pool. The rule routes a request for contoso-frontend.azurefd.net to myBackendPool.

- Step 1: Still in Create a Front Door, in Routing rules, select + to set up a routing rule.
- Step 2: In Add a rule, for Name, type LocationRule. Keep all the default values, then select Add to create the routing rule."

Warning
It's essential that you associate each of the frontend hosts in your Azure Front Door with a routing rule that has a default path /*. This means that you need to have at least one routing rule for each of your frontend hosts at the default path /* among all of your routing rules. Otherwise, your end-user traffic may not be routed properly.

Step 3: Select Review + create and verify the details. Then, select Create to start the deployment.



Review + create

< Previous

Next : Tags >

Download a template for automation

Note: Lowest latencies based traffic-routing

Deploying origins in two or more locations across the globe can improve the responsiveness of your applications by routing traffic to the destination that is 'closest' to your end users. Latency is the default traffic-routing method for your Front Door configuration. This routing method forwards requests from your end users to the closest origin behind Azure Front Door. This routing mechanism combined with the anycast architecture of Azure Front Door ensures that each of your end users gets the best performance based on their location.

The 'closest' origin isn't necessarily closest as measured by geographic distance. Instead, Azure Front Door determines the closest origin by measuring network latency.

Reference:

<https://learn.microsoft.com/en-us/azure/frontdoor/quickstart-create-front-door>

<https://learn.microsoft.com/en-us/azure/frontdoor/routing-methods>

Topic 2 - Question Set 2

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 two Azure virtual networks named Vnet1 and Vnet2.

You have a Windows 10 device named Client1 that connects to Vnet1 by using a Point-to-Site (P2S) IKEv2 VPN.

You implement virtual network peering between Vnet1 and Vnet2. Vnet1 allows gateway transit. Vnet2 can use the remote gateway.

You discover that Client1 cannot communicate with Vnet2.

You need to ensure that Client1 can communicate with Vnet2.

Solution: You reset the gateway of Vnet1.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

The VPN client must be downloaded again if any changes are made to VNet peering or the network topology.

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-point-to-site-routing>

Community vote distribution

B (100%)

 **AmalMOQ** Highly Voted 2 years, 3 months ago

correct !If you make a change to the topology of your network and have Windows VPN clients, the VPN client package for Windows clients must be downloaded and installed again in order for the changes to be applied to the client.

upvoted 12 times

 **liono** 1 year ago

Agree!

upvoted 1 times

 **FunkyB** 1 year, 5 months ago

Correct

About Point-to-Site VPN routing

If you make a change to the topology of your network and have Windows VPN clients, the VPN client package for Windows clients must be downloaded and installed again in order for the changes to be applied to the client.

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-point-to-site-routing>

upvoted 2 times

 **Verytutos** Most Recent 4 months, 2 weeks ago

Appeared on Exam 05 Sep 2023

upvoted 1 times

 **SLGUY** 5 months ago

Appeared on Exam 26 Aug 2023

upvoted 1 times

 **khanda** 9 months, 2 weeks ago

Selected Answer: B

VPN client must be downloaded again if any changes are made to VNet peering or the network topology.

upvoted 1 times

 **sunsetblvdfightclub** 10 months, 4 weeks ago

This question should be more clear that you made changes AFTER you have clients connecting via P2S. This one stumped on the test due to wording, thinking they were still explaining the scenario, not making changes from one sentence to the next

upvoted 1 times

 **Rajan395** 1 year ago

correct

upvoted 1 times

HasanHHH 1 year, 3 months ago

Selected Answer: B

If you make a change to the topology of your network and have Windows VPN clients, the VPN client package for Windows clients must be downloaded and installed again in order for the changes to be applied to the client.

upvoted 1 times

AdityaGupta 1 year, 4 months ago

Selected Answer: B

Since you implemented VNET peering later, you need to download and install VPN client to get topology changes.

upvoted 1 times

hogs 1 year, 5 months ago

Appeared on exam Aug2022

upvoted 1 times

kogunribido 1 year, 7 months ago

Appeared on exam 6/27/2022

upvoted 1 times

Edward1 1 year, 9 months ago

Selected Answer: B

correct

If you make a change to the topology of your network and have Windows VPN clients, the VPN client package for Windows clients must be downloaded and installed again in order for the changes to be applied to the client.

upvoted 1 times

Kimimoto 1 year, 11 months ago

Appeared in exam on 11/Feb/2022

upvoted 1 times

Ben_Dover2 1 year, 11 months ago

Selected Answer: B

download VPN config and reconnect

upvoted 3 times

AckeyGraham 1 year, 11 months ago

Would help if there was more context to such a question, presuming like an exam that was probably told prior to this question, as it isn't made clear when the client was downloaded onto the windows 10 machine.

upvoted 3 times

Takloy 2 years ago

Download the p2s configuration file and reconnect is the solution.

So correct answer here is, NO.

upvoted 2 times

AidenYoukhana 2 years ago

Selected Answer: B

Correct: NO.

upvoted 2 times

Pamban 2 years, 1 month ago

appeared on exam 5th Dec 2021

upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 two Azure virtual networks named Vnet1 and Vnet2.

You have a Windows 10 device named Client1 that connects to Vnet1 by using a Point-to-Site (P2S) IKEv2 VPN.

You implement virtual network peering between Vnet1 and Vnet2. Vnet1 allows gateway transit. Vnet2 can use the remote gateway.

You discover that Client1 cannot communicate with Vnet2.

You need to ensure that Client1 can communicate with Vnet2.

Solution: You enable BGP on the gateway of Vnet1.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

The VPN client must be downloaded again if any changes are made to VNet peering or the network topology.

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-point-to-site-routing>

Community vote distribution

B (100%)

 **Takloy** Highly Voted 2 years ago

Selected Answer: B

Solution: Download the P2S configuration package, install it on the client device and reconnect.

Answer: NO

upvoted 11 times

 **Verytutos** Most Recent 4 months, 2 weeks ago

Appeared on Exam 05 Sep 2023

upvoted 1 times

 **SLGUY** 5 months ago

Appeared on Exam 26 Aug 2023

upvoted 2 times

 **Rajan395** 1 year ago

Correct Answer! re-downloading of the client is required as topology changed

upvoted 1 times

 **HasanHHH** 1 year, 3 months ago

Selected Answer: B

If you make a change to the topology of your network and have Windows VPN clients, the VPN client package for Windows clients must be downloaded and installed again in order for the changes to be applied to the client.

upvoted 1 times

 **kogunribido** 1 year, 7 months ago

Appeared on exam 6/27/2022


upvoted 2 times

 **Edward1** 1 year, 9 months ago

Selected Answer: B

Correct!

upvoted 1 times

 **Kimimoto** 1 year, 11 months ago


Appeared in exam on 11/Feb/2022

upvoted 2 times

 **aftab7500** 2 years, 1 month ago

BGP is an optional feature you can use with Azure Route-Based VPN gateways.

upvoted 4 times

 **Charl** 2 years, 3 months ago

Correct!

upvoted 2 times

店铺: IT认证考试服务

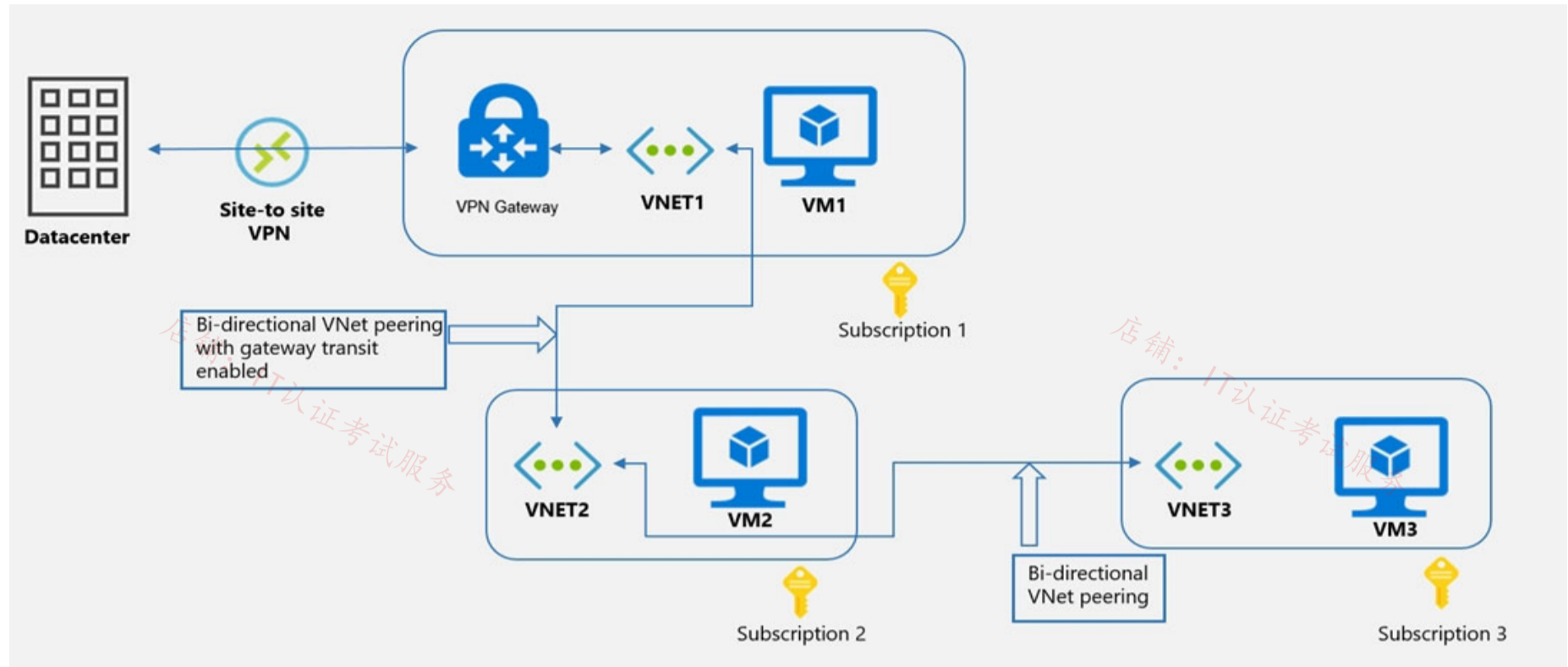
店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT -

You have the Azure environment shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

VM1 can communicate with (answer choice):

- VM2 only
- VM2 and VM3 only
- the on-premises datacenter and VM2 only
- the on-premises datacenter, VM2, and VM3 only

VM2 can communicate with (answer choice):

- VM1 only
- VM1 and VM3 only
- the on-premises datacenter and VM3 only
- the on-premises datacenter, VM1, and VM3 only

Correct Answer:

Answer Area














VM1 can communicate with (answer choice):



- VM2 only
- VM2 and VM3 only
- the on-premises datacenter and VM2 only
- the on-premises datacenter, VM2, and VM3 only

VM2 can communicate with (answer choice):

- VM1 only
- VM1 and VM3 only
- the on-premises datacenter and VM3 only
- the on-premises datacenter, VM1, and VM3 only

Reference:

-  **RickMorais** Highly Voted 2 years, 3 months ago
Given answers are correct
upvoted 36 times
-  **Vivek_Dwivedi** Highly Voted 2 years, 2 months ago
Use Remote gateway in VNET 2 peering is not mentioned. Which means VM2 can connect only to Vm1 and Vm3.
upvoted 18 times
-  **sallymaher** 2 years ago
That is mentioned in Enable transit gateway :- Virtual network gateway: Use this virtual network's gateway (in the vnet that contains the GW) and (Virtual network gateway: Use the remote virtual network's gateway) in the remote one so the answer is correct .
upvoted 11 times
-  **kpallivishal** 2 years ago
enable transit gateway means selecting both in vnet peering (Use this virtual network's gateway + Use the remote virtual network's gateway).
so above answer is correct as mentioned in diagram
upvoted 8 times
-  **Lazylinux** Most Recent 2 months, 3 weeks ago
Given answer is correct
upvoted 1 times
-  **Verytutos** 4 months, 2 weeks ago
Appeared on Exam 05 Sep 2023
upvoted 2 times
-  **fsgsfgs** 6 months ago
Given answers are correct
upvoted 2 times
-  **khanda** 9 months, 2 weeks ago
Given answer is correct.
upvoted 2 times
-  **liono** 1 year ago
Correct.
upvoted 2 times
-  **Goofer** 1 year, 1 month ago
VNET1 and VNET2 do not have a router configured to route traffic to another VNET
VNET2 and VNET3 do not have UDR configured to route traffic to the router.
VM1 --> on-premises and vm2
VM2 --> VM1 and VM3
upvoted 1 times
-  **Bill831231** 1 year, 3 months ago
what if for the S2S VPN without BGP enabled? VM2 can still communicate with On-premise?
upvoted 1 times
-  **HasanHHH** 1 year, 3 months ago
Correct:
1. VM1 Can Communicate with On-Premise datacenter due to S2S VPN and VM2 due to Bi-Directional VNet Peering
2. VM2 an Communicate with On-Premise datacenter, VM1 due Gateway transit(VNET1-VNET2) & S2S VPN (VNET1-Datacenter), and VM3 (VNET2-VNET3 VNet Peering)
upvoted 9 times
-  **sapien45** 1 year, 3 months ago
Repoonses provided are correGateway transit is a peering property that lets one virtual network use the VPN gateway in the peered virtual network for cross-premises or VNet-to-VNet connectivity.
It means that both options are selected in the vnettoVnet peering :
Use the remote virtual network's gateway
Use this virtual network's gateway

Therefore VM2 can communicate with on premises
upvoted 1 times
-  **AdityaGupta** 1 year, 4 months ago
Correct Answer
upvoted 1 times
-  **1particle** 1 year, 6 months ago
Correct.
VM2 uses VM1's gateway to reach the Datacenter.

upvoted 1 times

🗨️ 👤 **unclegrandfather** 1 year, 7 months ago

A slightly modified version of this was on the exam on 6/28/22. Make sure you understand WHY the answers are correct.

upvoted 2 times

🗨️ 👤 **WickedMJ** 1 year, 5 months ago

Can you advise whether it varies due to the placement of the "VPN Gateway" on the graph? TIA

upvoted 1 times

🗨️ 👤 **wsrudmen** 1 year, 8 months ago

Correct

VM1 can't access VM3 because (an UDR should be needed to achieve this): <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview>

upvoted 2 times

🗨️ 👤 **Edward1** 1 year, 9 months ago

Correct:

Gateway transit is a peering property that lets one virtual network use the VPN gateway in the peered virtual network for cross-premises or VNet-to-VNet connectivity.

upvoted 2 times

🗨️ 👤 **rockethack** 1 year, 11 months ago

This question was on the exam on 18th Feb 2022.

upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

You plan to deploy Azure virtual network.

You need to design the subnets.

Which three types of resources require a dedicated subnet? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Azure Bastion
- B. Azure Active Directory Domain Services (Azure AD DS)
- C. Azure Private Link
- D. Azure Application Gateway v2
- E. VPN gateway

Correct Answer: ADE

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-for-azure-services>

Community vote distribution

ADE (92%)

8%

 **srikanth1987** Highly Voted 2 years, 3 months ago

yes..ADE is the correct answer.

upvoted 26 times

 **d0bermann** Highly Voted 1 year, 11 months ago

Selected Answer: ADE

all GW types and Bastion must have dedicated subnets

upvoted 11 times

 **ESAJRR** Most Recent 10 months, 1 week ago

A. Azure Bastion = Name unique - AzureBastionSubnet

D. Azure Application Gateway v2 = Name does not have to be unique, just the subnet

E. VPN gateway = Name unique - GatewaySubnet

upvoted 6 times

 **somenick** 10 months, 3 weeks ago

Selected Answer: ADE


Correct

upvoted 1 times

 **liono** 1 year ago

Given answers are correct.

upvoted 1 times

 **nostroner89** 1 year, 1 month ago

FYI The answers are correct but AADS also needs a separate subnet it won't allow stuff to be deployed in this specific subnet.

upvoted 3 times

 **Webfacat33** 1 year, 1 month ago

Selected Answer: ADE

It's correct

upvoted 1 times

 **HasanHHH** 1 year, 3 months ago

Selected Answer: ADE

Network Application Gateway- WAF-Dedicated Subnet-YES

VPN Gateway-Dedicated Subnet-YES

Azure Firewall-Dedicated Subnet-YES

Azure Bastion-Dedicated Subnet-YES

Network Virtual Appliances-Dedicated Subnet-NO

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-for-azure-services#services-that-can-be-deployed-into-a-virtual-network>

upvoted 2 times

 **kevino81** 1 year, 4 months ago

Selected Answer: ADE

correct

upvoted 1 times

  **Alessandro365** 1 year, 4 months ago

Selected Answer: ADE

ADE are correct

upvoted 1 times

  **AdityaGupta** 1 year, 4 months ago

Selected Answer: ADE

Azure Bastion, Azure Application Gateway, VNET Gateway and Azure Firewall need dedicated subnet

upvoted 3 times

  **Jitusrit** 1 year, 5 months ago

Selected Answer: ADE

ADE are correct.

upvoted 2 times

  **1particle** 1 year, 6 months ago

A, D, & E

<https://docs.microsoft.com/en-us/azure/bastion/bastion-overview#architecture>

<https://docs.microsoft.com/en-us/azure/application-gateway/configuration-infrastructure>

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings#gwsub>

upvoted 4 times

  **unclegrandfather** 1 year, 7 months ago

Appeared on exam 6/28/22



upvoted 3 times

  **aldanetcloud** 1 year, 7 months ago

Selected Answer: ADE

ade correct answer

upvoted 3 times

  **lasmus** 1 year, 8 months ago

Selected Answer: ADE

ADE seems correct

upvoted 3 times

  **jpfsm** 1 year, 8 months ago

Selected Answer: ADE

Correct

upvoted 3 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT -

You have an Azure private DNS zone named contoso.com that is linked to the virtual networks shown in the following table.

Name	IP address
Vnet1	10.1.0.0/16
Vnet2	10.2.0.0/16

The links have auto registration enabled.

You create the virtual machines shown in the following table.

Name	IP address
VM1	10.1.10.10
VM2	10.2.10.10
VM3	10.2.10.11

You manually add the following entry to the contoso.com zone:

☞ Name: VM1

IP address: 10.1.10.9 -

▪

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
VM2 will resolve vm1.contoso.com to 10.1.10.10	<input type="radio"/>	<input type="radio"/>
Deleting VM1 will delete all VM1 records automatically	<input type="radio"/>	<input type="radio"/>
Changing the IP address of VM3 will update the DNS record of VM3 automatically	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
VM2 will resolve vm1.contoso.com to 10.1.10.10	<input type="radio"/>	<input checked="" type="radio"/>
Deleting VM1 will delete all VM1 records automatically	<input type="radio"/>	<input checked="" type="radio"/>
Changing the IP address of VM3 will update the DNS record of VM3 automatically	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: No -

The manual DNS record will overwrite the auto-registered DNS record so VM1 will resolve to 10.1.10.9.

Box 2: No -

The DNS record for VM1 is now a manually created record rather than an auto-registered record. Only auto-registered DNS records are deleted when a VM is deleted.

Box 3: No -

This answer depends on how the IP address is changed. To change the IP address of a VM manually, you would need to select 'Static' as the IP address assignment. In this case, the DNS record will not be updated because only DHCP assigned IP addresses are auto-registered.

Reference:

<https://docs.microsoft.com/en-us/azure/dns/dns-faq-private>

🗨️ **rakesh333** Highly Voted 2 years, 1 month ago

NNN

1. VM2 can't resolve v1.contoso.com to 10.1.10.10 because, there is a manual dns entry for vm1 points to 10.1.10.9 which over writes the automatic entry. So the answer is "NO"
2. Deleting a VM will delete only the automatic dns entry. Since we have a manual entry for vm1, that wouldn't be deleted when deleting the vm1. So the answer is "NO"
3. Manually changing the IP address of VM will not update the dns record. Auto DNS will only work if the VM gets ip via DHCP. So the answer is "NO":

upvoted 33 times

🗨️ **walkwolf3** Highly Voted 2 years, 2 months ago

Answer is correct, N,N,N, lab tested.

For box3, when IP of VM3 is changed, VM3 will reboot, DNS record will disappear. Then VM3 is back, and registers to the new IP in the DNS zone.

upvoted 33 times

🗨️ **wooyourdaddy** 10 months, 3 weeks ago

Agree that answer should be N,N,N as this link:

<https://learn.microsoft.com/en-us/azure/dns/private-dns-autoregistration#restrictions>

States:

DNS records are created automatically only if the primary virtual machine NIC is using DHCP. If you're using static IPs, such as a configuration with multiple IP addresses in Azure, auto registration doesn't create records for that virtual machine.

Assuming that "changing of the IP address of VM3" means that the NIC is configured with a static IP.

upvoted 2 times

🗨️ **Apptech** 9 months, 3 weeks ago

You say for question 3 answer should be YES! Private DNS zone will remove and re-add the new static IP address. But question asks for UPDATE the entry. Remove and Re-add after is not an Update, right?

upvoted 2 times

🗨️ **asdasd123123iu** 5 months, 3 weeks ago

There is no possibility to change ip address without rebooting vm so DNS will be updated automatically.

upvoted 1 times

🗨️ **yokoka2259** 2 years, 2 months ago

if it comes back and registers, then the answer is YES right?

upvoted 4 times

🗨️ **JamRackie** 2 years, 2 months ago

So are you saying answer 3 should be Yes as it registers itself after a reboot?

upvoted 5 times

🗨️ **Acrophat** 2 years, 1 month ago

I also labbed this out for question 3 and it should be YES! Private DNS zone will remove and re-add the new static IP address.

upvoted 13 times

🗨️ **Techbiz** Most Recent 4 months ago

The answer given is correct

upvoted 1 times

🗨️ **voldemort123** 4 months ago

changing the IP address of a VM in a VNet with auto registration to a private DNS zone will update the record if the following conditions are met:

- The VM is using DHCP for its primary NIC.
- The VM is in a registration virtual network that is linked to the private DNS zone with auto registration enabled.
- The VM is not using multiple IP addresses or multiple NICs.

If any of these conditions are not met, you will have to manually create or update the DNS records for the VM in the private DNS zone.

upvoted 1 times

🗨️ **_Cris** 4 months, 1 week ago

appears on exam, 19 Sept 2023

upvoted 1 times

🗨️ **SLGUY** 5 months ago

Appeared on Exam 26 Aug 2023

upvoted 3 times

🗨️ **ESAJRR** 10 months, 1 week ago

Answer is correct, N,N,N, lab tested too.

upvoted 1 times

🗨️ **AzureLearner01** 11 months ago

Lab tested - NNY


You can't add 2 entries with the same name in the zone. So this record would be set to auto registered NO. Due to this it would not be deleted by deleting the vm. The according DNS record would be deleted, yes but only if auto registered is yes.

upvoted 4 times

 **Madball** 12 months ago

By testing in my lab I get No, No and Yes. When you change the IP address of the VM, the VM will automatically reboot, in private DNS the A record disappears and reappears with the new IP address.

upvoted 8 times

 **Rajan395** 1 year ago

Answer is No, NO and YES

upvoted 5 times

 **zukako** 1 year ago

I think q3 is Yes because for VM, azure manage the DNS record automatically

upvoted 4 times

 **Kevmeister** 1 year, 2 months ago

I would definitely answer N,N,Y As per the MS site: <https://learn.microsoft.com/en-us/azure/dns/private-dns-overview> It clearly states: To resolve the records of a private DNS zone from your virtual network, you must link the virtual network with the zone. Linked virtual networks have full access and can resolve all DNS records published in the private zone. You can also enable autoregistration on a virtual network link. When you enable autoregistration on a virtual network link, the DNS records for the virtual machines in that virtual network are registered in the private zone. When autoregistration gets enabled, Azure DNS will update the zone record whenever a virtual machine gets created, changes its' IP address, or gets deleted.

The only way to change the IP address is to set it to static within the portal as changing it on the VM itself is a BIG no no. So as per the documentation this proves that the answer is Y for Box 3.

upvoted 8 times

 **Kevmeister** 1 year, 2 months ago

A few people also tested this in their LAB. The scenario provided in the FAQ page shown in the answer page I'm confident is an example of when a person sets a static IP at the OS level rather than from within the portal ipconfig. As tkcltoh mentioned, if you update in the portal and set an IP it should also then update the DNS record.

upvoted 2 times

 **HasanHHH** 1 year, 3 months ago

1.NO-overwrite the automatically registered DNS records with a manually created DNS record in the zone
2.NO-due VM1 record Created manually here -The private zone's records are populated by the Azure DHCP service, if deallocated, the autoregistered DNS records are removed.
3.NO-Manually changing the IP address of VM will not update the dns record. The private zone's records are populated by the Azure DHCP service.

upvoted 1 times

 **asbaleha** 1 year, 3 months ago

3 is yes if you change the IP address of the VM the machine will automatically restart , and the DNS will grab the new IP

upvoted 2 times

 **asbaleha** 1 year, 3 months ago

hi so i the correct answer is N N Y

1- N : in the manual configuration you will remove the auto-registration because u are overriding the DNS record

2- N : VM1 has manual configuration so the entry in the record will be static unless the whole DNS private zone is removed

3- Y : i changed the VM ip address from dynamic to static in the VNIC section , after the VM restarted , when the VM boot up the DNS record update the IP address to the new one

you can do the lab is easy just create resource group , 1 vnet , 2 subnet and 3 VM

upvoted 5 times

 **jellybiscuit** 1 year, 3 months ago

N, N, Y

The description supporting #3 is wrong, as are some of the discussions.

You don't updated IPs inside of a VM. You can, but it's the incorrect method. M\$ wouldn't asked you a question based on incorrect operations. If you change an IP correctly, meaning on the network interface, it will update in private DNS with auto registration enabled. It doesn't matter if you're changing it from dynamic to static, or changing the IP address from one static address to another.

upvoted 8 times

 **sapien45** 1 year, 4 months ago


NNN

<https://learn.microsoft.com/en-us/azure/dns/dns-faq-private>

I've reconfigured the OS in my virtual machine to have a new host name or static IP address. Why don't I see that change reflected in the private zone?

The private zone's records are populated by the Azure DHCP service; client registration messages are ignored. If you have disabled DHCP client support in the VM by configuring a static IP address, changes to the host name or static IP in the VM aren't reflected in the zone.

upvoted 1 times

 **tkcltoh** 1 year, 4 months ago

for q3, changing ip from dynamic to static via ipconfig1 in Azure portal will update the dns record but if you change the ip inside the VM WILL NOT update the dns record.

店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

HOTSPOT -

Your company has an Azure virtual network named Vnet1 that uses an IP address space of 192.168.0.0/20. Vnet1 contains a subnet named Subnet1 that uses an IP address space of 192.168.0.0/24.

You create an IPv6 address range to Vnet1 by using a CIDR suffix of /48.

You need to enable the virtual machines on Subnet1 to communicate with each other by using IPv6 addresses assigned by the company. The solution must minimize the number of additional IPv4 addresses.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Create an IPv6 subnet that uses a CIDR suffix of:

	▼
/20	
/24	
/48	
/64	

For each virtual machine, create an additional:

	▼
IP configuration	
NIC	
Public IPv6 address	

Answer Area

Create an IPv6 subnet that uses a CIDR suffix of:

	▼
/20	
/24	
/48	
/64	

Correct Answer:

For each virtual machine, create an additional:

	▼
IP configuration	
NIC	
Public IPv6 address	

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/ipv6-overview> <https://docs.microsoft.com/en-us/azure/virtual-network/ipv6-add-to-existing-vnet-powershell>

 **Wesgo** Highly Voted 2 years, 3 months ago

1) Correct: /64

Explanation: The subnets for IPv6 must be exactly /64 in size. This ensures future compatibility should you decide to enable routing of the subnet to an on-premises network since some routers can only accept /64 IPv6 routes.


Source: <https://docs.microsoft.com/en-us/azure/virtual-network/ip-services/ipv6-overview>

2) Correct: Public IPv6 Address

Explanation: Add IPv6 configuration to NIC. "Configure all of the VM NICs with an IPv6 address using Add-AzNetworkInterfaceIpConfig"

Source: <https://docs.microsoft.com/en-us/azure/load-balancer/ipv6-add-to-existing-vnet-powershell>

upvoted 27 times


 **ian2387** 1 year, 9 months ago

I didnt understand.


how can public ipv6 be correct.


It is IP configuration as per your explanation as well


upvoted 5 times


 **Windows98** 2 years, 2 months ago
Your IPV6 address is already public.


The powershell config for this has separate IPV4 and IPV6 config blocks and I think examtopics is correct in this instance.
upvoted 7 times


 **sleekdunga** 1 year, 11 months ago
The correct answer was even embedded in his powershell script "Add-AzNetworkInterfaceIpConfig" Implying IP Configurations at the NIC level.
upvoted 5 times


 **jelley** Highly Voted 2 years, 3 months ago
Even based on the stated it should make sense:
And regarding the total VNET uses /48, thus it can never be lower and considering the probable need for another subnet at a later point /64 is the most likely.
You can add multiple IP configurations to a NIC thus NIC is incorrect (1x ipv4 and an ipv6 to 1 NIC). It can't be public IP's because we are talking about internal transfers thus IP Configuration is correct
upvoted 12 times


 **_Cris** Most Recent 4 months, 1 week ago
appears on exam, 19 Sept 2023
upvoted 1 times


 **Billabongs** 6 months, 2 weeks ago
It shows ipv4 and ipv6 configured under the same NICs. (Configured using PowerShell)
<https://learn.microsoft.com/en-US/azure/load-balancer/ipv6-add-to-existing-vnet-powershell#view-ipv6-dual-stack-virtual-network-in-azure-portal>
upvoted 1 times

 **Ayokun** 11 months, 2 weeks ago
Wouldn't be better give a new NIC dedicated with the IPv6???
i think the correct answer is:
/64
NIC since you can't do it on the already existing one that uses the old subnet
upvoted 1 times

 **LeonTH** 11 months, 2 weeks ago
maledetti
upvoted 4 times

 **liono** 1 year ago
Given answers are correct!
upvoted 1 times


 **yamapan** 1 year, 1 month ago
URL is outdated;
this is latest
<https://learn.microsoft.com/en-US/azure/load-balancer/ipv6-add-to-existing-vnet-powershell>
upvoted 2 times


 **HasanHHH** 1 year, 3 months ago
Answer: /64 - IP configuration


#Add IPv6 prefix to the VNET
\$vnet.addressspace.addressprefixes.add("fd00:db8:deca::/48")

#Add IPv6 prefix to the Subnet (smaller than addressspace)
\$subnet.addressprefix.add("fd00:db8:deca::/64")
<https://learn.microsoft.com/en-us/azure/load-balancer/ipv6-add-to-existing-vnet-powershell>

A single service instance can connect with both IPv4 and IPv6, IPv6-only are not supported, each NIC must include at least one IPv4 IP configuration.
upvoted 5 times

 **Pradh** 1 year, 4 months ago
100% CORRECT ANSWER : /64 & IP Configuration .
upvoted 4 times

 **sapien45** 1 year, 4 months ago
100% unhelpful comment
upvoted 17 times

 **hogs** 1 year, 5 months ago
Appeared on exam Aug2022
upvoted 3 times

 **1particle** 1 year, 6 months ago

Correct. /64 and IP configuration

<https://docs.microsoft.com/en-us/azure/virtual-network/ip-services/ipv6-overview#capabilities>

<https://docs.microsoft.com/en-us/answers/questions/442977/unable-to-add-ipv6-address-to-existing-azure-netwo.html>

upvoted 4 times

 **unclegrandfather** 1 year, 7 months ago

Appeared on exam 6/28/22

upvoted 2 times

 **kogunribido** 1 year, 7 months ago

Appeared on exam 6/27/2022

upvoted 2 times

 **Edward1** 1 year, 9 months ago

Answer: /64 - IP configuration

You can add as many private and public IPv4 addresses as necessary to a network interface, within the limits listed in the Azure limits article. You can add a private IPv6 address to one secondary IP configuration (as long as there are no existing secondary IP configurations) for an existing network interface. Each network interface may have at most one IPv6 private address.

<https://docs.microsoft.com/en-us/azure/virtual-network/ip-services/virtual-network-network-interface-addresses>

upvoted 2 times

 **rockethack** 1 year, 11 months ago

This question was on the exam on 18th Feb 2022.

upvoted 1 times

 **Kimimoto** 1 year, 11 months ago

Appeared in exam on 11/Feb/2022

upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT -

You plan to deploy Azure Virtual WAN.

You need to deploy a virtual WAN hub that meets the following requirements:

- ☞ Supports 10 sites that will connect to the virtual WAN hub by using a Site-to-Site VPN connection
- ☞ Supports 8 Gbps of ExpressRoute traffic
- ☞ Minimizes costs

What should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Virtual WAN type:
 Basic
 Standard

Number of scale units:
 2
 4
 6
 8

Correct Answer:

Answer Area

Virtual WAN type:
 Basic
 Standard

Number of scale units:
 2
 4
 6
 8

Reference:
<https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about>

Bharat Highly Voted 2 years, 3 months ago

8 Gig Express Route. 2 GB per ER scale unit. Therefore number of scale units = $8/2 = 4$
<https://www.wwt.com/article/microsoft-azure-virtual-wan-cloud-networking-architecture>
 upvoted 43 times

Mirek 2 years, 3 months ago

<https://www.azure.cn/en-us/pricing/details/virtual-wan/>
 upvoted 6 times

walkwolf3 Highly Voted 2 years, 2 months ago

Answer is correct.

Basic virtual WAN supports Site-to-site VPN only

Standard virtual WAN supports



ExpressRoute
User VPN (P2S)
VPN (site-to-site)
Inter-hub and VNet-to-VNet transiting through the virtual hub
Azure Firewall
NVA in a virtual WAN



<https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about>



8G/2G = 4



Express Route Scale Units and Connectivity: Similar in concept to VPN scale units, customers seeking to deploy Express Route connectivity into their Virtual WAN Hubs will incur costs for the scale units provisioned in that hub, with options ranging from 1 to 10 with each representing 2Gbps of ER throughput.



<https://www.wwt.com/article/microsoft-azure-virtual-wan-cloud-networking-architecture>
upvoted 27 times

  **sapien45** 1 year, 4 months ago
Great link !
upvoted 2 times

  **Lazylinux** Most Recent 2 months, 3 weeks ago
Given answer is correct
upvoted 1 times



  **Techbiz** 4 months ago
The given answer is correct, Basic WANs don't support expressroutes
upvoted 1 times



  **raffylian** 5 months, 1 week ago
this is on my exam today 8/23
upvoted 1 times



  **daemon101** 6 months, 3 weeks ago
this is where you'll see the scale unit for ExpressRoute and VPN.
1 scale unit of VPN = 500 Mbps
1 scale unit of ExpressRoute = 2 Gbps



The requirement for Expressroute throughput is 8Gbps so 4 ER scale units are needed. The answer is correct.

<https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-faq>
upvoted 1 times



  **daemon101** 6 months, 3 weeks ago
I think the first requirement which is 10 sites that will connect to your virtual wan hub doesn't matter much as one virtual wan hub supports up to 1000 sites.
upvoted 1 times

  **bakamon** 8 months ago
Correct Answer :
:: Standard
:: 4
upvoted 1 times

  **DeepMoon** 1 year, 1 month ago
I don't see any reference on Azure Documentation (learn.microsoft.com) talking about 4 Scale Units give 8GB.
When I look for Virtual WAN Scale Units, all I find is this doc:
<https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-faq#for-user-vpn-point-to-site--how-many-clients-are-supported>
According to this chart 4 scale units is wrong.
So can someone explain; where did my thinking go wrong.
upvoted 1 times

  **charrua86** 6 months ago
<https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-faq#what-are-virtual-wan-gateway-scale-units>
upvoted 1 times

  **khanda** 9 months, 2 weeks ago
Each scale unit represents 500Mbps of VPN throughput.
upvoted 1 times

  **GBAU** 3 months ago
ER Scale units are 2GBps, 500Mbps is for P2S & S2S.
upvoted 1 times

  **HasanHHH** 1 year, 3 months ago

Standard-Available configurations:ExpressRoute,Site-to-Site VPN
Basic-Available configurations:Site-to-site VPN only
1 scale unit of ExpressRoute = 2 Gbps. So, 4 scale unit*2 Gbps=8Gbps
upvoted 1 times

🗨️ **iwikneerg** 1 year, 5 months ago

What are Virtual WAN gateway scale units?

A scale unit is a unit defined to pick an aggregate throughput of a gateway in Virtual hub. 1 scale unit of VPN = 500 Mbps. 1 scale unit of ExpressRoute = 2 Gbps. Example: 10 scale unit of VPN would imply 500 Mbps * 10 = 5 Gbps.

<https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-faq#what-are-virtual-wan-gateway-scale-units>

upvoted 2 times

🗨️ **1particle** 1 year, 6 months ago

Standard and 4

Hub Type Standard:

Standard ExpressRoute

User VPN (P2S)

VPN (site-to-site)

Inter-hub and VNet-to-VNet transiting through the virtual hub

Azure Firewall

NVA in a virtual WAN

<https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about#basicstandard>

Gateway Scale Units:

A scale unit is a unit defined to pick an aggregate throughput of a gateway in Virtual hub. 1 scale unit of VPN = 500 Mbps. 1 scale unit of ExpressRoute = 2 Gbps

<https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-faq#what-are-virtual-wan-gateway-scale-units>

upvoted 1 times

🗨️ **derrrp** 1 year, 6 months ago

Microsoft tryna trick us talking about Site-to-Site which ya'll know is BASIC but then they say ExpressRoute in the next section which we know makes it Standard.

upvoted 6 times

🗨️ **rockethack** 1 year, 11 months ago

This question was on the exam on 18th Feb 2022.

upvoted 1 times

🗨️ **Kimimoto** 1 year, 11 months ago

Appeared in exam on 11/Feb/2022

upvoted 1 times

🗨️ **KranthiChaitanya** 2 years ago

Came on exam 28/Jan/22

upvoted 1 times

🗨️ **Contactfornitish** 2 years ago

Appeared in exam on 17/01/2022

upvoted 1 times

🗨️ **Pravda** 2 years ago

Not on exam 1/6/2022

upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

DRAG DROP -

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

Name	Type	Location
WebApp1	Web app	West US
VNet1	Virtual network	East US

The IP Addresses settings for Vnet1 are configured as shown in the exhibit.

Basic **IP Addresses** Security Tags Review + create

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space

10.3.0.0/16 10.3.0.0 - 10.3.255.255 (65536 addresses)

Add IPv6 address space ⓘ

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

+ Add subnet Remove subnet

<input type="checkbox"/> Subnet name	Subnet address range	NAT gateway
<input type="checkbox"/> Subnet1	10.3.0.0/16	

i Use of a NAT gateway is recommended for outbound internet access from a subnet. You can deploy a NAT gateway and assign it to a subnet after you create the virtual network. [Learn more](#)

You need to ensure that you can integrate WebApp1 and Vnet1.

Which three actions should you perform in sequence before you can integrate WebApp1 and Vnet1? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Actions

- Create a service endpoint
- Deploy a VPN gateway
- Add a private endpoint
- Modify the address space of Vnet1
- Configure a Point-to-Site (P2S) VPN



Answer Area



店铺: IT认证考试服务

Correct Answer:

Actions

Create a service endpoint

Add a private endpoint

Answer Area

Modify the address space of Vnet1

Deploy a VPN gateway

Configure a Point-to-Site (P2S) VPN

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/web-sites-integrate-with-vnet#gateway-required-vnet-integration>

 **tkoutanis** Highly Voted 2 years, 3 months ago

Given answer is correct. Existing subnet space spans the entire address space of vnet, so it needs to be modified. Cross region vnet integration requires a vpn gateway and a point to site vpn connection. So you need to add the gateway, then configure the p2s to add address space.
<https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration#gateway-required-vnet-integration>
upvoted 52 times

 **walkwolf3** Highly Voted 2 years, 2 months ago

Answer is correct, it talks about cross region vent integration.

Service endpoint is for regional or same region virtual network integration.

Private endpoint is to use private DNS integration.
upvoted 15 times

 **Lazylinux** Most Recent 2 months, 3 weeks ago

Given answer is correct as per tis link considering both vnet and App service in different regions and hence vnet integration is NOT applicable here
<https://learn.microsoft.com/en-us/azure/app-service/configure-gateway-required-vnet-integration>
upvoted 2 times

 **Lazylinux** 2 months, 3 weeks ago

this is the future and hence question maybe too old now
<https://learn.microsoft.com/en-us/azure/app-service/overview-vnet-integration>
upvoted 1 times

 **homer_simpson** 3 months, 3 weeks ago

It is the correct answer.

We need to modify the address space of vnet 1 because we need a dedicated subnet to deploy a vpn gateway. Then we deploy the vpn gateway and configure point the site vpn. web app to the vnet vpn connection because the Vnet1 and Webapp are in different regions.
upvoted 1 times

 **bp_a_user** 4 months, 1 week ago

The provided link <https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration#gateway-required-vnet-integration> seems not to mention VPN? Is the question outdated?
upvoted 1 times

 **azure_2563** 5 months, 1 week ago

Guy's any video is available to this problem?
upvoted 1 times

 **Lazylinux** 2 months, 3 weeks ago

Yes on Netflix!!
upvoted 2 times

 **CiscoExam** 3 weeks, 3 days ago

hahaha :D
upvoted 1 times

 **kira1kira22** 1 month, 3 weeks ago

no , it's on disney plus :D
upvoted 1 times

 **galahad** 6 days, 6 hours ago

No, it's on HULU
upvoted 1 times

🗨️ **tester2023** 12 months ago

I tested in the lab, and when attempting to add vNet integration to the App Service, the Portal menu allows same region automatically, but it shows "Other regions (requires a Virtual Network Gateway configured with Point to Site VPN).

upvoted 5 times

🗨️ **AdityaGupta** 1 year, 4 months ago

The virtual network integration feature has two variations:

1) Since you need to deploy a VNET Gateway, address space need to be modified, currently subnet is consuming entire address space.

2) You must a deploy a VPN Gateway, since Web App and VNet are in different regions.

a. Regional virtual network integration: When you connect to virtual networks in the same region, you must have a dedicated subnet in the virtual network you're integrating with.

b. Gateway-required virtual network integration: When you connect directly to virtual networks in other regions or to a classic virtual network in the same region, you need an Azure Virtual Network gateway created in the target virtual network.

3) Requires a virtual network route-based gateway configured with an SSTP point-to-site VPN before it can be connected to an app.

upvoted 3 times

🗨️ **1particle** 1 year, 6 months ago

Correct

Gateway-required virtual network integration supports connecting to a virtual network in another region or to a classic virtual network. Gateway-required virtual network integration: Requires a virtual network route-based gateway configured with an SSTP point-to-site VPN before it can be connected to an app.

<https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration#gateway-required-virtual-network-integration>

upvoted 2 times

🗨️ **Takloy** 1 year, 6 months ago

If you look at the resources locations, both of them are on a different region. So Service and Private is out of the picture. Must prioritize VPN connectivity first.

upvoted 2 times

🗨️ **derrp** 1 year, 6 months ago

Remember:

Modify the VNET so you can add the VPN.

Add the VPN.

Then configure it.

upvoted 4 times

🗨️ **unclegrandfather** 1 year, 7 months ago

Appeared on exam 6/28/22

upvoted 1 times

🗨️ **ash21** 1 year, 7 months ago

The mentioned answer is correct, <https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration>.

upvoted 1 times

🗨️ **Stanley3427** 1 year, 7 months ago

the answer is 413, this question will not use vpn services

upvoted 2 times

🗨️ **petermogaka91** 1 year, 9 months ago

Answers are correct. Check the link below

<https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration>

upvoted 1 times

🗨️ **Edward1** 1 year, 9 months ago

The answers are correct.

Virtual network integration doesn't enable your apps to be accessed privately.

upvoted 1 times

🗨️ **Pravda** 2 years ago

on exam 1/6/2022

upvoted 3 times

DRAG DROP -

You have Azure virtual networks named Hub1 and Spoke1. Hub1 connects to an on-premises network by using a Site-to-Site VPN connection. You are implementing peering between Hub1 and Spoke1.

You need to ensure that a virtual machine connected to Spoke1 can connect to the on-premises network through Hub1.

How should you complete the PowerShell script? To answer, drag the appropriate values to the correct targets. Each value 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.

NOTE: Each correct selection is worth one point.

Select and Place:

Values	Answer Area
-AllowForwardedTraffic	\$hub = Get-AZVirtualNetwork -ResourceGroup "RG1" -Name "Hub1"
-AllowGatewayTransit	\$spoke = Get-AZVirtualNetwork -ResourceGroup "RG2" -Name "Spoke1"
-UseRemoteGateways	Add-AZVirtualNetworkPeering -Name "Hub1-Spoke1" -VirtualNetwork \$hub
	-RemoteVirtualNetworkId \$spoke.id <input type="text" value="Value"/>
	Add-AZVirtualNetworkPeering -Name "Spoke1-Hub1" -VirtualNetwork \$spoke
	-RemoteVirtualNetworkId \$hub.id <input type="text" value="Value"/>

Correct Answer:


Values	Answer Area
-AllowForwardedTraffic	\$hub = Get-AZVirtualNetwork -ResourceGroup "RG1" -Name "Hub1"
-AllowGatewayTransit	\$spoke = Get-AZVirtualNetwork -ResourceGroup "RG2" -Name "Spoke1"
-UseRemoteGateways	Add-AZVirtualNetworkPeering -Name "Hub1-Spoke1" -VirtualNetwork \$hub
	-RemoteVirtualNetworkId \$spoke.id <input type="text" value="-AllowGatewayTransit"/>
	Add-AZVirtualNetworkPeering -Name "Spoke1-Hub1" -VirtualNetwork \$spoke
	-RemoteVirtualNetworkId \$hub.id <input type="text" value="-UseRemoteGateways"/>

Reference:

<https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke?tabs=cli#virtual-network-peering>

 **Bharat** Highly Voted 2 years, 3 months ago

The answer is correct. However, this is a better reference: <https://docs.microsoft.com/en-us/azure/firewall/tutorial-hybrid-ps>
upvoted 27 times

 **jeepTango123456** 1 year, 5 months ago

From the link the example, the answer here seems to be reversed.

Peer hub to spoke

Add-AzVirtualNetworkPeering -Name HubtoSpoke -VirtualNetwork \$VNetHub -RemoteVirtualNetworkId \$VNetSpoke.Id -AllowGatewayTransit

Peer spoke to hub

Add-AzVirtualNetworkPeering -Name SpoketoHub -VirtualNetwork \$VNetSpoke -RemoteVirtualNetworkId \$VNetHub.Id -

AllowForwardedTraffic -UseRemoteGateways

upvoted 7 times

 **MrBlueSky** 10 months ago

No, Bharat is correct. Not sure why you said that the answers are reversed because even in your example the peering performed on the hub network is set to AllowGatewayTransit and the peering set on the Spoke network is 'UseRemoteGateways'

upvoted 1 times

 **walkwolf3** Highly Voted 2 years, 2 months ago

Answer is correct

-AllowGatewayTransit

Select Use this virtual network's gateway or Route Server:

- If you have a virtual network gateway attached to this virtual network and want to allow traffic from the peered virtual network to flow through

the gateway.

-UseRemoteGateways

Select Use the remote virtual network gateway or Route Server:

- If you want to allow traffic from this virtual network to flow through a virtual network gateway attached to the virtual network you're peering with.

Box1: Hub told spoke to use hub's VPN gateway to reach on-premise network

Box2: Spoke told hub to use hub's VPN gateway to reach on-premise network

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering>

upvoted 20 times

 **kikocu** Most Recent 2 weeks, 1 day ago

Answer is correct, please check the Powershell Sample command in this link

<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-peering-gateway-transit>

upvoted 1 times

 **Sant25** 2 weeks, 5 days ago

Peer hub to spoke

Add-AzVirtualNetworkPeering -Name HubtoSpoke -VirtualNetwork \$VNetHub -RemoteVirtualNetworkId \$VNetSpoke.Id -AllowGatewayTransit

Peer spoke to hub

Add-AzVirtualNetworkPeering -Name SpoketoHub -VirtualNetwork \$VNetSpoke -RemoteVirtualNetworkId \$VNetHub.Id -AllowForwardedTraffic -

UseRemoteGateways

upvoted 1 times


 **Lazylinux** 2 months, 3 weeks ago

Given answer is correct

AT Hub side, we AllowGatewayTransit

AT Spoke side, we need UseRemoteGateway

upvoted 1 times

 **MikeSA** 7 months, 2 weeks ago

Confusing because the second part could be either allowforwarded or userremotegateways. Seems to be missing one of the options.

Peer spoke to hub

Add-AzVirtualNetworkPeering -Name SpoketoHub -VirtualNetwork \$VNetSpoke -RemoteVirtualNetworkId \$VNetHub.Id -AllowForwardedTraffic -

UseRemoteGateways

upvoted 1 times

 **Himank20** 9 months ago

Given answer is correct.

In the hub, we need to enable AllowGatewayTransit and in the spoke we need to enable UseRemoteGateway

upvoted 1 times

 **mauchi** 11 months, 4 weeks ago

I think the answer should be reversed, as per the docu <https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke?tabs=cli#virtual-network-peering%20%20%20Previous%20QuestionsNext%20Questions>

- Configure the peering connection in the hub to allow gateway transit.

- Configure the peering connection in each spoke to use remote gateways.

upvoted 2 times

 **sshera** 1 year ago

In exam 04jan23

upvoted 2 times

 **sapien45** 1 year, 3 months ago

Make sure to set AllowGatewayTransit when peering VNet-Hub to VNet-Spoke and UseRemoteGateways when peering VNet-Spoke to VNet-Hub.

<https://learn.microsoft.com/en-us/azure/firewall/tutorial-hybrid-ps>

upvoted 3 times

 **sapien45** 1 year, 4 months ago

Allow forwarded traffic does not apply here, Allow forwarded traffic is so you can have a network appliance (NVA) in the hub that routes traffic between two spokes. When the NVA goes to forward the traffic from spoke 1 into spoke 2, this setting needs to be enabled or else Azure SDN will drop the traffic.

Details on <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke#spoke-connectivity>

upvoted 1 times

 **derrrp** 1 year, 6 months ago

It will help to remember that the hub needs to know the remote networks available from on-prem (-UseRemoteGateways) whereas a spoke network which will be connected to the hub is where you'll need to worry about making it transitive so that traffic can route through (-AllowGatewayTransit)

-AllowForwardedTraffic does not get used at all but let's move FORWARD onto the next question now that we've got this one memorized.

upvoted 2 times

🗨️ 👤 **Edward1** 1 year, 9 months ago

The answers are correct.
upvoted 1 times

🗨️ 👤 **jj22222** 1 year, 9 months ago

on test April 10 2022
upvoted 1 times

🗨️ 👤 **Joshalom** 1 year, 11 months ago

on exam 6/2/2022
upvoted 1 times

🗨️ 👤 **Joshalom** 1 year, 12 months ago

on exam 28/1/2022
upvoted 1 times

🗨️ 👤 **Takloy** 2 years ago

Seems correct...

I find the article below better.

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-peering-gateway-transit#ps-same>

upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

DRAG DROP -

You have three on-premises sites. Each site has a third-party VPN device.

You have an Azure virtual WAN named VWAN1 that has a hub named Hub1. Hub1 connects two of the three on-premises sites by using a Site-to-Site VPN connection.

You need to connect the third site to the other two sites by using Hub1.

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.

Select and Place:

Actions

Download the VPN configuration file from VWAN1

In a Hub1, create a VPN gateway

In a Hub1, create a VPN site

In a Hub1, create a connection to the VPN site

Configure the VPN device

Answer Area

Correct Answer:

Actions

In a Hub1, create a VPN gateway

Answer Area

In a Hub1, create a VPN site

In a Hub1, create a connection to the VPN site

Download the VPN configuration file from VWAN1

Configure the VPN device

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-site-to-site-portal>

 **derrp** Highly Voted 1 year, 6 months ago

To help remember, visualize:

You've already got the VPN infrastructure setup in Azure so you need to create the Site, Create the connection to the site, Download the stuff, then setup the on-prem side.

Make the site, connect to site, download the thing, config the on-prem.

upvoted 41 times

 **Stevy_nash** 1 year ago

your way of explaining stuff is so funny but I it thx (^_^)

upvoted 2 times

 **srikanth1987** Highly Voted 2 years, 3 months ago


Answer is correct. As already two VPN S2S are formed, means that, VGW is there.

upvoted 38 times

 **jeffangel28** 1 year, 5 months ago

Right!

upvoted 1 times

 **Takloy** 1 year, 6 months ago

You're right.

upvoted 1 times

🗄️ **Techbiz** Most Recent 4 months ago

The answer is correct and the Gateway is already isn't due to the existence of the first two vpn connections
upvoted 1 times

🗄️ **jakubklapka** 4 months ago

In exam Sep, 2023
upvoted 1 times

🗄️ **Rajan395** 1 year ago

Correct Answer
upvoted 1 times

🗄️ **sujay1982** 1 year, 4 months ago

Right Answer
upvoted 2 times

🗄️ **GGbis** 1 year, 6 months ago

Answer is correct. <https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-site-to-site-portal#vnet>
upvoted 1 times

🗄️ **bmulvIT** 1 year, 11 months ago

On exam 3/3/2022
upvoted 4 times

🗄️ **rockethack** 1 year, 11 months ago

This question was on the exam on 18th Feb 2022.
upvoted 4 times

🗄️ **Kimimoto** 1 year, 11 months ago

Appeared in exam on 11/Feb/2022
upvoted 3 times

🗄️ **KranthiChaitanya** 2 years ago

Came on exam 28/Jan/22
upvoted 2 times

🗄️ **Pravda** 2 years ago

on exam 1/6/2022
upvoted 3 times

🗄️ **AidenYoukhana** 2 years ago

CORRECT ANSWER.
upvoted 2 times

🗄️ **JoMa** 2 years, 1 month ago

Correct answer
upvoted 4 times

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT -

You are planning an Azure solution that will contain the following types of resources in a single Azure region:

- ☞ Virtual machine
- ☞ Azure App Service
- ☞ Virtual Network gateway
- ☞ Azure SQL Managed Instance

App Service and SQL Managed Instance will be delegated to create resources in virtual networks.

You need to identify how many virtual networks and subnets are required for the solution. The solution must minimize costs to transfer data between virtual networks.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Virtual Networks:

1
2
3
4

Subnets:

1
2
3
4

Answer Area

Correct Answer:

Virtual Networks:

1
2
3
4

Subnets:

1
2
3
4

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-for-azure-services#services-that-can-be-deployed-into-a-virtual-network>

Pravda Highly Voted 2 years, 1 month ago

Question was on exam 11/2021
I believe the answer to be 1 and 4.

Web page given in answer, and below states App Service Environment requires a dedicated subnet.

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-for-azure-services#services-that-can-be-deployed-into-a-virtual-network>
upvoted 35 times

prepper666 Highly Voted 2 years, 2 months ago

Correct answer is 1 Vnet. 3 Subnets are needed.

Gateway subnet for VPN Gateway.



Default subnet for VM

Dedicated subnet for SQL Managed instance.

<https://azure.microsoft.com/en-gb/resources/templates/sql-managed-instance-azure-environment/>

No subnet is needed for App Service. Build it and dont just believe the answers written here as many answers are wrong.

upvoted 14 times

  **volto** 4 months, 1 week ago

App service needs Vnet -> "App Service (...) will be delegated to create resources in virtual networks."

upvoted 1 times

  **roshingrg** 7 months ago

Yes, you need a dedicated subnet for Azure App Service if you want to integrate your app with an Azure virtual network. The subnet must be allocated an IPv4 /28 block (16 addresses). We recommend that you have a minimum of 64 addresses (IPv4 /26 block) to allow for maximum horizontal scale.

If you don't integrate your app with an Azure virtual network, you don't need a dedicated subnet. However, your app will be exposed to the public internet, which may not be desirable for some applications.

Here are the subnet requirements for Azure App Service Environment:

The subnet must be empty.

The subnet must be delegated to Microsoft. Web/hostingEnvironments.

The size of the subnet should be at least /26 (64 addresses).

If you are using Windows Containers, you will need to allocate an additional IP address per app for each App Service plan instance. This means that if you have 10 Windows Container App Service plan instances with 4 apps running, you will need 50 IP addresses and additional addresses to support horizontal (up/down) scale.

upvoted 1 times

  **leonmflai4exam** 1 year, 10 months ago

For Azure WebApp, we need to add webapp-integration subnet. <https://docs.microsoft.com/en-us/azure/app-service/networking/nat-gateway-integration>

upvoted 6 times

  **Ajdlfasudfo** 1 year, 1 month ago

you better get some experience before shouting so loud lol

upvoted 1 times

  **NSF2** Most Recent 3 weeks, 4 days ago

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-for-azure-services#services-that-can-be-deployed-into-a-virtual-network>

1 and 4 are correct.

upvoted 1 times

  **AzureLearner01** 10 months, 2 weeks ago

Provided answer is correct. You need a subnet for the vm, a dedicated for the gateway, app service (vnet integration) and sql managed instance.

upvoted 4 times

  **Libaax01** 10 months, 3 weeks ago

The provided answer is correct and can be confirmed by the original linked shared.

1 Virtual Network (Vnet)

4 Subnets (Default subnet where the VMs will reside, Dedicated subnet for APP Services, Dedicated subnet for Virtual Network Gateway, and finally dedicated subnet for SQL Managed services)

upvoted 1 times

  **Rajan395** 1 year ago

Given answer is correct.

upvoted 1 times

  **sapien45** 1 year, 3 months ago

The solution must minimize costs to transfer data between virtual networks.

Meaning App service Gateway-required virtual network integration is not an option.

The regional virtual network integration feature enables you to place the back end of your app in a subnet in a Resource Manager virtual network in the same region as your app. This feature isn't available from an App Service Environment, which is already in a virtual network.

<https://learn.microsoft.com/en-us/azure/app-service/networking-features>

4 it is

upvoted 3 times

  **Jamesat** 1 year, 5 months ago

This was on my exam on 22/08/2022

The correct answer did indeed seem to be 1 and 4.

A subnet for the VPN Gateway

Subnet for VMs

Subnet for App Service VNET integration (as delegated)

Subnet for SQL Managed Instance (as delegated)

upvoted 7 times

🗨️ **1particle** 1 year, 6 months ago

1 and 4

<https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/connectivity-architecture-overview?view=azuresql#high-level-connectivity-architecture>

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-for-azure-services#services-that-can-be-deployed-into-a-virtual-network>

VPN gateway of course needs a VPN subnet

VM will be in the 4th

upvoted 1 times

🗨️ **Payday123** 1 year, 7 months ago

"App Service and SQL Managed Instance will be delegated to create resources in virtual networks" so App service requires delegates subnet for integration!

upvoted 2 times

🗨️ **Whatsamattr81** 1 year, 8 months ago

Correct is 4. 2 subnets for the VPN gateway, the app service and vm can be on the same one, and Azure SQL Managed Instance must be deployed within an Azure virtual network and the subnet dedicated for managed instances only.

upvoted 1 times

🗨️ **Madball** 1 year, 9 months ago

I believe the given answer is correct, my reasoning for this is as follows.

1. Azure SQL Managed Instance requires its own subnet.

2. A Virtual Network Gateway requires its own subnet.

3. An app service by default does not connect to a virtual network and is accessible by its public frontend. It is my understanding that if you want an app service to integrate with a virtual network you need to enable VNET integration, which requires its own subnet.

4. The VM can share subnets, however in this question there are 4 resources and three of them require their own subnet, meaning the VM will require its own subnet in this instance.

upvoted 8 times

🗨️ **bmulvIT** 1 year, 11 months ago

On exam today 3/3/2022

upvoted 1 times

🗨️ **rockethack** 1 year, 11 months ago

This question was on the exam on 18th Feb 2022.

upvoted 1 times

🗨️ **Beitran** 1 year, 11 months ago

"Virtual network integration depends on a dedicated subnet. "

<https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration#gateway-required-vnet-integration>

So yes, 4 subnets is correct

upvoted 1 times

🗨️ **Kimimoto** 1 year, 11 months ago

Appeared in exam on 11/Feb/2022

upvoted 1 times

🗨️ **Contactfornitish** 2 years ago

Appeared in exam on 17/01/2022

upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 two Azure virtual networks named Vnet1 and Vnet2.

You have a Windows 10 device named Client1 that connects to Vnet1 by using a Point-to-Site (P2S) IKEv2 VPN.

You implement virtual network peering between Vnet1 and Vnet2. Vnet1 allows gateway transit. Vnet2 can use the remote gateway.

You discover that Client1 cannot communicate with Vnet2.

You need to ensure that Client1 can communicate with Vnet2.

Solution: You download and reinstall the VPN client configuration.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

The VPN client must be downloaded again if any changes are made to VNet peering or the network topology.

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-point-to-site-routing>

Community vote distribution

A (100%)

 **d0bermann** Highly Voted 1 year, 11 months ago

Selected Answer: A

A.The VPN client must be downloaded again if any changes are made to VNet peering or the network topology
upvoted 9 times

 **Verytutos** Most Recent 4 months, 2 weeks ago


Appeared on Exam 05 Sep 2023
upvoted 1 times

 **JennyHuang36** 11 months, 1 week ago


In exam Feb, 2023
upvoted 1 times

 **Rajan395** 1 year ago

Given answer is correct
upvoted 1 times

 **yyts** 1 year, 3 months ago

Does Windows10 work with IKEv2 P2S VPN?
upvoted 2 times

 **jilguens** 1 year, 4 months ago

Selected Answer: A

right a
upvoted 1 times

 **AckeyGraham** 1 year, 11 months ago

Questions in wrong order - you get the answer on earlier pages, but again with no context. Doesn't tell you that the client was downloaded prior to any changes being made to an existing network, then peering setup...then the client has an issue - not sure if that will be told in the actual exam - i'd hope so.
upvoted 2 times

 **Joshalom** 1 year, 12 months ago

correct....on exam 28/1/2022
upvoted 1 times

 **AidenYoukhana** 2 years ago

CORRECT ANSWER.
upvoted 1 times

🗨️ 👤 **Pravda** 2 years ago

On exam. 11/2021

upvoted 2 times

🗨️ 👤 **Cova16** 2 years, 2 months ago

correct

upvoted 1 times

🗨️ 👤 **prepper666** 2 years, 2 months ago

Agreed. Initial config was downloaded before vNet1 and vNet2 were peered.

upvoted 1 times

🗨️ 👤 **Sbgani** 2 years, 3 months ago

correct

upvoted 4 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

You have an Azure virtual network named Vnet1 that hosts an Azure firewall named FW1 and 150 virtual machines. Vnet1 is linked to a private DNS zone named contoso.com. All the virtual machines have their name registered in the contoso.com zone.

Vnet1 connects to an on-premises datacenter by using ExpressRoute.

You need to ensure that on-premises DNS servers can resolve the names in the contoso.com zone.

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

NOTE: Each correct selection is worth one point.

- A. Modify the DNS server settings of Vnet1.
- B. For FW1, configure custom DNS server.
- C. For FW1, enable DNS proxy.
- D. On the on-premises DNS servers, configure forwarders that point to the frontend IP address of FW1.
- E. On the on-premises DNS servers, configure forwarders that point to the Azure provided DNS service at 168.63.129.16.

Correct Answer: CD

Reference:

<https://docs.microsoft.com/en-us/azure/private-link/private-endpoint-dns#on-premises-workloads-using-a-dns-forwarder>

<https://azure.microsoft.com/en-gb/blog/new-enhanced-dns-features-in-azure-firewall-now-generally-available/>

Community vote distribution

CD (100%)

 **erima21** Highly Voted 1 year, 4 months ago

Requests sent to Azure DNS Private Zones go to the platform address of 168.63.129.16 that is only reachable from inside of Azure. Therefore, if the DNS request originates from on-premises (outside of Azure), there is a requirement to proxy the DNS request via a service inside of a Virtual Network.

With this general availability announcement, Azure Firewall DNS proxy is an option to meet this DNS forwarding requirement, applicable with a hub-and-spoke model. To do this, configure your on-premises DNS server to conditionally forward requests to Azure Firewall for the required zone name.

upvoted 12 times

 **Whatsamattr81** Highly Voted 1 year, 8 months ago

C and D... whilst E looks correct, it isn't a viable answer. Currently that IP address resolves to ns1-02.azure-dns.com - on which your custom domain may not even sit. If the on-premise DNS was bind, it probably skip the dns proxy stuff and just put forwarders in but the question and possible answers don't mention that scenario.

upvoted 9 times

 **MrBlueSky** 10 months ago

Put more simply, the reason why E is wrong is because an Azure Private DNS Zone cannot be used by on-premises resources. For that they would need to use Azure DNS Private Resolver. It's a specific resource for this exact scenario described in the question:

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

upvoted 1 times

 **CristianM99** Most Recent 6 months ago

Selected Answer: CD

C and D

upvoted 2 times

 **AzureLearner01** 10 months, 2 weeks ago

Correct Answer, you need conditional forwarding for the on-prem DNS to the Azure Firewall. In the firewall policy enable DNS Proxy.

upvoted 1 times

 **sapien45** 1 year, 4 months ago

Selected Answer: CD

Azure Firewall DNS proxy is an option to meet this DNS forwarding requirement, applicable with a hub-and-spoke model. To do this, configure your on-premises DNS server to conditionally forward requests to Azure Firewall for the required zone name. Ensure that your private DNS zone is linked to the Virtual Network within which the Azure Firewall resides. Configure Azure Firewall to use the default Azure DNS for lookups, and enable DNS proxy in Azure Firewall DNS settings.

<https://azure.microsoft.com/en-us/blog/new-enhanced-dns-features-in-azure-firewall-now-generally-available/>

upvoted 5 times

 **AdityaGupta** 1 year, 4 months ago

Selected Answer: CD

Explanation provided by "Erima21" is best. There are two ways to do it.

1) Create DNS Proxy on Azure Firewall in Hub VNET to forward all external DNS requests (from On-prem) to Azure DNS (168.63.129.16) and configure your on-prem DNS server with forwarder to Azure Firewall DNS Proxy. In this case you can still use Azure DNS in VNETs or configure them with Azure Firewall DNS Proxy IP (Custom DNS server)

1) Provision a VM as custom DNS Server in Hub VNET and configure all your private zones requests and external DNS requests to be forwarded to Azure DNS (168.63.129.16) and configure your on-prem DNS server with forwarder to Azure DNS VM.

upvoted 5 times

  **Takloy** 1 year, 6 months ago

Can someone explain why the answers are CD?
I thought E would be one of the answers.

upvoted 2 times

  **john6732** 1 year, 6 months ago

Technically you would need to perform both B and C, but enable DNS proxy is the best exam answer. You need to add the custom server and then turn on Proxy so that the AFW sends DNS to said server.

DNS proxy listens for requests on TCP port 53 and forwards them to Azure DNS or the custom DNS specified.

upvoted 2 times

  **unclegrandfather** 1 year, 7 months ago

A version of this question appeared on the exam. Make sure you know WHY these are correct

upvoted 2 times

  **kinder2** 1 year, 7 months ago

Selected Answer: CD

DNS proxy configuration requires three steps:

Enable DNS proxy in Azure Firewall DNS settings.

Optionally configure your custom DNS server or use the provided default.

Finally, you must configure the Azure Firewall's private IP address as a custom DNS server in your virtual network DNS server settings. This ensures DNS traffic is directed to Azure Firewall.


upvoted 7 times

  **milan92stankovic** 1 year, 8 months ago

Selected Answer: CD

C and D are correct.

upvoted 4 times

  **mdnick** 1 year, 8 months ago

Provided answers are correct. This is similar to private link resolution.



<https://github.com/adstuart/azure-privatelink-dns-azurefirewall>

upvoted 4 times

  **madsa** 1 year, 8 months ago

So it would be A and C, not E as per the link, I would much appreciate it if someone can clarify this question for me, what is the actual answer and why?

upvoted 1 times

  **RVR** 1 year, 8 months ago

A & E would be better options?

upvoted 2 times

  **jkklm** 1 year, 9 months ago

ae - the answer

upvoted 1 times

  **jamelia1303** 1 year, 9 months ago

better explanation : <https://azure.microsoft.com/en-us/blog/new-enhanced-dns-features-in-azure-firewall-now-generally-available/>

upvoted 2 times

You are planning the IP addressing for the subnets in Azure virtual networks.
Which type of resource requires IP addresses in the subnets?

- A. internal load balancers
- B. storage account
- C. Azure Virtual Networks NAT
- D. service endpoint policies

Correct Answer: A

Reference:

<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview>

Community vote distribution

A (100%)

 **SOMINAZURE** 10 months, 3 weeks ago

Selected Answer: A

yes correct

upvoted 4 times

 **JennyHuang36** 11 months, 1 week ago


In exam Feb,2023

upvoted 2 times

 **sellamibassem** 11 months, 1 week ago

A is correct

upvoted 1 times

 **Rajan395** 1 year ago

A is correct for sure

upvoted 1 times

 **degiro** 1 year, 3 months ago

Selected Answer: A

Answer is correct.

upvoted 1 times

 **Prutser2** 1 year, 3 months ago

Selected Answer: A

for sure

upvoted 1 times

 **Jawad1462** 1 year, 3 months ago

Selected Answer: A

Answer is correct A

upvoted 1 times

 **Alessandro365** 1 year, 4 months ago

Selected Answer: A

A, correct answer


upvoted 1 times

 **AdityaGupta** 1 year, 4 months ago

Selected Answer: A


Undoubtly A, Internal Load Balancer.

upvoted 1 times

 **naidu** 1 year, 4 months ago

Yes Correct answer

upvoted 2 times

 **Villaran** 1 year, 4 months ago

Selected Answer: A

A. internal load balancers
upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT -

You have an Azure subscription.

You have the on-premises sites shown the following table.

Name	Number of users	Connection type to Azure
Site 1	500	ExpressRoute
Site 2	100	Site-to-Site VPN
Site 3	1	Point-to-Site (P2S) VPN

You plan to deploy Azure Virtual WAN.

You are evaluating Virtual WAN Basic and Virtual WAN Standard.

Which type of Virtual WAN can you use for each site? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Virtual WAN Basic:

	▼
Site2 only	
Site3 only	
Site2 and Site3 only	
Site1, Site2, and Site3	

Virtual WAN Standard:

	▼
Site1 only	
Site1 and Site3 only	
Site2 and Site3 only	
Site1, Site2, and Site3	

Correct Answer:

Answer Area

Virtual WAN Basic:

	▼
Site2 only	
Site3 only	
Site2 and Site3 only	
Site1, Site2, and Site3	

Virtual WAN Standard:

	▼
Site1 only	
Site1 and Site3 only	
Site2 and Site3 only	
Site1, Site2, and Site3	

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about>

AdityaGupta Highly Voted 1 year, 4 months ago

VWAN Type Hub type Available configurations

Basic Basic Site-to-site VPN only

Standard Standard ExpressRoute

User VPN (P2S)

VPN (site-to-site)

Inter-hub and VNet-to-VNet transiting through the virtual hub

Azure Firewall

NVA in a virtual WAN

upvoted 12 times

galahad Most Recent 6 days, 3 hours ago

In exam Jan 20, 2024

upvoted 2 times

jakubklapka 4 months ago

In exam Sep, 2023

upvoted 1 times

raffylian 5 months, 1 week ago

on exam 8-23

upvoted 2 times

omgMerrick 11 months, 2 weeks ago

Given answer is correct.

<https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about#basicstandard>

upvoted 2 times

Rajan395 1 year ago

Answer is correct. Basic sku supports Site-to-Site only

upvoted 2 times

Jawad1462 1 year, 3 months ago

That's correct

upvoted 3 times

fun_and_games 1 year, 4 months ago

Vitual WAN

Basic

Site-to-site Only

Standard

ExpressRoute

User VPN (P2S)

VPN (site-to-site)

Inter-hub and VNet-to-VNet transiting through the virtual hub

Azure Firewall

NVA in a virtual WAN

<https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about#basicstandard>

upvoted 4 times

Cristoicach91 1 year, 4 months ago

This is correct.

upvoted 3 times

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT -

You have an Azure subscription that contains two virtual networks named Vnet1 and Vnet2.

You register a public DNS zone named fabrikam.com. The zone is configured as shown in the Public DNS Zone exhibit.

The screenshot displays the configuration for the public DNS zone 'Fabrikam.com'. The 'Essentials' section shows the following details:

- Resource group (change): rg1
- Subscription (change): Subscription1
- Subscription ID: 169d1bba-ba4c-471c-b513-092eb7063265
- Name server 1: ns1-06.azure-dns.com.
- Name server 2: ns2-06.azure-dns.net.
- Name server 3: ns3-06.azure-dns.org.
- Name server 4: ns4-06.azure-dns.info.
- Tags (change): Click here to add tags

A message indicates: "You can search for record sets that have been loaded on this page. If you don't see what you're looking for, you can try scrolling to allow more record sets to load."

The 'Search record sets' section contains the following table:

Name	Type	TTL	Value
@	NS	172800	ns1-06.azure-dns.com. ns2-06.azure-dns.net. ns3-06.azure-dns.org. ns4-06.azure-dns.info.
@	SOA	3600	Email: azuredns-hostmaster.microsoft.com Host: ns1-06.azure-dns.com. Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 300 Serial number: 1
appservice1	A	3600	131.107.1.1
www	CNAME	3600	appservice1.fabrikam.com

You have a private DNS zone named fabrikam.com. The zone is configured as shown in the Private DNS Zone exhibit.



+ Record set → Move v Delete zone Refresh

Essentials

JSON View

Resource group (change) : rg1

Subscription (change) : Subscription1

Subscription ID : 169d1bba-ba4c-471c-b513-092eb7063265

Tags (change) : [Click here to add tags](#)

i You can search for record sets that have been loaded on this page. If you don't see what you're looking for, you can try scrolling to allow more record sets to load.

Search record sets

Name	Type	TTL	Value	Auto registered
@	SOA	3600	Email: azureprivatedns-host.microsoft.co... Host: azureprivatedns.net Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 10 Serial number: 1	False

Subscription (change) : Subscription1

Subscription ID : 169d1bba-ba4c-471c-b513-092eb7063265

Tags (change) : [Click here to add tags](#)

i You can search for record sets that have been loaded on this page. If you don't see what you're looking for, you can try scrolling to allow more record sets to load.

Search record sets

Name	Type	TTL	Value	Auto registered
@	SOA	3600	Email: azureprivatedns-host.microsoft.co... Host: azureprivatedns.net Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 10 Serial number: 1	False
appservice1	A	3600	131.107.100.10	False
server1	A	3600	131.107.100.1	False
server2	A	3600	131.107.100.2	False
server3	A	3600	131.107.100.3	False
www	CNAME	3600	appservice1.fabrikam.com	False

You have a virtual network link configured as shown in the Virtual Network Link exhibit.

+ Add Refresh

Search virtual network links

Link Name	Link status	Virtual network	Auto-Registration	
vnet1_link	Completed	Vnet1	Disabled	...

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Queries for www.fabrikam.com from the internet are resolved to 131.107.1.1.	<input type="checkbox"/>	<input type="checkbox"/>
Queries for server1.fabrikam.com can be resolved from the internet.	<input type="checkbox"/>	<input type="checkbox"/>
Queries for www.fabrikam.com from Vnet2 are resolved to 131. 107.100. 10.	<input type="checkbox"/>	<input type="checkbox"/>

Correct Answer:

Answer Area

Statements	Yes	No
Queries for www.fabrikam.com from the internet are resolved to 131.107.1.1.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Queries for server1.fabrikam.com can be resolved from the internet.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Queries for www.fabrikam.com from Vnet2 are resolved to 131. 107.100. 10.	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Box 1: Yes -

DNS queries from the internet use the public DNS zone. In the public DNS zone, www.fabrikam.com is a CNAME record that resolves to appservice1.fabrikam.com which resolves to 131.107.1.1.

Box 2: No -

DNS queries from the internet use the public DNS zone. There is no DNS record for server1.fabrikam.com in the public DNS zone.

Box 3: No -

The private DNS zone is linked to VNet1, not VNet2. Therefore, resources in VNet2 cannot query the private DNS zone.

AdityaGupta Highly Voted 1 year, 4 months ago

The given answers and explanations are correct, please pay attention to following details if you are confused.

1) Public DNS Zones are created for Internet Dns requests.

2) Private DNS Zones are created to cater internal DNS requests.

3) Private DNS Zones must be linked (private links) to VNETs to ensure that resources inside that VNET can make use of private dns zone. In this case it "VNET1_Link" created but no "VNET2_Link" is created.

upvoted 30 times

 **wsrudmen** Highly Voted 1 year, 8 months ago

CORRECT!!

upvoted 12 times

 **Techbiz** Most Recent 4 months ago

Answer and explanation given are correct

upvoted 1 times

 **_fvt** 9 months, 4 weeks ago

They say : "You register a Public DNS zone" but not "and you delegate your domain from your registrar to the Public DNS zone" so this step is missing. The wording for the Private DNS is "You have" so this is different here they don't mention any step. I think the difference is important and the fact that they choose this for the Public DNS is probably because the delegate step is missing.

<https://learn.microsoft.com/en-us/azure/dns/dns-delegate-domain-azure-dns>

Should be NNN (for the last one VNet2 is not linked to private DNS so cannot resolve names in the private DNS)

upvoted 1 times

 **Rajan395** 1 year ago

absolutely correct.

upvoted 1 times

 **DeepMoon** 1 year ago

Public dns zone doesn't have cname record for www. So how can internet queries for www resolve to 131.107.1.1?

Box 1 should be NO.

Box 2 should be NO - there is no server1 record on public dns.

Box 3 No. vnet 2 is not linked to the private dns zone.

upvoted 2 times

 **Skankhunt** 12 months ago

Look carefully there's a host-A record for appservice1 in Public DNS Zone.

upvoted 5 times

 **sshera** 1 year ago

In exam 04Jan23

upvoted 2 times

 **Prutser2** 1 year, 3 months ago

correct,

upvoted 1 times

 **jeffangel28** 1 year, 5 months ago

Given answer and explanation is correct

upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT -

You have two Azure virtual networks named VNet1 and VNet2 in an Azure region that has three availability zones.

You deploy 12 virtual machines to each virtual network, deploying four virtual machines per zone. The virtual machines in VNet1 host an app named App1. The virtual machines in VNet2 host an app named App2.

You plan to use Azure Virtual Network NAT to implement outbound connectivity for App1 and App2.

You need to identify the minimum number of subnets and Virtual Network NAT instances required to meet the following requirements:

- ☞ A failure of two zones must NOT affect the availability of either App1 or App2.
- ☞ A failure of two zones must NOT affect the outbound connectivity of either App1 or App2.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Minimum number of subnets:

	▼
1	
2	
6	
12	

Minimum number of Virtual Network NAT instances:

	▼
1	
2	
6	
12	

Correct Answer:

Answer Area

Minimum number of subnets:

	▼
1	
2	
6	
12	

Minimum number of Virtual Network NAT instances:

	▼
1	
2	
6	
12	

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-overview>

 **pinchocr** Highly Voted 1 year, 7 months ago

You cannot assign more than one nat gw to a subnet. 6 subnets are required (3 in vnet1 and 3 in vnet2). Then assign zonal nat gateways to each subnet

upvoted 29 times

 **Komy** 1 year, 7 months ago

Not right. Even though you can not assign multiple NAT GW to th same subnet - however - Multiple subnets within the same virtual network can use the same NAT gateway. so we can create 2 Subnets(1 per each VNET) and 2 NAT GW (1 per each Vnet/subnet).. and because NAT GW is zonal, we will have to multiply that by 3 = 6 NAT GW

2 subnets/ 6 NAT GW
upvoted 10 times

🗨️ 👤 **Komy** 1 year, 7 months ago

Correction: Reviewing the below architecture, answer should be: 6 Subnets / 6 NAT GW

<https://docs.microsoft.com/en-us/azure/architecture/networking/guide/well-architected-network-address-translation-gateway>

upvoted 21 times

🗨️ 👤 **john6732** 1 year, 6 months ago

This is correct:

Availability zone isolation cannot be provided, unless each subnet only has resources within a specific zone. Instead, deploy a subnet for each of the availability zones where VMs are deployed, align the zonal VMs with matching zonal NAT gateways, and build separate zonal stacks. For example, a virtual machine in availability zone 1 is on a subnet with other resources that are also only in availability zone 1. A NAT gateway is configured in availability zone 1 to serve that subnet.

upvoted 7 times

🗨️ 👤 **sapien45** 1 year, 4 months ago

I concur, but best is to prove your point with official Azure Litteraure

<https://learn.microsoft.com/en-us/azure/architecture/networking/guide/well-architected-network-address-translation-gateway>

upvoted 3 times

🗨️ 👤 **Jorex** Highly Voted 1 year, 8 months ago

I would say 2 subnets, because the subnets are regional resources, hence they exists in all zones and 6 NAT gateways (Virtual NAT refers to virtual NAT gateway: <https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-overview>), because the NAT gateway is zonal, so you have to deploy a NAT gateway in each zone to have the full redundancy. (<https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-overview#virtual-network-nat-basics>)

upvoted 19 times

🗨️ 👤 **khanda** 9 months, 2 weeks ago

You cant attach multiple NAT gateways to a single subnet.

upvoted 1 times

🗨️ 👤 **Goofer** 1 year ago

See - <https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-availability-zones#zonal-nat-gateway-resource-for-each-zone-in-a-region-to-create-zone-resiliency>

upvoted 1 times

🗨️ 👤 **Sanaz90** 1 year, 4 months ago

Multiple NAT gateways can't be attached to a single subnet.

upvoted 3 times

🗨️ 👤 **Arkadeep** 1 year, 7 months ago

1 subnet can have only 1 nat gateway, so 6 subnets are required for 6 nat gateway.

upvoted 9 times

🗨️ 👤 **NSF2** Most Recent 3 weeks, 4 days ago

As fas I can see, the given answer is correct.
See below.

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview#virtual-networks-and-availability-zone>

"Virtual networks and subnets span all availability zones in a region. You don't need to divide them by availability zones to accommodate zonal resources. For example, if you configure a zonal VM, you don't have to take into consideration the virtual network when selecting the availability zone for the VM. The same is true for other zonal resources."

upvoted 1 times

🗨️ 👤 **DumpMaster69** 2 months, 2 weeks ago

1 subnet for all VMs hosting App1 in VNet1.

1 subnet for all VMs hosting App2 in VNet2.

Subnets are zone-redundant. They consist of 3 zones and an outage of 2 does not impact the workload.

1 NAT GW instance per VNet that stretch all VMs per 1 subnet.

Awnser is correct.

upvoted 3 times

🗨️ 👤 **groox** 5 months ago

I think it will be 2 NATs as these Virtual Networks are not peered and they will have their own NATs. No of subnets wont change the no of NATs needed because the subnets share the address space from the network they are in.

upvoted 1 times

🗨️ 👤 **mein17** 5 months, 1 week ago



We cannot associate multiple NAT Gateways to single subnet.

But

Can a single NAT Gateway be applied to multiple subnets within a single VNet??

If yes then the answer is = 6 Subnets + 2 NAT Gateways.



upvoted 2 times

  **mein17** 5 months, 1 week ago

If No.

Then 6 Subnets + 6 NAT Gateways.



upvoted 2 times

  **mein17** 5 months, 1 week ago

NAT gateway can provide outbound connectivity for virtual machines from other availability zones different from itself. The virtual machine's subnet needs to be configured to the NAT gateway resource to provide outbound connectivity. Additionally, multiple subnets can be configured to the same NAT gateway resource.

While virtual machines in subnets from different availability zones can all be configured to a single zonal NAT gateway resource, this configuration doesn't provide the most effective method for ensuring zone-resiliency against zonal outages.

upvoted 1 times

  **mein17** 5 months, 1 week ago

So if we consider the most effective method

then

6 Subnets + 6 NAT Gateways would be the most fulfilling answer for this question.

upvoted 4 times

  **charrua86** 6 months ago

according to this reference documentation, we must create a subnet for our resources in each availability zone, therefore, we must have 6 subnets and 6 nat gateway to guarantee resilience. There would be 3 Nat gateways on vnet 1 and 3 nat gateways on vnet 2.

<https://learn.microsoft.com/pt-br/azure/architecture/networking/guide/well-architected-network-address-translation-gateway#reliability>

upvoted 4 times

  **roshingrg** 7 months, 1 week ago

The minimum number of subnets required is 6, and the minimum number of Virtual Network NAT instances required is 3.

Here is the reasoning:

To meet the requirement that a failure of two zones must not affect the availability of either App1 or App2, we need to place the virtual machines for each app in at least two different zones. This means that we need a total of 6 zones, 3 for each app.

To meet the requirement that a failure of two zones must not affect the outbound connectivity of either App1 or App2, we need to place a Virtual Network NAT instance in each zone. This means that we need a total of 3 NAT instances.

Therefore, the minimum number of subnets required is 6, and the minimum number of Virtual Network NAT instances required is 3.

Answer:

Minimum number of subnets: 6

Minimum number of Virtual Network NAT instances: 3

upvoted 2 times

  **roshingrg** 7 months, 1 week ago

The number of NAT instances that can be deployed in a single region is 1, 2, 6, or 12. Therefore, the minimum number of NAT instances required in this case is 2.

The answer would then be:

Minimum number of subnets: 6

Minimum number of Virtual Network NAT instances: 2

I apologize for the error in my previous response.

upvoted 2 times

  **occupatissimo** 9 months ago

NAT GW is a zonal resource

To have complete availability configure 6+6

upvoted 4 times

  **michealnghe** 10 months ago

Correct answer must be

6 subnets

6 NAT Gateways

<https://azure.microsoft.com/en-us/blog/ensure-zone-resilient-outbound-connectivity-with-nat-gateway/>

upvoted 8 times

  **MightyMonarch74** 10 months, 1 week ago

Correct answer should be 6 subnets with 6 NAT GW, using a zonal NAT gateway resource for each zone in a region as per

<https://docs.microsoft.com/en-us/azure/architecture/networking/guide/well-architected-network-address-translation-gateway>

upvoted 4 times

  **AzureLearner01** 10 months, 2 weeks ago

NAT gateway resources are highly available in one availability zone and span multiple fault domains. NAT gateway can be deployed to "no zone" in which Azure automatically selects a zone to place NAT gateway. NAT gateway can also be isolated to a specific zone by a user.

Availability zone isolation cannot be provided, unless each subnet only has resources within a specific zone. Instead, deploy a subnet for each of the availability zones where VMs are deployed, align the zonal VMs with matching zonal NAT gateways, and build separate zonal stacks. For example, a virtual machine in availability zone 1 is on a subnet with other resources that are also only in availability zone 1. A NAT gateway is configured in availability zone 1 to serve that subnet.

See the diagram at

<https://learn.microsoft.com/en-us/azure/architecture/networking/guide/well-architected-network-address-translation-gateway>

upvoted 1 times

  **stack120566** 10 months, 2 weeks ago

One subnet in each zone for each Vnet =6 subnets

need to Nat gateways in each zone .Nat gateways can not be associated with subnets from different vnets .. only 1 Nat gateway per subnet. = 6 Nat gateways

upvoted 1 times

  **zukako** 10 months, 4 weeks ago

NAT gateway cannot associate subnet across VNETS->2

Azure subnet can has vms in multi-Az->2

upvoted 1 times

  **omgMerrick** 11 months, 1 week ago

6 and 6.

The minimum number of subnets required is six, one for each zone in each virtual network. This way, you can associate a NAT gateway resource to each subnet and provide outbound connectivity for all compute resources in that subnet2.

The minimum number of Virtual Network NAT instances required is six, one for each subnet. This way, you can ensure that a failure of two zones will not affect the availability or outbound connectivity of either App1 or App2.

upvoted 3 times

  **Madball** 12 months ago

I personally believe the answer should be 6 and 6, the reason for this is as follows, you have 24 VMs in total with 12 deployed to each VNET. To help with availability you will deploy 4 VMs to each availability zone.

The first question is how many subnets are required (minimum), and this is the part that will trick people into the wrong answer if they are unsure on how NAT gateway is deployed. Technically at this point you would only need two subnets because VNETS do not care about zones, however you cannot deploy two or more NAT gateways to the same subnet and NAT gateways are zonal.

This means that to cover 3 availability zones, you will need 3 NAT gateways, which then in turn means you need to link each NAT gateway to a separate subnet (3 subnets) giving a total of 6 NAT gateways and 6 subnets across the two VNETS.

upvoted 7 times

  **sandydh** 1 year ago

Zonal NAT gateway resource for each zone in a region to create zone-resiliency. <https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-availability-zones>.

Exact scenario is given in simpler form.

Since, it is expected to provide protection against 2 zone failures, hence, 3 subnets per vNET is needed and 4 VM's per Zone making it 12.

Answer should be 6 Subnets and 6 NAT

upvoted 4 times

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT -

You have the Azure resources shown in the following table.

Name	Type	Location
Vnet1	Virtual network	East US
Vnet1\Subnet1	Subnet	East US
Vnet1\GatewaySubnet	Subnet	East US
Vnet2	Virtual network	West US
Vnet2\Subnet1	Subnet	West US
Vnet2\GatewaySubnet	Subnet	West US
WebApp1	Azure App Service web app	East US

WebApp1 uses the Standard pricing tier.

You need to ensure that WebApp1 can access the virtual machines deployed to Vnet1\Subnet1 and Vnet2\Subnet1. The solution must minimize costs.

What should you create in each virtual network? To answer, select the appropriate options in the answer area.

Hot Area:

Answer Area:

Vnet1:

<input type="checkbox"/>	An additional subnet
<input type="checkbox"/>	A peering connection
<input type="checkbox"/>	A private endpoint
<input type="checkbox"/>	A VPN gateway

Vnet2:

<input type="checkbox"/>	An additional subnet
<input type="checkbox"/>	A peering connection
<input type="checkbox"/>	A private endpoint
<input type="checkbox"/>	A VPN gateway

Correct Answer:

Answer Area:

Vnet1:

<input type="checkbox"/>	An additional subnet
<input type="checkbox"/>	A peering connection
<input type="checkbox"/>	A private endpoint
<input type="checkbox"/>	A VPN gateway

Vnet2:

<input type="checkbox"/>	An additional subnet
<input type="checkbox"/>	A peering connection
<input type="checkbox"/>	A private endpoint
<input checked="" type="checkbox"/>	A VPN gateway

Box 1: An additional subnet -

Regional virtual network integration: When you connect to virtual networks in the same region, you must have a dedicated subnet in the

virtual network you're integrating with.

Box 2: A VPN gateway -

Gateway-required virtual network integration: When you connect directly to virtual networks in other regions or to a classic virtual network in the same region, you need an Azure Virtual Network gateway created in the target virtual network.

Note: If your app is in an App Service Environment, it's already in a virtual network and doesn't require use of the VNet integration feature to reach resources in the same virtual network.

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration>

  **Cristoicach91** Highly Voted 1 year, 4 months ago

Answer is correct. You need to create for VNET1 a subnet, because you can do Regional VNET integration since the web app and the VNET1 are in the same region. VNET2 is in a different region so you would need a VPN gate and a P2S (consider that in VNET2 you already have a GatewaySubnet which doesn't necessarily mean you have a VPN gate created, it just means you created a subnet called GatewaySubnet).
upvoted 28 times

  **Flacky_Penguin32** 1 year, 1 month ago

not to mention "minimize costs"; peering is free.
upvoted 3 times

  **sapien45** 1 year, 4 months ago

Thanks Cristoicach91 !
upvoted 2 times

  **leaviu1** Highly Voted 1 year ago

Answer given is not correct.

Correct answer: Vnet1 - an additional subnet

Correct answer: Vnet2 - a peering connection

From same attached documentation:

<https://learn.microsoft.com/en-us/azure/app-service/overview-vnet-integration>

Regional virtual network integration: When you connect to virtual networks in the same region, you must have a dedicated subnet in the virtual network you're integrating with.

Using regional virtual network integration enables your app to access:

Resources in the virtual network you're integrated with.

Resources in virtual networks peered to the virtual network your app is integrated with including global peering connections.

(you could use a gateway if you wanted to connect directly, but it is not a requirement here. Cost is.)

upvoted 13 times

  **aklas** 9 months, 2 weeks ago

This is the answer as it says minimizing costs and the public doc says integration allows access to include global peering connections.
upvoted 1 times

  **AzureLearner01** Most Recent 10 months, 4 weeks ago

I think there are multiple right answers to this. After evaluating in my lab i would go for private endpoint. Why? Because it establishes a connection between the PaaS Service WebApp and your VM. Private endpoints are typically less expensive than VPN Gateways, so i would go for it. VNet peering seems also a way but, the App is not in a Vnet and the question is what are you creating in each VNet, so I would go for Private Endpoint. Let me know what you think about this.

upvoted 2 times

  **AzureLearner01** 10 months, 2 weeks ago


Correct myself. Private endpoint is only used for incoming traffic to your app. Outgoing traffic won't use this private endpoint. You can inject outgoing traffic to your network in a different subnet through the virtual network integration feature. So i would go for subnet in the same region an VNet peering

upvoted 3 times

  **Skankhunt** 12 months ago

Answer is correct. There is no need to have connectivity between Vnet1 and Vnet2 (might actually not be allowed)..The requirements only states App Service needs connection to Vnet1 and Vnet2

upvoted 3 times

  **MrBlueSky** 9 months, 2 weeks ago

It mentions minimizing cost. The most cost effective way to achieve the goal is to use a new subnet (for app integration) + peering
upvoted 2 times

  **Rajan395** 1 year ago

exam topic answer seem to be correct
upvoted 1 times

  **TJ001** 1 year ago

because there are 2 VNETs involved and now VNET integration supports global peering connections ..I will go with vnet peering for second question..first is correct

upvoted 1 times

🗨️ 👤 **TJ001** 1 year ago

If it is single VNET scenario where App Service and VNET are in different region then the only option for direct integration is set up VPN gateway and SSTP P2S VPN

upvoted 1 times

🗨️ 👤 **DerekKey** 1 year ago

Answer:

An additional subnet -----> Regional virtual network integration: When you connect to virtual networks in ---> the same region <--- , you must have a dedicated subnet in the virtual network you're integrating with.

A VPN gateway -----> Gateway-required virtual network integration: When you connect directly to virtual networks in ---> other regions <--- or to a classic virtual network in the same region, you need an Azure Virtual Network gateway created in the target virtual network.

upvoted 1 times

🗨️ 👤 **Tightbot** 1 year, 1 month ago

Ans: Additional subnet and Peering connection

Explanation:

Using regional virtual network integration enables your app to access:

- 1)Resources in the virtual network you're integrated with.
- 2)Resources in virtual networks peered to the virtual network your app is integrated with including global peering connections.

<https://learn.microsoft.com/en-us/azure/app-service/overview-vnet-integration#regional-virtual-network-integration>

upvoted 3 times

🗨️ 👤 **Flacky_Penguin32** 1 year, 1 month ago

I feel since these are both connected by the Azure global network and if these are both in the same tenant and owned by the same owner, if you have a vnet in US East and a vnet is US West, then in my mind Answer 1 is 'vnet peering' and Answer 2 is 'vnet peering'.

upvoted 1 times

🗨️ 👤 **Flacky_Penguin32** 1 year, 1 month ago

having the gateway subnet is irrelevant, its meant to confuse.

upvoted 1 times

🗨️ 👤 **Flacky_Penguin32** 1 year, 1 month ago

not to mention "minimize costs"; peering is free.

upvoted 1 times

🗨️ 👤 **jellybiscuit** 1 year, 3 months ago

I agree that the first option is an additional subnet for vnet integration.

For the second option, I would personally create a peering (between vnet1 and vnet2)

- it works
- it requires no additional steps
- cost difference is hard to know without knowing the traffic details

VPN: pay for 2 gateways and egress traffic

Peering: pay for ingress/egress traffic

Problems with the VPN choice

- it does not work without also creating a VPN gateway in vnet 1
- Does the existence of gateway subnets imply that I can use them? Or that they are in use? I have no way of knowing.
- Not addressed in the question, but it limits my bandwidth.

upvoted 4 times

🗨️ 👤 **wooyourdaddy** 10 months, 2 weeks ago

Think the flaw in the logic is that VNET1 and VNET2 have to have connectivity. App Service plans can't have more than two virtual network integrations per App Service plan. Multiple apps in the same App Service plan can use the same virtual network integration. Currently you can only configure the first integration through Azure portal. The second integration must be created using Azure Resource Manager templates or Azure CLI commands.

The suggested answer assumes you use the VNET integration model to connect to VNET1, and the Gateway required VNET integration model to connect to VNET2. No interconnectivity between VNET1 and VNET2.

The documentation is not clear on if these 2 models can exist together. I would go with peering myself for the 2nd answer.

upvoted 1 times

🗨️ 👤 **wooyourdaddy** 10 months, 2 weeks ago

So found some additional information that provides the correct context for this question.

The question states 'WebApp1 uses the Standard pricing tier.' Not sure what it was at the time of the question months ago, but when you create an App Service Plan, only the Windows Operating System option has a Standard pricing tier.

When I create a standard Windows App Service Plan and go to the Networking section under settings and then click on 'Click here to manage', I am brought to the VNET Integration management page where it states:

Regional VNET Integrations 0/2

Gateway required VNET Integrations 0/5

This confirms that the 2 models can exist together. So the correct answer is an additional subnet in VNET1 and a virtual network gateway in VNET2.

upvoted 4 times

🗨️ 👤 **Aanandan** 1 year, 3 months ago

your right... Same question raised for me... if enabled peering between Vnet-1 and vnet-2 ,it will be less cost and easy to manage the connectivity... But if we used VPN gateway need more configuration for enable the connectivity

upvoted 1 times

🗨️ 👤 **AdityaGupta** 1 year, 4 months ago

correct.

upvoted 3 times

🗨️ 👤 **sapien45** 1 year, 4 months ago

So helpful, truly appreciate your valuable contributions

upvoted 9 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT -

You have the Azure App Service app shown in the App Service exhibit.

The VNet Integration settings for as12 are configured as shown in the Vnet Integration exhibit.

The Private Endpoint connections settings for as12 are configured as shown in the Private Endpoint connections exhibit.

Private Endpoint connections

+ Add Refresh | ✓ Approve ✗ Reject 🗑 Remove



Private Endpoint connections

Private access to services hosted on the Azure platform, keeping your data on the Microsoft network [Learn more](#)

Filter by name or description

All connection states

Connection name ↑↓ Connection state ↑↓ Private endpoint ↑↓ Description

No results.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements

Yes

No

Subnet2 can contain only App Service apps in the ASP1 App Service plan

As12 will use an IP address from Subnet2 for network communications

Computers in Vnet1 will connect to a private IP address when they connect to as12

Correct Answer:

Answer Area

Statements

Yes

No

Subnet2 can contain only App Service apps in the ASP1 App Service plan

As12 will use an IP address from Subnet2 for network communications

Computers in Vnet1 will connect to a private IP address when they connect to as12

Box 1: Yes -

The integration subnet can be used by only one App Service plan.

Box 2: No -

No Private Endpoint connections defined.

When regional virtual network integration is enabled, your app makes outbound calls through your virtual network. The outbound addresses that are listed in the app properties portal are the addresses still used by your app. However, if your outbound call is to a virtual machine or private endpoint in the integration virtual network or peered virtual network, the outbound address will be an address from the integration subnet.

Box 3: Yes -

Apps in App Service are hosted on worker roles. Regional virtual network integration works by mounting virtual interfaces to the worker roles with addresses in the delegated subnet. Because the from address is in your virtual network, it can access most things in or through your virtual network like a VM in your virtual network would.

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration>

YYN

Y / <https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration#limitations>

Y / VNet integrated App Service uses IP from dedicated subnet to communicate resources in the VNet. (vNet integration : outbound / private endpoint : inbound)

<https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration#how-regional-virtual-network-integration-works>

N / There's no private endpoint.

upvoted 37 times

 **AdityaGupta** Highly Voted 1 year, 4 months ago

Correct Answer is: YYN

1) Subnet2 is delegated to ASP.

2) Virtual network integration gives your app access to resources in your virtual network, but it doesn't grant inbound private access to your app from the virtual network. Private site access refers to making an app accessible only from a private network, such as from within an Azure virtual network. Virtual network integration is used only to make outbound calls from your app into your virtual network.

<https://learn.microsoft.com/en-us/azure/app-service/overview-vnet-integration#gateway-required-vnet-integration>:~:text=Virtual%20network%20integration%20gives%20your%20app%20access%20to%20resources%20in,make%20outbound%20calls%20from%20your%20app%20into%20your%20virtual%20network.

3) There is no Private Endpoint configured and again VNET integration only allows outbound network communication, no inbound communication is allowed.

upvoted 18 times

 **DumpMaster69** Most Recent 2 months, 2 weeks ago

Y - It is limited to the service plan (delegate)

N - Only outbound calls to resources in the VNet will use a private IP. I define the words 'network communication' as 'all communication', which will not use a derived private IP.

Y - Computer is in the same VNet, so outbound calls will use a private IP from the subnet

upvoted 1 times

 **Lazylinux** 1 month ago

U R clueless, it is YYN and as per others comments

upvoted 1 times

 **khanda** 9 months, 2 weeks ago

YYN are the correct answers. App will use private IP from the vnet-intergration subnet for outbound calls.

upvoted 2 times

 **mrgreat** 10 months ago

YYN is the correct

upvoted 1 times

 **ruirosamendes** 10 months, 2 weeks ago

Y - Subnet2 is delegated to ASP

N - Network comunication (IN/OUT). Only Out is possible!

Y - APP goes out, and presents to VMs or ourthes devics on the network with the "From IP". An IP from the delegated subnet. So VM connects back to the IP in private IP of the subnet

upvoted 1 times

 **AzureLearner01** 10 months, 4 weeks ago

YYN, a Subnet is delegated to an App service plan. without PE it wouldn't use the internal IPs from the VNet.

upvoted 1 times

 **AzureLearner01** 10 months, 2 weeks ago

Have to correct myself. YYN

When virtual network integration is enabled, your app makes outbound calls through your virtual network. The outbound addresses that are listed in the app properties portal are the addresses still used by your app. However, if your outbound call is to a virtual machine or private endpoint in the integration virtual network or peered virtual network, the outbound address is an address from the integration subnet.

upvoted 1 times

 **Ayokun** 11 months, 2 weeks ago

YYN

1,2)Uses ip from the subnet only for outbound connectivity

3 Uses ip from the subnet only for outbound connectivity

upvoted 2 times

 **mm2** 1 year ago

YYN

1) it's one subnet one app sp

2) AP service will use IP from integration vnet for communication but just for outbound connection (and responses back, but traffic have to be initiated by App service)

3) N - because if you need inbound traffic - so clients would like to reach app service first - then you need private endpoint which has not been configured in our example

upvoted 3 times

 **Tightbot** 1 year, 1 month ago

3)Ans: N

Explanation: Private Endpoint is only used for incoming flows to your Web App. Outgoing flows won't use this Private Endpoint. You can inject outgoing flows to your network in a different subnet through the virtual network integration feature.

Since there is no private endpoint configured for the app service, the VMs in the same vnet cannot reach the app service. So, the correct statement would be; Computers in Vnet1 will connect to a private IP address when they connect to as12 "when there is a private endpoint for the app created on Vnet1"

<https://learn.microsoft.com/en-us/azure/app-service/networking/private-endpoint#conceptual-overview>

upvoted 2 times

  **kimalto452** 1 year, 4 months ago

YNN

The inbound rules don't apply because>>> you can't use virtual network integration to provide inbound access to your app.

upvoted 6 times

  **Cristoicach91** 1 year, 4 months ago

YNN. You can have only 1 subnet per APP service plan. You don't have a PE defined. You don't have a PE defined.

upvoted 1 times

  **Cristoicach91** 1 year, 4 months ago

Correction. The Private Endpoint uses an IP from the Subnet and it will be used for an WEB APP service. In the image it doesn't show one configured, because there might not exist a WEB APP service yet, so answer is YYY.

upvoted 1 times

  **jellybiscuit** 1 year, 4 months ago

You were right the first time. There is no PE configured.

upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

You have a hub-and-spoke topology. The topology includes multiple on-premises locations that connect to a hub virtual network in Azure via ExpressRoute circuits.

You have an Azure Application Gateway named GW1 that provides a single point of ingress from the internet.

You plan to migrate the hub-and-spoke topology to Azure Virtual WAN.

You need to identify which changes must be applied to the existing topology. The solution must ensure that you maintain a single point of ingress from the internet.

Which three changes should you include in the solution? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Add user-defined routes.
- B. Add virtual network peerings.
- C. Replace the user-defined routes used by the current topology.
- D. Create virtual network connections.
- E. Remove the existing virtual network peerings.
- F. Redeploy GW1.

Correct Answer: CDE

Transition connectivity to virtual WAN hub:

Step 1. (E) Delete the existing peering connections from Spoke virtual networks to the old customer-managed hub. Access to applications in spoke virtual networks is unavailable until steps 1-3 are complete.

Step 2. (D) Connect the spoke virtual networks to the Virtual WAN hub via VNet connections.

Step 3. (C) Remove any user-defined routes (UDR) previously used within spoke virtual networks for spoke-to-spoke communications. This path is now enabled by dynamic routing available within the Virtual WAN hub.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-wan/migrate-from-hub-spoke-topology>

Community vote distribution

CDE (100%)

 **AdityaGupta** Highly Voted 1 year, 4 months ago

Selected Answer: CDE

The given answers are correct and in correct sequence.

First you need to remove existing VNET peering (E) then add VNET connections from VWAN Hub to same spoke VNETs (D) and later removed any existing UDRs you defined earlier. (C).

There is no need to replot App Gateway. Since it is VWAN there will be Vnet connection, no VNET peering.

upvoted 11 times

 **AdityaGupta** 1 year, 4 months ago

There is no new UDRs required as it will be replaced by VWAN Hub Dynamic Routing.

upvoted 3 times

 **flurgen248** Highly Voted 11 months, 1 week ago

Selected Answer: CDE

The answers are correct. They're specifically listed order on this page: <https://learn.microsoft.com/en-us/azure/virtual-wan/migrate-from-hub-spoke-topology#step-5-transition-connectivity-to-virtual-wan-hub>

a. Delete the existing peering connections from Spoke virtual networks to the old customer-managed hub. Access to applications in spoke virtual networks is unavailable until steps a-c are complete.

b. Connect the spoke virtual networks to the Virtual WAN hub via VNet connections.

c. Remove any user-defined routes (UDR) previously used within spoke virtual networks for spoke-to-spoke communications. This path is now enabled by dynamic routing available within the Virtual WAN hub.

upvoted 5 times

 **jakubklapka** Most Recent 4 months ago

In exam Sep, 2023

upvoted 1 times

You have an application named App1 that listens for incoming requests on a preconfigured group of 50 TCP ports and UDP ports.

You install App1 on 10 Azure virtual machines.

You need to implement load balancing for App1 across all the virtual machines. The solution must minimize the number of load balancing rules.

What should you include in the solution?

- A. Azure Application Gateway V2 that has multiple listeners
- B. Azure Standard Load Balancer that has Floating IP enabled
- C. Azure Standard Load Balancer that has high availability (HA) ports enabled
- D. Azure Application Gateway v2 that has multiple site hosting enabled

Correct Answer: A

Azure Application Gateway is limited to 100 active listeners that are routing traffic. Active listeners = total number of listeners - listeners not active.

If a default configuration inside a routing rule is set to route traffic (for example, it has a listener, a backend pool, and HTTP settings) then that also counts as a listener.

Note: Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications.

Application Gateway can make routing decisions based on additional attributes of an HTTP request, for example URI path or host headers.

This type of routing is known as application layer (OSI layer 7) load balancing.

Incorrect:

Not B: Floating IP. Some application scenarios prefer or require the same port to be used by multiple application instances on a single VM in the backend pool.

Common examples of port reuse include:

clustering for high availability

network virtual appliances

exposing multiple TLS endpoints without re-encryption.

Not D: Multiple site hosting enables you to configure more than one web application on the same port of application gateways using public-facing listeners. It allows you to configure a more efficient topology for your deployments by adding up to 100+ websites to one application gateway. Each website can be directed to its own backend pool.

Reference:

<https://github.com/MicrosoftDocs/azure-docs/blob/main/includes/application-gateway-limits.md>

Community vote distribution

C (100%)

 **Cristoicach91** Highly Voted 1 year, 4 months ago

Selected Answer: C

C. Azure Standard Load Balancer that has high availability (HA) ports enabled

App1 is installed on 10 VMs which can be put in a Backend pool. The req is to minimize the number of load balancing rules. If you select HA it will allow you to have 1 rule for TCP and UDP ports, if you don't select HA you will need to have a minimum of 2 rules for TCP and UDP with a * range.

upvoted 20 times

 **sshera** Highly Voted 1 year ago

In exam 04Jan23

upvoted 8 times

 **vigklk** 8 months, 2 weeks ago

what was the answer?

upvoted 1 times

 **jakubklapka** Most Recent 4 months ago

In exam Sep, 2023

upvoted 2 times

 **Ben_88** 7 months, 2 weeks ago

Selected Answer: C

As stated in <https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-ha-ports-overview>

Load balance a large number of ports

You can also use HA ports for applications that require load balancing of large numbers of ports. You can simplify these scenarios by using an internal standard load balancer with HA ports. A single load-balancing rule replaces multiple individual load-balancing rules, one for each port.
upvoted 3 times

🗨️ **Oklama** 8 months, 1 week ago

Selected Answer: C

C is correct
upvoted 1 times

🗨️ **tomtom2022** 9 months ago

Selected Answer: C

C is correct
upvoted 1 times

🗨️ **mrgreat** 10 months, 1 week ago

C is correct

When you enable high availability (HA) ports on the load balancer, it creates a single rule for all the ports of the virtual machines in the back-end pool.

upvoted 1 times

🗨️ **jellybiscuit** 1 year, 3 months ago

Selected Answer: C

<https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-ha-ports-overview>

upvoted 1 times

🗨️ **sapien45** 1 year, 4 months ago

Selected Answer: C

Load balance a large number of ports

You can also use HA ports for applications that require load balancing of large numbers of ports. You can simplify these scenarios by using an internal standard load balancer with HA ports. A single load-balancing rule replaces multiple individual load-balancing rules, one for each port.

<https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-ha-ports-overview>

upvoted 2 times

🗨️ **AdityaGupta** 1 year, 4 months ago

Selected Answer: C

Here the requirement is on TCP and UDP ports, not HTTP or HTTPS, hence application gateway is ruled out.

Incorrect Answer B: Some application scenarios prefer or require the same port to be used by multiple application instances on a single VM in the backend pool. Common examples of port reuse include:

clustering for high availability

network virtual appliances

exposing multiple TLS endpoints without re-encryption.

If you want to reuse the backend port across multiple rules, you must enable Floating IP in the rule definition.

<https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-floating-ip>

Correct Answer is C: - The HA ports load-balancing rules are configured when you set the front-end and back-end ports to 0 and the protocol to All. The internal load balancer resource then balances all TCP and UDP flows, regardless of port number

<https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-ha-ports-overview>

upvoted 7 times

🗨️ **Alessandro365** 1 year, 4 months ago

Selected Answer: C

C is correct
upvoted 1 times

🗨️ **Alessandro365** 1 year, 4 months ago

Selected Answer: C

C is correct
upvoted 2 times

🗨️ **Sayden** 1 year, 4 months ago

C. <https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-faq>. UDP is layer 4. Application gateway is layer 7.

upvoted 1 times

🗨️ **zenithcsa1** 1 year, 4 months ago

Selected Answer: C

Application gateway does not support UDP protocol.

In order to minimize the number of load-balancing rules, HA ports load-balancing rule should be used.

upvoted 4 times

DRAG DROP -

You register a DNS domain with a third-party registrar.

You need to host the DNS zone on 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.

Select and Place:

Actions	Answer Area
Identify the FQDNs of the name servers.	
Create a public DNS zone.	
Identify the IP addresses of the name servers.	
Modify the SOA records for the domain.	
Modify the NS records for the domain.	

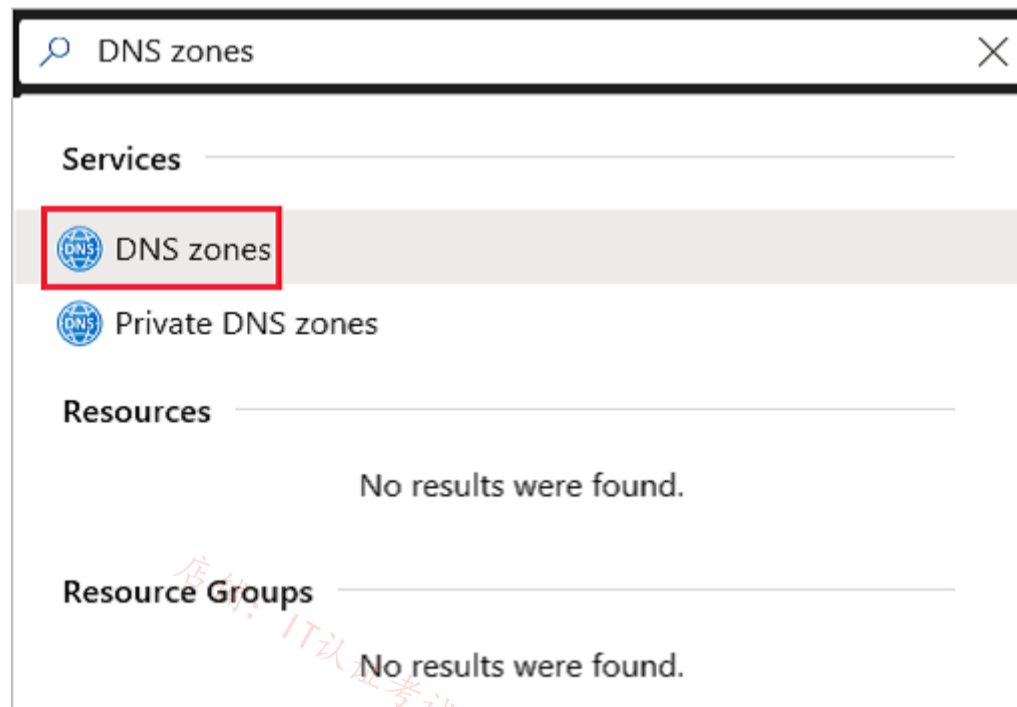
Correct Answer:

Actions	Answer Area
	Create a public DNS zone.
	Identify the FQDNs of the name servers.
Identify the IP addresses of the name servers.	Modify the NS records for the domain.
Modify the SOA records for the domain.	

Step 1: Create a public DNS zone.

Create a DNS zone -

1. Go to the Azure portal to create a DNS zone. Search for and select DNS zones.



2. Select Create DNS zone.

3. On the Create DNS zone page, enter the following values, and then select Create.

Step 2: Identify the FQDNs of the name servers.

Retrieve name servers.

Before you can delegate your DNS zone to Azure DNS, you need to know the name servers for your zone. Azure DNS gives name servers from a pool each time a zone is created.

With the DNS zone created, in the Azure portal Favorites pane, select All resources. On the All resources page, select your DNS zone. If the subscription you've selected already has several resources in it, you can enter your domain name in the Filter by name box to easily access the application gateway.

Retrieve the name servers from the DNS zone page. In this example, the zone contoso.net has been assigned name servers ns1-01.azure-dns.com, ns2-

01.azure-dns.net, *ns3-01.azure-dns.org, and ns4-01.azure-dns.info:

Home > Resource groups > ContosoRG > contoso.net

contoso.net
DNS zone

Search (Ctrl+/)

Record set Move Delete zone Refresh

Resource group (change)
contosorg

Subscription (change)
Microsoft Azure Internal Consumption

Subscription ID
xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

Tags (change)
Click here to add tags

Name server 1
ns1-08.azure-dns.com.

Name server 2
ns2-08.azure-dns.net.

Name server 3
ns3-08.azure-dns.org.

Name server 4
ns4-08.azure-dns.info.

SETTINGS

Properties

Locks

Automation script

MONITORING

Metrics (Preview)

Alerts

SUPPORT + TROUBLESHOOTING

New support request

Search record sets

NAME	TYPE	TTL	VALUE
@	NS	172800	ns1-08.azure-dns.com. ns2-08.azure-dns.net. ns3-08.azure-dns.org. ns4-08.azure-dns.info.
@	SOA	3600	Email: azuredns-hostmaster.microsoft.com Host: ns1-08.azure-dns.com. Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 300 Serial number: 1

Azure DNS automatically creates authoritative NS records in your zone for the assigned name servers.

Step 3: Modify the NS records for the domain.

Delegate the domain -

Once the DNS zone gets created and you have the name servers, you'll need to update the parent domain with the Azure DNS name servers. Each registrar has its own DNS management tools to change the name server records for a domain.

1. In the registrar's DNS management page, edit the NS records and replace the NS records with the Azure DNS name servers.
2. When you delegate a domain to Azure DNS, you must use the name servers that Azure DNS provides. Use all four name servers, regardless of the name of your domain. Domain delegation doesn't require a name server to use the same top-level domain as your domain.

Reference:

<https://docs.microsoft.com/en-us/azure/dns/dns-delegate-domain-azure-dns>

omgMerrick Highly Voted 11 months, 1 week ago

The answer is correct.

Source:

<https://learn.microsoft.com/en-us/azure/dns/dns-delegate-domain-azure-dns>

upvoted 7 times

Lazylinux Most Recent 2 months, 3 weeks ago

Given Answer is correct

upvoted 1 times

Rajan395 1 year ago

correct answers

upvoted 2 times

TJ001 1 year ago

correct answers

upvoted 1 times

Jawad1462 1 year, 3 months ago

Correct

upvoted 1 times

[Removed] 1 year, 4 months ago

Correct..

upvoted 1 times

 **AdityaGupta** 1 year, 4 months ago

Correct : - <https://learn.microsoft.com/en-us/azure/dns/dns-delegate-domain-azure-dns>
upvoted 4 times

 **Cristoicach91** 1 year, 4 months ago

correct
upvoted 2 times

店铺：IT认证考试服务

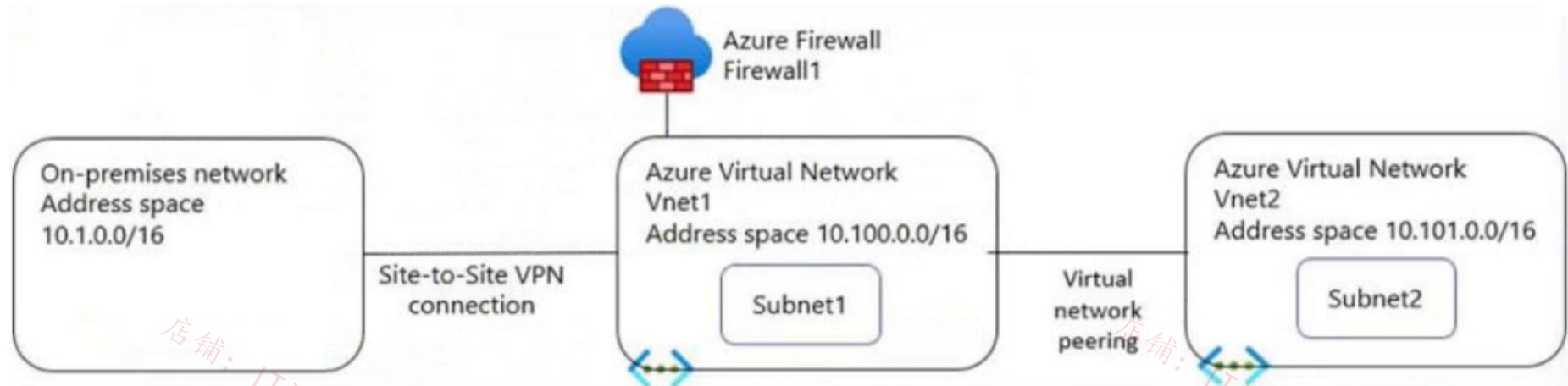
店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

HOTSPOT -

You have the network topology shown in the Topology exhibit. (Click the Topology tab.)



You have the Azure firewall shown in the Firewall1 exhibit. (Click the Firewall1 tab.)

All services > Firewalls >

Firewall1

Firewall

Delete Lock

Visit Azure Firewall Manager to configure and manage this firewall. →

Essentials JSON View

Resource group (change) RG2	Firewall sku Standard
Location North Europe	Firewall subnet AzureFirewallSubnet
Subscription (change) Visual Studio Premium with MSDN	Firewall public IP Firewall1-IP1
Subscription ID 8372f433-2dcd-4361-b5ef-5b188fed87d0	Firewall private IP 10.100.253.4
Virtual network Vnet1	Management subnet -
Firewall policy FirewallPolicy	Management public IP -
Provisioning state Succeeded	Private IP Ranges Managed by Firewall Policy
Tags (change) Click here to add tags	

You have the route table shown in the RouteTable1 exhibit. (Click the RouteTable1 tab.)

店铺: IT认证考试服务

店铺: IT认证考试服务

RouteTable1

Route table



» → Move ▾ 🗑️ Delete ↻ Refresh 🗨️ Give feedback

^ Essentials

JSON View

Resource group (change)
RG1

Associations
1 subnet associations

Location
North Europe

Subscription (change)
Visual Studio Premium with MSDN

Subscription ID
8372f433-2dcd-4361-b5ef-5b188fed87d0

Tags (change)
Click here to add tags

Routes

🔍 Search routes

Name	↑↓	Address prefix	↑↓	Next hop type	↑↓	Next hop IP address	↑↓
Route1		10.1.0.0/16		Virtual network gateway		-	...
Route2		0.0.0.0/0		Virtual appliance		10.100.253.4	...

Subnets

🔍 Search subnets

Name	↑↓	Address range	↑↓	Virtual network	↑↓	Security group	↑↓
Subnet1		10.100.1.0/24		Vnet1		-	...

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
The resources in Subnet1 can connect to the internet through Firewall1.	<input type="radio"/>	<input type="radio"/>
The resources in Subnet1 can connect to the resources in Vnet2.	<input type="radio"/>	<input type="radio"/>
The resources in Subnet2 can connect to the internet through Firewall1.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
The resources in Subnet1 can connect to the internet through Firewall1.	<input checked="" type="radio"/>	<input type="radio"/>
The resources in Subnet1 can connect to the resources in Vnet2.	<input checked="" type="radio"/>	<input type="radio"/>
The resources in Subnet2 can connect to the internet through Firewall1.	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: Yes -

Resources in Subnet1 will use the Route2 and its Next hop ID address to the Firewall to reach the Internet.

Box 2: Yes -

Yes, with network network peering.

Box 3: No -

Resources in Subnet2 can only reach resources in Subnet1, as gateway transit for virtual network peering has not been configured.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview> <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-peering-gateway-transit>

🗄️ 👤 **Sheriboy** Highly Voted 1 year, 4 months ago

Answer seems correct,
Y - it will go through VA which is firewall
Y - there is a peering, so subnet and subnet2 can communicate
N - there is no route for subnet 2 through VA/firewall
upvoted 18 times

🗄️ 👤 **AdityaGupta** 1 year, 4 months ago

Look at the exhibits again, the route table is associated to only subnet1 and not to subnet2.

Even though there is peering enabled, since route table is not associated with subnet2, it can't connect to Internet using Route Table.

It is worth noting that there is no mention of gateway transit in VNET peering, as explained in given answers "gateway transit for virtual network peering has not been configured."

Routes to the gateway-connected virtual networks or on-premises networks will propagate to the routing tables for the peered virtual networks using gateway transit. You can disable the automatic route propagation from the VPN gateway. Create a routing table with the "Disable BGP route propagation" option, and associate the routing table to the subnets to prevent the route distribution to those subnets.

<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-peering-gateway-transit#:~:text=Routes%20to%20the,to%20those%20subnets.>

upvoted 2 times

🗄️ 👤 **charlesr1700** Highly Voted 1 year, 4 months ago

I would say correct:
Y: Traffic will flow through the FW because of the 0.0.0.0/0 rule
Y: Traffic will flow through the FW then onto vNet 2 through the peer.
N: No route for subnet 2 through the FW so it will use Azure default to connect to the web
upvoted 9 times

🗄️ 👤 **Murad01** Most Recent 1 month, 3 weeks ago

Appeared on Exam November - 2023
upvoted 1 times

🗄️ 👤 **Lazylinux** 2 months, 3 weeks ago

given answer is correct
Y - it will go through firewall which route rule 2
Y - there is a peering, hence vnet-vnet communication ok
N - there is no route for subnet 2 to firewall as routing table is only associated to subnet1
upvoted 1 times

🗄️ 👤 **Qunlay** 9 months ago

Transit gateway or remote gateway must be enable for resources in Vnet1 to talk to Vnet2. Therefore Subnet1 and subnet2 cannot communicate.
Answer is Y,N,N
upvoted 2 times

🗄️ 👤 **Qunlay** 9 months ago

Correct answer is Y,N,N
upvoted 2 times

🗄️ 👤 **_fvt** 9 months, 3 weeks ago

I would have put YYN.
Y - the firewall has a public IP and Route Table applied to Subnet 1 is correct and making traffic to internet go through FW.
Y - But maybe with asymmetric routing ? User-Defined routes takes precedence over Default routes (<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview>), so the traffic from Subnet 1 to Subnet 2 will go through Firewall, then through the peering to Subnet 2. Subnet 2 however don't have UDR assigned so then answer will go through default route, not the Firewall. If the traffic was initiated from Subnet 2 the answer from Subnet 1 to Subnet 2 will go through azure FW and likely be dropped as no first packet (SYN) was found (not gone though FW from Subnet 2 to 1). So communication from Subnet 1 to Subnet 2 => YES, but from Subnet 2 to Subnet 1 would have not been possible.
N - Not UDR applied to Subnet 2 so it will use default routes and not go through Firewall.
upvoted 1 times

🗄️ 👤 **Accounts** 10 months ago

YYN
Y- Will go through FW - 0.0.0.0 route
N- subnet2 doesn't have RT
N- No route through FW
upvoted 3 times

🗄️ 👤 **Rajan395** 1 year ago

Answers seem to be correct
upvoted 1 times

🗄️ 👤 **TJ001** 1 year ago

YYN
Second yes, because peering route takes precedence over UDR
upvoted 1 times

☒ **DerekKey** 1 year ago

YYN

Second YES - explanation

Traffic between directly peered VNets is routed directly even if a UDR points to Azure Firewall as the default gateway. To send subnet-to-subnet traffic to the firewall in this scenario, a UDR must contain the target subnet network prefix explicitly on both subnets.

upvoted 1 times

☒ **zukako** 1 year ago

Y

Y

N- explanation is wrong. The reason is udr is not attached to subnet2

upvoted 1 times

☒ **sapien45** 1 year, 4 months ago

YYN

Route for 0.0.0.0/0 would direct any flow going to VNET2 to go through the Firewall, and therefore going nowhere.

There are no routes for peering VNET1-VNET2

upvoted 6 times

☒ **sapien45** 1 year, 3 months ago

YYN. I stand corrected.

The screenshot just show the detail on ONE route table.

the resulting routes in EFFECTIVE routes is not shown there, since the two VNETS are peered, VNET peering CDIR range takes priority

upvoted 7 times

☒ **Cristoicach91** 1 year, 4 months ago

YYN. The default for subnet one is NH to FW NVA. The effective routes doesn't show that you are aware of the VNET2 address space (no route).

There is no Subnet2 associated to the RT1.

upvoted 2 times

☒ **zenithcsa1** 1 year, 4 months ago

There's peering between Vnet1 and Vnet2. Effective routes can be seen in Network Interface menu, not Route Table.

upvoted 3 times

☒ **[Removed]** 1 year, 4 months ago

Peering is there just to connect. If no route configured, will use system route but here in subnet 1, there is route, says 0.0.0.0/0 to NVA.. traffic will go via FW only. answer is YNN

upvoted 1 times

☒ **[Removed]** 1 year, 4 months ago

YYN

The question is asking if Subnet1 can connect to the resources in Vnet2, not about how it is connecting to Vnet2.

So yes, Subnet1 can connect to Vnet2 via Firewall1

upvoted 3 times

店铺: IT认证考试服务

店铺: IT认证考试服务

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 two Azure virtual networks named Vnet1 and Vnet2.

You have a Windows 10 device named Client1 that connects to Vnet1 by using a Point-to-Site (P2S) IKEv2 VPN.

You implement virtual network peering between Vnet1 and Vnet2. Vnet1 allows gateway transit. Vnet2 can use the remote gateway.

You discover that Client1 cannot communicate with Vnet2.

You need to ensure that Client1 can communicate with Vnet2.

Solution: You resize the gateway of Vnet1 to a larger SKU.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

The VPN client must be downloaded again if any changes are made to VNet peering or the network topology.

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-point-to-site-routing>

Community vote distribution


B (100%)

 **Stevy_nash** Highly Voted 1 year ago

"You resize the gateway of Vnet1 to a larger SKU"

Bro why would u do that ? are u okay ?

upvoted 7 times

 **anishk** 7 months, 1 week ago

Bro, why give options

upvoted 1 times

 **AdityaGupta** Most Recent 1 year, 4 months ago

You need to download VPN client again, since there are topology changes.

upvoted 4 times

 **jilguens** 1 year, 4 months ago

Selected Answer: B

correct

upvoted 2 times

You have an Azure subscription that contains the virtual networks shown in the following table.

Name	In resource group	Location
Vnet1	RG1	West US
Vnet2	RG1	Central US
Vnet3	RG2	Central US
Vnet4	RG2	West US
Vnet5	RG3	East US

You plan to deploy an Azure firewall named AF1 to RG1 in the West US Azure region.

To which virtual networks can you deploy AF1?

- A. Vnet1 and Vnet4 only
- B. Vnet1, Vnet2, Vnet3, and Vnet4
- C. Vnet1 only
- D. Vnet1 and Vnet2 only
- E. Vnet1, Vnet2, and Vnet4 only

Correct Answer: C

Azure Firewall operates in a single VNET.

Azure Firewall is a regional service.

Yes. Vnet1: Same VNET and same region.

No. Vnet2: Same Resource Group but different VNET and different region. Must be in the same region.

No. Vnet3: Different VNET, different region. Must be in the same region.

No. Vnet4: Different VNET, same region.

Reference:

<https://docs.microsoft.com/en-us/azure/architecture/networking/guide/well-architected-framework-azure-firewall>

Community vote distribution

C (91%)

9%

 **IvanMtz** Highly Voted 1 year, 4 months ago

Selected Answer: C

The answer correct is C. I created a Lab with especification and i tried to select the vnet in rg2 when i recived the message "Azure firewall cannot be used with a from a different resource group". The lab was created from Azure Portal.

upvoted 27 times

 **jellybiscuit** Highly Voted 1 year, 3 months ago

Selected Answer: C

<https://learn.microsoft.com/en-us/azure/firewall/firewall-faq#are-there-any-firewall-resource-group-restrictions>

upvoted 24 times

 **Lazylinux** Most Recent 2 months, 3 weeks ago

Selected Answer: C

I C is correct as per

Are there any firewall resource group restrictions?

Yes. The firewall, VNet, and the public IP address all must be in the same resource group.

<https://learn.microsoft.com/en-us/azure/firewall/firewall-faq>

and one FW per region

upvoted 2 times

 **Techbiz** 4 months ago

The right answer is C, an Azure firewall instance can only be deployed to a single VNet. The rest of the VNets can consume the firewall through a Hub-Spoke topology and Firewall policies

upvoted 1 times

 **Ben_88** 7 months, 2 weeks ago

Selected Answer: C

Firewall and VNET must be from the same RG

<https://learn.microsoft.com/en-us/azure/firewall/firewall-faq#are-there-any-firewall-resource-group-restrictions>

upvoted 4 times

☒ **[Removed]** 9 months ago

Selected Answer: C

Azure firewall cannot be used with a from a different resource group
upvoted 3 times

☒ **somenick** 10 months, 3 weeks ago

Selected Answer: C

<https://learn.microsoft.com/en-us/azure/firewall/firewall-faq#are-there-any-firewall-resource-group-restrictions>
upvoted 4 times

☒ **Rajan395** 12 months ago

Correct Answer : C

upvoted 2 times

☒ **TJ001** 1 year ago

>VNET, PIP, FW, all in same region and resource group
>Firewall subnet should be names AzureFirewallSubnet
upvoted 3 times

☒ **Akodo_Shado** 1 year ago

Selected Answer: C

The firewall, VNet, and the public IP address all must be in the same resource group.
upvoted 3 times

☒ **sshera** 1 year ago

In exam 04jan23

upvoted 3 times

☒ **abdulmoiz** 1 year, 1 month ago

Should be only Vnet with RG-1

upvoted 1 times

☒ **Takloy** 1 year, 1 month ago

Are there any firewall resource group restrictions? Yes. The firewall, VNet, and the public IP address all must be in the same resource group.

So, answer here is just VNET 1.

<https://learn.microsoft.com/en-us/azure/firewall/firewall-faq#are-there-any-firewall-resource-group-restrictions>

upvoted 3 times

☒ **Andre369** 1 year, 1 month ago

Selected Answer: C

<https://learn.microsoft.com/en-us/azure/firewall/firewall-faq#are-there-any-firewall-resource-group-restrictions>

upvoted 1 times

☒ **Azuriste** 1 year, 3 months ago

Correct

upvoted 1 times

☒ **JerT** 1 year, 3 months ago

The firewall, VNet, and the public IP address all must be in the same resource group.

<https://learn.microsoft.com/en-us/azure/firewall/firewall-faq>

upvoted 3 times

☒ **BlackZeros** 1 year, 4 months ago

Selected Answer: C

vnet 1 only

upvoted 1 times

店铺: IT认证考试服务

IT认证考试服务

店铺: IT认证考试服务

HOTSPOT

-

You have two Azure App Service instances that host the web apps shown the following table.

Name	Web app URLs
As1.contoso.com	https://app1.contoso.com/ https://app2.contoso.com/
As2.contoso.com	https://app3.contoso.com/ https://app4.contoso.com/

You deploy an Azure 2 that has one public frontend IP address and two backend pools.

You need to publish all the web apps to the application gateway. Requests must be routed based on the HTTP host headers.

What is the minimum number of listeners and routing rules you should configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Listeners:

Routing rules:

Correct Answer:

Listeners:

Routing rules:

🗄️ 👤 **TJ001** Highly Voted 1 year ago

Answer seems correct

- 1) 1 Multi site Listener mapping each backend app service (total 2)
- 2) 1 routing rule mapping per listener/backend pool with Multi site option (total 2)

upvoted 15 times

🗄️ 👤 **ieboaix** 1 week, 3 days ago

the given answer is correct <https://learn.microsoft.com/en-us/training/modules/configure-azure-application-gateway/3-determine-routing>

upvoted 1 times

🗄️ 👤 **daemon101** 6 months, 3 weeks ago

When configuring path-based routing, you will see this "You can route traffic from this rule's listener to different backend targets based on the URL path of the request. You can also apply a different set of Backend settings based on the URL path.". With this, I would go for 1 listener and 1 routing rule.

upvoted 3 times

🗄️ 👤 **JohnAvlakitotis** 8 months, 1 week ago

I also went to the portal to deploy it, and there seems to be the only way to do that. Even if the listener is a wildcard listener you will not be able to split it to 2 different back end pools from the same listener IMHO

upvoted 3 times

🗄️ 👤 **Webesciaki** 1 month ago

agree - as we need to have 2 different backends we need 2 rules. You can't reuse listener for diff rule. so IMHO 2 rules and 2 listeners (multi site)

upvoted 1 times

🗄️ 👤 **TJ001** 1 year ago

pls note if the no of site per app Service is 1 in that case also total no of routing rule will be 2. because the front end listeners are different and it is scenario of creating Basic site listener still requiring rule mapping per listener

upvoted 1 times

🗄️ 👤 **TJ001** 1 year ago

small correction...in this case as well ...Multi site listener will be created and there is a sub option ... single site/multiple site within the Multi site selection..so both the case Multi site listener is created but there could be 1 or more sites within that selection

upvoted 1 times

🗄️ 👤 **Zeppoonstream** Highly Voted 9 months, 2 weeks ago

what is meant by "You deploy an Azure 2" ??

upvoted 8 times

🗄️ 👤 **daemon101** 6 months, 3 weeks ago

I guess it's supposed to be Application Gateway Standard V2

upvoted 6 times

🗄️ 👤 **sam881989** Most Recent 2 weeks, 4 days ago

Was able to configure with 1 rule and 1 Listener.

Also did multiple variations like adding 2 web apps in 2 different pools and 4 web apps in both the pools and still it worked with 1 rule and 1 listener.

Had to use path based routing and multisite option to make it work!

upvoted 2 times

🗄️ 👤 **sam881989** 2 weeks, 4 days ago

Correction. The answer is correct. Path based routing does not work in this situation

upvoted 2 times

🗄️ 👤 **NSF2** 3 weeks, 1 day ago

I am quite agree with below, since it was tested in the lab.

So the answer is not correct

Listener:

Create a single multi-site listener with the wildcard hostname configuration:

Multi-site Listener: Hostname: *.contoso.com

Routing rules:

Create 4 routing rules to route requests to the respective backend pools based on the host header:

Rule 1: Hostname: app1.contoso.com -> Backend pool (as1.contoso.com)

Rule 2: Hostname: app2.contoso.com -> Backend pool (as1.contoso.com)

Rule 3: Hostname: app3.contoso.com -> Backend pool (as2.contoso.com)

Rule 4: Hostname: app4.contoso.com -> Backend pool (as2.contoso.com)

By using a multi-site listener, you can minimize the number of listeners you need to configure:

1 multi-site listener

4 routing rules

upvoted 1 times

🗄️ 👤 **Lazylinux** 1 month ago

First for those mixing between Basic and multi-site

If you create Basic listener than you will not be prompted to enter FQDN for that specific listener meaning that the App Gateway, will be listening to ONLY one Domain or sub-domain and NOTHING else and this is achieved by using DNS either A-record that points to IP address of the App-GWY or CNAME that points to FQDN of the App GWY

If you chose multi-site (SINGLE) it means you are hosting more than 1 domain/subdomain (as the name indicates) and you can use A-record or CNAME as mentioned above, however the difference here is that each request is intercepted by App GWY and directed to the correct listener which in turn processed by the associated routing rule hence backend. Which is the case in this question.

see below further

upvoted 1 times

🗨️ 👤 **Lazylinux** 1 month ago

Now if you chose Multi-site (Multiple/wildcard), this allows you to add upto 5 hostnames as most people have indicated in the posts, however what they are missing here is the fact you have two separate backend App services that service 2 hostnames each and hence even though we can use 5 hostnames, it is NOT possible to separate the backend using one listener or routing rule. The thing to remember routing rules and listener go in relation 1-1 and hence if a listener is already associated with one routing rule you CANNOT use it with another routing rule i.e. when you create routing rule, you will get this error "There are no unassociated listeners available. Create a new listener and then try again." So we are here restricted by the fact we have 2 backends (App services) that respond to certain FQDN as per table in the question.

See below Further

upvoted 1 times

🗨️ 👤 **Lazylinux** 1 month ago

Therefore we need 2 Multi-site (Multiple/wildcard) and 2 routing rules as per below

Listener 1- Multi-site (Multiple/wildcard)

Hostnames: app1.contoso.com and app2.contoso.com

Backend1= As1.contoso.com

RoutingRule1= Listener1+backend1 and httpsetting1 with health probe

Listener 2- Multi-site (Multiple/wildcard)

Hostnames: app3.contoso.com and app4.contoso.com

Backend2= As2.contoso.com

RoutingRule2= Listener2+backend2 and httpsetting1 with health probe

See below further

upvoted 1 times

🗨️ 👤 **Lazylinux** 1 month ago

Note: You could use the same health probe and Https settings on differ listeners/routing rules if they are all same i.e. front port 43 and backend port is 43

Also if we did NOT have Multi-site (Multiple/wildcard) i.e. we have Multi-site (SINGLE) as per application Gateway version 1 then we would need 4 listeners and 4 routing rules with 2 backends because you can only have one hostname per listener and YES you can use wild card such as * but if you did like *.contoso.com or app*.contoso.com but you will have problem of directing all traffic to ONE BACKEND

More info found here:

<https://learn.microsoft.com/en-us/azure/application-gateway/multiple-site-overview#allowed-characters-in-the-host-names-field>

upvoted 1 times

🗨️ 👤 **IE17** 4 months ago

1 Multi-listener and 2 routing rules...

<https://learn.microsoft.com/en-us/azure/application-gateway/create-multiple-sites-portal>

upvoted 1 times

🗨️ 👤 **c2e9cb4** 3 weeks, 4 days ago

The URL is a good reference but on same url yo share they're showing 2 routing rule with a Distinct listener for each rule

2Rules*1Listener(each) = 2Listener

upvoted 1 times

🗨️ 👤 **WMG** 9 months, 2 weeks ago

Answer is wrong, created this setup in our lab environment. Read: <https://learn.microsoft.com/en-us/azure/application-gateway/multiple-site-overview#wildcard-host-names-in-listener>

upvoted 1 times

🗨️ 👤 **henryhung** 9 months, 3 weeks ago

From ChatGPT Plus(GPT-4)

You can use a multi-site listener to consolidate your configuration. A multi-site listener allows you to host multiple web apps on a single application gateway, routing requests based on the host header. In this case, you can create just one multi-site listener and configure the necessary routing rules.

Listener:

Create a single multi-site listener with the wildcard hostname configuration:

Multi-site Listener: Hostname: *.contoso.com

Routing rules:

Create 4 routing rules to route requests to the respective backend pools based on the host header:

Rule 1: Hostname: app1.contoso.com -> Backend pool (as1.contoso.com)

Rule 2: Hostname: app2.contoso.com -> Backend pool (as1.contoso.com)

Rule 3: Hostname: app3.contoso.com -> Backend pool (as2.contoso.com)

Rule 4: Hostname: app4.contoso.com -> Backend pool (as2.contoso.com)

By using a multi-site listener, you can minimize the number of listeners you need to configure:

1 multi-site listener
4 routing rules
upvoted 4 times

🗨️ 👤 **MrBlueSky** 9 months, 2 weeks ago

You posting these ChatGPT answers is not helpful dude.
upvoted 28 times

🗨️ 👤 **Lazylinux** 1 month ago

Because he is dumplings!!
upvoted 1 times

🗨️ 👤 **drprepper_** 10 months, 3 weeks ago

You only need 1 multi-site listener I think? <https://learn.microsoft.com/en-us/azure/application-gateway/multiple-site-overview#wildcard-host-names-in-listener> You can wildcard the start of the FQDN then just two routing rule 1 for each pool? So 1 and 2?
upvoted 5 times

🗨️ 👤 **wooyourdaddy** 10 months, 3 weeks ago

I agree that it is 1 multi-site listener using either wildcard or up 5 hostnames as per the link you cited. Then it would be a routing rule for each backend, so 2 in total.
upvoted 2 times

🗨️ 👤 **flurgen248** 11 months, 1 week ago

Answer is correct: <https://learn.microsoft.com/en-us/azure/application-gateway/application-gateway-components#types-of-listeners>
Create a multi-site listener for each Azure App Service, and each listener needs one rule.
upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

Your company has four branch offices and an Azure subscription. The subscription contains an Azure VPN gateway named GW1.

The branch offices are configured as shown in the following table.

Name	Local router	Local network gateway	Connection	VPN gateway
Branch1	RTR1	LNG1	Connection1	GW1
Branch2	RTR2	LNG2	Connection2	GW1
Branch3	RTR3	LNG3	Connection3	GW1
Branch4	RTR4	LNG4	Connection4	GW1

The branch office routers provide internet connectivity and Site-to-Site VPN connections to GW1.

The users in Branch1 report that they can connect to internet resources, but cannot access Azure resources.

You need to ensure that the Branch1 users can connect to the Azure resources. The solution must meet the following requirements:

- Minimize downtime for all users.
- Minimize administrative effort.

What should you do first?

- A. Recreate LNG1.
- B. Reset RTR1.
- C. Reset Connection1.
- D. Reset GW1.

Correct Answer: C

Community vote distribution

C (100%)

 **Goofer** Highly Voted 1 year ago

Answer C

The VPN gateway is not the problem, Branch2, 3, 4 are still working
Reset the connection

<https://learn.microsoft.com/en-us/azure/vpn-gateway/reset-gateway>

upvoted 14 times

 **Zeinovich** Most Recent 4 months, 1 week ago

why not recreate LNG1? may be the IP or BGP incorrect?

upvoted 2 times

 **LaurentvM** 3 days, 7 hours ago

More effort, you need to redeploy the connection as well.

upvoted 1 times

 **Oklama** 8 months, 1 week ago

Selected Answer: C

The Correct answer is C

upvoted 1 times

 **sunsetblvdfightclub** 10 months, 3 weeks ago

<https://learn.microsoft.com/en-us/azure/vpn-gateway/reset-gateway#reset-a-connection>

upvoted 1 times

 **Rajan395** 12 months ago

C is correct

upvoted 1 times

🗨️ **DerekKey** 1 year ago

Answer D

Problem: After you configure a site-to-site VPN connection between an on-premises network and an Azure virtual network, the VPN connection suddenly stops working and cannot be reconnected.

Solution: To resolve the problem, >>first try to reset the Azure VPN gateway<< and reset the tunnel from the on-premises VPN device.

upvoted 1 times

🗨️ **fz2021** 1 year ago

GW1 is common for multiple connections and it shall increase the downtime

upvoted 3 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

DRAG DROP

-

You have an Azure subscription that contains a virtual network named Vnet1 and an Azure SQL database named SQL1. SQL1 has a private endpoint on Vnet1.

You have a partner company named Fabrikam, Inc. Fabrikam has an Azure subscription that contains a virtual network named Vnet2 and a virtual machine named VM1. VM1 is connected to Vnet2.

You need to provide VM1 with access to SQL1 by using an Azure Private Link service.

What should you implement on each virtual network? To answer, drag the appropriate resources to the correct virtual networks. Each resource 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.

NOTE: Each correct selection is worth one point.

Resources	Answer Area
A NAT gateway	Vnet1: <input type="text"/>
A peering link	Vnet2: <input type="text"/>
A private endpoint	
A service endpoint	
An Azure application gateway	
An Azure load balancer	

Answer Area
<p>Correct Answer:</p> <p>Vnet1: <input type="text" value="A private endpoint"/></p> <p>Vnet2: <input type="text" value="A peering link"/></p>

🗨️ 👤 **Wis10** Highly Voted 1 year ago

Correct Answer:

- Vnet1 = Standard Load Balancer
- Vnet2 = Private Endpoint

Justification:

<https://learn.microsoft.com/en-us/azure/private-link/private-link-service-overview#workflow>

upvoted 41 times

🗨️ 👤 **asd123123iu** 5 months, 4 weeks ago

Agree, SQL already have private endpoint so we need load balancer in VNET1 and private link in VNET2.

upvoted 2 times

🗨️ 👤 **DavidSapery** Highly Voted 1 year ago

<https://learn.microsoft.com/en-us/azure/private-link/private-link-service-overview> indicates that a Load Balancer is needed on the SQL side (vnet1) and a Private Endpoint on the VM side (vnet2).

upvoted 20 times

🗨️ 👤 **Lazylinux** Most Recent 2 months, 3 weeks ago

Given answer is WRONG - For sure as others pointed out
Vnet1 - STD LB used to allow access to backend pool that allows access to resources, also NAT GWY is deployed
Vnet2 - PE - private end point
upvoted 2 times

🗨️ **Azused** 4 months, 3 weeks ago

Correct Answer:
- Vnet1 = Standard Load Balancer
- Vnet2 = Private Endpoint
<https://learn.microsoft.com/en-us/azure/private-link/private-link-service-overview#workflow>
upvoted 3 times

🗨️ **ronin201** 6 months, 3 weeks ago

I have the same config (only posgreSQL) I have private endpoint and 2 peering links in 2 networks, the current description already has private endpoint.
upvoted 3 times

🗨️ **GBAU** 3 months ago

While I thought this was the answer as it would work, I think the question is testing knowledge of private link services, where only specific services are provided across the private link, not access to the full vNet.
upvoted 1 times

🗨️ **ronin201** 6 months, 3 weeks ago

wrong answer: Vnet1 already has private endpoint. peering links in both vnets must be created
upvoted 3 times

🗨️ **AzureLearner01** 10 months, 3 weeks ago

To establish the private link service you need a load balancer in VNet 1 and for sure the private link service resource. In the partner company tenant you need an private endpoint that connects to this private link service. To answer the question correctly we might answer to create standard load balancer and private link service in vnet1 an pe in vnet2.
upvoted 4 times

🗨️ **Ayokun** 11 months ago

Load balancer
Private Link
<https://learn.microsoft.com/it-it/azure/private-link/private-link-overview>
upvoted 1 times

🗨️ **Ayokun** 11 months ago

Sorry i correct "You need to provide VM1 with access to SQL1 by using an Azure Private Link service" hence it is required the last part of the config which is a private endpoint on VM1
LB
Private Endpoint
upvoted 2 times

🗨️ **tester2023** 12 months ago

VNET1: Peering Link
VNET2: Peering Link

The question notes a Private Endpoint is already configured on the SQL Server (PaaS) resource. As such, vNet peering will allow the VM on vNet 2 to reach the database on vNet 1.

A private endpoint is part of the Private Link Service (<https://learn.microsoft.com/en-us/azure/private-link/private-link-faq#what-is-azure-private-endpoint-and-azure-private-link-service->)

For those selecting Load Balancer, you are correct it requires a Private Link Service (PLS), but that isn't one of the available answers. Also, a PLS requires a VM or VM Scale Set Load Balancer backend pool (see <https://learn.microsoft.com/en-us/azure/private-link/private-link-service-overview>). Testing revealed I couldn't use the private IP address of the SQL PaaS server private endpoint for the PLS.
upvoted 4 times

🗨️ **KeenOnTech** 4 months, 2 weeks ago

As we have a Private Endpoint in VNet-1, the LB is already installed at SQL subnet. All is needed is to allow VM @Vnet2 access PE @Vnet1. Peering is all is needed: "The private endpoint can be reached from globally peered virtual networks and on premises using private VPN or ExpressRoute connections." <https://learn.microsoft.com/en-us/azure/private-link/private-link-service-overview#details>
upvoted 1 times

🗨️ **flurgen248** 11 months, 1 week ago

The prompt says "You need to provide VM1 with access to SQL1 by using an Azure Private Link service."

A private link service requires a load balancer.
VNET1: Load Balancer
VNET2: Private Endpoint

<https://learn.microsoft.com/en-us/azure/private-link/private-link-service-overview>
upvoted 4 times

🗨️ **lingxian** 10 months, 2 weeks ago

I would agree with this. How to use an LB with the Azure SQL database as a backend? We have already the private endpoint in VNet1, setting up peering should be enough for VMs in VNet2 talking to the SQL service.

upvoted 2 times

🗨️ 👤 **4729** 12 months ago

VNET1: Private Link
VNET2: Private Endpoint
upvoted 4 times

🗨️ 👤 **amt2022** 1 year ago

Correct answer
- VNET1 = Standard LB
-VNET2 = Private EndPoint
Check this sample from MS.
<https://learn.microsoft.com/en-us/azure/private-link/create-private-link-service-powershell>
upvoted 8 times

🗨️ 👤 **DerekKey** 1 year ago

VNet 1: Load Balancer
VNet 2: Private Endpoint
Microsoft docs: <https://learn.microsoft.com/en-us/azure/private-link/private-link-service-overview>
upvoted 5 times

🗨️ 👤 **chatlisi** 1 year ago

VNET1 - Azure Load Balancer - your existing service must be behind a load balancer
VNET2 - Private link
upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

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

Name	Type	Description
Vnet1	Virtual network	None
Subnet1	Virtual subnet	Hosted in Vnet1
GatewaySubnet	Virtual subnet	Hosted in Vnet1
VM1	Virtual machine	Connected to Subnet1 Basic SKU public IP address
VM2	Virtual machine	Connected to Subnet2 Standard SKU public IP address

You plan to deploy an Azure Virtual Network NAT gateway named Gateway1. The solution must meet the following requirements:

- VM1 will access the internet by using its public IP address.
- VM2 will access the internet by using its public IP address.
- Administrative effort must be minimized.

You need to ensure that you can deploy Gateway1 to Vnet1.

What is the minimum number of subnets required on Vnet1?

- A. 2
- B. 3
- C. 4
- D. 5

Correct Answer: B

Community vote distribution

C (64%)

B (33%)

 **amt2022** Highly Voted 1 year ago

Correct Answer : 4

1. GatewaySubnet
2. Subnet 2


3. Subnet 1 with Basic SKU for Public IP

4. NAT Gateway requires in VNET 1 and hence 4. Otherwise you could have used Subnet2 to avoid creating 4th Subnet. Requirement is to create NAT GW in VNET1 so you need 4th Subnet.

<https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-overview>


Check out - NAT gateway and basic SKU resources section

upvoted 16 times

 **c2e9cb4** 3 weeks, 4 days ago


This is wrong : a nat gateway doesnt require a subnet at all tested on lab ==>corret answer 3

upvoted 3 times

 **tester2023** 12 months ago

Another reason this makes sense is the requirement for the two VMs to continue using their own Public IPs instead of the NAT Gateway. As soon as a NAT Gateway is associated with a vNet, it overrides the instance-level IPs (see <https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource#connect-to-the-internet-with-nat-gateway>).

upvoted 4 times

 **MrBlueSky** 9 months, 3 weeks ago

Wrong. It only applies to within the same subnet.

So if you use the GatewaySubnet to deploy the NAT Gateway (I don't see why you wouldn't), then the answer is 3.

upvoted 3 times

 **MrBlueSky** 9 months, 2 weeks ago

Correction: NATGateway cannot be associated to GatewaySubnet

However, NATGateway doesn't need it's own subnet and is instead associated to subnets.

Answer is still 3
upvoted 2 times

🗄️ 👤 **jarz** 9 months, 1 week ago

Order of operations <https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-overview>

The order of operations for outbound connectivity follows this order of precedence: Virtual appliance UDR / ExpressRoute >> NAT gateway >> Instance-level public IP addresses on virtual machines >> Load balancer outbound rules >> default system
upvoted 3 times

🗄️ 👤 **MrBlueSky** 9 months, 3 weeks ago

Why could you not just deploy the NAT Gateway into the GatewaySubnet?
upvoted 1 times

🗄️ 👤 **JohnnyChimpo** 7 months, 3 weeks ago

GatewaySubnet has nothing to do with NAT Gateway resources. GatewaySubnet is the azure naming convention for subnet used with Virtual Network Gateways
upvoted 1 times

🗄️ 👤 **jarz** 9 months, 1 week ago

according to this page <https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-overview> NAT GW cannot be deployed into a GW Subnet.
upvoted 3 times

🗄️ 👤 **wooyourdaddy** Highly Voted 10 months, 3 weeks ago

Selected Answer: C

The correct answer is 4.

1. The Gateway Subnet must exist on its own.

2. As per this link <https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-overview#nat-gateway-and-basic-sku-resources>

Basic resources, such as basic load balancer or basic public IPs aren't compatible with Virtual Network NAT. Basic resources must be placed on a subnet not associated to a NAT gateway.

3. The question also states that VM1 and VM2 will access the internet by using their respective public IP address. From the same link above we have the statement:

NAT gateway takes precedence over other outbound scenarios (including Load balancer and instance-level public IP addresses) and replaces the default Internet destination of a subnet.

So to meet that requirement, we would need a 4th subnet where the NAT gateway is deployed.

upvoted 14 times

🗄️ 👤 **_NoobMaster69** 10 months, 2 weeks ago

Agree +1
upvoted 1 times

🗄️ 👤 **Webesciaki** 3 weeks ago

agree:

1 subnet for vng

1 subnet for NAT gw deployment as at least 1 needs to be assigned during creation

1 subnet for VM1 – as it cant be assigned to NAT gw as needs to go out with its own public IP

1 subnet for VM2 – it has basic public IP so cant even be assigned to NAT gw + the same reason as above

upvoted 1 times

🗄️ 👤 **NSF2** Most Recent 3 weeks, 1 day ago

Selected Answer: B

B seems to be the right answer, because NAT GW doesn't need a dedicated subnet. Rather it can be attached to existing subnets for workload to use it.

upvoted 1 times

🗄️ 👤 **vikrants31** 4 weeks ago

As per details I think Subnet2 not hosted in Vnet1

upvoted 2 times

🗄️ 👤 **GBAU** 3 months ago

4: Least admin effort requires no changes to existing subnets or VMs, just add a subnet for the NAT Gateway to apply to. This also means the existing VMs keep their use of their PIPs and the GateWaySubnet is unchanged.

upvoted 1 times

🗄️ 👤 **Faizee** 4 months ago

Just to deploy the NAT gateway, we do not need to assign it to any subnet at time of creation. So no extra subnet required just to deploy NAT gateway

upvoted 4 times

🗨️ **ConanBarb** 3 months, 3 weeks ago

Portal: "To use the NAT gateway, at least one subnet must be selected. You can add and remove subnets after creating the NAT gateway."

I.e. 3 Subnets

upvoted 1 times

🗨️ **LaurentvM** 3 days, 7 hours ago

This is not true, you can deploy a NAT gateway without linking subnets.

upvoted 1 times

🗨️ **Azused** 4 months, 3 weeks ago

Selected Answer: C

NAT Gateway requires in VNET 1 and hence 4. Otherwise you could have used Subnet2 to avoid creating 4th Subnet. Requirement is to create NAT GW in VNET1 so you need 4th Subnet.

Reference:

<https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-overview>

upvoted 1 times

🗨️ **daemon101** 6 months, 3 weeks ago

Selected Answer: C

Answer seems to be 4 subnets.

1. Subnet1 for VM1

2. Subnet2 for VM2 - you can't associate the NAT gateway with this subnet as the requirement says VM2 needs to use its public IP address. NAT gateway takes precedence over other outbound connectivity methods, including Load balancer, instance-level public IP addresses, and Azure Firewall.

3. Subnet 3 for GatewaySubnet

4. Subnet 4 for NAT Gateway - NAT gateway doesn't need a delegated subnet but you associate it with subnet for the LBs and VMs outbound connectivity. Also, one of the requirements is to deploy NAT gateway.

<https://learn.microsoft.com/en-us/azure/nat-gateway/nat-overview>

upvoted 4 times

🗨️ **Lazylinux** 6 months, 3 weeks ago

Selected Answer: C

As per my explanation

upvoted 1 times

🗨️ **Lazylinux** 6 months, 3 weeks ago

Based on the below facts and per link

vNET NAT GWY > Basic SKU resources, such as basic load balancer or basic public IPs aren't compatible with NAT gateway. NAT gateway can't be used with subnets where basic SKU resources exist. Basic load balancer and basic public IP can be upgraded to standard to work with a NAT gateway

vNET NAT gateway takes precedence over other outbound connectivity methods, including Load balancer, instance-level public IP addresses, and Azure Firewall.

Gateway subnet cannot have any VMs or NVA except for VPN GWY VMs (instances), and as per MS restrictions "A NAT gateway can't be deployed in a gateway subnet."

Hence total required is 4 FOR SURE

<https://learn.microsoft.com/en-us/azure/nat-gateway/nat-overview>

upvoted 3 times

🗨️ **Zika69** 7 months, 3 weeks ago

Selected Answer: B

Question is asking only to deploy. You can deploy to vnet and not associate with any subnet. So there is no need to create any new subnet.

upvoted 1 times

🗨️ **roshingrg** 7 months, 3 weeks ago

C. 4

Here's an explanation:

GatewaySubnet: This subnet is required to host the NAT gateway (Gateway1). It is dedicated to the NAT gateway and its associated resources.

Subnet1: This subnet is needed for VM1 to connect to Vnet1. It allows VM1 to access the internet using its public IP address.

Subnet2: This subnet is required for VM2 to connect to Vnet1. It enables VM2 to access the internet using its public IP address.

Subnet3: This subnet is necessary for internal resources or other virtual machines that do not require direct internet access. It allows for segmentation and organization within the virtual network.

Therefore, with these four subnets (GatewaySubnet, Subnet1, Subnet2, Subnet3), you can deploy Gateway1 to Vnet1 while ensuring that VM1 and VM2 can access the internet via their public IP addresses, and also minimizing administrative effort.

upvoted 2 times

🗨️ **Kipper_2022** 8 months, 1 week ago

Selected Answer: C

Agree with amt2022

upvoted 1 times

🗨️ **[Removed]** 9 months ago

Selected Answer: C

NAT gateway takes precedence over public IP if it was attached to a subnet 1 or subnet 2, so an additional subnet is required. In total four subnets are required.

upvoted 2 times

🗨️ **hal01** 9 months ago

Selected Answer: C

4 subnets

upvoted 1 times

🗨️ **ckyp** 9 months, 3 weeks ago

Tested in lab, the condition for VM2 to use its own public ip address can still be achieved if I diassociate the Standard SKU public IP address, then go to NATGateway, change the outbound IP to that public ip address. In this way, we dont need the fourth Subnet. However the question said Admistrative effort must be minimized, so I supposed creating a new subnet will be effortless. Subnet 1 cannot be added because of the Basic SKU public IP address. GatewaySubnet cannot be selected in the Subnet association. Thus the answer should be 4.

upvoted 3 times

🗨️ **_fvt** 9 months, 3 weeks ago

Selected Answer: B

You have Subnet 1 with VM1 and Subnet 2 with VM2.

You and want to deploy a NAT Gateway which will not interact/handle the traffic of VM1 and VM2, so Subnet 1 and Subnet 2.

=> Just create a 3rd Subnet and deploy a Zonal gateway to this Subnet 3 (<https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-availability-zones>)

upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT

-

You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Location	IP address space
Vnet1	East US 2	10.5.0.0/16
Vnet2	East US 2	10.3.0.0/16
Vnet3	East US 2	10.4.0.0/16

You have a virtual machine named VM5 that has the following IP address configurations:

- IP address:10.4.0.5
- Subnet mask:255.255.255.0
- Default gateway: 10.4.0.1
- DNS server: 168.63.129.16

You have an Azure Private DNS zone named fabrikam.com that contains the records shown in the following table.

Name	Type	Value
app1	CNAME	lb1.fabrikam.com
lb1	A	10.3.0.7
vm1	A	10.3.0.4

The virtual network links in the fabrikam.com DNS zone are configured as shown in the exhibit. (Click the Exhibit tab.)

Home > Private DNS zones > fabrikam.com

fabrikam.com | Virtual network links

Private DNS zone

Search (Ctrl+/) << + Add Refresh

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Virtual network links
- Properties
- Locks

Search virtual network links

Link Name	Link status	Virtual network	Auto-Registration
link1	Completed	vnet2	Enabled

VM5 fails to resolve the IP address for app1.fabrikam.com.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Updating the IP address configurations of VM5 to use a DNS server address of 10.4.0.2 will enable the virtual machine to resolve app1.fabrikam.com.	<input type="radio"/>	<input type="radio"/>
Enabling a virtual network link for Vnet3 in the fabrikam.com DNS zone will enable VM5 to resolve app1.fabrikam.com.	<input type="radio"/>	<input type="radio"/>
Adding an A record for app1.fabrikam.com to the fabrikam.com DNS zone will enable VM5 to resolve app1.fabrikam.com.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Statements	Yes	No
Updating the IP address configurations of VM5 to use a DNS server address of 10.4.0.2 will enable the virtual machine to resolve app1.fabrikam.com.	<input checked="" type="radio"/>	<input type="radio"/>
Enabling a virtual network link for Vnet3 in the fabrikam.com DNS zone will enable VM5 to resolve app1.fabrikam.com.	<input checked="" type="radio"/>	<input type="radio"/>
Adding an A record for app1.fabrikam.com to the fabrikam.com DNS zone will enable VM5 to resolve app1.fabrikam.com.	<input type="radio"/>	<input checked="" type="radio"/>

Madball Highly Voted 11 months, 3 weeks ago
NYN

VM5 is in VNET3 and VNET3 isn't linked to the fabrikam.com private DNS zone. This means it won't be able to resolve anything in that private DNZ zone until it is linked.
upvoted 35 times

Gabaky Highly Voted 11 months, 2 weeks ago
NYN
10.4.0.2 and 10.4.0.5 are within same subnet that was initially not resolving
upvoted 16 times

NSF2 Most Recent 3 weeks, 1 day ago
This is NYN because the problem is that there is no link to VNET3
upvoted 1 times

Murad01 1 month, 3 weeks ago
Appeared on Exam November - 2023
upvoted 1 times

Lazylinux 6 months, 2 weeks ago
I vote NYN and reason below, i believe on option 1 and 3 we all agree N but 2 is question Mark

First the DNS provide 168.63.129.16 is also know as internal.cloudapp.net which is the default Azure provided DNS and all vNETS have access to it by default
So when you create V network link to vNET3 where vm resides this will enable vm5 to resolve any FQDN in the private DNS, however very important POINT, the default DNS is still can be used to resolve name that are not in the private DNS i.e. that are using the default Azure DNS - see link below

<https://learn.microsoft.com/en-us/azure/dns/dns-faq-private>

One important point, IF you statically configured the IP and DNS within the OS to another DNS server and you link the vNET where VM reside to Azure Private DNS than the statically assigned configurations take precedence and in this case vm5 will not resolve app1
upvoted 1 times

g_mindset 3 months, 4 weeks ago
My doubts were on the configuration: DNS server: 168.63.129.16. Thanks for clarifying that when a virtual network link is linked to VNET3, the VM resources automatically start using the fabrikam.com private DNS zone to resolve FQDNs. Correct answer: NYN
upvoted 1 times

ronin201 6 months, 3 weeks ago
NNN
1) How DNS address will resolve app1.fabricam.zom hostname if there is no connection between DNS zone and VNet3?
2) link to Vnet3 is not enough because there is no DNS record to VM5, and conflicting DNS records app1.fabricam.com CNAME
upvoted 1 times

Aziza_Adam 11 months, 3 weeks ago
No
Yes
No
upvoted 5 times

 **bobg** 11 months, 3 weeks ago

n/y/n . There is no mention of 10.4.0.2 and what it is in the question.

upvoted 5 times

 **Madball** 11 months, 3 weeks ago

10.4.0.2 is the DNS servers for that IP address space, but since there is no private DNS zone linked to the VNET it won't resolve the load balancer FQDN.

upvoted 7 times

店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

Your company has five offices. Each office has a firewall device and a local internet connection. The offices connect to a third-party SD-WAN.

You have an Azure subscription that contains a virtual network named Vnet1. Vnet1 contains a virtual network gateway named Gateway1. Each office connects to Gateway1 by using a Site-to-Site VPN connection.

You need to replace the third-party SD-WAN with an Azure Virtual WAN.

What should you include in the solution?

- A. Delete Gateway1.
- B. Create new Point-to-Site (P2S) VPN connections on the firewall devices.
- C. Create an Azure Traffic Manager profile.
- D. Enable active-active mode on Gateway1.

Correct Answer: B

Community vote distribution

A (100%)

 **flurgen248** Highly Voted 11 months, 1 week ago

Selected Answer: A

Virtual Wan requires a Wan Hub Gateway, so Gateway1 should be deleted (after the new gateway is connected).

<https://learn.microsoft.com/en-us/azure/virtual-wan/migrate-from-hub-spoke-topology#step-5-transition-connectivity-to-virtual-wan-hub>
upvoted 10 times

 **omgMerrick** Highly Voted 11 months, 1 week ago

Selected Answer: A

A. Delete Gateway1

A hub gateway isn't the same as a virtual network gateway that you use for ExpressRoute and VPN Gateway. For example, when using Virtual WAN, you don't create a site-to-site connection from your on-premises site directly to your VNet. Instead, you create a site-to-site connection to the hub. The traffic always goes through the hub gateway.

*** This means that your VNets don't need their own virtual network gateway. Virtual WAN lets your VNets take advantage of scaling easily through the virtual hub and the virtual hub gateway.

Source:

<https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about#resources>
upvoted 5 times

 **Lazylinux** Most Recent 2 months, 3 weeks ago

Selected Answer: A

Answer is A as per

<https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about>
upvoted 1 times

 **Azused** 4 months, 3 weeks ago

Selected Answer: A

Explanation

Virtual Wan requires a Wan Hub Gateway, so Gateway1 should be deleted (after the new gateway is connected).

Reference:

<https://learn.microsoft.com/en-us/azure/virtual-wan/migrate-from-hub-spoke-topology#step-5-transition-connectivity-to-virtual-wan-hub>
upvoted 3 times

 **WaleedSaleh** 7 months, 1 week ago

Selected Answer: A

Correct

upvoted 1 times

🗄️ **tomtom2022** 9 months ago

Selected Answer: A

A is correct
upvoted 1 times

🗄️ **ayoubneo** 10 months, 3 weeks ago

Selected Answer: A

Correct
upvoted 1 times

🗄️ **AP78** 11 months ago

Selected Answer: A

Correct
upvoted 1 times

🗄️ **Ayokun** 11 months, 1 week ago

Enable active - active and then delete.
upvoted 1 times

🗄️ **drprepper_** 10 months, 3 weeks ago

Are u ok bro?
upvoted 8 times

🗄️ **samir111** 11 months, 2 weeks ago

Selected Answer: A

delete Gateway1
upvoted 2 times

🗄️ **certacc** 11 months, 2 weeks ago

I believe the answer is A. The vWAN migration doc states you would create new VPN connections to the HUB (making sure the existing route is still prioritised), then test the new connection with a test VNet attached to the HUB, and then when ready delete the old connections and gateway to failover.
upvoted 4 times

🗄️ **Bbb78** 11 months, 3 weeks ago

Why p2s ? I would delete GW first!
upvoted 3 times

🗄️ **Ayboum** 11 months, 3 weeks ago

Don't think so, i say active active mode on gateway to be able to create a connection to the Virtual WAN
<https://learn.microsoft.com/en-us/azure/virtual-wan/connect-virtual-network-gateway-vwan>
upvoted 5 times

🗄️ **wooyourdaddy** 10 months, 3 weeks ago

I agree after reading that link, where it states "Creating a connection from a VPN Gateway (virtual network gateway) to a Virtual WAN (VPN gateway) is similar to setting up connectivity to a virtual WAN from branch VPN sites."

The answer should be D, to enable active-active mode on Gateway1 as per step 1 in the link.
upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

You are planning the IP addressing for the subnets in Azure virtual networks.

Which type of resource requires IP addresses in the subnets?

- A. internal load balancers
- B. Azure DDoS Protection for virtual networks
- C. service endpoint policies
- D. service endpoints

Correct Answer: A

Community vote distribution

A (100%)

 **omgMerrick** Highly Voted 11 months, 1 week ago

Selected Answer: A

A. Internal Load Balancers

Internal load balancers require IP addresses in the subnets because they distribute network traffic among resources that are located in a private network.

You do not need IP addresses for Azure DDoS Protection for virtual networks because it is a service that protects your resources from distributed denial-of-service (DDoS) attacks.

You do not need IP addresses for service endpoint policies because they are used to filter network traffic from a subnet to an Azure service.

You do not need IP addresses for service endpoints because they are logical connections from a virtual network subnet to an Azure service.

Source:

<https://learn.microsoft.com/en-us/training/modules/design-ip-addressing-for-azure/>
upvoted 5 times

 **WaleedSaleh** Most Recent 7 months, 1 week ago

Selected Answer: A

A. Internal Load Balancers

upvoted 2 times

 **flurgen248** 11 months, 1 week ago

Selected Answer: A

<https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-overview>


An internal (or private) load balancer is used where private IPs are needed at the frontend only. Internal load balancers are used to load balance traffic inside a virtual network.

upvoted 2 times

 **JennyHuang36** 11 months, 1 week ago

In exam Feb, 2023

upvoted 1 times

 **mVic** 11 months, 1 week ago

Selected Answer: A

Internal Load Balancers is the right option.

upvoted 3 times

 **Ayboum** 11 months, 3 weeks ago

Correct

upvoted 2 times

 **harshit101** 11 months, 2 weeks ago

ok sir, very good, god bless.

upvoted 1 times

You have an Azure subscription that contains four virtual networks named VNet1, VNet2, VNet3, and VNet4.

You plan to deploy a hub and spoke topology by using virtual network peering.

You need to configure VNet1 as the hub network. The solution must meet the following requirements:

- Support transitive routing between spokes.
- Maximize network throughput.

What should you include in the solution?

- A. Azure VPN Gateway
- B. Azure Route Server
- C. Azure Private Link
- D. Azure Firewall

Correct Answer: A

Community vote distribution

D (100%)

 **Ayboum** Highly Voted 11 months, 3 weeks ago

Selected Answer: D

Azure Firewall is the best response
Communication through an NVA

If you need connectivity between spokes, consider deploying Azure Firewall or another NVA in the hub. Then create routes to forward traffic from a spoke to the firewall or NVA, which can then route to the second spoke. In this scenario, you must configure the peering connections to allow forwarded traffic.

You can also use a VPN gateway to route traffic between spokes, although this choice affects latency and throughput. For configuration details, see Configure VPN gateway transit for virtual network peering.

<https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke?tabs=cli>

upvoted 15 times


 **mammoot** 11 months, 1 week ago

I agree with this, especially since they say to maximise throughput.
VPN Gateways have less throughput in comparison

<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways#benchmark>

<https://learn.microsoft.com/en-us/azure/firewall/firewall-faq#how-can-i-increase-my-firewall-throughput>

upvoted 2 times

 **mVic** 11 months, 1 week ago

Agree with firewall.

VPN Gateways might even not be required since it's not specified the VNets are in a different region. And it specifies you use peerings.

upvoted 1 times

 **omgMerrick** Highly Voted 11 months, 1 week ago

Selected Answer: D

Forgot to vote. Wish you could edit your posts...

Source:

<https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke?tabs=cli#spoke-network-communications>

upvoted 5 times


 **Lazylinux** Most Recent 2 months, 3 weeks ago

Selected Answer: D

Agree answer is D here is more

<https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke?tabs=cli>

upvoted 1 times

 **Azused** 4 months, 3 weeks ago

Selected Answer: D

Explanation

There are two main ways to allow spoke virtual networks to communicate with each other:

Communication via an NVA like a firewall and router. This method incurs a hop between the two spokes.

Communication by using virtual network peering or Virtual Network Manager direct connectivity between spokes. This approach doesn't cause a hop between the two spokes and is recommended for minimizing latency.

Communication through an NVA. If you need connectivity between spokes, consider deploying Azure Firewall or another NVA in the hub. Then create routes to forward traffic from a spoke to the firewall or NVA, which can then route to the second spoke. In this scenario, you must configure the peering connections to allow forwarded traffic.

Reference:

<https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke?tabs=cli#spoke-networkcommunications>

upvoted 1 times

 **Billabongs** 6 months, 2 weeks ago

Selected Answer: D

I think to maximize throughput NVA is the best choice.

upvoted 1 times

 **daemon101** 6 months, 2 weeks ago

Selected Answer: D

First requirement is "Support transitive routing between spokes". Both VPN GW and Azure Firewall can accomplish this.

Second requirement is "Maximize network throughput". Azure firewall has a higher throughput than VPN GW.

VPN GW throughput reference:

<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways>

Azure Firewall throughput reference:

<https://learn.microsoft.com/en-us/azure/firewall/firewall-faq#:~:text=Azure%20Firewall's%20initial%20throughput%20capacity,100%20Gbps%20for%20Premium%20SKU.>

upvoted 2 times

 **ronin201** 6 months, 3 weeks ago

Given answer is correct hub and spoke topology is 1 VPN + vnet with option use current VPN GW, other vnets with peering option and using remote GW. Route server would not work without VPN GW, Firewall is for security approach

upvoted 2 times

 **KyDD** 4 months ago

Agreed and last sentence is the key why choice b not complete.

upvoted 1 times

 **MrBlueSky** 9 months, 3 weeks ago

This is a trick question as you'd never use Azure Firewall to accomplish this unless you need the other features of it. The question doesn't mention any of these additional features of Azure Firewall as a requirement.

However, there are no other suitable answers so clearly what they are testing on here is your knowledge of if Azure Firewalls can be used at all.

Answer is D

upvoted 2 times

 **omgMerrick** 11 months, 1 week ago

D. Azure Firewall

There are two main ways to allow spoke virtual networks to communicate with each other:

Communication via an NVA like a firewall and router. This method incurs a hop between the two spokes.

Communication by using virtual network peering or Virtual Network Manager direct connectivity between spokes. This approach doesn't cause a hop between the two spokes and is recommended for minimizing latency.

Communication through an NVA

If you need connectivity between spokes, consider deploying Azure Firewall or another NVA in the hub. Then create routes to forward traffic from a spoke to the firewall or NVA, which can then route to the second spoke. In this scenario, you must configure the peering connections to allow forwarded traffic.

Source:

<https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke?tabs=cli#spoke-networkcommunications>

upvoted 4 times

 **Ayboum** 11 months, 3 weeks ago



Azure Firewall is the best response
Communication through an NVA

If you need connectivity between spokes, consider deploying Azure Firewall or another NVA in the hub. Then create routes to forward traffic from a spoke to the firewall or NVA, which can then route to the second spoke. In this scenario, you must configure the peering connections to allow forwarded traffic.

You can also use a VPN gateway to route traffic between spokes, although this choice affects latency and throughput. For configuration details, see Configure VPN gateway transit for virtual network peering.



<https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke?tabs=cli>

upvoted 3 times

  **Bbb78** 11 months, 3 weeks ago

b.Azure Router Service is probably a better answer than VPN GW

upvoted 3 times

  **Kafura** 9 months, 2 weeks ago

Use Azure Route Server to enable dynamic routing between your network appliances and gateways in Azure, instead of using static routing. Azure Route Server provides Border Gateway Protocol (BGP) endpoints using standard routing protocol to exchange routes.

upvoted 1 times

  **_fvt** 9 months, 3 weeks ago

You need an NVA/FW for ARS, it's just to facilitate the routing setup not handle it: <https://learn.microsoft.com/fr-fr/azure/route-server/overview>

upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT

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

Name	Location
RG1	East US
RG2	East US
RG3	UK West

You have the virtual networks shown in the following table.

Name	Location	IP address space	Resource group
Vnet1	East US	10.1.0.0/16	RG1
Vnet2	West US	10.2.0.0/16	RG2
Vnet3	UK West	10.1.0.0/16	RG3

You have the subnets shown in the following table.

Name	Virtual network	IP address range
Subnet1-1	Vnet1	10.1.1.0/24
Subnet2-1	Vnet2	10.2.1.0/24
Subnet3-1	Vnet3	10.1.1.0/24

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Vnet1 can be moved to RG3.	<input type="radio"/>	<input type="radio"/>
Three hundred virtual machines can be deployed to the East US Azure region.	<input type="radio"/>	<input type="radio"/>
A new virtual network named Vnet2 can be created in RG2 in the East US Azure region.	<input type="radio"/>	<input type="radio"/>

Statements	Yes	No
Vnet1 can be moved to RG3.	<input checked="" type="radio"/>	<input type="radio"/>
Three hundred virtual machines can be deployed to the East US Azure region.	<input type="radio"/>	<input checked="" type="radio"/>
A new virtual network named Vnet2 can be created in RG2 in the East US Azure region.	<input type="radio"/>	<input checked="" type="radio"/>

Correct Answer:

Madball Highly Voted 11 months, 3 weeks ago
YNN

You can move VNET1 to RG3.

You cannot deploy 300 VMs to East US Azure region because the subnet in VNET1 is a /24 which isn't large enough.

You cannot create a new VNET called VNET2 in RG2 because there is already a VNET with that name in the resource group.
upvoted 18 times

ubdubdoo 8 months, 2 weeks ago

you're wrong. you can deploy two vnets in the same RG, as long as they are in different regions.
upvoted 2 times

c2e9cb4 2 weeks, 5 days ago

No you can't, i just tested it on lab!
upvoted 1 times

jarz 9 months, 1 week ago

I'd say YYN they talk of the region, not the subnet. And yes the Subnet is a /24, but the VNET is a /16. Or am I splitting hairs here?

upvoted 3 times

  **[Removed]** 8 months, 3 weeks ago

Yes, you could add a new subnet to fit the total of 300 machines but you are supposed to evaluate the situation as described in the question. Only the /24 subnet is mentioned which has 251 free IP addresses. Hence it should be YNN

upvoted 3 times

  **staffo** Highly Voted 11 months, 2 weeks ago

I thought it was NNN but just tested and you can move VNET1 to RG3. They are in different locations so its fine. So Answer is YNN.

upvoted 8 times

  **Lazylinux** 6 months, 2 weeks ago

Not sure how you tested, must be Azure located in MARS!! sorry we are on Earth!!

upvoted 1 times

  **[Removed]** 9 months ago


Even if both are in the same location you can create however with a different name. Basically, you can create everything same but with a different name for the VNET.

upvoted 1 times

  **Supreem** Most Recent 3 months, 1 week ago

Such poorly written question, especially point 2. Thanks again Microsoft.

upvoted 2 times

  **Lazylinux** 6 months, 2 weeks ago

Yes you can Move the vNET1 to RG3 because the method used to move, allows you to change the Address Space or subnet addressing scope before deployment of the arm template - see link below

Address Space: Before you save the file, you can alter the address space of the virtual network by modifying the resources > addressSpace section and changing the addressPrefixes propert

<https://learn.microsoft.com/en-us/azure/virtual-network/move-across-regions-vnet-portal>

This one is really really tricky and crab to say least because YES in the region (because mentions regions NOT SUBNET) you can delpoy more than 300 VMS because when you create VM it give the the option to join existing vNET or Subnet or create NEW vNET or Subnet and hence yes once the first subnet gets full and you create the next new VM it will automatically create new subnet for you as an option

So if comes in the exam i will chose sadly and confusingly YES

upvoted 3 times

  **Lazylinux** 6 months, 2 weeks ago

Finished the rest off here

NO- Having two vNETS in same RG differnt region with same name is NOT ALLOWED, due to the fact that vNET naming is RG scope limit see link below

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/resource-name-rules>

So my final answer is YYN

upvoted 2 times

  **Himank20** 9 months ago

I think it should be NYY

- A. Both Vnets have same range so Vnet1 can't be moved
- B. If we consider the /16 range of Vnet, 500 VMs can be deployed
- C. Two Vnets can have same name if they are in different region

Correct me if I'm wrong

upvoted 4 times

  **crypto700** 9 months, 1 week ago

NNN

-you cannot move Vnet to RG3. because they have the same subnet.

-you cannot deploy 300 VMs, Because the subnet size is /24.

upvoted 1 times

  **[Removed]** 8 months, 3 weeks ago

You can move the vnet to RG3. Just because they are in the same resource group doesn't mean there is any interaction between these networks. You could deploy as many vnets as you like with the same address range within this resource groups as long as the names are different. What you won't be able to do is to setup peering between these networks because their address ranges overlap.

upvoted 5 times

  **crypto700** 8 months, 2 weeks ago

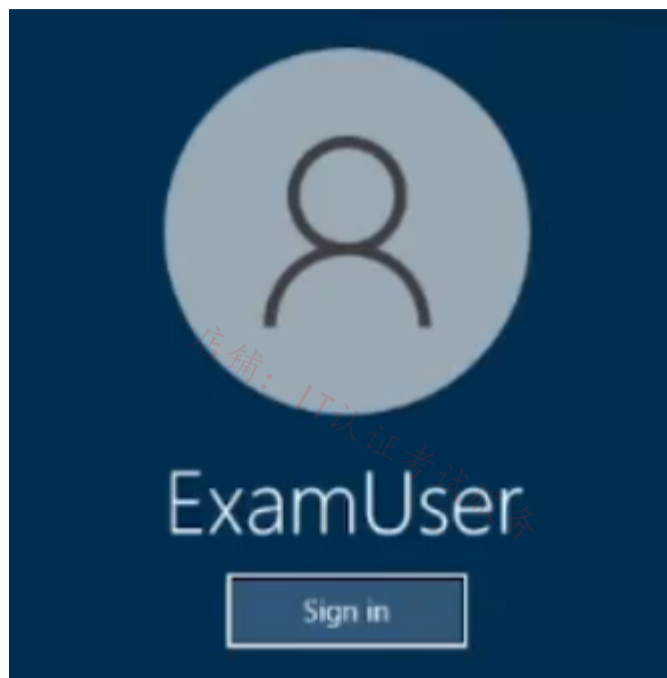
You are right... just tested in the Lab

YNN

upvoted 3 times

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You need to ensure that all hosts deployed to subnet3-2 connect to the internet by using the same static public IP address. The solution must minimize administrative effort when adding hosts to the subnet.

To complete this task, sign in to the Azure portal.

Correct Answer:

NAT gateway provides outbound internet connectivity for one or more subnets of a virtual network. Once NAT gateway is associated to a subnet, NAT provides source network address translation (SNAT) for that subnet. NAT gateway specifies which static IP addresses virtual machines use when creating outbound flows.

Plan:

Stage 1: Create a NAT gateway

Stage 2: Edit subnet subnet3-2 and link it to the NAT gateway

Stage 1: Create a NAT gateway

Step 1: Sign in to the Azure portal.

Step 2: In the search box at the top of the portal, enter NAT gateway. Select NAT gateways in the search results.

Step 3: Select + Create.

Step 4: In Create network address translation (NAT) gateway, enter or select this information in the Basics tab:

* NAT gateway name: Enter myNATgateway

Step 5: Select the Outbound IP tab, or select the Next: Outbound IP button at the bottom of the page.

Step 6: In the Outbound IP tab, enter or select the following information:

Public IP addresses - Select Create a new public IP address.

In Name, enter myPublicIP.

Select OK.

Step 7: Select the Review + create tab, or select the blue Review + create button at the bottom of the page.

Step 8: Select Create.

Stage 2: Edit subnet subnet3-2 and link it to the NAT gateway

Change subnet settings

Step 1: Go to the Azure portal to view your virtual networks. Search for and select Virtual networks.

Step 2: Select the name of the virtual network containing the subnet you want to change.

Step 3: From Settings, select Subnets.

Step 4: In the list of subnets, select the subnet you want to change settings for. Here choose subnet3-2 connect.

Step 5: In the subnet page, change the NAT Gateway to myNATgateway (the one we created in Stage 1).

Step 6: Select Save.

Reference:

<https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource>

<https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/quickstart-create-nat-gateway-portal>

 **Lazylinux** 2 months, 3 weeks ago

Yep Just deploy Azure NAT Gateway and nothing else
upvoted 1 times

 **trashbox** 3 months ago

Just deploy an Azure NAT Gateway. You don't need to create an UDR.

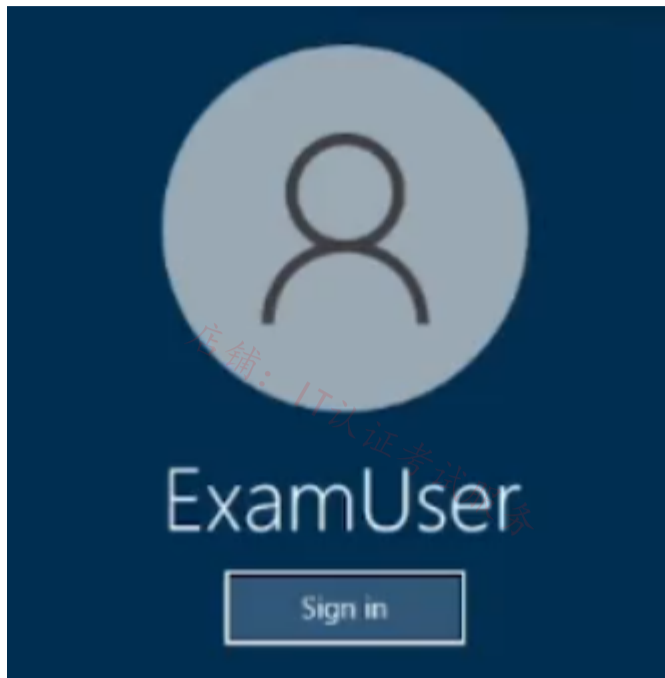
"When you create an instance of the Azure NAT Gateway service, your subnet is reconfigured so that it sends all outbound traffic to the NAT gateway service. There's no need to create routes, because it happens automatically."

<https://learn.microsoft.com/en-us/training/modules/intro-to-azure-nat-gateway/5-deploy-configure-azure-nat-gateway>

upvoted 1 times

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You need to ensure that subnet 4-3 can accommodate 507 hosts.

To complete this task, sign in to the Azure portal.

Correct Answer:

Change subnet settings

Step 1: Go to the Azure portal to view your virtual networks. Search for and select Virtual networks.

Step 2: Select the name of the virtual network containing the subnet you want to change.

Step 3: From Settings, select Subnets.

Step 4: In the list of subnets, select the subnet you want to change settings for. We select subnet 4-3.

Step 5: In the subnet page, change the Subnet address range setting:
For 507 hosts we need a 9-bit address range or larger, that is /23.

Change to address to /23. For example: 10.0.0.0/23 will work fine.

Note: For example, in a virtual network with address space 10.0.0.0/16, you might define a subnet address space of 10.0.0.0/22. The smallest range you can specify is /29, which provides eight IP addresses for the subnet. Azure reserves the first and last address in each subnet for protocol conformance. Three more addresses are reserved for Azure service usage. As a result, defining a subnet with a /29 address range results in three usable IP addresses in the subnet.

Step 6: Select Save.

Reference:

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-subnet>

 **mabalon** Highly Voted 5 months, 1 week ago

/23 can fit 507 addresses.
512 hosts - 5 reserved = 507.
The reserved ip address are .0 .1 .2 .3 and .255
upvoted 6 times

 **NahgotPride** Most Recent 2 months, 2 weeks ago

Correct
X.X.1.0/23
would be X.X.0.0 - X.X.1.255 (507 + 5 Azure reserved addresses)
upvoted 1 times

 **Techbiz** 4 months ago

We need to borrow 9 host bits from the host bit and assuming that the default address space was a /16 CIDR, then we will need $(2^9 - 5)$ to give us 507 ip address which is a /23
upvoted 1 times

 **Sein** 5 months, 1 week ago

/23 subnet won't be able to have 507 hosts, as azure reserves 5 IP addresses. You need /22 subnet.
upvoted 3 times

 **VeryOldITGuy** 5 days, 1 hour ago

Weird that MS says that if you create a /23, you get 507 + 5 Azure reserved addresses.
x.x.0.0 to x.x.1.255 makes 510 IP addresses total in my calculator and even on calculator sites.
Remove 0 at the beginning, 255 at the end and you are left with 508, then remove .1, .2 and .3 that Azure take and that leaves you 505.
Where does the 507 come from?
upvoted 1 times

You are planning the IP addressing for the subnets in Azure virtual networks.

Which type of resource requires IP addresses in the subnets?

- A. internal load balancers
- B. Azure DDoS Protection for virtual networks
- C. service endpoint policies
- D. service endpoints

Correct Answer: A

 **Henryjb3** 2 weeks, 1 day ago

Repeat question.
upvoted 1 times

 **NSF2** 3 weeks, 1 day ago

The question is bit vague.
The internal LB require dedicated subnet, but the question is asking about the IP address requirement within a subnet.
upvoted 1 times

 **GBAU** 3 months ago

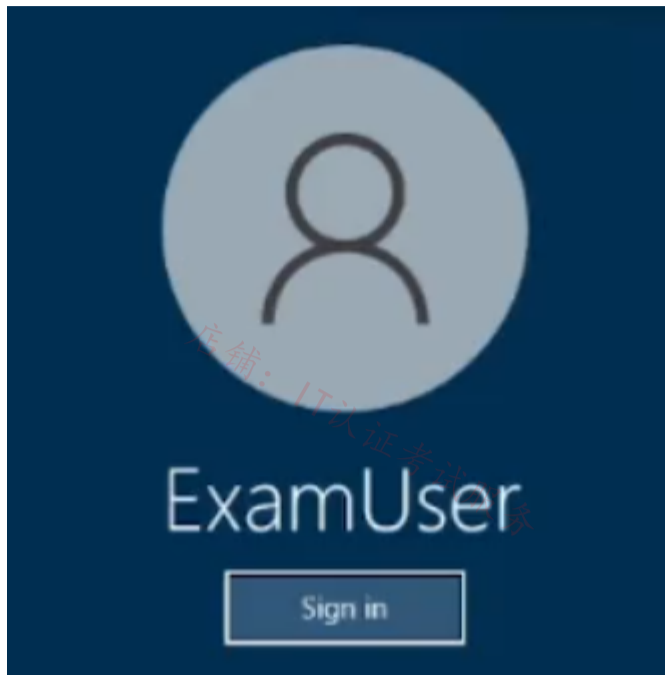
A,D
A) internal load balancers need an internal IP on the subnet to listen on of course
D) Service Endpoints: "Service Endpoints enables private IP addresses in the VNet to reach the endpoint of an Azure service without needing a public IP address on the VNet."
<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview>
upvoted 1 times

 **GBAU** 3 months ago

Ignore D above, that just means OTHER IPs in the vNet can reach the SE, not that it gives it a private IP in the vNet. Ma bad...
upvoted 1 times

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You need to ensure that virtual machines on VNET1 and VNET2 are included automatically in a DNS zone named contosoazure. The solution must ensure that the virtual machines on VNET1 and VNET2 can resolve the names of the virtual machines on either virtual network.

To complete this task, sign in to the Azure portal.

What is the auto registration feature in Azure DNS private zones?

The Azure DNS private zones auto registration feature manages DNS records for virtual machines deployed in a virtual network. When you link a virtual network with a private DNS zone with this setting enabled, a DNS record gets created for each virtual machine deployed in the virtual network.

For each virtual machine, an A record and a PTR record are created. DNS records for newly deployed virtual machines are also automatically created in the linked private DNS zone. When a virtual machine gets deleted, any associated DNS records also get deleted from the private DNS zone.

Step 1: Locate the DNS zone contosoazure

Step 2: On the left pane, select Virtual network links.

Step 3: Select Add.

privatecontoso.com

Link name *

Virtual network details

Only virtual networks with Resource Manager deployment model are supported for linking with Private DNS zones. Virtual networks with Classic deployment model are not supported.

I know the resource ID of virtual network ⓘ

Subscription * ⓘ

Azure Subscription

Virtual network *

Configuration

Enable auto registration ⓘ

OK

Correct Answer:

Step 4: Type myLink for the Link name.

Step 5: For Virtual network, select VNET1.

Step 6: Select the Enable auto registration check box.

To enable auto registration, select the checkbox for "Enable auto registration" when you create the virtual network link.

Step 7: Select OK.

Step 8: Repeat procedure for VNET2.

Reference:

<https://learn.microsoft.com/en-us/azure/dns/private-dns-autoregistration>

<https://learn.microsoft.com/en-us/azure/dns/private-dns-getstarted-portal#link-the-virtual-network>

Lazylinux 2 months, 3 weeks ago

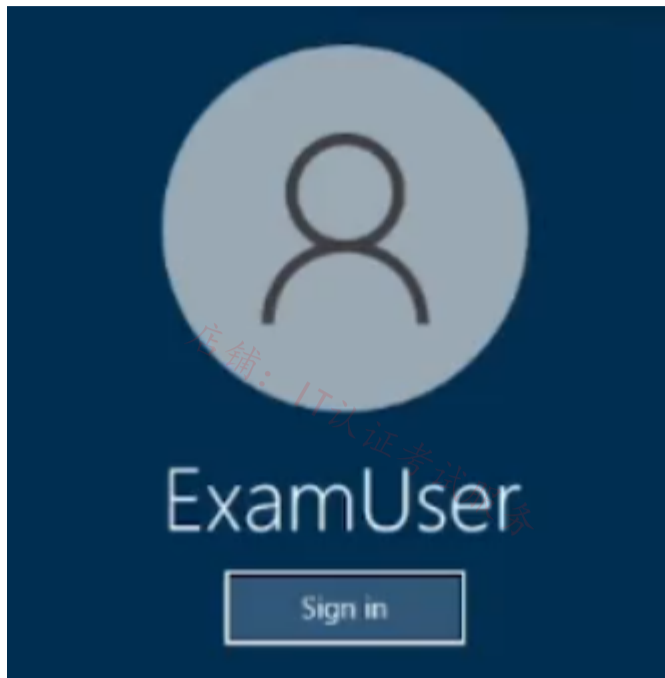
Yep create 2 virtual links to private DNS zone for Vnet 1 and 2 and enable Auto-registration for both
upvoted 1 times

Izariqi 4 months, 2 weeks ago

Answer is right.
upvoted 2 times

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You need to ensure that you can deploy Azure virtual machines to the France Central Azure region. The solution must ensure that virtual machines in the France Central region are in a network segment that has an IP address range of 10.5.1.0/24.

To complete this task, sign in to the Azure portal.

You can create a virtual network before you create a virtual machine or you can create the virtual network as you create a virtual machine.

You create these resources to support communication with a virtual machine:

Network interfaces
IP addresses
Virtual network and subnets

Create a virtual network

Step 1: Select Create a resource in the upper left-hand corner of the portal.

Step 2: In the search box, enter Virtual Network. Select Virtual Network in the search results.

Step 3: In the Virtual Network page, select Create.

Step 4: In Create virtual network, enter or select this information in the Basics tab:

Create virtual network ...

Basics IP Addresses Security Tags Review + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. [Learn more about virtual network](#)

Project details

Subscription * ⓘ Contoso Subscription

Resource group * ⓘ myResourceGroup
[Create new](#)

Instance details

Name * myVNet ✓

Region * East US

[Review + create](#) [< Previous](#) [Next: IP Addresses >](#) [Download a template for automation](#)

Correct Answer:

Step 5: Enter Region: France Central

Step 6: Select the IP Addresses tab, or select the Next: IP Addresses button at the bottom of the page and enter in the following information then select Add:

[Home](#) > [Create a resource](#) > [Marketplace](#) > [Virtual network](#) >

Create virtual network ...

Basics **IP Addresses** Security Tags Review + create

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space

10.1.0.0/16 ✓

Add IPv6 address space ⓘ

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

+ Add subnet [Remove subnet](#)

<input type="checkbox"/> Subnet name	Subnet address range	NAT gateway
<input type="checkbox"/> MySubnet	10.1.0.0/24	-

i Use of a NAT gateway is recommended for outbound internet access from a subnet. You can deploy a NAT gateway and assign it to a subnet after you create the virtual network. [Learn more](#)

Step 7: For IPv4 address space enter: 10.5.1.0/16

Step 8: Click Add subnet

Step 9: For Subnet address range Enter 10.5.1.0/24.

Step 10: Finish the wizard.

Reference:

<https://learn.microsoft.com/en-us/azure/virtual-network/quick-create-portal>

mein17 5 months, 1 week ago

In the Given Answer

Step 7: VNet Address Space they mentioned 10.5.1.0/16 but It Should be 10.5.0.0/16.
for subnet given answer is correct.

upvoted 2 times

 **Crazysaffer** 8 months, 1 week ago

Remember to select the right location. (France Central Azure region)

upvoted 3 times

店铺：IT认证考试服务

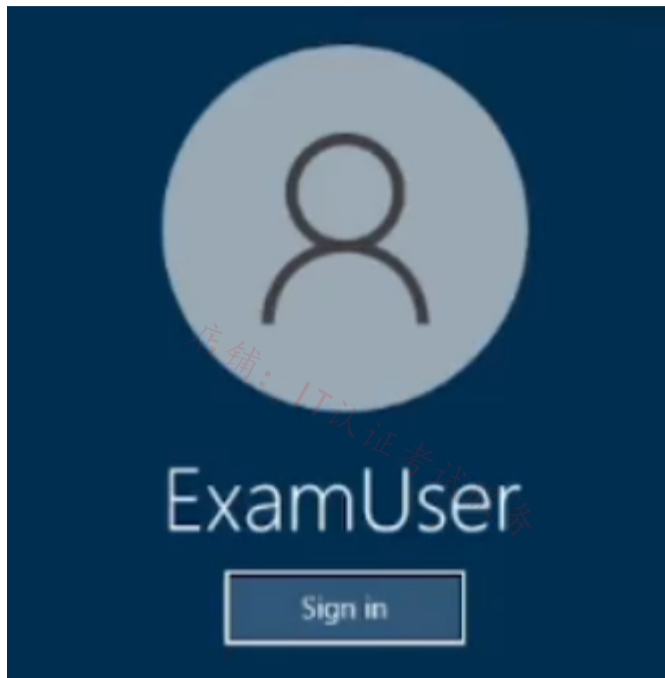
店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

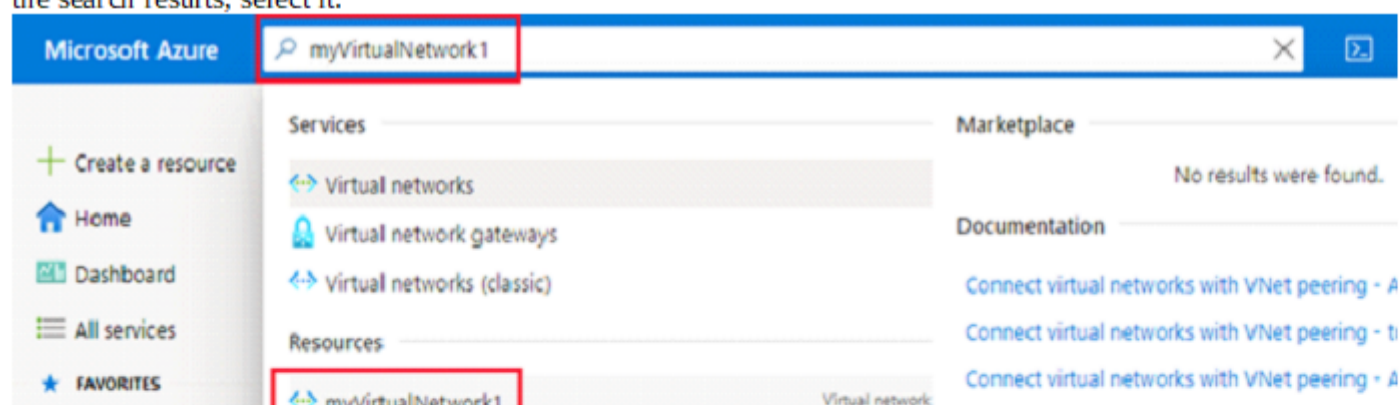
-

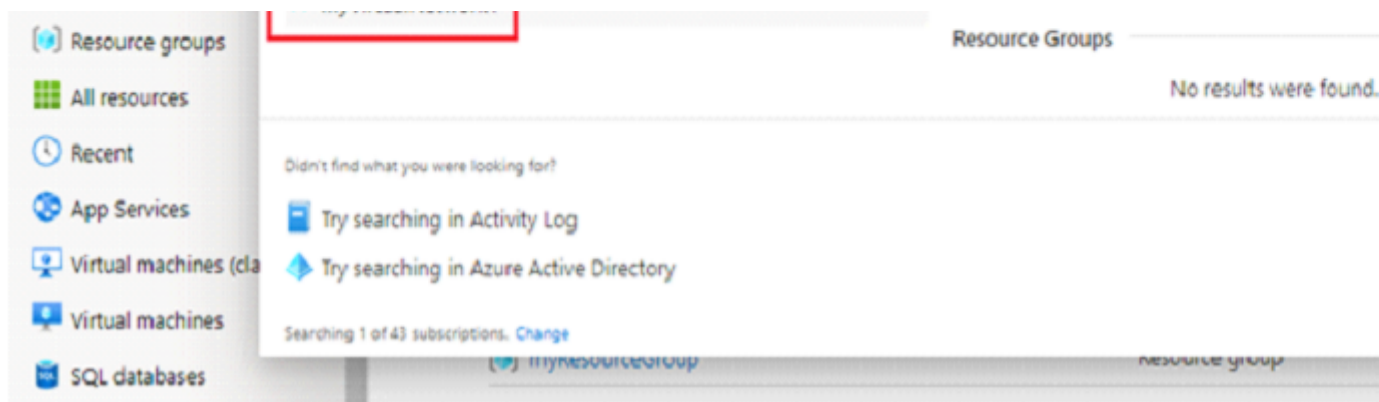
You need to ensure that hosts on VNET1 and VNET2 can communicate. The solution must minimize latency between the virtual networks.

To complete this task, sign in to the Azure portal.

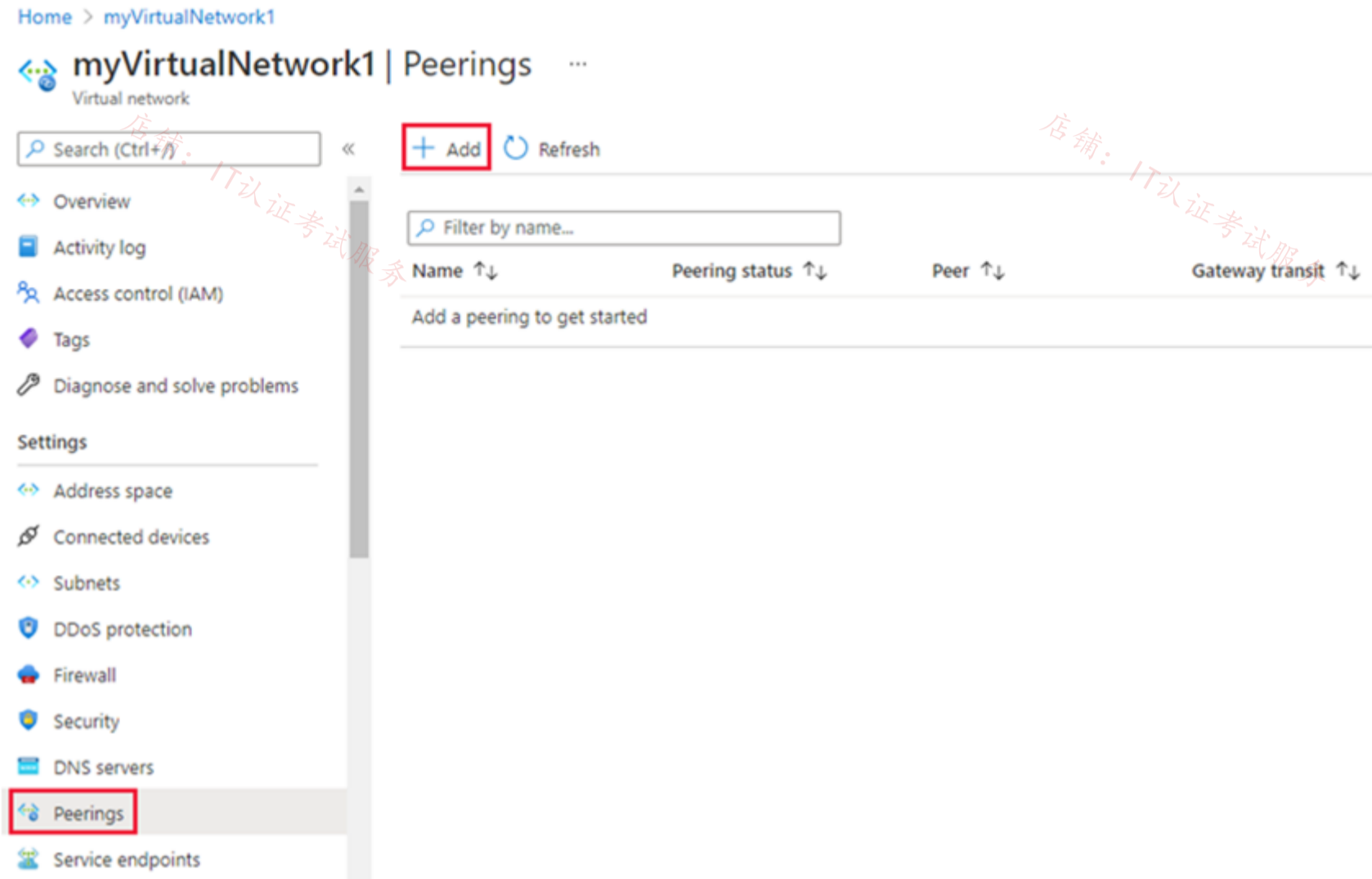
Correct Answer:**Peer virtual networks**

Step 1: In the search box at the top of the Azure portal, look for VNet1. When VNET1 appears in the search results, select it.





Step 2: Under Settings, select Peerings, and then select + Add, as shown in the following picture:

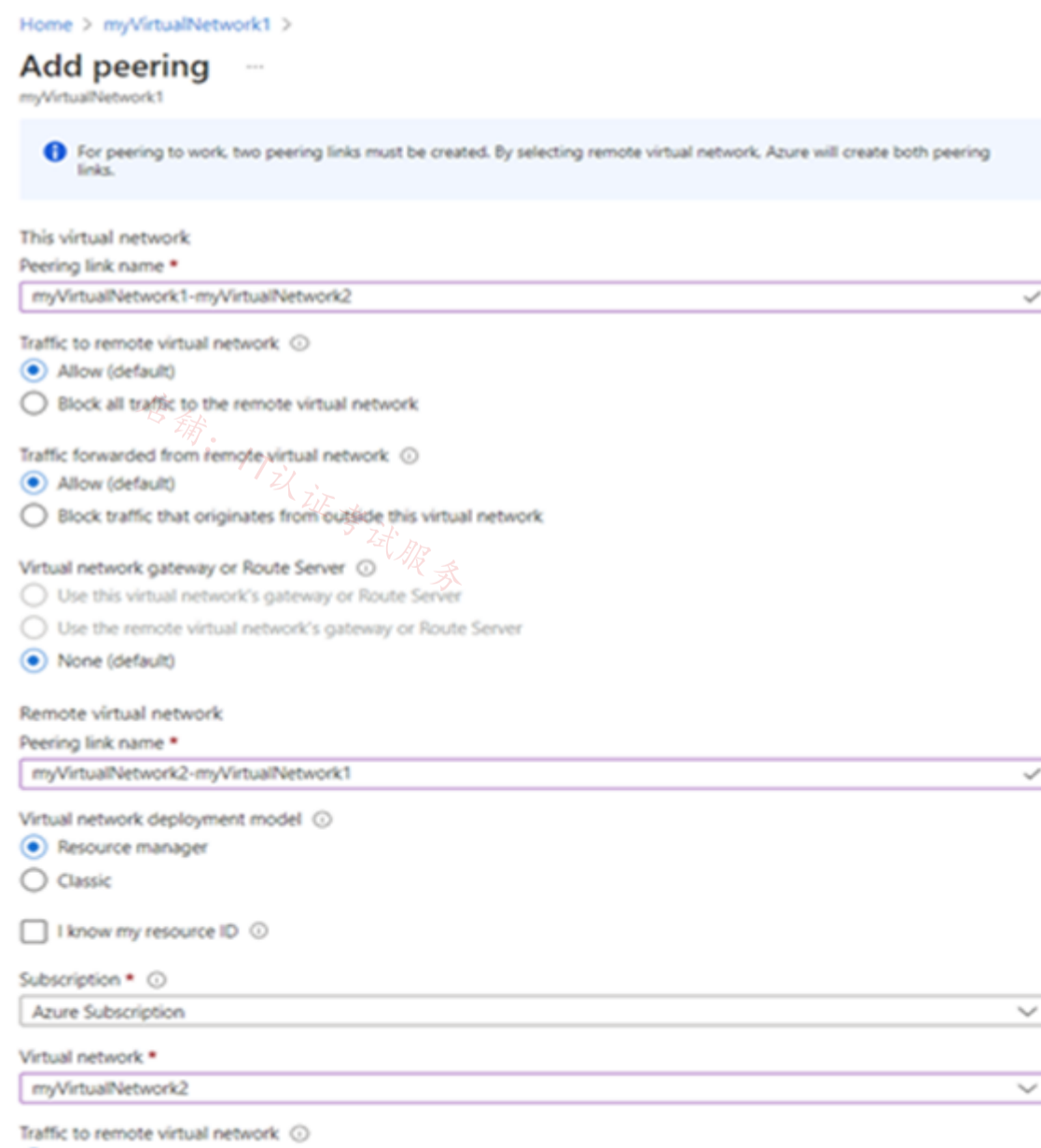


Step 3: Enter or select the following information, accept the defaults for the remaining settings, and then select Add.

* ..

* Virtual network

Select VNET2 for the name of the remote virtual network. The remote virtual network can be in the same region of VNET1 or in a different region.



- Allow (default)
 - Block all traffic to the remote virtual network
- Traffic forwarded from remote virtual network
- Allow (default)
 - Block traffic that originates from outside this virtual network
- Virtual network gateway or Route Server
- Use this virtual network's gateway or Route Server
 - Use the remote virtual network's gateway or Route Server
 - None (default)

Add

Step 4: Click Add

In the Peerings page, the Peering status is Connected, as shown in the following picture:

Home > myVirtualNetwork1

myVirtualNetwork1 | Peerings

Virtual network

Search (Ctrl+/) << + Add Refresh

Filter by name...

Name ↑↓	Peering status ↑↓	Peer ↑↓	Gateway transit ↑↓
myVirtualNetwork1-myVirtualNetwork2	Connected	myVirtualNetwork2	Disabled

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

Reference:

<https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-connect-virtual-networks-portal>

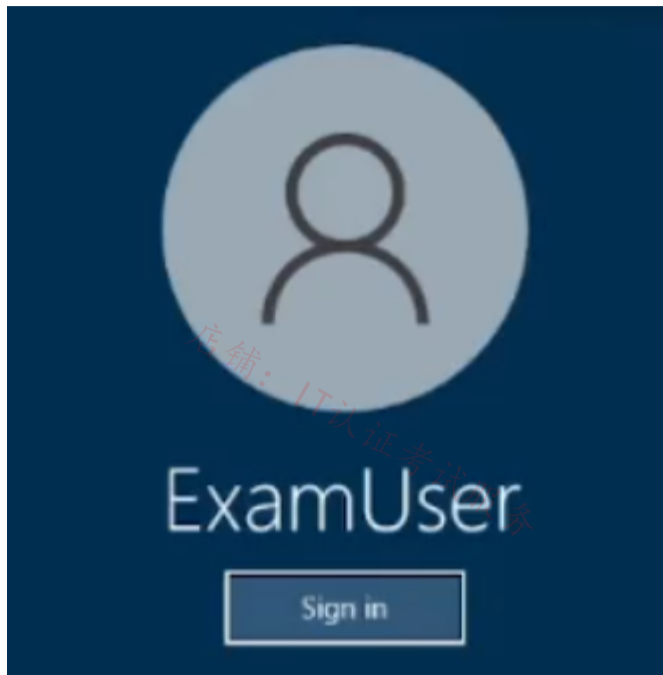
Currently there are no comments in this discussion, be the first to comment!

店铺: IT认证考试服务

店铺: IT认证考试服务

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You need to ensure that the owner of VNET3 receives an alert if an administrative operation is performed in the virtual network.

To complete this task, sign in to the Azure portal.

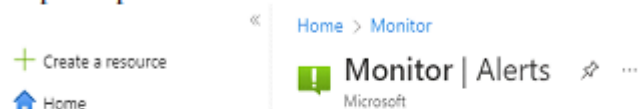
Correct Answer:**Monitoring Azure virtual network Alerts**

Azure Monitor alerts proactively notify you when important conditions are found in your monitoring data. They allow you to identify and address issues in your system before your customers notice them. You can set alerts on metrics, logs, and the activity log.

Create a new alert rule in the Azure portal

Step 1: In the portal, select Monitor > Alerts.

Step 2: Open the + Create menu and select Alert rule.



Step 3: On the Select a resource pane, set the scope for your alert rule. You can filter by subscription, resource type, or resource location. We select Virtual Network.

The Available signal types for your selected resources are at the bottom right of the pane.

Step 4: Select Include all future resources to include any future resources added to the selected scope.

Step 5: Select Done.

Step 6: Select Next: Condition at the bottom of the page.

Step 7: On the Select a signal pane, filter the list of signals by using the signal type and monitor service:

* **Signal type:** The type of alert rule you're creating. We select Activity log

* **Monitor service:** The service sending the signal. This list is pre-populated based on the type of alert rule you selected. We select Activity log – Administrative (The service that provides the Administrative activity log events)

Step 8: On the Actions tab, select to create the required action group.

[Review + create](#) [Previous](#) [Next: Details >](#)

Step 9: Configure basic action group settings

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

Resource group * ⓘ [Create new](#)

Instance details

Action group name * ⓘ ✓

Display name * ⓘ ✓
This display name is limited to 12 characters

[Review + create](#) [Previous](#) [Next: Notifications >](#)

Step 10: Configure notifications. To open the Notifications tab, select Next: Notifications. Alternately, at the top of the page, select the Notifications tab.

Step 11: Define a list of notifications to send when an alert is triggered.
Notification: Email Azure Resource Manager Role
Name: Notify Owner

Step 12: Select OK.

Step 13: Finish the remaining steps in the wizard.

Reference:

- <https://learn.microsoft.com/en-us/azure/virtual-network/monitor-virtual-network>
- <https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-create-new-alert-rule?tabs=metric#create-a-new-alert-rule-in-the-azure-portal>

ABYGG (Highly Voted) 7 months, 4 weeks ago

1. Monitor > Alerts > Alert Rule
2. Alert Rule
 - Scope > Select VNet3 > Apply
 - Condition > See all signals > Activity Log > All Administrative Operation > Apply
 - Actions > Create Action Group

Basic Tab

Notification > Email/SMS-message/Push Voice > Put the email > Name

Actions > Not required for this scenario just notification is enough

Tags > You can assign a necessary tag for the action group

Review+Create

- Details

Alert Rule Name > VNET3 Notification

Description > Notify the admin for any changes on VNET3

- Tags > Put any tag that represent the Alert Rule

- Review+Create

upvoted 11 times

Lazylinux 2 months, 3 weeks ago

Incorrect and im shocked 11 people voted you UP!!! see my explanation, you are totally wrong at the NOTIFCATION TYPE, question asked to email OWNER!!!

upvoted 2 times

 **Lazylinux** Most Recent 2 months, 3 weeks ago

What ABIYGK mentioned below is NOT CORRECT specially the part Notification type should be Email Azure Resource Manager Role

Personally i DO NOT go to Azure monitor as it will take long before you can filter to the resource in question, go to Vnet and from there follow the below

Vnet>Monitoring>Alerts>Create Alert>Signal>Select "All administrative Operations">
Create Action Group>Put in necessary details like names etc>This is IMPORTANT => Select Email Azure Resource Manager ROLE> select OWNER and fill in the name> Bypass actions and tags tab>Review and create> DONE

upvoted 4 times

店铺：IT认证考试服务

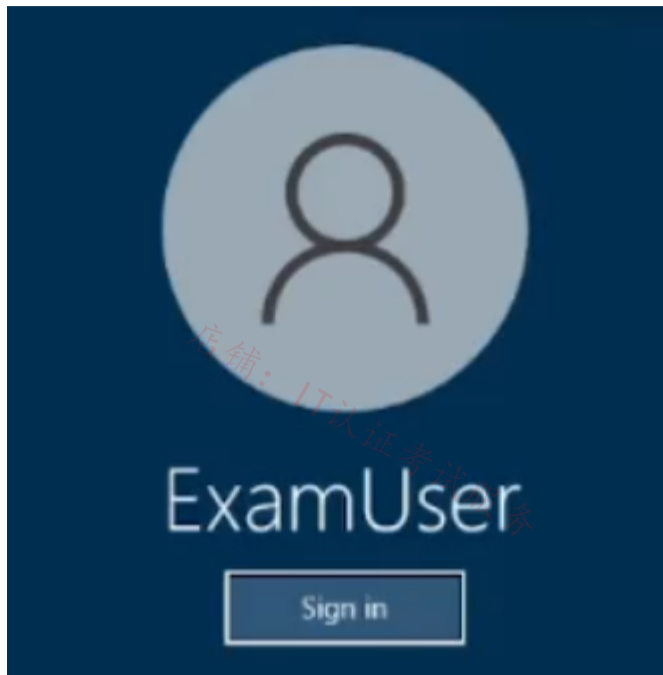
店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You need to archive all the metrics of VNET1 to an existing storage account.

To complete this task, sign in to the Azure portal.

Monitoring Azure virtual network
Azure virtual network uses Azure Monitor.

Data platform
Azure Monitor stores data in data stores for each of the pillars of observability: metrics, logs, distributed traces, and changes. Each store is optimized for specific types of data and monitoring scenarios.

Retention of metrics
You can send platform metrics for Azure Monitor resources to a Log Analytics workspace for long-term trending.

Send to Azure Storage
Send resource logs to Azure Storage to retain them for archiving. After you've created the diagnostic setting, a storage container is created in the storage account as soon as an event occurs in one of the enabled log categories.

one of the enabled log categories.

Create a diagnostic setting to send resource logs to a Log Analytics workspace or to a Storage Account.

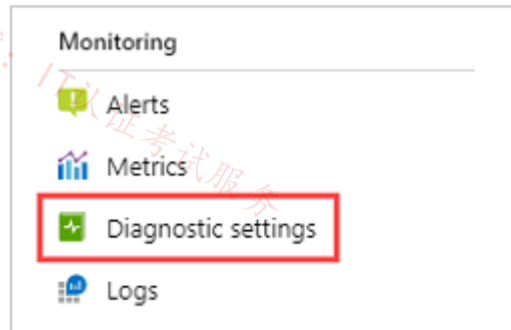
Archiving logs and metrics to a Storage account is useful for audit, static analysis, or backup. Compared to using Azure Monitor Logs or a Log Analytics workspace, Storage is less expensive, and logs can be kept there indefinitely.

Create diagnostic settings

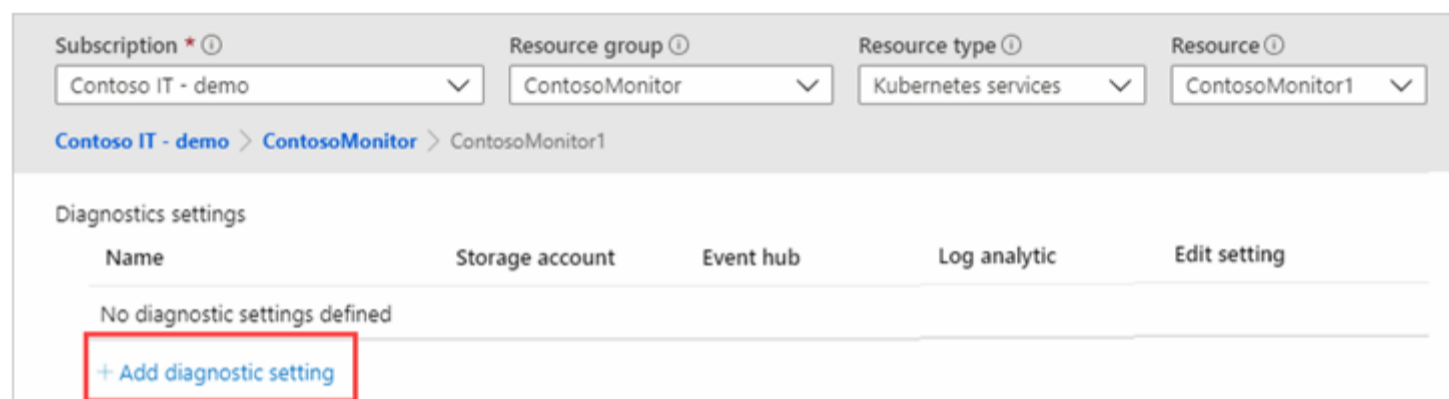
You can configure diagnostic settings in the Azure portal either from the Azure Monitor menu or from the menu for the resource.

Step 1: Select the Virtual Network VNET1.

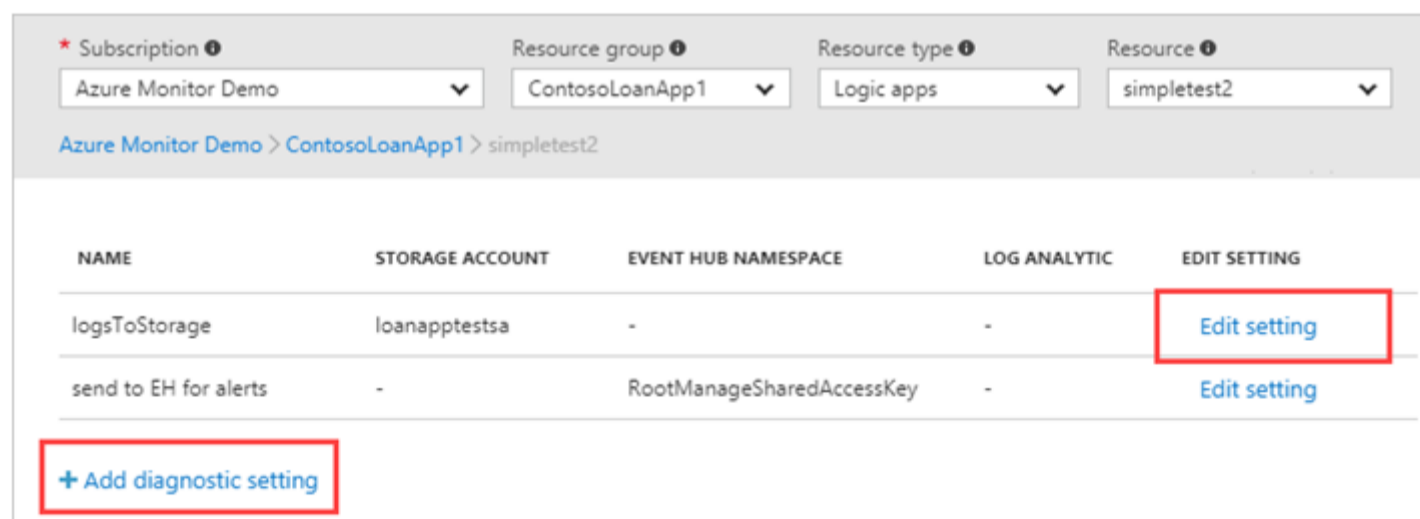
Step 2: Select Diagnostic settings under Monitoring on the resource's menu.



Step 3: If no settings exist on the resource you've selected, you're prompted to create a setting. Select Add diagnostic setting.



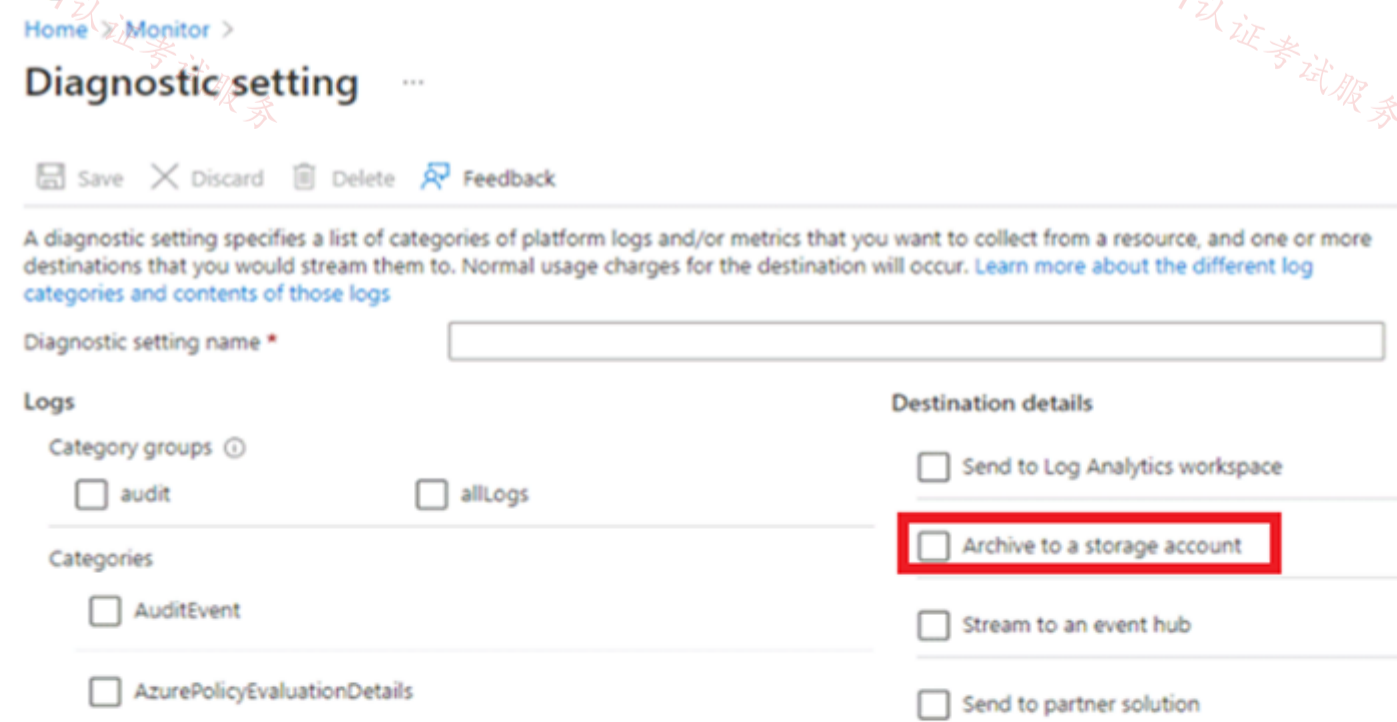
If there are existing settings on the resource, you see a list of settings already configured. Select Add diagnostic setting to add a new setting. Or select Edit setting to edit an existing one. Each setting can have no more than one of each of the destination types.



Correct Answer:

Step 4: Give your setting a name if it doesn't already have one.

Step 5: Logs and metrics to route: Select AllMetrics if you want to store metrics in Azure Monitor Logs too.



Metrics

AllMetrics

Step 6: Destination details. Select Archive to a storage account

Step 7: Storage: Select the Subscription, Storage account, and Retention policy.

Category details	Destination details
<p>log</p> <hr/> <p><input type="checkbox"/> WorkflowRuntime</p> <p>Retention (days)</p> <input type="text" value="0"/>	<p><input type="checkbox"/> Send to Log Analytics</p> <hr/> <p><input checked="" type="checkbox"/> Archive to a storage account</p> <hr/> <p>i Showing all storage accounts including classic storage accounts</p>
<p>metric</p> <hr/> <p><input type="checkbox"/> AllMetrics</p> <p>Retention (days)</p> <input type="text" value="0"/>	<p>Location: West US</p> <p>Subscription: AI - SRT- Dev ...</p> <p>Storage account *: azmonitorbidev</p> <p><input type="checkbox"/> Stream to an event hub</p>
<p>i Retention only applies to storage account. Retention policy ranges from 1 to 365 days. If you do not want to apply any retention policy and retain data forever, set retention (days) to 0.</p>	

Step 8: Select Save.

Reference:

<https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/diagnostic-settings>
<https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/data-platform-metrics>

H0zwei 2 months, 1 week ago

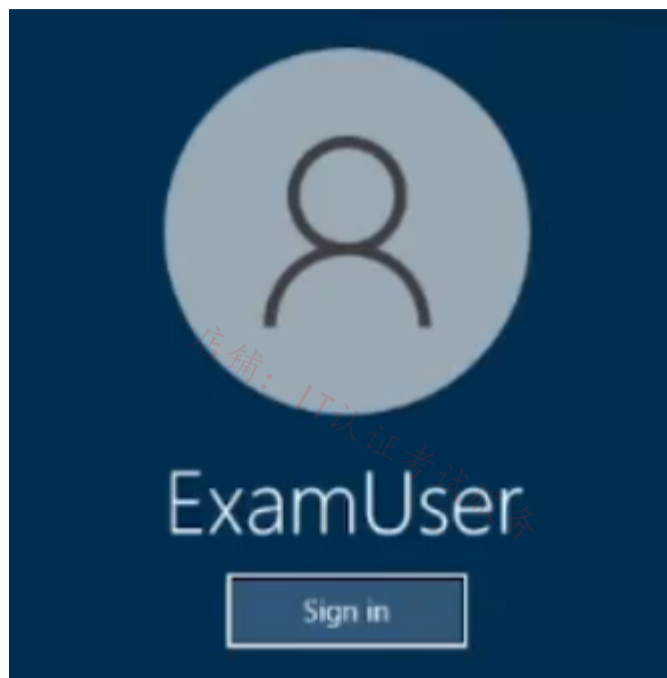
This answer is outdated: Storage retention via diagnostic settings is being deprecated and new rules can no longer be configured. To maintain your existing retention rules please migrate to Azure Storage Lifecycle Management by September 30th 2025. What do I need to do?
upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You plan to deploy 100 virtual machines to subnet-1. The virtual machines will NOT be assigned a public IP address. The virtual machines will call the same API which is hosted by a third party. The virtual machines will make more than 10,000 calls per minute to the API.

You need to minimize the risk of SNAT port exhaustion. The solution must minimize administrative effort.

To complete this task, sign in to the Azure portal.

SNAT exhaustion occurs when a backend instance runs out of given SNAT Ports. A load balancer can still have unused SNAT ports. If a backend instance's used SNAT ports exceed its given SNAT ports, it will be unable to establish new outbound connections.

Use a NAT gateway for outbound connectivity to the Internet
Virtual network NAT gateway is a highly resilient and scalable Azure service that provides outbound connectivity to the internet from your virtual network. A NAT gateway's unique method of consuming SNAT ports helps resolve common SNAT exhaustion and connection issues.

(Basic load balancers and basic public IP addresses aren't compatible with NAT.)

Create a NAT gateway

Step 1: Sign in to the Azure portal.

Step 2: In the search box at the top of the portal, enter NAT gateway. Select NAT gateways in the search results.

Step 3: Select + Create.

Step 4: In Create network address translation (NAT) gateway, enter or select this information in the Basics tab.

* Details omitted *

Step 5: Select the Outbound IP tab, or select the Next: Outbound IP button at the bottom of the page.

Step 6: In the Outbound IP tab, enter or select the following information:

* Public IP addresses

Select Create a new public IP address.

In Name, enter myPublicIP.

Select OK.

Step 7: Select the Review + create tab, or select the blue Review + create button at the bottom of the page.

Step 8: Select Create.

Reference:

<https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-outbound-connections>

<https://learn.microsoft.com/en-us/azure/load-balancer/troubleshoot-outbound-connection>

Correct Answer:

 **Lazylinux** 1 month ago


Key here as mentioned is the Public IP Prefix, since no mention of the Ports to be used I would go for Max i.e. /28 here is more from MS doco
A single NAT gateway can scale up to 16 IP addresses. Each NAT gateway public IP address provides 64,512 SNAT ports to make outbound connections. NAT gateway can scale up to over 1 million SNAT ports.

NAT gateway can use up to 16 public IP addresses. NAT gateway can use any combination of public IP addresses and public IP prefixes totaling to 16 addresses. NAT gateway can support the following prefix sizes: /28 (16 addresses), /29 (8 addresses), /30 (4 addresses), and /31 (2 addresses).
More here

<https://learn.microsoft.com/en-us/azure/nat-gateway/nat-gateway-snat#nat-gateway-snat-port-selection-and-reuse>

<https://learn.microsoft.com/en-us/azure/nat-gateway/faq>

upvoted 1 times

 **bp_a_user** 3 months, 1 week ago

key is here to use a ip-address prefix

upvoted 3 times

 **Techbiz** 4 months ago


The right solution involves provisioning a NAT gateway and integrating it with the subnet

upvoted 1 times

 **Shimi** 9 months, 3 weeks ago

Shouldn't this be a standard load balancer?

upvoted 2 times

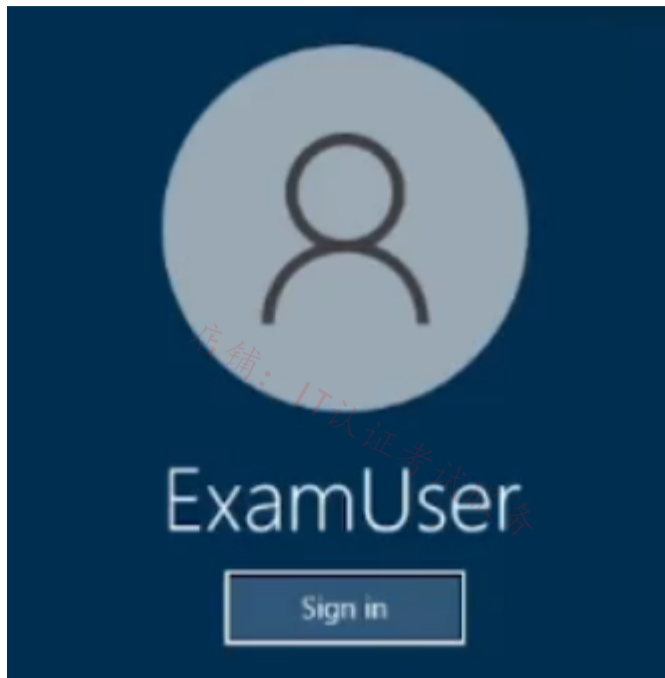
 **MrBlueSky** 9 months, 2 weeks ago

No. When you see SNAT Port exhaustion the answer they want you to pick is likely NAT Gateway as it specifically addresses this problem that LBs have

upvoted 8 times

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You plan to deploy an appliance to subnet3-2. The appliance will perform packet inspection and will have an IP address of 10.3.2.100.

You need to ensure that all traffic to the internet from subnet3-1 is forwarded to the appliance for inspection.

To complete this task, sign in to the Azure portal.

Plan:**Stage 1: Create a route table****Stage 2: Create a route****Stage 3: Associate a route table to a subnet****Stage 1: Create a route table****Step 1: On the Azure portal menu or from the Home page, select Create a resource.****Step 2: In the search box, enter Route table. When Route table appears in the search results, select it.****Step 3: In the Route table page, select Create.**

Step 4: In the Create route table dialog box:

* Details omitted*

Step 5: Select Review + create and then Create to create your new route table.

Stage 2: Create a route

Step 6: Make sure the route table you created is selected.

Step 7: From the route table menu bar, choose Routes and then select + Add.

Step 8: Enter a unique Route name for the route within the route table.

Add route

myRouteTable

Route name *

Address prefix destination * ⓘ

Next hop type * ⓘ

Next hop address * ⓘ

Add

Step 9: Enter the Address prefix, in Classless Inter-Domain Routing (CIDR) notation, that you want to route traffic to. The prefix can't be duplicated in more than one route within the route table, though the prefix can be within another prefix. For example, if you defined 10.0.0.0/16 as a prefix in one route, you can still define another route with the 10.0.0.0/22 address prefix. Azure selects a route for traffic based on longest prefix match.

Enter the following:

Address prefixes: 0.0.0.0/0

Next hop type: Internet

Next hop address: 10.3.2.100

Step 10: Click Add.

Correct Answer: Stage 3: Associate a route table to a subnet

Step 11: In the virtual network list, choose the virtual network that contains the subnet you want to associate a route table to.

Step 12: In the virtual network menu bar, choose Subnets.

Step 13: Select the subnet you want to associate the route table to. In our case select subnet3-1, (You need to ensure that all traffic to the internet from subnet3-1 is forwarded to the appliance for inspection.)

Step 14: In Route table, choose the route table you want to associate to the subnet. Select the one you created earlier.

default

VNetA

Name

Subnet address range * ⓘ

10.0.0.0 - 10.0.0.255 (251 + 5 Azure reserved addresses)

Add IPv6 address space ⓘ

NAT gateway ⓘ

Network security group

Route table

None
myRouteTable

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ
0 selected

SUBNET DELEGATION

Delegate subnet to a service ⓘ
None

Save Cancel

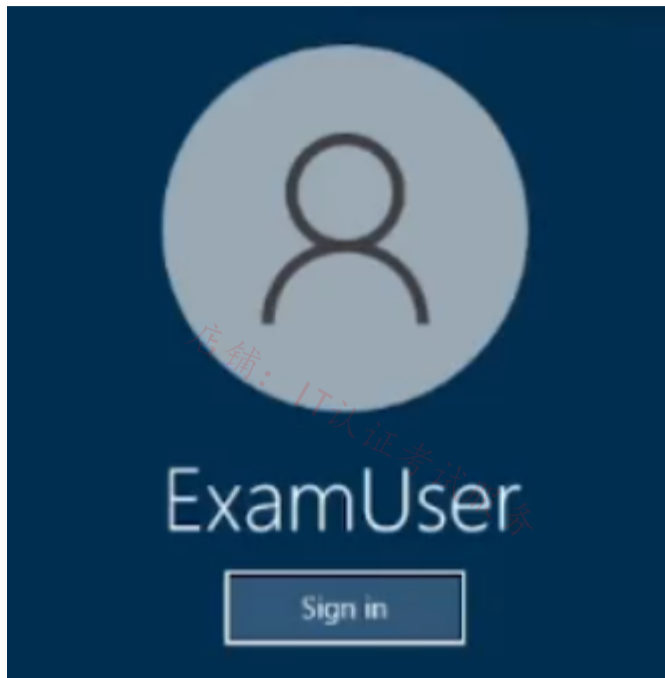
Step 15: Select Save.

Reference:
<https://learn.microsoft.com/en-us/azure/virtual-network/manage-route-table>
<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview#how-azure-selects-a-route>

- khanda** Highly Voted 9 months, 2 weeks ago
Next hop should not be internet if you want to send your internet traffic to an NVA. It should be "Virtual appliance"
upvoted 20 times
- occupatissimo** 8 months, 2 weeks ago
you're right
upvoted 2 times
- trashbox** 3 months ago
You are right. I have confirmed that when "Internet" is specified in the next hop type, the next hop address cannot be entered.
upvoted 3 times
- Lazylinux** Most Recent 1 month ago
You need to create route table as per below – Called InternetAccess
Destination type – IP Address
Destination IP address/CIDR ranges – 0.0.0.0/0
Next Hop type – Virtual Appliance
Next Hop Address - 10.3.2.100
Save and now associate the InternetAccess route table with subnet - subnet3-1
All done
upvoted 1 times

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You plan to use VNET4 for an Azure API Management implementation.

You need to configure a policy that can be used by an Azure application gateway to protect against known web attack vectors. The policy must only allow requests that originate from IP addresses in Canada. You do NOT need to create the application gateway to complete this task.

To complete this task, sign in to the Azure portal.

Correct Answer:

Azure Front Door web application firewall (WAF) protects web applications from common vulnerabilities and exploits. Azure-managed rule sets provide an easy way to deploy protection against a common set of security threats.

You can restrict access to your web applications by country/region.

Plan:

Stage 1: Create a WAF policy

Stage 2: Create a custom WAF Geo location rule that blocks all traffic outside Canada

Stage 3: Create a custom WAF Geo location rule that allows traffic from Canada

First, create a basic WAF policy with a managed Default Rule Set (DRS) using the Azure portal.

Step 1: On the upper left side of the portal, select Create a resource. Search for WAF, select Web Application Firewall, then select Create.

Step 2: On Create a WAF policy page, Basics tab, enter or select the following information and accept the defaults for the remaining settings:

* details omitted *

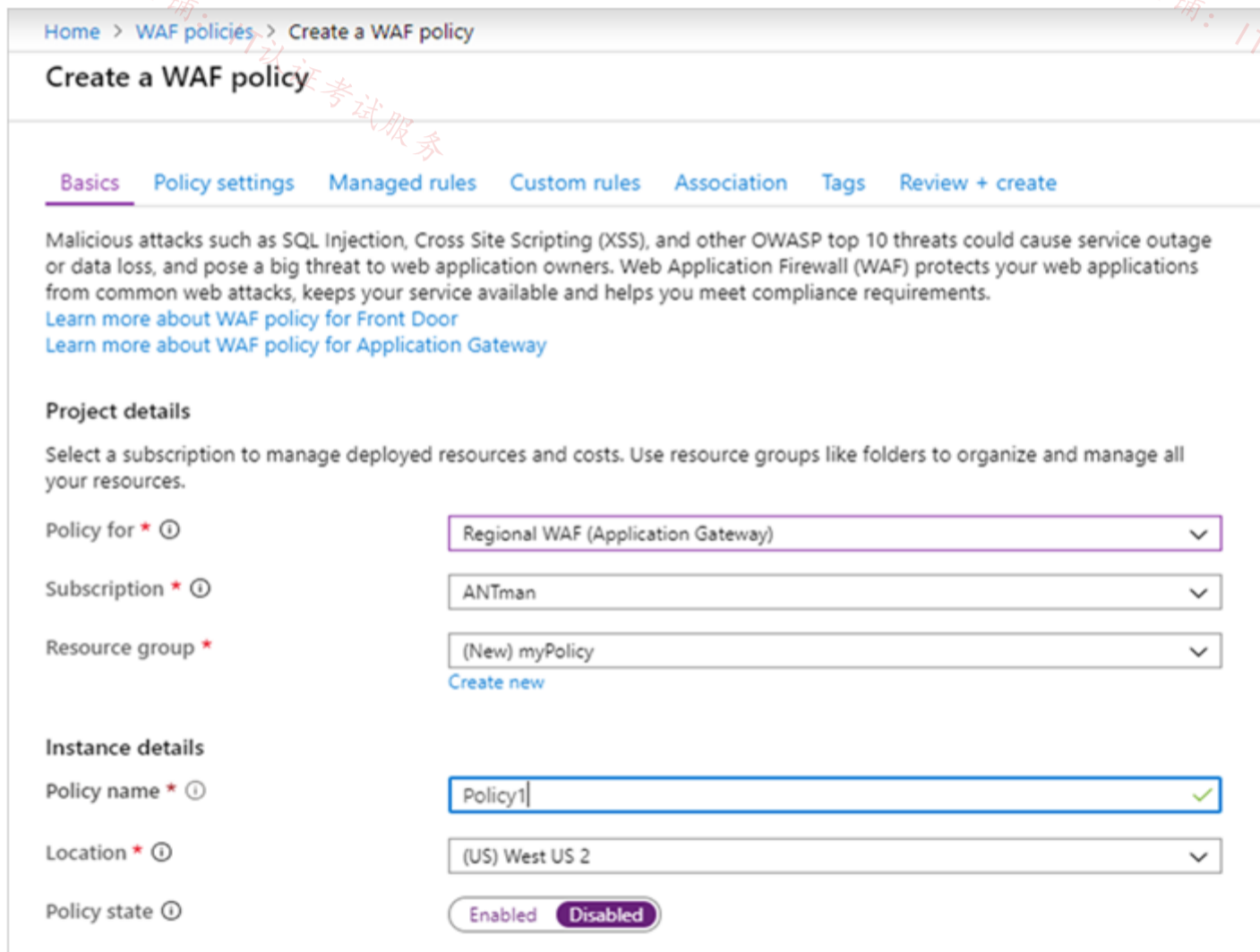
Step 3: On the Association tab, select Add association, then select one of the following settings:

Application Gateway: Select the application gateway, and then select Add.

HTTP Listener: Select the application gateway, select the listeners, then select Add.

Route Path: Select the application gateway, select the listener, select the routing rule, and then select Add.

Step 4: Select Review + create, then select Create.



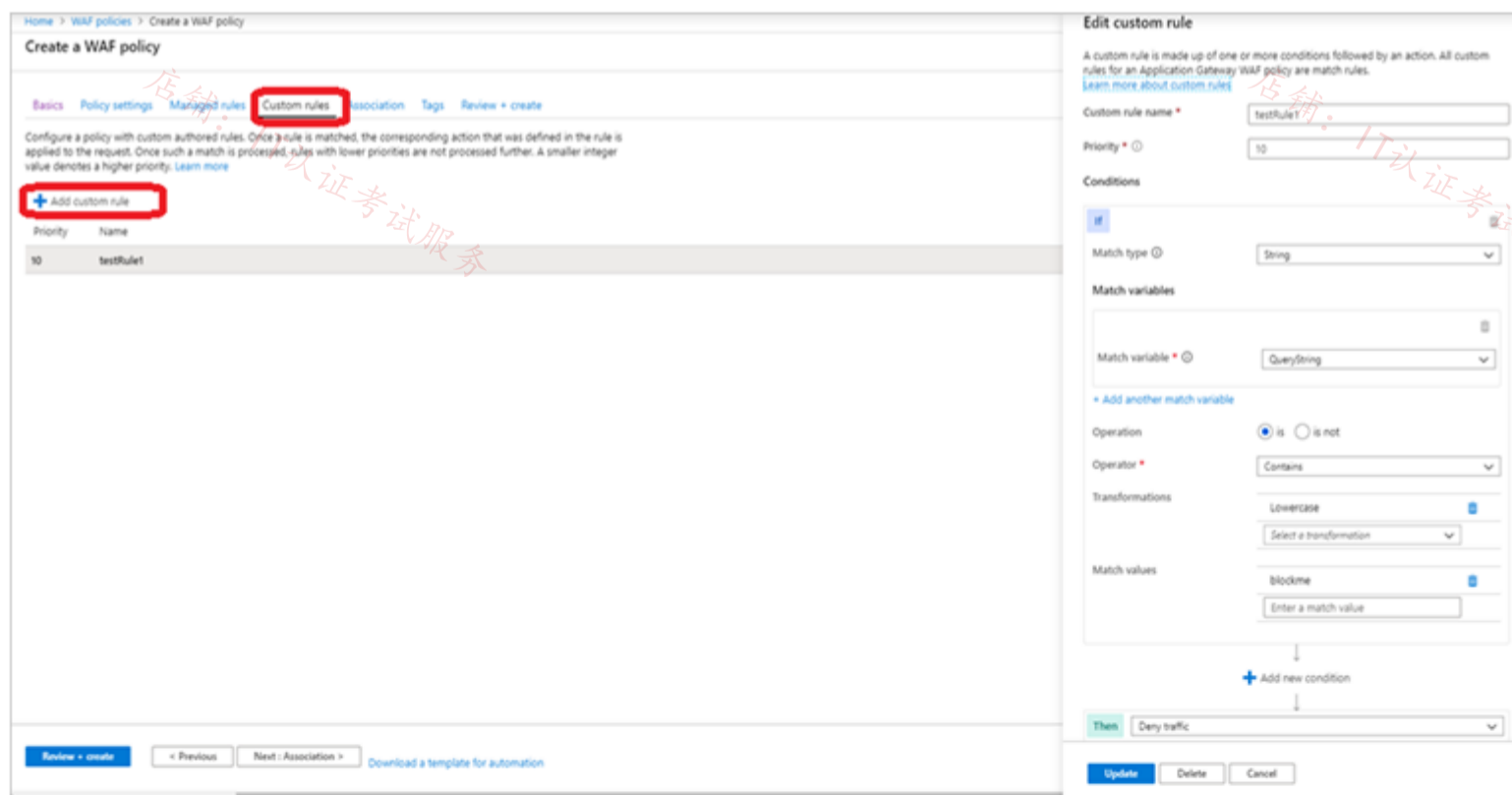
Stage 2: Create a custom WAF Geo location rule that blocks all traffic outside Canada

Configure WAF rules

When you create a WAF policy, by default it is in Detection mode. In Detection mode, WAF doesn't block any requests. Instead, the matching WAF rules are logged in the WAF logs. To see WAF in action, you can change the mode settings to Prevention. In Prevention mode, matching rules defined in the CRS Ruleset you selected are blocked and/or logged in the WAF logs.

Custom rules

Step 5: To create a custom rule, select Add custom rule under the Custom rules tab. This opens the custom rule configuration page.



Step 6: To create a geo-filtering custom rule in the Azure portal, simply select Geo location as the

Match Type, and then select the country/region or countries/regions you want to allow/block from your application.

Step 7: Select Add Custom rule

Step 8: Select Geo location

Create your Custom Rule with an appropriate name and priority, then choose 'Geo location' from the Match type drop down as above. Next, you'll want to ensure you choose RemoteAddr as the match variable, and decide what logic you want to apply. By logic I mean the pattern that will fire the rule. In this example, I want all traffic except Ireland blocked. So I will choose the Operation 'Is not', then location Ireland, then Deny. If I wanted all traffic allowed and Ireland blocked, I would simply choose the Operation 'Is'. I recommend figuring out your pattern then working your way through the final section of the CR.

Step 9: Set Match variable to Canada, choose IS NOT, Choose country Canada, and finally Then: Deny traffic.

Stage 3: Create a custom WAF Geo location rule that allows traffic from Canada

Step 10: Repeat steps 5 to 9 but instead use:
Operation: IS
Country/Region: Canada
Then: Allow traffic


Step 11: Finish the creation of the policy. Click Review+Create


Reference:

<https://learn.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-drs>

<https://wedoazure.ie/2021/08/09/how-to-enable-web-application-firewall-geomatch-custom-rules/>

<https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/create-waf-policy-ag>

 **occupatissimo** Highly Voted 8 months, 2 weeks ago
one rule blocking all that isn't from canada is enough
upvoted 11 times

 **Lazylinux** Most Recent 2 months, 3 weeks ago
Key point here in Custom rule under WAF policy intended for App gateway not Front Door is to ensure Match type is Geo location > Match variable is remote addr > Operation IS NOT selected > country/region should be Canada > THEN should be set to DENY TRAFFIC
upvoted 2 times

店铺: IT认证考试服务

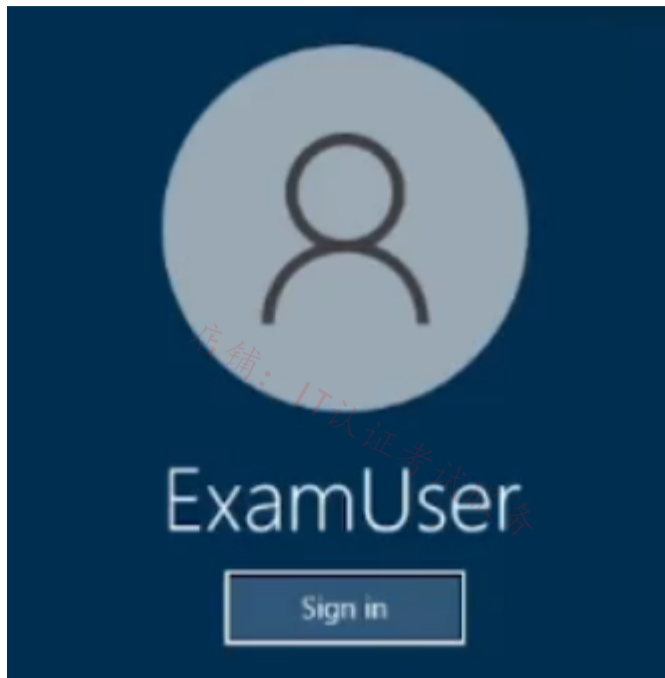
店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You plan to deploy several virtual machines to subnet1-2.

You need to prevent all Azure hosts outside of subnet1-2 from connecting to TCP port 5585 on hosts on subnet1-2. The solution must minimize administrative effort.

To complete this task, sign in to the Azure portal.

Correct Answer:

You can use a network security group to filter inbound and outbound network traffic to and from Azure resources in an Azure virtual network.

Plan

Stage 1: Create a network security group

Stage 2: Associate network security group to subnet

Stage 3: Create security rule

Stage 1: Create a network security group

A network security group (NSG) secures network traffic in your virtual network.

Step 1: From the Azure portal menu, select + Create a resource > Networking > Network security group, or search for Network security group in the portal search box.

Step 2: Select Create.

Step 3: On the Basics tab of Create network security group, enter or select this information:

Details omitted

Step 4: Select the Review + create tab, or select the blue Review + create button at the bottom of the page.

Step 5: Select Create.

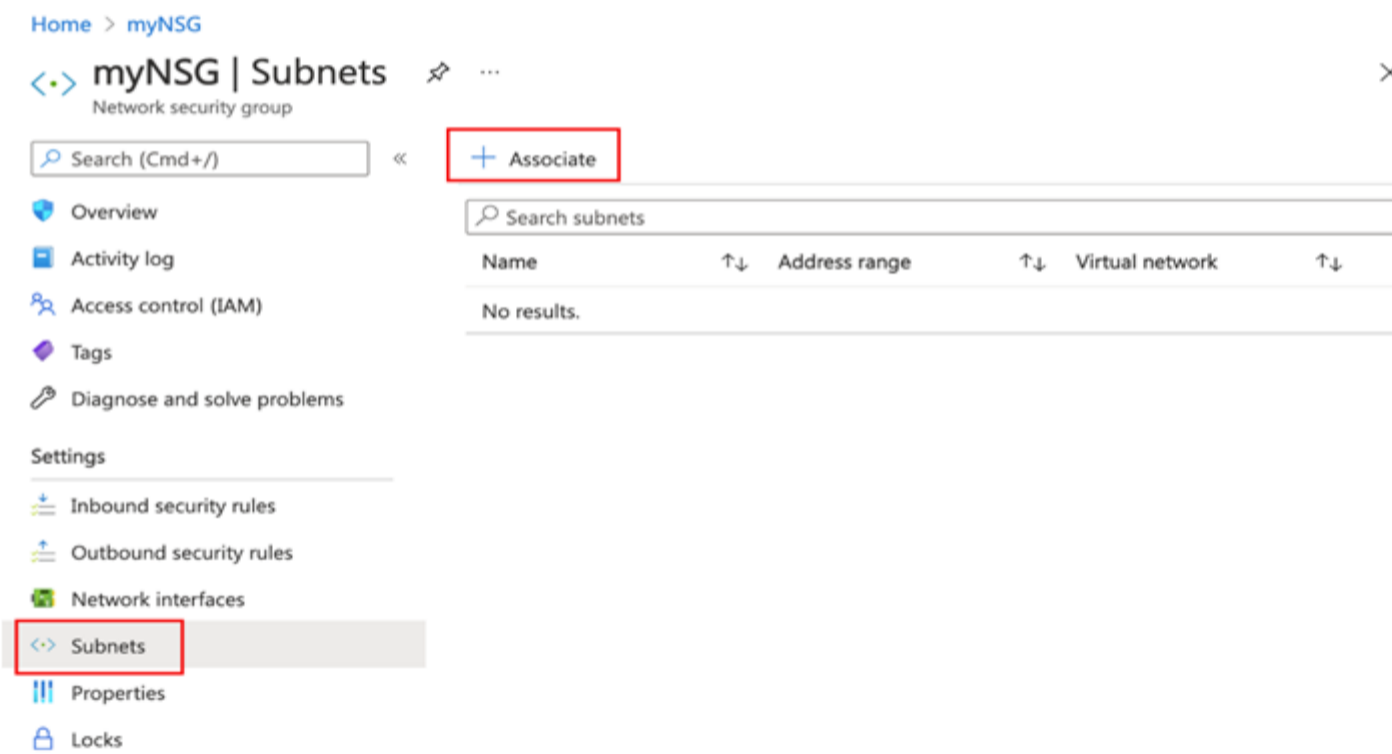
Stage 2: Associate network security group to subnet

In this section, you'll associate the network security group with the subnet of the virtual network you created earlier.

Step 6: Search for myNSG (the name you give in stage 1) in the portal search box.

Step 7: Select Subnets from the Settings section of myNSG.

Step 8: In the Subnets page, select + Associate:



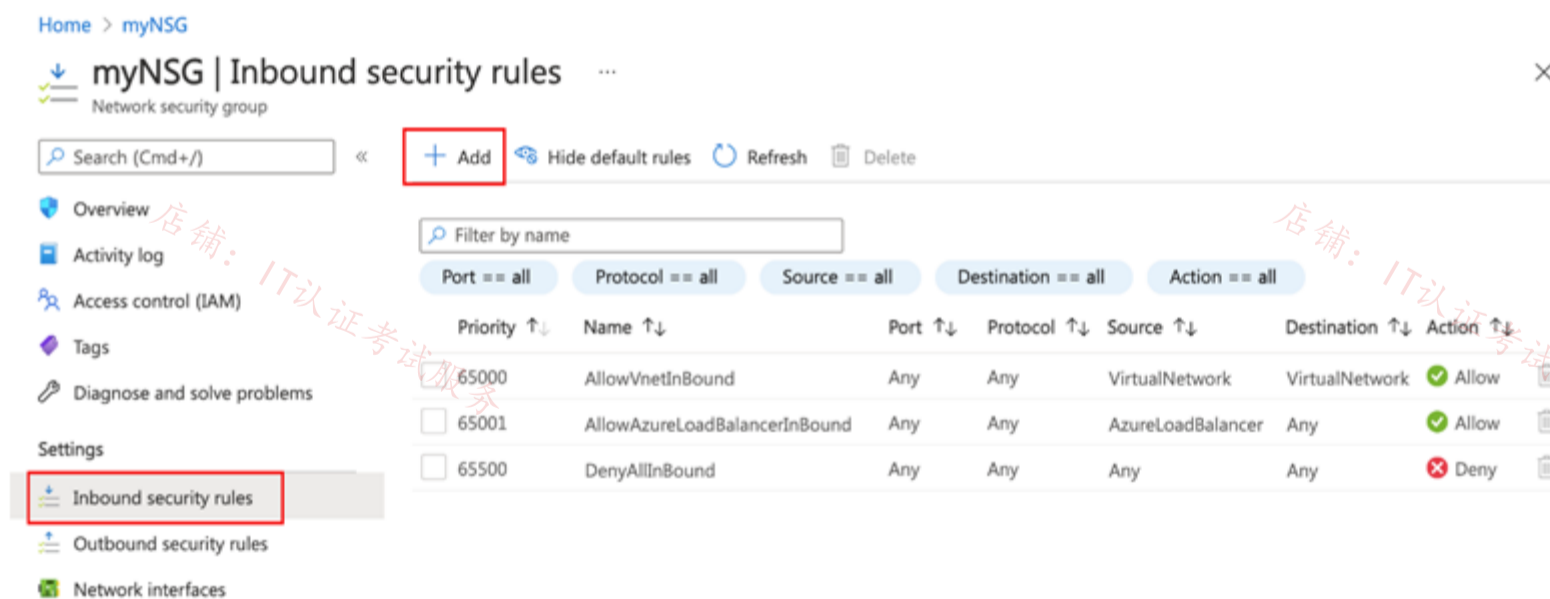
Step 9: Under Associate subnet, select myVNet (the virtual network that is available) for Virtual network.

Step 10: Select subnet1-2 for Subnet, and then select OK.

Stage 3: Create security rule

Step 11: Select Inbound security rules from the Settings section of myNSG.

Step 12: In Inbound security rules page, select + Add:



Step 13: Create a security rule that blocks TCP port 5585 to the network security group you created earlier. In Add inbound security rule page, enter or select this information:
(You need to prevent all Azure hosts outside of subnet1-2 from connecting to TCP port 5585 on hosts on subnet1-2.)

Source: Leave the default of Any.

Source port ranges: Leave the default of (*).

Destination: Select Network security group.

Destination Network security groups: Select the network security group you created earlier.

Service: Leave the default of Custom.

Destination port ranges: Enter 5585

Protocol: Select TCP.
Action: Deny
Priority Leave the default of 100.
Name: Enter something

Add inbound security rule ✕

myNSG

Source [ⓘ]
Any

Source port ranges * [ⓘ]
*

Destination [ⓘ]
Application security group

Destination application security group * [ⓘ]
myAsgWebServers

Service [ⓘ]
Custom

Destination port ranges * [ⓘ]
80,443

Protocol
 Any
 TCP
 UDP
 ICMP

Action
 Allow
 Deny

Priority * [ⓘ]
100

Name *
Allow-Web-All

Description

Step 14: Select Add.

Reference:

<https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic>

ABIYGK Highly Voted 7 months, 4 weeks ago

The lab is about creating NSG only, The NSG needs to deny traffic on port 5585 to the Subnet1-2. The image is not correct. Create an NSG with deny inbound traffic on port 5585 and associate the NSG with Subnet1-2.

Step 1: Create NSG

Upper left side of the portal Search for Network Security Group

Put > Subscription > Resource Group > Name > Region

Tags

Review+Create

Step 2: Add Inbound Security

Source > Any

Port Range > *

Destination > IP address

Destination IP address/CIDR Range > Range of Subnet1-2

Service > Custom

Destination Port Range > 5585

Protocol > Any

Action > Deny

Priority > 100


Name > DenyAnyCustom8080Inbound

Add

Step 3: Associate the NSG with the subnet
Go to Virtual Network
Select the Subnet1-2
On NSG section > select the proper name of the NSG that you create earlier
Save
upvoted 9 times

 **trashbox** 3 months ago

Allow TCP 5585 access from the specified Subnet's IP address range with a priority of 100 NSG. Then deny TCP 5585 access from Any with an NSG of priority 200.
upvoted 4 times


 **volto** 3 months, 1 week ago

You need 2 rules, also allowing traffic inside the vnet, as @mabalon wrote.
upvoted 1 times

 **Lazylinux** Most Recent 2 months, 3 weeks ago

Based on this
<https://learn.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works>

you need 2 inbound NSG security rules 1- Allow intra-subnet communication priority 110 and other is DENY as per requirement and priority 130 as example but must be of higher number than the allow and hence processed after
upvoted 1 times

 **njana94** 3 months ago


You have to create 2 inbound policies.
Priority 100: Allow subnet1-2 to subnet1-2 on port 5585
Priority 200: Deny Any to subnet1-2 on port 5585

or
a single deny policy (any to subnet1-2, port 5585) at priority 65200
upvoted 2 times

 **mabalon** 5 months ago

I think that also we need to add a rule for allow the traffic from the subnet. If we only create the DENY Rule all the traffic will be blocked, also the intra-subnet traffic.

<https://learn.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works#intra-subnet-traffic>
upvoted 4 times

 **ABIYGK** 7 months, 4 weeks ago

The lab is about creating NSG only, The NSG needs to deny traffic on port 5585 to the Subnet1-2. The image is not correct. Create an NSG with deny inbound traffic on port 5585 and associate the NSG with Subnet1-2.

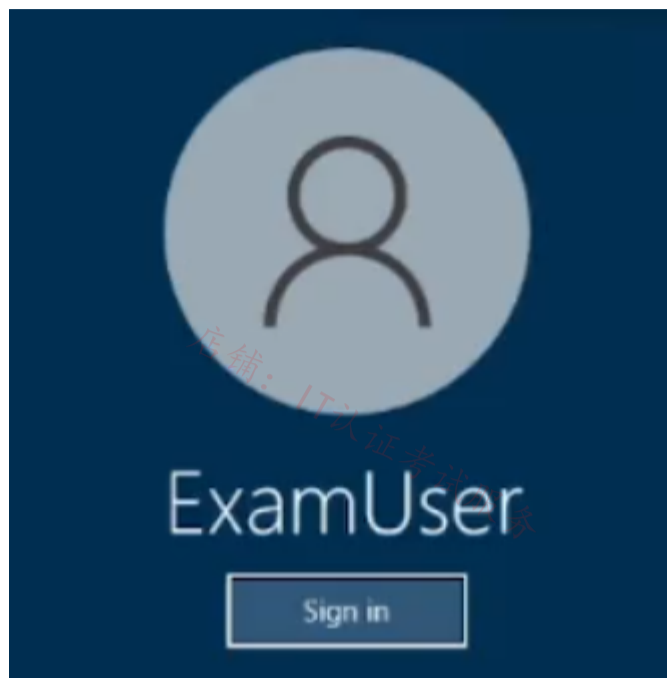
Step 1: Create NSG
Upper left side of the portal Search for Network Security Group
Put > Subscription > Resource Group > Name > Region
Tags
Review+Create
Step 2: Add Inbound Security
Source > Any
Port Range > *
Destination > IP address
Destination IP address/CIDR Range > Range of Subnet1-2
Service > Custom
Destination Port Range > 5585
Protocol > Any
Action > Deny
Priority > 100
Name > DenyAnyCustom8080Inbound
Add
Step 3: Associate the NSG with the subnet
Go to Virtual Network
Select the Subnet1-2
On NSG section > select the proper name of the NSG that you create earlier
Save
upvoted 2 times

 **JohnAvlakitotis** 8 months, 1 week ago

The "Add inbound rule" image is misleading. The text above for the rule is correct.
upvoted 2 times

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You need to ensure that only hosts on VNET1 can access the storage123456789 storage account. The solution must ensure that access occurs over the Azure backbone network.

To complete this task, sign in to the Azure portal.

Use private endpoints for Azure Storage

You can use private endpoints for your Azure Storage accounts to allow clients on a virtual network (VNet) to securely access data over a Private Link. The private endpoint uses a separate IP address from the VNet address space for each storage account service. Network traffic between the clients on the VNet and the storage account traverses over the VNet and a private link on the Microsoft backbone network, eliminating exposure from the public internet.

Connect to a storage account using an Azure Private Endpoint

Create a private endpoint

Step 1: In the search box at the top of the portal, enter Storage account. Select Storage accounts in the search results.

Step 2: Locate and select the Storage Account storage123456789

Step 3: Select the Networking tab or select Next: Advanced then Next: Networking.

Correct Answer: Step 4: In the Networking tab, under Network connectivity select Disable public access and use private access.

Step 5: In Private endpoint, select + Add private endpoint.

Step 6: In Create private endpoint enter or select the following information:
Details omitted

* Virtual network: Select VNET1.

Step 7: Select OK.

Step 8: Select Review.

Step 9: Select Create.

Reference:

<https://learn.microsoft.com/en-us/azure/storage/common/storage-private-endpoints>

<https://learn.microsoft.com/en-us/azure/private-link/tutorial-private-endpoint-storage-portal>

🗨️ 👤 **Lazylinux** 2 months, 3 weeks ago

I would NORMALLY go for Service Endpoint 3 reasons

1- SP enables private IP addresses in Vnet to reach the endpoint if resource/azure service without needing public IP done via Azure backbone network

2- SP allows you to chose all Subnets in Vnet whereas Private Endpoint you are restricted to one Subnet and hence not ALL subnets in Vnet are allowed!

3- You can use SP policy to further restrict access to the Vnet in question ONLY

Of course this ONLY effective if you first DISABLED public Access at the networking option of the storage account and once that is done then by default the FW at storage level will BLOCK all traffic unless explicitly allowed via SP or Private endpoint

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

upvoted 2 times

🗨️ 👤 **Lazylinux** 2 months, 3 weeks ago

Following Further - reached words limit

HOWEVER if you are following Microsoft WAY then answer is Private Endpoint and confusingly i will be going this way in the exam based on this paragraph from MS link above

Note: Microsoft recommends use of Azure Private Link and private endpoints for secure and private access to services hosted on the Azure platform. Azure Private Link provisions a network interface into a virtual network of your choosing for Azure services such as Azure Storage or Azure SQL.

upvoted 1 times

🗨️ 👤 **cschefer** 3 months, 4 weeks ago

Can i use Storage Account Firewall to permit access only to VNET1?

upvoted 1 times

🗨️ 👤 **jakubklapka** 4 months ago

I got this one today, Service Endpoint would be sufficient as others mentioned. But in my exam I've actually created Private Endpoint into VNET1 as part of previous task (all lab tasks are in one environment.) and also, I had peering from VNET1 to some others as part of different task.

So in my case, Service Endpoint won't do it, because other vnets could access the storage via peering and private endpoint. In this setup, it would need intricate setup of NSGs and Private Endpoint policies. At the end, I figured, that MS just didn't think through that combination (as other tasks were quite easy) and I've created Service Endpoint.

upvoted 1 times

🗨️ 👤 **IE17** 4 months ago

Please correct me if I am wrong, the provided answer here is correct which was creating private endpoint to storage acct. Thanks

upvoted 1 times

🗨️ 👤 **IE17** 4 months ago

i mean inside the storage creation
upvoted 1 times

🗨️ **magnem66** 4 months, 3 weeks ago

Wouldn't you need to use a Service Endpoint as Private Endpoints are applied to a subnet.
upvoted 2 times

🗨️ **aBAN** 7 months ago

The question says 'only hosts on VNET1' -> private endpoint.
with service endpoint storage can be accessed access over the internet.
upvoted 2 times

🗨️ **Lazylinux** 2 months, 3 weeks ago

Totally INCORRECT - please read before you write so u can understanding what you writing!!

Virtual Network (VNet) service endpoint provides secure and direct connectivity to Azure services over an optimized route over the Azure backbone network. Endpoints allow you to secure your critical Azure service resources to only your virtual networks. Service Endpoints enables private IP addresses in the VNet to reach the endpoint of an Azure service without needing a public IP address on the VNet.

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

upvoted 1 times

🗨️ **ubdubdoo** 7 months ago

private endpoints seem correct: <https://learn.microsoft.com/en-us/azure/storage/common/storage-private-endpoints>
upvoted 1 times

🗨️ **MrIMG** 9 months, 1 week ago

You can also use Service Endpoints:

<https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?toc=%2Fazure%2Fvirtual-network%2Ftoc.json&tabs=azure-portal#grant-access-from-a-virtual-network>

+

You need Service Endpoints Policies:

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoint-policies-overview>

upvoted 4 times

🗨️ **Ben_88** 7 months, 2 weeks ago

The only condition is that the traffic stays in the backbone (not specifically in the vnet) so yeah service endpoint fits too
upvoted 2 times

🗨️ **JohnAvlakitotis** 8 months, 1 week ago

This should be the only solution as it states that the access should happen over the Azure backbone. Service Endpoint is the correct option.
upvoted 2 times

🗨️ **CristianM99** 6 months ago

Actually Private endpoints traffic also is in the azure backbone. The difference is the interface created in the VNET to receive the traffic. So I think both services endpoints and private endpoints are correct answers

upvoted 1 times

HOTSPOT

-

You have an Azure virtual network named Vnet1 that contains two subnets named Subnet1 and Subnet2. Both subnets contain virtual machines.

You create a NAT gateway named NATgateway1 as shown in the following exhibit.

Create network address translation (NAT) gateway ...

 Validation passed

Basics Outbound IP Subnet Tags Review + create

Basics

Subscription	Subscription1
Resource group	RG1
Name	NATgateway1
Region	North Europe
Availability zone	-
Idle timeout (minutes)	4

Outbound IP

Public IP address	None
Public IP prefix	(New) NATgateway1-prefix (28)

Subnets

Virtual network	Vnet1
Subnets	None

Tags

None

[Create](#)

[< Previous](#)

[Next >](#)

[Download a template for automation](#)

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

NATgateway1 can be linked to [answer choice].

only GatewaySubnet
only Subnet1 or Subnet2
both Subnet1 and Subnet2
only Vnet1

NATgateway1 is assigned [answer choice].

0 IP addresses
1 IP addresses
2 IP addresses
16 IP addresses
28 IP addresses

店铺: IT认证考试服务

店铺: IT认证考试服务

Answer Area

NATgateway1 can be linked to [answer choice].

only GatewaySubnet
only Subnet1 or Subnet2
both Subnet1 and Subnet2
only Vnet1

Correct Answer:

NATgateway1 is assigned [answer choice].

0 IP addresses
1 IP addresses
2 IP addresses
16 IP addresses
28 IP addresses

MrBlueSky Highly Voted 9 months, 3 weeks ago

NAT Gateway can be associated to multiple subnets as long as they are in the same VNET.

The (28) indicates that the public IP prefix is a /28, which allows 16 IP addresses.

Correct answer
upvoted 5 times

Lazylinux Most Recent 2 months, 3 weeks ago

Answer is correct - both subnets and 16 addresses as it is 2 to power of 4,

Note:

NAT Gateway - can have any subnets except for the following

Subnet that contains any of the following

Basic IP or Basic Load balancer

has existing NAT Gateway

VPN Gateway subnet

upvoted 1 times.

khanda 9 months, 2 weeks ago

Answer is correct.

upvoted 3 times

ESAJRR 9 months, 3 weeks ago

Same Vnet add all SubNets.

SUBNET 1 2 4 8 [16] 32 64 128 256

HOST 256 128 64 32 [16] 8 4 2 1

MASK /24 /25 /26 /27 [28]/29 /30 /31 /32

upvoted 2 times

sunsetblvdfightclub 9 months, 3 weeks ago

<https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/faq#can-nat-gateway-be-attached-to-multiple-subnets>

upvoted 4 times

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT

You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains the resources shown in the following table.

Name	Type	Description
AG1	Azure Application Gateway	Will automatically scale up to three instances
VMSS1	Virtual machine scale set	Consists of four virtual machines that run an app named App1

You need to publish App1 by using AG1 and a URL of https://app1.contoso.com. The solution must meet the following requirements:

- TLS connections must terminate on AG1.
- Minimize the number of targets in the backend pool of AG1.
- Minimize the number of deployed copies of the SSL certificate of App1.

How many locations should you import to the certificate, and how many targets should you add to the backend pool of AG1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Certificates:

▼

1

2

3

4

5

Backend pool targets:

▼

1

2

3

4

Answer Area

Certificates:

▼

1

2

3

4

5

Correct Answer:

Backend pool targets:

▼

1

2

3

4

 **seth_saurabh84** Highly Voted 9 months, 4 weeks ago

why not 1 and 1? VMSS itself can be a backend target and not the 4 VM's making the VMSS.
Certificate can come from Key Vault.

upvoted 28 times

 **_fvt** 9 months, 3 weeks ago


Agrees

upvoted 6 times

  **Tasli6** 7 months ago

The question doesn't mention a Key Vault. That's why the certificate needs to be installed on the individual VMs.

upvoted 3 times

  **daemon101** 6 months, 1 week ago

it did not mention the traffic should apply end-to-end encryption. so you only need one certificate and upload it to the listener.

upvoted 7 times

  **crypto700** Highly Voted  9 months, 1 week ago

correct answer 1 & 1

upvoted 10 times

  **rishabr019** Most Recent  2 weeks, 2 days ago

Correct answer is 1-1

upvoted 1 times

  **Lazylinux** 2 months, 2 weeks ago

Yep 1 and 1

1- VMSS is eligible to be a backend pool target

1- Key vault for cert management and provisioning - Remember App GWY V1 is NOT key vault integrated

Also need to configure SSL profile and associate with listener and hence https/TLS connections are terminated at App GWY and not app services

upvoted 2 times

  **cloudselflearner** 9 months, 2 weeks ago

Correct answer 1-1

upvoted 7 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT

-

You have an Azure subscription that contains a virtual network named Vnet1. Vnet1 has a /24 IPv4 address space.

You need to subdivide Vnet1. The solution must maximize the number of usable subnets.

What is the maximum number of IPv4 subnets you can create, and how many usable IP addresses will be available per subnet? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Usable IP addresses:

IPv4 subnets:

Answer Area

Correct Answer:

Usable IP addresses:

IPv4 subnets:

 **Himank20** Highly Voted 9 months ago

Correct.

Using a /24 will give us 256 IPs. Now, In azure we can create a minimum subnet of /29 which gives us 8 IPs per subnet. Dividing 256/8 we get 32 thus we can have 32 IPv4 subnets. Out of each these subnets 5 IP from them will be used by azure so number of usable IP in each subnet is 3.

upvoted 14 times

 **Lazylinux** Highly Voted 6 months ago

Yes Answer is correct it is 3 IPs and 32 Subnets as smallest subnet in Azure is /29 dues to 5 reserved IPs out of any subnet and largest is /2 - example here from MS

Are there any restrictions on using IP addresses within these subnets?

Yes. Azure reserves the first four and last IP address for a total of 5 IP addresses within each subnet.

For example, the IP address range of 192.168.1.0/24 has the following reserved addresses:

192.168.1.0 : Network address

192.168.1.1 : Reserved by Azure for the default gateway

192.168.1.2, 192.168.1.3 : Reserved by Azure to map the Azure DNS IPs to the VNet space

192.168.1.255 : Network broadcast address.

upvoted 5 times

 **bakamon** Most Recent 7 months, 4 weeks ago

Answer :

3

32

sidhi baat no bakwas

upvoted 3 times

 **[Removed]** 9 months ago



This was on 24/04/2023

upvoted 2 times

  **twaller78** 9 months, 2 weeks ago

Correct. /24 gives you 256 ip addresses. Divide that by 32 is 8. Take off 5 ip addresses that azure reserves gives 3 usable ip`s


upvoted 2 times

  **khanda** 9 months, 2 weeks ago

Answer is correct.


Azure can allow a minimum mask of /29, which gives you 6 usable IP's and Azure reserves the first 3 which leaves you with 3 IP's. You can have 32 /29 from a /24. This does require some networking subnetting skill. Hop on to --> <https://www.freecodecamp.org/news/subnet-cheat-sheet-24-subnet-mask-30-26-27-29-and-other-ip-address-cidr-network-references/>

upvoted 3 times

  **Lapiduse** 9 months, 3 weeks ago



Correct!

upvoted 1 times

  **seth_saurabh84** 9 months, 4 weeks ago

Can someone explain the logic of the answer here?

upvoted 1 times

  **Lapiduse** 9 months, 3 weeks ago

Azure Reserves 3 addresses for itself.

The first and last are the network address and the broadcast

Total 5 addresses. Hence the minimum mask /29. Amount of a Class C 32

upvoted 2 times

  **_fvt** 9 months, 3 weeks ago

a VNet with a /24 ip space can be splitted to multiple /29 subnets.

So it's 32 /29 subnets for a /24 VNet.

/29 have 6 Hosts IP Free, but Azure reserve the 4 first IP addresses so you have only 2 usable Addresses. That's also why you cannot split to /30 subnets (not enough IP addresses per subnet for Azure).

So the answer is 32 and 2. (<https://jodies.de/ipcalc?host=192.168.0.1&mask1=24&mask2=29>)

upvoted 1 times

  **_fvt** 9 months, 3 weeks ago

Sorry Azure reserves only firsts 3 IP Addresses (5 if you count the Network and Broadcast IP) (<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-faq>)

So the answer is well 32 and 30

upvoted 1 times

  **_fvt** 9 months, 3 weeks ago

32 and 3

upvoted 3 times

店铺: IT认证考试服务

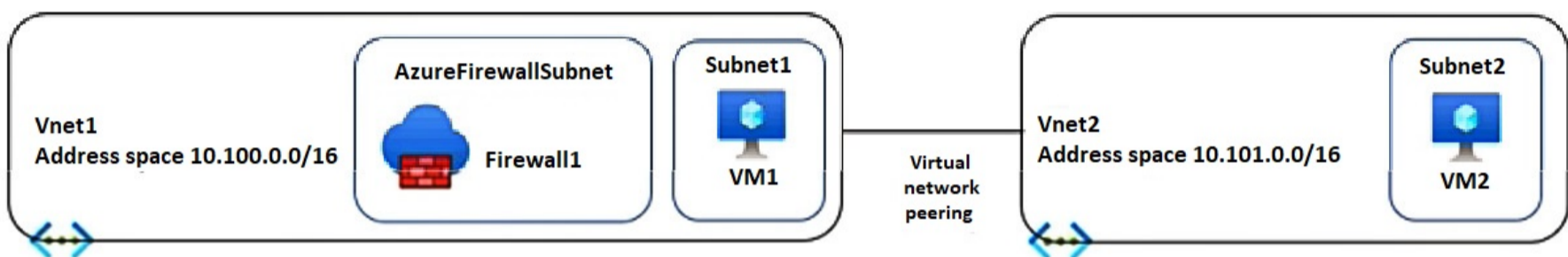
店铺: IT认证考试服务

HOTSPOT

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

Name	Type
Vnet1	Virtual network
Vnet2	Virtual network
Firewall1	Azure Firewall
Subnet1	Virtual subnet
Subnet2	Virtual subnet
VM1	Virtual machine
VM2	Virtual machine

The virtual network topology is shown in the following exhibit.



Firewall1 is configured as shown in following exhibit.

The screenshot shows the configuration page for Firewall1 in the Azure portal. It includes a header with the resource name and type, and a list of properties under the 'Essentials' section.

Property	Value
Resource group	RG1
Location	North Europe
Subscription	Subscription1
Subscription ID	169d1bba-ba4c-471c-b513-092eb7063265
Virtual network	Vnet1
Firewall policy	FirewallPolicy1
Provisioning state	Succeeded
Tags	Click here to add tags
Firewall sku	Standard
Firewall subnet	AzureFirewallSubnet
Firewall public IP	Firewall1-IP1
Firewall private IP	10.100.253.4
Management subnet	-
Management public IP	-
Private IP Ranges	Managed by Firewall Policy

FirewallPolicy1 contains the following rules:

- Allow outbound traffic from Vnet1 and Vnet2 to the internet.

- Allow any traffic between Vnet1 and Vnet2.

No custom private endpoints, service endpoints, routing tables, or network security groups (NSGs) were created.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area	Statements	Yes	No
	A routing table must be associated with Subnet1 and Subnet2 to ensure that all internet traffic for VM1 and VM2 is sent via Firewall1.	<input type="radio"/>	<input type="radio"/>
	The enable remote gateway setting must be enabled on the virtual net peering to provide VM2 Internet access by using Firewall1.	<input type="radio"/>	<input type="radio"/>
	Firewall1 can be configured to limit access to websites by categories.	<input type="radio"/>	<input type="radio"/>

Answer Area	Statements	Yes	No
Correct Answer:	A routing table must be associated with Subnet1 and Subnet2 to ensure that all internet traffic for VM1 and VM2 is sent via Firewall1.	<input type="radio"/>	<input checked="" type="radio"/>
	The enable remote gateway setting must be enabled on the virtual net peering to provide VM2 Internet access by using Firewall1.	<input checked="" type="radio"/>	<input type="radio"/>
	Firewall1 can be configured to limit access to websites by categories.	<input checked="" type="radio"/>	<input type="radio"/>

_fvt Highly Voted 9 months, 3 weeks ago

Should be YNY

Y - You need to add User Defined Route to the Firewall Appliance from the subnets (<https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal>)

N - The firewall is not a VPN Gateway, and we do not have any connection with On-Premises here (<https://learn.microsoft.com/en-us/answers/questions/516530/how-to-set-up-a-multi-spoke-virtual-network-in-azu>)

Y - Azure Firewall can filter by web categories (<https://learn.microsoft.com/en-us/azure/firewall/web-categories>)

upvoted 37 times

KyleHodg Highly Voted 8 months ago

The Firewall SKU states standard. Wouldn't Premium be required for filtering by category? Meaning YNN?

upvoted 6 times

Azused 4 months, 3 weeks ago

To filter Web categories standard is enough.

upvoted 1 times

Apptech 7 months, 2 weeks ago

Standard SKU supports category filtering. "Azure Firewall Standard is recommended for customers looking for Layer 3–Layer 7 firewall and needs autoscaling to handle peak traffic periods of up to 30 Gbps. It supports enterprise features like threat intelligence, DNS proxy, custom DNS, and web categories." <https://learn.microsoft.com/en-us/azure/firewall/choose-firewall-sku>

upvoted 4 times

toto74500 Most Recent 3 weeks, 4 days ago

YNY

1- Yes because the route priority for the same address prefix is

1. UDR

2. BGP

3. System-route

here the 3rd option will take place because we have a vnet peering between Vnet1 and Vnet2

so to "force" traffic between them to reach each other via FW, you need to assign UDR to both subnets.

2- No because FW is an NVA not a VNG

3- yes Azure Firewall standard can handle web content filtering

upvoted 1 times

GBAU 3 months ago

YNY

1:

SN1 required RT to change 0.0.0.0/0 to Virtual Appliance of FW otherwise it will go out the Wire Service.

SN2 required RT to change 0.0.0.0/0 to point to Firewall somehow otherwise it will also go out its wire service. Not sure if this would be a Virtual

Appliance or Internal IP route without trying it.

2: N: Route table in 1 will get it to the Firewall interface, otherwise it doesn't know it exists and will go out the wire service of its own subnet.

3: Seems so, Standard can do web site category filtering. = Y

700 is all we need right?

upvoted 1 times

🗨️ **ConanBarb** 3 months, 3 weeks ago

NNY

1. No, not a routing table, but a UDR would be needed (at least for VM2)
2. No, that wont help for that. Again a UDR
3. Yes. <https://learn.microsoft.com/en-us/azure/firewall/choose-firewall-sku>

upvoted 1 times

🗨️ **volto** 3 months, 1 week ago

You need a Routing Table or Azure Route Server to add UDR.

upvoted 2 times

🗨️ **Lazylinux** 6 months ago

YNY

- 1- Y - because - routing table is required- You need to create routing table, add a router - next hop type select VNA and put the firewall local ip - in this case the private IP
- 2- N Because there is no VPN GWY but alos you need one vNET2 to tick use REMOTE GWY and one vNET1 tick allow GWY Transit
- 3- YES as per this link <https://learn.microsoft.com/en-us/azure/firewall/choose-firewall-sku> check the table at bottom

upvoted 3 times

🗨️ **TheBigMan** 7 months, 4 weeks ago

Think it should be NNN

- 1) Question is about gateway nor UDR
- 3) Firewall is standard, only premium has categories

upvoted 1 times

🗨️ **makkelijkzat** 6 months, 3 weeks ago

3) Standard has categories

<https://learn.microsoft.com/en-us/azure/firewall/choose-firewall-sku>

upvoted 2 times

🗨️ **daemon101** 6 months, 2 weeks ago

The support for Web Categories with standard SKU must be implemented recently. It used to be only with Premium SKU. Anyway, thank you for the reference.

upvoted 1 times

🗨️ **occupatissimo** 8 months ago

question ask for a routing table, not for a udr, be awareNNY

upvoted 3 times

🗨️ **khanda** 9 months, 2 weeks ago

Answer should be YNY, see @_fvt comment.

upvoted 2 times

🗨️ **ckyap** 9 months, 2 weeks ago

YNN -

Yes - routing table is required- Create a routing table, add a router - next hop type select Virtual Appliance and put the firewall1 local ip (<https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal#create-a-default-route>)

No - Vnet1 and Vnet2 is not used for Virtual network gateway or route server, the remote gateway setting will be greyed out if you try to configure the settings in the Peering.

No - Network rule is prioritised before application rules thus application rules like website blocking will not be enforced(<https://learn.microsoft.com/en-us/training/modules/design-implement-network-security-monitoring/6-azure-firewall#:~:text=Outbound%20connectivity%20using%20network%20rules%20and%20application%20rules>)

upvoted 1 times

🗨️ **Tasli6** 7 months ago

But in the question it says "Firewall1 can be configured to limit access to websites by categories." Technically it can be by removing the network rule and configuring an applicaiton rule instead.

upvoted 2 times

🗨️ **ajinkyap** 9 months, 3 weeks ago

it should be YNY

upvoted 3 times

HOTSPOT

-

Your company has 40 branch offices across North America and Europe.

You have an Azure subscription that contains the following virtual networks:

- Two networks in the East US Azure region
- Three networks in the West Europe Azure region

You need to implement Azure Virtual WAN. The solution must meet the following requirements:

- Each branch office in North America must have an ExpressRoute circuit and a Site-to-Site VPN that connects to the East US region.
- Each branch office in Europe must have an ExpressRoute circuit and a Site-to-Site VPN that connects to the West Europe region.
- Transitive connections must be supported between all the branch offices and all the virtual networks.
- Costs must be minimized.

What is the minimum number of Virtual WAN resources required? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Virtual WAN:

One Basic virtual WAN
One Standard virtual WAN
Two Basic virtual WANs
Two Standard virtual WANs

Virtual WAN hub:

One virtual WAN hub
Two virtual WAN hubs
Four virtual WAN hubs
Five virtual WAN hubs

Virtual network gateway:

One virtual network gateway
Two virtual network gateways
Four virtual network gateways
Five virtual network gateways

Correct Answer:

Virtual WAN:

One Basic virtual WAN
One Standard virtual WAN
Two Basic virtual WANs
Two Standard virtual WANs

Virtual WAN hub:

One virtual WAN hub
Two virtual WAN hubs
Four virtual WAN hubs
Five virtual WAN hubs

Virtual network gateway:

One virtual network gateway
Two virtual network gateways
Four virtual network gateways
Five virtual network gateways

MrBlueSky Highly Voted 9 months, 2 weeks ago

1 Standard VWAN (all hubs can be connected globally across regions with Standard VWAN)

2 VHUBS (one for each region)

4 Gateways (1 ER Gateway in US, 1 VPNGW in US + 1 ER Gateway in Europe + 1 VPNGW in Europe)

upvoted 33 times

[Removed] 9 months ago

Appreciate the proper explanation.

vHUB regional based

VPN and ER need separate gateways (per vHUB)

upvoted 4 times

stack120566 Highly Voted 9 months, 4 weeks ago

"When multiple hubs are enabled in a single virtual WAN, the hubs are automatically interconnected via hub-to-hub links, thus enabling global connectivity between branches and Vnets that are distributed across multiple regions."

ref: <https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-global-transit-network-architecture>

1 wan 2 hubs . 2 gateways

each gateway supporting the vpn connections to the offices

upvoted 11 times

BenyIR 9 months, 3 weeks ago

it shouldnot be 4 gateways ? since it is said that needs Express route and VPN ? I mean 2 gateways in one hub or to configure both express route and vpn one gateway is enough ?

upvoted 5 times

_fvt 9 months, 3 weeks ago

Yes I agree

upvoted 1 times

Webesciaki Most Recent 4 weeks, 1 day ago

Something is wrong in that question:

1) x1 - Standard vWan for sure

2) considering that each branch supposed to have its own ExR circuit and we don't know their locations there is a limit on it

<https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-expressroute-about#expressroute-limits-in-virtual-wan>

Maximum number of circuits in the same peering location connected to the same virtual hub = 4

Maximum number of circuits in different peering locations connected to the same virtual hub = 8

let's assume they are in diff peering locations - that would mean 5 hubs just to cover 40 branches with ExR circuits

3) then I have not clue how to count VNGs - 5 just for ExR + at least 2 for VPNs ?

upvoted 1 times

y0eri 1 week, 1 day ago

They seem to assume you have a Private WAN per region, although this is not mentioned in the question. -> <https://learn.microsoft.com/en-us/azure/virtual-wan/migrate-from-hub-spoke-topology#architecture>

upvoted 1 times

Opala79 1 month, 2 weeks ago

1 standard vwan

2 vhubs

4 gateways

<https://learn.microsoft.com/en-us/azure/virtual-wan/migrate-from-hub-spoke-topology?source=recommendations#scenario>

upvoted 1 times

Lazylinux 6 months ago

Answer is 1 STD VWAN + 2 vHUBS and 4 VPNGWY and ER GWY

1 Standard VWAN as it will cross region support and hence connect both regions

2 vHUBS - each region will require one

4 Gateways - Most people i witnessed get this one wrong even in other questions that related to VPN, one MUST know when you create ER or S2S connection, the gateway for ER and S2S are different and hence you need to create one for each - so here 1 for ER and 1 for S2S in each region so total is 4

upvoted 3 times

bakamon 8 months ago

: One standard virtual WAN


: 2 hubs

: 4 gateways


upvoted 2 times

Qunlay 9 months ago

1 Standard VWAN, 2 VHub, 5 VPNGWs
upvoted 2 times

☒  **Chief_D11** 9 months, 2 weeks ago

To meet the requirements, you need to create a minimum of 1 Virtual WAN resource, 2 Virtual WAN hubs (one in the East US region and one in the West Europe region), and 5 virtual network gateways (one for each virtual network). Each branch office will connect to the nearest Virtual WAN hub using an ExpressRoute circuit and a Site-to-Site VPN. The Virtual WAN hubs will provide transitive connectivity between all the branch offices and all the virtual networks. The virtual network gateways will be used to connect the virtual networks to the Virtual WAN hubs. This solution minimizes costs by using a single Virtual WAN resource and by connecting each branch office to the nearest Virtual WAN hub.
upvoted 4 times

☒  **khanda** 9 months, 2 weeks ago

1 Standard vWAN
2 Hubs, one for each region
4 NGWs, which is two on each region, because ER and VPN cant coexist on one gateway.
upvoted 3 times


☒  **manny72** 9 months, 3 weeks ago

1 Standard VWan - more hubs can coexist in a VWan - <https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-faq>

2 Hubs, one for each region.

2 GWs - Express Route and VPN GWs can coexist in a Standard VWan - <https://learn.microsoft.com/en-us/azure/expressroute/expressroute-howto-coexist-resource-manager>

upvoted 5 times


☒  **silvarohit** 9 months, 3 weeks ago

Standard Virtual WAN - 1

Hub - 2

VPN GW - 4

upvoted 4 times

☒  **MrBlueSky** 9 months, 3 weeks ago

It's definitely one Standard VWAN and 2 hubs.

The question is can a single VNET Gateway support both an ExpressRoute connection and a S2S connection simultaneously? While it doesn't explicitly address this, the documentation seems to suggest that they each need their own Gateway: <https://learn.microsoft.com/en-us/azure/expressroute/expressroute-howto-coexist-resource-manager>

upvoted 6 times

店铺: IT认证考试服务

店铺: IT认证考试服务

DRAG DROP

-

You have a DNS domain named contoso.com that is hosted by a third-party domain name registrar.

You have an Azure subscription.

You need to ensure that all DNS queries for the contoso.com domain are resolved by using Azure DNS.

What should you create in the registrar, and what should you create in Azure? To answer, drag the appropriate options to the correct targets. Each option 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.

NOTE: Each correct selection is worth one point.

Options

- A delegation
- A DNS subdomain
- A forwarder
- A primary DNS zone
- A private DNS zone
- A public DNS zone
- A secondary DNS zone

Answer Area

Registrar:

Azure:

Answer Area

Correct Answer:

Registrar:

Azure:

 **Lazylinux** 6 months ago

Yes answer is correct and as per below

**Create your public DNS zone.

**Retrieve a list of name servers from Azure portal of Zone.

**Delegate the domain. Go to your Domain Registrar and remove their NS and replace with Azure ones ... you MUST use all 4 NS provided by Azure and include the end period i.e. dot at end indicating end of FQDN

Verify the delegation is working by running the following command `nslookup -type=SOA yourDomainName`

You may need to wait at least 10 minutes after you complete the delegation, before you can successfully verify that it's working. It can take a while for changes to propagate through the DNS system and You don't have to specify the Azure DNS name servers. If the delegation is set up correctly, the normal DNS resolution process finds the name servers automatically.

upvoted 2 times

 **vigklk** 8 months, 2 weeks ago

is it correct?

upvoted 2 times

 **khksoma** 8 months, 2 weeks ago

Yes. Delegate, create zone and then modify NS records

upvoted 4 times

HOTSPOT

-

You have an on-premises network.

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

Name	Type	Description
Vnet1	Virtual network	None
VM1	Virtual machine	Connect to Vnet1
VM2	Virtual machine	Connect to Vnet1
SQL1	Azure SQL Database	Internet accessible

You need to implement an ExpressRoute circuit to access the resources in the subscription. The solution must ensure that the on-premises network connects to the Azure resources by using the ExpressRoute circuit.

Which type of peering should you use for each connection? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Connection to Vnet1:

▼

- Microsoft peering
- Private peering
- Public peering
- Virtual network peering

Connection to SQL1:

▼

- Microsoft peering
- Private peering
- Public peering
- Virtual network peering

Answer Area

Connection to Vnet1:

▼

- Microsoft peering
- Private peering
- Public peering
- Virtual network peering

Correct Answer:

Connection to SQL1:

▼

- Microsoft peering
- Private peering
- Public peering
- Virtual network peering

 **UR** Highly Voted 8 months, 3 weeks ago

The answer is correct!

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-circuit-peering>

upvoted 11 times

 **Lazylinux** Most Recent 6 months ago

Yep given answer is correct

upvoted 2 times

You are planning the IP addressing for the subnets in Azure virtual networks.

Which type of resource requires IP addresses in the subnets?

- A. storage account
- B. internal load balancers
- C. service endpoints
- D. virtual network peering

Correct Answer: B

Community vote distribution

B (100%)

 **trashbox** 3 months ago

Selected Answer: B

The answer is correct.
upvoted 2 times

 **sibishrewd** 7 months ago

answer is correct
upvoted 2 times

 **UR** 8 months, 3 weeks ago

The answer is correct.
B
upvoted 4 times

店铺: IT认证考试服务

店铺: IT认证考试服务

You have the on-premises networks shown in the following table.

Name	ASN	IP address space	Connection type	Description
Branch1	64551	10.50.0.0/24,10.61.0.0/16	VPN	Is an on-premises datacenter
Branch2	64551	10.50.0.0/16,10.61.0.0/16	VPN and ExpressRoute	AS Path has a prefix of 64551,64551,64551
Branch3	64551	10.50.2.0/24,10.61.0.0/16	ExpressRoute	None

You have an Azure subscription that contains an Azure virtual WAN named VWAN1 and a virtual network named VNet1. VWAN is connected to the on-premises networks and VNet1 in a full mesh topology. The virtual hub routing preference for VWAN1 is AS Path.

You need to route traffic from VNet1 to 10.61.1.5.

Which path will be used?

- A. the VPN connection to Branch1
- B. the VPN connection to Branch2
- C. the ExpressRoute connection to Branch2
- D. the ExpressRoute connection to Branch3

Correct Answer: B

Community vote distribution

0 (100%)

 **crypto700** Highly Voted 8 months, 3 weeks ago

Selected Answer: D

D- Branch3
for two reasons
1- VWAN prefers ER over VPN
2- it doesn't have BGP prepend .. Branch 2 has three AS hops so it is less preferred
upvoted 18 times

 **ronin201** Most Recent 3 months, 2 weeks ago

Pls carefully see ASN!!! ER uses standard ASN 12076 not mentioned in BGP AS
upvoted 1 times

 **CiscoTerminator** 5 months, 2 weeks ago

Answer is expressroute and not because of the answers I see below but this:

AS Path

Prefer routes with the shortest BGP AS-Path length irrespective of the source of the route advertisements. For example, whether the routes are learned from on-premises connected via S2S VPN or ER.

Prefer routes from connections local to the virtual hub over routes learned from remote hub.

If there are routes from both ER and S2S VPN connections, then see below. Else proceed to the next rule.

If all the routes are local to the virtual hub, then choose routes from ER connections.

If all the routes are through remote virtual hubs, then choose routes from S2S VPN connections.

hence routes local to HUB, choose ER over S2S.

upvoted 1 times

 **CristianM99** 6 months ago

D
Crypto700 explanation is right.
upvoted 1 times

 **Lazylinux** 6 months ago

Selected Answer: D

D is answer
ER is preferred over VPN S2S all time and also Nothing appended to it in terms of AS

upvoted 1 times

 **roshingrg** 7 months, 3 weeks ago

B. the VPN connection to Branch2

The AS Path routing preference in the virtual hub (VWAN1) will determine the path selection. In this case, the AS Path for Branch2 includes a prefix of ExpressRoute (64551,64551,64551), indicating that traffic should be routed through the ExpressRoute connection to Branch2. However, the VPN connection to Branch2 has a more specific IP address space (10.50.0.0/16) than the ExpressRoute connection to Branch3 (10.50.2.0/24). Since the destination IP address (10.61.1.5) falls within the IP address space of the VPN connection to Branch2, the traffic will be routed through the VPN connection to Branch2.

Therefore, the correct path for routing traffic from VNet1 to 10.61.1.5 is the VPN connection to Branch2.

upvoted 2 times

 **roshingrg** 7 months, 3 weeks ago

Apologies for the confusion in my previous response. Let's reassess the routing based on the updated information:

Given the following information:

Branch1: 64551, 10.50.0.0/24, VPN

Branch2: 64551, 10.50.0.0/16, VPN, AS Path has a prefix of ExpressRoute (64551, 64551, 64551)

Branch3: 64551, 10.50.2.0/24, 10.61.0.0/16, ExpressRoute

You need to route traffic from VNet1 to 10.61.1.5.


In this case, the AS Path for Branch2 includes a prefix of ExpressRoute, indicating that traffic can be routed through the ExpressRoute connection to Branch2. However, the destination IP address (10.61.1.5) does not fall within the IP address spaces of Branch1 or Branch2.

Branch3 has an IP address space (10.61.0.0/16) that includes the destination IP address (10.61.1.5). Although Branch3 is connected via ExpressRoute and doesn't have an AS Path, the destination IP address matches its IP address space.

Therefore, the correct path for routing traffic from VNet1 to 10.61.1.5 is:


D. the ExpressRoute connection to Branch3

upvoted 3 times

 **jayrush** 3 months, 3 weeks ago

all 3 branch has the 10.61.0.0/16 range

upvoted 2 times

 **Kipper_2022** 8 months, 1 week ago

Selected Answer: D

Agree with crypto700

upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT

-

Case Study

-

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

-

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview

-

Contoso, Ltd. is a consulting company that has a main office in San Francisco and a branch office in Dallas.

Contoso recently purchased an Azure subscription and is performing its first pilot project in Azure.

Existing Environment

-

Azure Network Infrastructure

-

Contoso has an Azure Active Directory (Azure AD) tenant named contoso.com.

The Azure subscription contains the virtual networks shown in the following table.

Name	Resource group	IP address space	Location	Peered with
Vnet1	RG1	10.1.0.0/16	West US	Vnet2, Vnet3
Vnet2	RG1	172.16.0.0/16	Central US	Vnet1, Vnet3, Vnet4
Vnet3	RG2	192.168.0.0/16	Central US	Vnet1, Vnet2
Vnet4	RG2	10.10.0.0/16	West US	Vnet2
Vnet5	RG3	10.20.0.0/16	East US	None

Vnet1 contains a virtual network gateway named GW1.

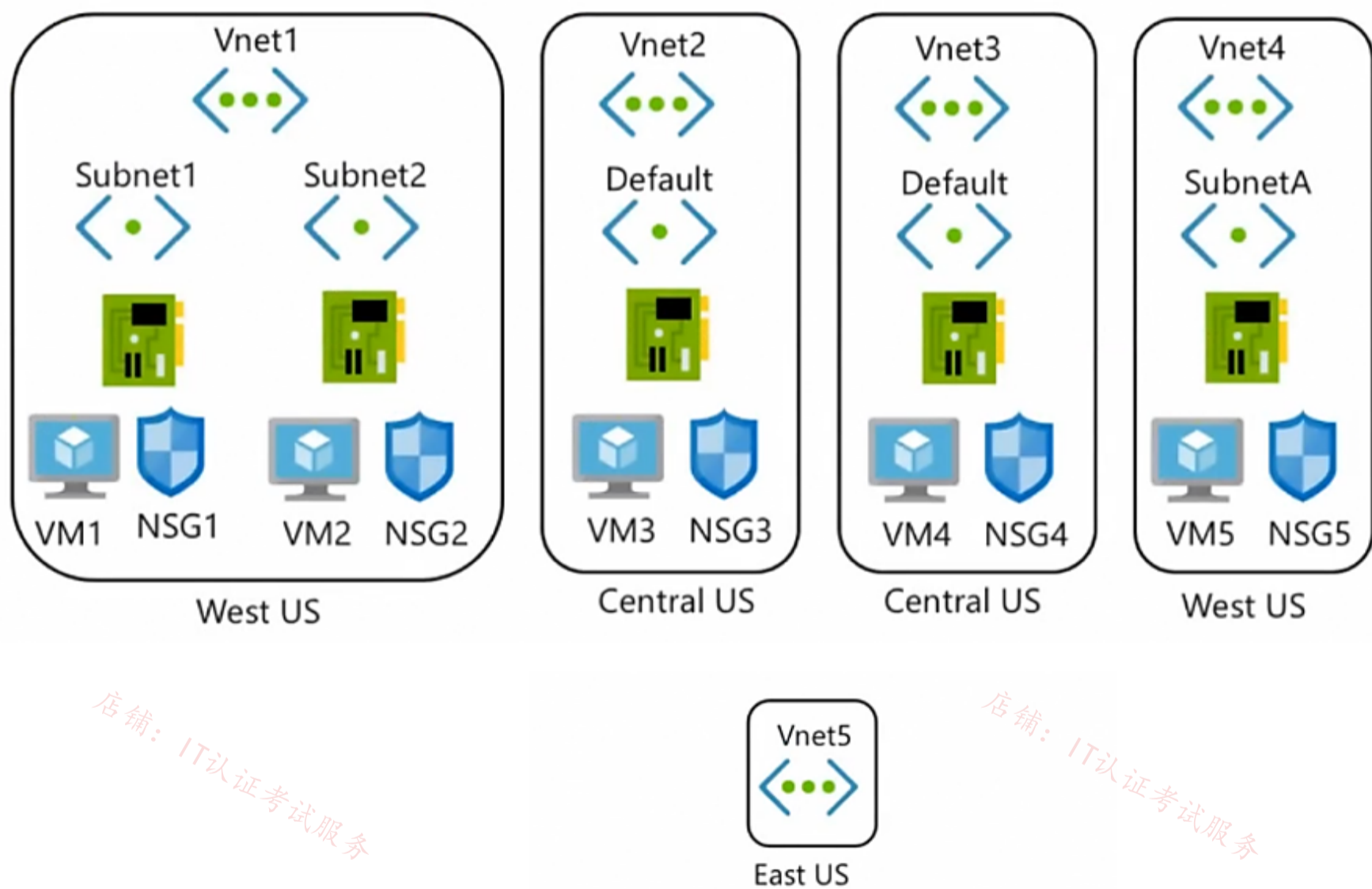
The Azure subscription contains virtual machines that run Windows Server 2019 as shown in the following table.

Name	Location	Connected to	Network security group (NSG)
VM1	West US	Vnet1/Subnet1	NSG1
VM2	West US	Vnet1/Subnet2	NSG2
VM3	Central US	Vnet2/Default	NSG3
VM4	Central US	Vnet3/Default	NSG4
VM5	West US	Vnet4/SubnetA	NSG5

The NSGs are associated to the network interfaces on the virtual machines. Each NSG has one custom security rule that allows RDP connections from the internet. The firewall on each virtual machine allows ICMP traffic.

An application security group named ASG1 is associated to the network interface of VM1.

Azure Network Infrastructure Diagram



The Azure subscription contains the Azure private DNS zones shown in the following table.

Name	Location
zone1.contoso.com	Central US
zone2.contoso.com	West US

Zone1.contoso.com has the virtual network links shown in the following table.

Name	Virtual Network	Auto registration
Link1	Vnet2	No
Link2	Vnet3	Yes

Other Azure Resources

-

The Azure subscription contains additional resources as shown in the following table.

Name	Type	Location
DB1	Azure SQL Database	West US
storage1	Azure Storage account	West US
Registry1	Azure Container Registry	Central US
KeyVault1	Azure Key Vault	Central US

Requirements

-

Virtual Network Requirements

-

Contoso has the following virtual network requirements:

- Create a virtual network named Vnet6 in West US that will contain the following resources and configurations:
 - o Two container groups that connect to Vnet6
 - o Three virtual machines that connect to Vnet6
 - o Allow VPN connections to be established to Vnet6
 - o Allow the resources in Vnet6 to access KeyVault1, DB1, and Vnet1 over the Microsoft backbone network.
- The virtual machines in Vnet4 and Vnet5 must be able to communicate over the Microsoft backbone network.
- A virtual machine named VM-Analyze will be deployed to Subnet1. VM-Analyze must inspect the outbound network traffic from Subnet2 to the internet.

Network Security Requirements

-

Contoso has the following network security requirements:

- Configure Azure Active Directory (Azure AD) authentication for Point-to-Site (P2S) VPN users.
- Enable NSG flow logs for NSG3 and NSG4.
- Create an NSG named NSG10 that will be associated to Vnet1/Subnet1 and will have the custom inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
500	3389	TCP	10.1.0.0/16	Any	Deny
1000	Any	ICMP	10.10.0.0/16	VirtualNetwork	Deny

- Create an NSG named NSG11 that will be associated to Vnet1/Subnet2 and will have the custom outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
200	3389	TCP	10.1.0.0/16	VirtualNetwork	Deny

You are implementing the virtual network requirements for Vnet6.

What is the minimum number of subnets and service endpoints you should create? To answer, select the appropriate options in the answer

area.

NOTE: Each correct selection is worth one point.

Answer Area

Subnets:

- 0
- 1
- 2
- 3
- 4

Service endpoints:

- 0
- 1
- 2
- 3
- 4

Answer Area

Correct Answer:

Subnets:

- 0
- 1
- 2
- 3
- 4

Service endpoints:

- 0
- 1
- 2
- 3
- 4

ironbornson Highly Voted 5 months, 2 weeks ago

My take is answer is correct because:

A-3 subnets for: subnet1 for the 3+1 VM, subnet2 as per requirements, GatewaySubnet for VPN

B-Two service endpoints for keyvault and DB1, VNET1 connection can use peering

upvoted 5 times

c2e9cb4 3 weeks, 3 days ago

Thinks should be 2 subnets not 3 since subnet2 is on vnet1

upvoted 1 times

bp_a_user Most Recent 4 months ago

I would say 0 service endpoints: private endpoints could be used for both, key vault and azure sql db

upvoted 1 times



rga91 5 months, 1 week ago

I think the answer should be:

A- 4 subnets. 1 Gateway Subnet, a dedicated subnet for DB1, a dedicated subnet for container instances, a default subnet for the VMs. Please check the following link to see what services need a dedicated subnet: <https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-for-azure-services#services-that-can-be-deployed-into-a-virtual-network>

B- Two service endpoints, one for keyvault and another for DB1

upvoted 3 times

  **rga91** 5 months, 1 week ago

Correction: since we are not using a vnet integration with the DB (VNET and DB are in the same region), no dedicated subnet is required for the DB. So only 3 subnets are needed.

Please check the image in the link (the example is with a storage account): <https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview>

upvoted 5 times

Question #58

Topic 2

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

You deploy several web apps and configure the apps to use private endpoints on VNet1.

You need to identify which DNS records the web apps registered automatically.

Where will the records be created?

- A. an Azure DNS zone named privatelink.azurewebsites.net
- B. an Azure Private DNS zone named azurewebsites.net
- C. an Azure Private DNS zone named privatelink.azurewebsites.net
- D. an Azure DNS zone named azurewebsites.net

Correct Answer: C

Community vote distribution

C (100%)

  **Lazylinux** 2 months, 2 weeks ago

Selected Answer: C

I C is correct :)

upvoted 1 times

  **Acaer** 4 months, 3 weeks ago

Selected Answer: C

On creating a private endpoint in portal:

Your private endpoint will be integrated with the private DNS zone 'privatelink.azurewebsites.net' in the resource group of the selected subnet. If the private DNS zone does not exist, it will be created automatically.

C. an Azure Private DNS zone named privatelink.azurewebsites.net

upvoted 2 times

HOTSPOT

You have an Azure subscription that contain a storage account named st1 in the East US Azure region.

You have the virtual networks shown in the following table.

Name	Location	IP address space
Vnet1	UK West	10.1.0.0/16
Vnet2	East US	10.2.0.0/16
Vnet3	West US	10.3.0.0/16

You have the subnets shown in the following table.

Name	Virtual network	IP address range	Subnet resources
Subnet1-1	Vnet1	10.1.1.0/24	Five virtual machines that each has one private IP address
Subnet2-1	Vnet2	10.2.1.0/25	Five virtual machines that each has one private IP address
Subnet3-1	Vnet3	10.3.1.0/26	Five virtual machines that each has one private IP address

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
You can deploy Azure Bastion to Subnet1-1.	<input type="radio"/>	<input type="radio"/>
You can deploy 100 additional virtual machines to Subnet2-1.	<input type="radio"/>	<input type="radio"/>
You can change the IP address range of Subnet3-1 to 10.3.1.0/16.	<input type="radio"/>	<input type="radio"/>

Answer Area

Statements	Yes	No
Correct Answer: You can deploy Azure Bastion to Subnet1-1.	<input type="radio"/>	<input checked="" type="radio"/>
You can deploy 100 additional virtual machines to Subnet2-1.	<input checked="" type="radio"/>	<input type="radio"/>
You can change the IP address range of Subnet3-1 to 10.3.1.0/16.	<input type="radio"/>	<input checked="" type="radio"/>

Acaer Highly Voted 4 months, 3 weeks ago

NYN

1.N

Azure Bastion requires a dedicated subnet: AzureBastionSubnet.

You must create this subnet in the same virtual network that you want to deploy Azure Bastion to.

The subnet must have the following configuration:

Subnet name must be AzureBastionSubnet.

Subnet size must be /26 or larger.

<https://learn.microsoft.com/en-us/azure/bastion/configuration-settings#subnet>

2.Y

With /25 we have more than 100 IP's left to use.

Should not be a problem to deploy 100 additional VM's with a single IP.

3.N

You can not change the IP address range of subnet3-1 range to 10.3.1.0/16.

Azure will give this error '10.3.1.0/16 is not a valid CIDR block' because its higher than the Vnet's IP address space of 10.3.0.0/16

upvoted 14 times

 **gooru** 4 months, 1 week ago

correct

upvoted 1 times

 **Lazylinux** Most Recent 2 months, 2 weeks ago


NYN

1-N as per <https://learn.microsoft.com/en-us/azure/bastion/configuration-settings>

2-Y $2^{\text{power of } 7} = 128$ take 10 away 5 reserved and 5VMS =118 hence can take 100 more

3- N 10.3.1.0/16 is INVALID CIDR

upvoted 1 times

 **Yodao** 4 months, 1 week ago

what's the correct answer?

upvoted 1 times

 **KeenOnTech** 4 months, 2 weeks ago

1. Y: AzureBastionSubnet should be /26 which falls within Subnet1-1 i.e. /24. There we can fit in AzureBastionSubnet /26 + 5x VMs /32 within Subnet1-1 /24

2. Y: 100 VMs easily fit within Subnet2-1 /25

3. Y: 10.3.1.0/16 is smaller than 10.3.0.0/16 and so can fit within VNet3.

upvoted 1 times

 **JackeD** 4 months, 1 week ago

except 2, this is wrong. 1. you can change the subnet, and readjust everything but thats not what the question is asking. 2. 10.3.1.0/16 isnt a real subnet, a /16 confines the subnet to the first two octets.

Please do not answer if you do not know, this is practice and no points are awarded.

upvoted 4 times

 **sam881989** 2 weeks, 4 days ago

You can't change the subnet address without removing the resources from it and each subnets already have 5 VM with the IPs in it.

upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

You are planning the IP addressing for the subnets in Azure virtual networks.

Which type of resource requires IP addresses in the subnets?

- A. storage account
- B. internal load balancers
- C. service endpoints
- D. service endpoint policies

Correct Answer: B

Community vote distribution

B (100%)

MCCC454 4 days, 11 hours ago

Why is this question here again and again?
upvoted 1 times

kay000001 2 months, 2 weeks ago

Awfully repetitive question...
upvoted 1 times

trashbox 3 months ago

Selected Answer: B

The answer is correct.
upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

You have the Azure virtual networks shown in the following table.

Name	Subnet	Subnet address space	Peered with
Vnet1	Subnet1-1	10.1.1.0/24	Vnet3
Vnet2	Subnet2-1	10.2.1.0/24	Vnet3
Vnet3	AzureFirewallSubnet	10.3.1.0/24	Vnet1, Vnet2

You deploy Azure Firewall to Vnet3.

You need to ensure that the traffic from Subnet1-1 to Subnet2-1 passes through the firewall.


What should you configure?

- A. peering links between Vnet1 and Vnet2
- B. a route table associated to Subnet1-1 and Subnet2-1
- C. an Azure private DNS zone
- D. a route table associated to AzureFirewallSubnet

Correct Answer: B

Community vote distribution

B (100%)

 **Lazylinux** 2 months, 2 weeks ago

Selected Answer: B

B is Honey - use RT to point to FW as next hop with CIDR 0.0.0.0/0
upvoted 1 times

 **Acaer** 4 months, 3 weeks ago

B. a route table associated to Subnet1-1 and Subnet2-1

1. You have to create a route table first
2. Next you create the route in the table like this

Route name: toFW

Destination type: IP Addresses

Destination IP addresses/CIDR ranges: 0.0.0.0/0

Next hop type: Virtual appliance

Next hop address: Firewall IP

3. Go to Subnets

Select the Vnet

Associate Subnet1-1 and Subnet2-1

upvoted 2 times

 **Acaer** 4 months, 3 weeks ago

<https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal#create-a-default-route>

upvoted 3 times

You plan to implement an Azure virtual network that will contain 10 virtual subnets. The subnets will use IPv6 addresses. Each subnet will host up to 200 load-balanced virtual machines.

You need to recommend which subnet mask size to use for the virtual subnets.

What should you recommend?

- A. /64
- B. /120
- C. /48
- D. /24

Correct Answer: D

Community vote distribution

A (80%) 10% 10%

 **kghosh4** 1 month, 1 week ago

Selected Answer: A

Definitely A
upvoted 1 times

 **Lazylinux** 2 months, 2 weeks ago

Selected Answer: A

Definitely answer is A and most people not accepting A as answer is because their mindset is still WIRED to IPv4
IPV6 /64 will take billions of hosts not such 200 vms...you have to remember /64 is IPv6 as IPv4 is max /32 hence both are totally different but same concept, read below for more info
Thus routing prefix is /64 and host portion is 64 bits. We can further subnet the network beyond 16 bits of Subnet ID, by borrowing host bits; but it is recommended that 64 bits should always be used for hosts addresses because auto-configuration requires 64 bits.
IPv6 subnetting works on the same concept as Variable Length Subnet Masking in IPv4.
/48 prefix can be allocated to an organization providing it the benefit of having up to /64 subnet prefixes, which is 65535 sub-networks, each having 264 hosts. A /64 prefix can be assigned to a point-to-point connection where there are only two hosts (or IPv6 enabled devices) on a link.
upvoted 1 times

 **c2e9cb4** 3 weeks, 3 days ago

This is wrong, a /120 can host 2^8 (256) ips
upvoted 1 times

 **c2e9cb4** 2 weeks, 5 days ago

my bad -->not accepted below /64
so response 1 /64
upvoted 1 times

 **Lazylinux** 2 months, 2 weeks ago

more info here
<https://docs.netgate.com/pfsense/en/latest/network/ipv6/subnets.html>
upvoted 1 times

 **voldemort123** 3 months, 4 weeks ago

IPv6-only Virtual Machines or Virtual Machines Scale Sets aren't supported, each NIC must include at least one IPv4 IP configuration.
<https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/ipv6-overview>

So in that case its dual-stack, the ipv4 subnet mask for 200 VMs is /24. And Ipv6 subnet mask is /64. But its not clear mask which is asked in the question... assuming it is referring to ipv6 as mentioned initially, answer will be /64
upvoted 2 times

 **MrAmaeg** 4 months ago

Selected Answer: A

"The subnets for IPv6 must be exactly /64 in size. This ensures future compatibility should you decide to enable routing of the subnet to an on-premises network since some routers can only accept /64 IPv6 routes."

<https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/ipv6-overview#capabilities>
upvoted 2 times


 **Abra_2021** 4 months, 1 week ago

Selected Answer: D

/ 24, Because of the number of host 254. from the question "Each subnet will host up to 200 load-balanced virtual machines."
upvoted 1 times

 **Lazylinux** 2 months, 2 weeks ago

Totally wrong your mindset is WIRED to IPv4, this is about IPv6, read my explanation
upvoted 1 times

 **Yodao** 4 months, 1 week ago

Selected Answer: C

Chatgpt: /48 subnet mask in IPv6 provides 65,536 subnets, each with a vast address space of 18,446,744,073,709,551,616 addresses. This is more than enough to accommodate your requirement of hosting up to 200 load-balanced virtual machines in each of the 10 virtual subnets, and it allows for future scalability and flexibility in your network design.

upvoted 1 times

 **PandaTuga** 1 month, 3 weeks ago

and this is why I don't use chatGPT ;)
upvoted 1 times

 **Acaer** 4 months, 3 weeks ago

/64

The subnets for IPv6 must be exactly /64 in size. This ensures future compatibility should you decide to enable routing of the subnet to an on-premises network since some routers can only accept /64 IPv6 routes.

<https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/ipv6-overview#capabilities>

upvoted 3 times

 **tomasek88** 4 months, 3 weeks ago

Selected Answer: A

IPv6 does NOT have /24 --> D is correct --> /64

upvoted 4 times

 **Lazylinux** 2 months, 2 weeks ago


U Mean A

upvoted 1 times

 **Bigfatdavey** 4 months, 3 weeks ago

should be /64

upvoted 2 times

 **Thulas** 4 months, 3 weeks ago

What is your explaining Bigfatdavey?

upvoted 1 times


 **ConanBarb** 3 months, 3 weeks ago

<https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/ipv6-overview#capabilities>

"Important

The subnets for IPv6 must be exactly /64 in size. This ensures future compatibility should you decide to enable routing of the subnet to an on-premises network since some routers can only accept /64 IPv6 routes."

upvoted 1 times

 **Azused** 4 months, 3 weeks ago

Could you explain ?

upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

DRAG DROP

You have two on-premises datacenters.

You have an Azure subscription that contains four virtual networks named VNet1, VNet2, VNet3, and VNet4.

You create an Azure virtual WAN named VWAN1. VWAN1 contains a single virtual hub that is connected to both on-premises datacenters and all the virtual networks in a full mesh topology.

You create a route table named RT1.

You need to configure VWAN1 to meet the following requirements:

- Connectivity between VNet1 and VNet2 and both on-premises datacenters must be allowed.
- Connectivity between VNet3 and VNet4 and both on-premises datacenters must be allowed.
- VNet1 and VNet2 must be isolated from VNet3 and VNet4.

How should you configure routing for VNet1 and VNet2 and for both on-premises datacenters? To answer, drag the appropriate route tables and route table propagation to the correct requirements. Each route table and route table propagation 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.

NOTE: Each correct selection is worth one point.

Route solutions

Associated route table: Default
Propagating to route tables: RT1 and Default

Associated route table: Default;
Propagating to route tables: RT1

Associated route table: RT1;
Propagating to route tables: Default

Associated route table: RT1;
Propagating to route tables: RT1 and Default

Answer Area

VNet1 and VNet2:

On-premises datacenters:

Answer Area

Correct Answer:

VNet1 and VNet2: Associated route table: RT1;
Propagating to route tables: Default

On-premises datacenters: Associated route table: Default
Propagating to route tables: RT1 and Default

y0eri 1 week, 1 day ago



Because you need connectivity between VNet1 and VNet2, their routes need to be propagated to their associated route table. VNet3 and VNet4 can be associated to route table Default and only propagate their routes to route table Default. This way there is full connectivity between all VNets and the on-prem data centers, between VNet1 and VNet2, between VNet3 and VNet4, but not between VNet1/2 and VNet3/4.

VNet1 and VNet2:
- Associated route table: RT1
- Propagating to route tables: RT1 and Default

On-premises datacenters:
- Associated route table: Default
- Propagating to route tables: RT1 and Default



VNet3 and VNet4:

- Associated route table: Default
 - Propagating to route tables: Default
- upvoted 2 times

  **CiscoExam** 5 days, 9 hours ago

you are propagating from VNET1 and VNET2 to Default. Then you're associating VNET3 & 4 to Default. This will make all 4 VNETs talk to each other. So, this couldn't be correct. We need another routing table RT2 to be able to execute this scenario fully. Or else, it's not possible.

upvoted 1 times

  **NSF2** 3 weeks ago

The similar scenario described in the link below, along with testing in the LAB, I can say that the answer is correct.

<https://learn.microsoft.com/en-us/azure/virtual-wan/scenario-isolate-vnets>

upvoted 1 times

  **Acaer** 4 months, 3 weeks ago

Looks correct

We can see such example here:

<https://learn.microsoft.com/en-us/azure/virtual-wan/scenario-isolate-vnets>

VNet1 + VNet2

Associated route table: RT1

Propagating to route tables: Default

On-premises

Associated route table: Default

Propagating to route tables: RT1 and Default

I was overthinking this a bit with this design

<https://learn.microsoft.com/en-us/azure/virtual-wan/scenario-isolate-vnets-custom>

but i guess VNet3 + 4 could be associated to route table Default since we isolate VNet1 + 2 from 3 + 4

upvoted 4 times

  **Webesciaki** 4 weeks, 1 day ago

IMHO its wrong

VNET1 and VNET2 supposed to talk to each other that means it is not met with given answer.

upvoted 1 times

  **Webesciaki** 4 weeks, 1 day ago

I'd go for:

VNET1 + VNET2:

associated route table: RT1

propagated route table: RT1 + default

on-Prem

associated route table Default

propagated to RT1

none of the answer covers VNET3 and VNET4 though

upvoted 1 times

  **ironbornson** 4 months ago

I guess VNET3 and VNET 4 will be in RT1 also, and because we do not propagate RT1 in RT1 no VNETs will be aware of each other. Kind of misleading question if you ask me.

From your link: "I think the question is a bit misleading. When they specify "Connection between Vnet1 and Vnet2 and on-prem" they can make you understand they want vnet1 and vnet2 to be reachable each other but with the given responses that would be impossible as per your link says: "Notice that since only branches propagate to the route table RT_VNET, those will be the only prefixes that VNets will learn, and not those of other VNets.""

upvoted 1 times

You are planning the IP addressing for the subnets in Azure virtual networks.

Which type of resource requires IP addresses in the subnets?

- A. Azure Virtual Network NAT
- B. service endpoint policies
- C. internal load balancers
- D. virtual network peering

Correct Answer: C

 **Kanoniermalri** 2 months, 3 weeks ago

This question comes up for the 4th or 5th time in this course
upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT

-

You have an Azure subscription that contains an Azure key vault named Vault1 and an app registration for an Azure AD app named App1.

You have a DNS domain named contoso.com that is hosted by a third-party DNS provider.

You plan to deploy App1 by using Azure App Service. App1 will have the following configurations:

- App1 will be hosted across five App Service apps.
- Users will access App1 by using a URL of https://app1.contoso.com.
- The user traffic of App1 will be managed by using Azure Front Door.
- The traffic between Front Door and the App Service apps will be sent by using HTTP.
- App1 will be secured by using an SSL certificate from a third-party certificate authority (CA).

You need to support the Front Door deployment.

Which two DNS records should you create, and to where should you import the SSL certificate for App1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

DNS records:

- A CNAME record and a TXT record
- An A record and a SRV record
- An A record and a CNAME record
- A TXT record and a SRV record

Import the certificate to:

- The app registration for App1
- The App Service apps
- Vault1

Answer Area

DNS records:

- A CNAME record and a TXT record
- An A record and a SRV record
- An A record and a CNAME record**
- A TXT record and a SRV record

Correct Answer:

Import the certificate to:

- The app registration for App1
- The App Service apps
- Vault1**

 **Lazylinux** 2 months, 2 weeks ago

Given answer is WRONG, i am NOT sure why no contribution from others on this point considering it is fundamentals of Azure FD

- 1- First thing to know is this is fresh install i.e. FD is NOT associated with App services
- 2- To know is that Both the FD and App services already have A records registered to them by MS and are accessible via internet
- 3- Third Party DNS provider is being utilized and NOT azure managed DNS
- 4- The domain contoso.com is already registered and has the relevant DNS records

following in next paragraph
upvoted 3 times

🗨️ 👤 **Lazylinux** 2 months, 2 weeks ago

Adding further
So based on the above and the link provided

- 1- I dont see any reason to create A record for any other the services being mentioned
- 2- Both TXT and CNAME are required in order to use custom Domain name with Azure FD
- 3- TXT is used to verify ownership of the domain, since we are suing third party DNS host/registrar and hence you must manually validate the domain by entering prompted DNS TXT records.
- 4- CNAME is used to point the custom domain to Azure FD azurefd.net. Remember the default frontend host will have a subdomain of azurefd.net when you first deploy Azure FD and associate to any Internet facing service

upvoted 4 times

🗨️ 👤 **Lazylinux** 2 months, 2 weeks ago

and hence the answer should be CNAME and TXT DNS records and second box is key vault
<https://learn.microsoft.com/en-us/azure/frontdoor/standard-premium/how-to-add-custom-domain#add-a-new-custom-domain>

<https://learn.microsoft.com/en-us/azure/frontdoor/front-door-how-to-onboard-apex-domain?pivots=front-door-standard-premium>
upvoted 9 times

🗨️ 👤 **MattM70** 2 months, 2 weeks ago

I believe the answer is:

DNS records: A CNAME and a TXT record

See link: <https://learn.microsoft.com/en-us/azure/frontdoor/standard-premium/how-to-add-custom-domain#prerequisites>

Import the certificate to:

Vault1

See link: <https://learn.microsoft.com/en-us/azure/frontdoor/standard-premium/how-to-configure-https-custom-domain?tabs=powershell#using-your-own-certificate>

upvoted 1 times

🗨️ 👤 **seedati** 2 months, 3 weeks ago

Correct

upvoted 1 times

🗨️ 👤 **Lazylinux** 2 months, 2 weeks ago

U WRONG, read my comments

upvoted 1 times

🗨️ 👤 **jorgesoma** 2 months, 2 weeks ago

Could you explain it?

upvoted 1 times

🗨️ 👤 **itsmenida1** 1 month, 1 week ago

Read Lazylinux previous comment ;)

upvoted 4 times

店铺: IT认证考试服务

店铺: IT认证考试服务

You have an Azure subscription that contains a virtual network named VNet1. VNet1 has a subnet mask of /24.

You plan to implement an Azure application gateway that will have the following configurations:

- Public endpoints: 1
- Private endpoints: 1
- Minimum instances: 1
- Maximum instances: 10

You need to configure the address space for the subnet of the application gateway. The solution must minimize the number of IP addresses allocated to the application gateway subnet.

What is the minimum number of assignable IP addresses required?

- A. 1
- B. 2
- C. 11
- D. 12
- E. 20

Correct Answer: C

Community vote distribution

C (100%)

 **OrangeSG** 2 months, 1 week ago

Selected Answer: C

Application Gateway uses one private IP address per instance, plus another private IP address if a private frontend IP is configured.

<https://learn.microsoft.com/en-us/azure/application-gateway/configuration-infrastructure#size-of-the-subnet>

upvoted 1 times

 **Lazylinux** 2 months, 2 weeks ago

Selected Answer: C

I C is correct!!

For App gateway V1 subnet of 27 is required and for V2 the recommended is 24 CIDR, however based on the current configuration i.e. whole Address space for the vnet is /24 and fact max we have is 10 App GWY instances deployed at anytime then we can assign /28 CIDR for the address space for the App GWY

this allows for 16 IP address of which 5 are reserved for Azure resources and this leaves us with 11 which is about enough for 1 Private Endpoint and 10 App GWY instances

as for the Public IP it has nothing to do with private IP unless the App GWY requires private IP in which is not the case here

upvoted 2 times

 **Discussions22** 2 months, 4 weeks ago

Why not 12?

upvoted 1 times

 **ExamTopics2_EIS** 2 months, 4 weeks ago

Max 10 + 1 Private = 11

Public is not used from that scope.. it has a public IP

upvoted 4 times

HOTSPOT

Your on-premises network contains a server named DNS1 that runs Windows Server 2022. DNS1 has the DNS server role and an IP address of 10.1.0.1. The network contains computers that use DNS1 for name resolution.

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

Name	Type	Description
private.fabrikam.com	Azure Private DNS zone	Linked to Vnet1
Vnet1	Virtual network	None
SQL1	Azure SQL Database	Has a private endpoint in Vnet1 that is registered in private.fabrikam.com
DNS2	Server that runs Windows Server 2022	Has the DNS server role and an IP address of 10.100.0.1

The on-premises network connects to Vnet1 by using a Site-to-Site VPN.

You need to ensure that the computers on the on-premises network can resolve the IP address for sql1.private.fabrikam.com.

What should you do on DNS1 and DNS2? To answer, drag the appropriate actions to the correct servers. 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.

NOTE: Each correct selection is worth one point.

Answer Area

DNS1:

- Configure forwarding to 10.1.0.1.
- Configure forwarding to 10.100.0.1.
- Configure forwarding to 168.63.129.16.
- Create a secondary zone for private.fabrikam.com.
- Create a stub zone for private.fabrikam.com.

DNS2:

- Configure forwarding to 10.1.0.1.
- Configure forwarding to 10.100.0.1.
- Configure forwarding to 168.63.129.16.
- Create a secondary zone for private.fabrikam.com.
- Create a stub zone for private.fabrikam.com.

Answer Area

Correct Answer:

DNS1:

- Configure forwarding to 10.1.0.1.
- Configure forwarding to 10.100.0.1.
- Configure forwarding to 168.63.129.16.
- Create a secondary zone for private.fabrikam.com.
- Create a stub zone for private.fabrikam.com.

DNS2:

- Configure forwarding to 10.1.0.1.
- Configure forwarding to 10.100.0.1.
- Configure forwarding to 168.63.129.16.
- Create a secondary zone for private.fabrikam.com.
- Create a stub zone for private.fabrikam.com.

🗨️ **aminiasin** 1 month, 3 weeks ago

With the options the correct solution is.
DNS1: Configure Conditional forwarding to DNS2
DNS2: Configure Conditional forwarding to 168.xx.xx.x

In Decembre 2023 is posible avoid DNS2 with a new service DNS Private Resolver.
upvoted 3 times

🗨️ **Lazylinux** 2 months, 2 weeks ago

The provided answer is INCORRECT

On-prem DNS server DNS1 should be configured have conditional forwarder to forward traffic to AZ DNS server on IP 10.100.0.1 which acts as Azure DNS forwarder

The Azure DNS server DNS2 - then forwards the DNS traffic to Azure recursive resolvers (IP 168.63.129.16) which in turn resolves the request to the on-prem client

As NOTE: As of now and onwards - MS Azure no longer uses this method for name resolution to and from on-Prem - they have service called Azure DNS private resolver with inbound-outbound Endpoints with rule in place
see link below - pay attention to the diagram

<https://learn.microsoft.com/en-us/azure/private-link/private-endpoint-dns#virtual-network-and-on-premises-workloads-using-a-dns-forwarder>

<https://learn.microsoft.com/en-us/azure/virtual-network/what-is-ip-address-168-63-129-16>

upvoted 2 times

🗨️ **Discussions22** 2 months, 3 weeks ago

What is correct if we have no?

upvoted 1 times

🗨️ **ExamTopics2_EIS** 2 months, 3 weeks ago

Clearly this is not correct. DNS2 is creating a forwarding to it's own IP address?

upvoted 1 times

🗨️ **Dungeon_Master** 2 months, 4 weeks ago

DNS1: Configure COnditional forwarding to DNS2
DNS2: Configure COnditional forwarding to 168.x.x.x

upvoted 3 times

🗨️ **jorgesoma** 2 months, 2 weeks ago

I think it's correct.

DNS1 (On-Prem): Forward to DNS2 (VM on Azure)
DNS2 (Azure): Forward to 168.x.x.x (Azure DNS)

upvoted 3 times

🗨️ **jorgesoma** 2 months, 4 weeks ago

Is it correct?

upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

DRAG DROP

-

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

Name	Type	Description
Gateway1	NAT gateway	Unconfigured
NIC1	Network interface	A network interface with a statically assigned public IP address named PIP1
PIP1	Public IP address	A Basic SKU public IP address
VNet1	Virtual network	Contains a subnet named Subnet1
Subnet1	Virtual subnet	Part of VNet1
VM1	Virtual machine	Connected to Subnet1 via NIC1

You need to associate Gateway1 with Subnet1. The solution must minimize downtime on VM1.

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.

Actions**Answer Area**

Disassociate PIP1 from NIC1.

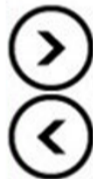
Change the PIP1 SKU to Standard.

Change Assignment to Dynamic for PIP1.

Shutdown VM1.

Start VM1.

Associate PIP1 to NIC1.

**Answer Area****Correct Answer:**

Disassociate PIP1 from NIC1.

Change the PIP1 SKU to Standard.

Associate PIP1 to NIC1.

CiscoExam 4 days, 17 hours ago

<https://learn.microsoft.com/en-us/azure/nat-gateway/tutorial-migrate-ilip-nat>
upvoted 1 times

CiscoExam 4 days, 17 hours ago

This is correct
upvoted 1 times

HOTSPOT

-

Your on-premises network contains the subnets shown in the following table.

Name	IPv4 network address
Subnet1	192.168.10.0/24
Subnet2	192.168.20.0/24

The network contains a firewall named FW1 that uses a public IP address of 131.107.100.200.

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

Name	Type	Description
VNet1	Virtual network	Uses an address space of 10.1.0.0/16
GW1	Virtual network gateway	<ul style="list-style-type: none"> Uses a public IP address of 20.231.231.174 Uses a private IP address of 10.1.255.10
GatewaySubnet	Subnet	Uses an address space of 10.1.255.0/27
LNG1	Local network gateway	None

You plan to configure a Site-to-Site (S2S) VPN named VPN1 that will connect GW1 to FW1.

You need to configure LNG1 to support VPN1. The solution must meet the following requirements:

- Ensure that the resources on Subnet1 and Subnet2 can communicate with the resources on VNet1.
- Minimize administrative effort.

How should you configure LNG1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Address space:

	▼
10.1.0.0/16	
10.1255.0/27	
192.168.10.0/23	
192.168.10.0/24 and 192.168.20.0/24	

IP address:

	▼
10.1.0.1	
10.1.255.10	
20.231231.174	
131.107.100.200	

Answer Area

Address space:

10.1.0.0/16
10.1255.0/27
192.168.10.0/23

Correct Answer:

192.168.10.0/24 and 192.168.20.0/24

IP address:

10.1.0.1
10.1.255.10
20.231231.174
131.107.100.200

 **SJHCI** 1 week, 1 day ago

Correct Answer!

upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT

-

Case Study

-

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

-

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview

-

Contoso, Ltd. is a consulting company that has a main office in San Francisco and a branch office in Dallas.

Contoso recently purchased an Azure subscription and is performing its first pilot project in Azure.

Existing Environment

-

Azure Network Infrastructure

-

Contoso has an Azure Active Directory (Azure AD) tenant named contoso.com.

The Azure subscription contains the virtual networks shown in the following table.

Name	Resource group	IP address space	Location	Peered with
Vnet1	RG1	10.1.0.0/16	West US	Vnet2, Vnet3
Vnet2	RG1	172.16.0.0/16	Central US	Vnet1, Vnet3, Vnet4
Vnet3	RG2	192.168.0.0/16	Central US	Vnet1, Vnet2
Vnet4	RG2	10.10.0.0/16	West US	Vnet2
Vnet5	RG3	10.20.0.0/16	East US	None

Vnet1 contains a virtual network gateway named GW1.

Azure Virtual Machines

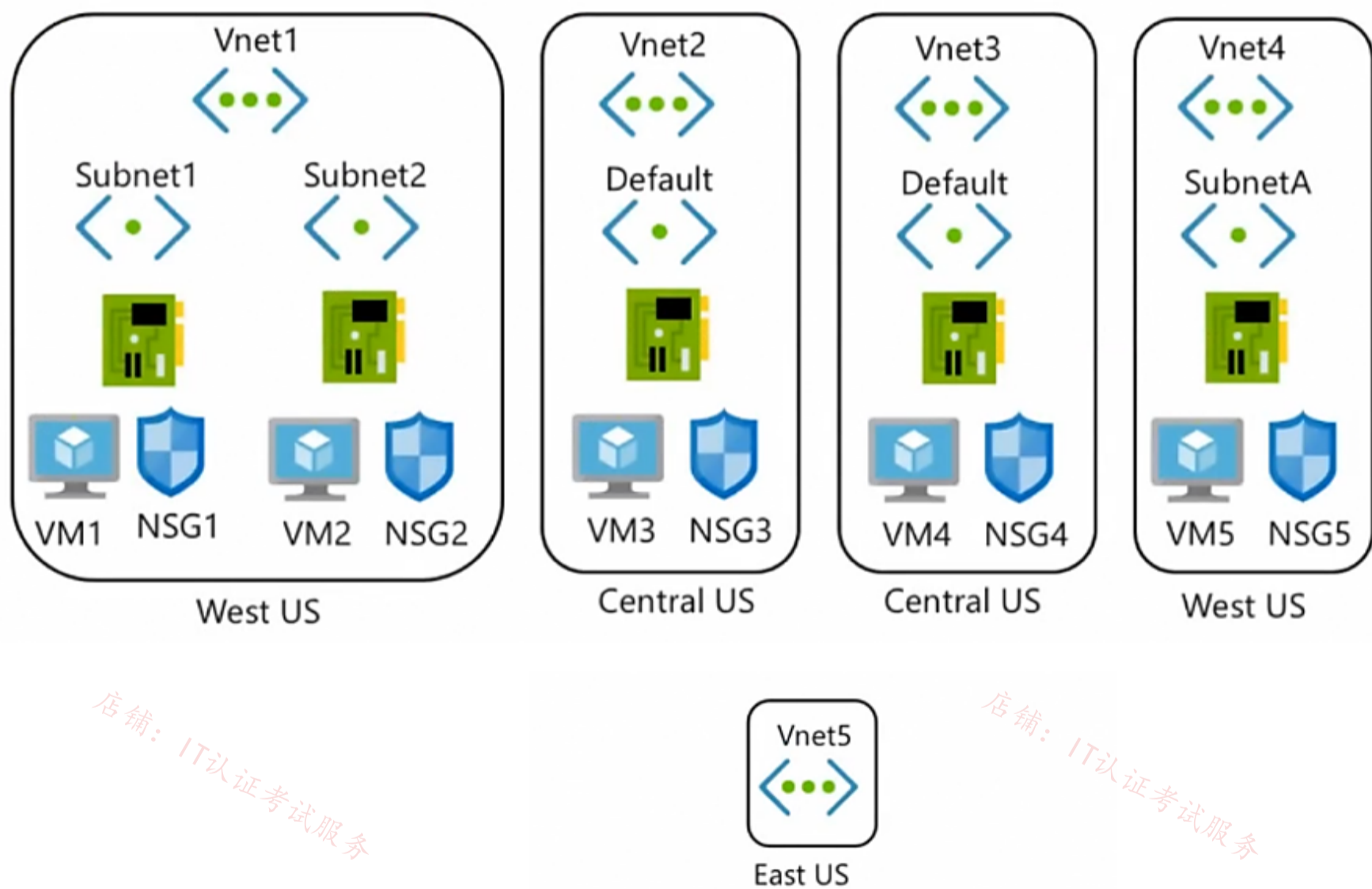
The Azure subscription contains virtual machines that run Windows Server 2019 as shown in the following table.

Name	Location	Connected to	Network security group (NSG)
VM1	West US	Vnet1/Subnet1	NSG1
VM2	West US	Vnet1/Subnet2	NSG2
VM3	Central US	Vnet2/Default	NSG3
VM4	Central US	Vnet3/Default	NSG4
VM5	West US	Vnet4/SubnetA	NSG5

The NSGs are associated to the network interfaces on the virtual machines. Each NSG has one custom security rule that allows RDP connections from the internet. The firewall on each virtual machine allows ICMP traffic.

An application security group named ASG1 is associated to the network interface of VM1.

Azure Network Infrastructure Diagram



Azure Private DNS Zones

The Azure subscription contains the Azure private DNS zones shown in the following table.

Name	Location
zone1.contoso.com	Central US
zone2.contoso.com	West US

Zone1.contoso.com has the virtual network links shown in the following table.

Name	Virtual Network	Auto registration
Link1	Vnet2	No
Link2	Vnet3	Yes

Other Azure Resources

-

The Azure subscription contains additional resources as shown in the following table.

Name	Type	Location
DB1	Azure SQL Database	West US
storage1	Azure Storage account	West US
Registry1	Azure Container Registry	Central US
KeyVault1	Azure Key Vault	Central US

Requirements

-

Virtual Network Requirements

-

Contoso has the following virtual network requirements:

- Create a virtual network named Vnet6 in West US that will contain the following resources and configurations:
 - o Two container groups that connect to Vnet6
 - o Three virtual machines that connect to Vnet6
 - o Allow VPN connections to be established to Vnet6
 - o Allow the resources in Vnet6 to access KeyVault1, DB1, and Vnet1 over the Microsoft backbone network.
- The virtual machines in Vnet4 and Vnet5 must be able to communicate over the Microsoft backbone network.
- A virtual machine named VM-Analyze will be deployed to Subnet1. VM-Analyze must inspect the outbound network traffic from Subnet2 to the internet.

Network Security Requirements

-

Contoso has the following network security requirements:

- Configure Azure Active Directory (Azure AD) authentication for Point-to-Site (P2S) VPN users.
- Enable NSG flow logs for NSG3 and NSG4.
- Create an NSG named NSG10 that will be associated to Vnet1/Subnet1 and will have the custom inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
500	3389	TCP	10.1.0.0/16	Any	Deny
1000	Any	ICMP	10.10.0.0/16	VirtualNetwork	Deny

- Create an NSG named NSG11 that will be associated to Vnet1/Subnet2 and will have the custom outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
200	3389	TCP	10.1.0.0/16	VirtualNetwork	Deny

Which virtual machines can VM1 and VM4 ping successfully before NSG10 and NSG11 are created? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

VM1:	<div style="border: 1px solid black; padding: 5px;"><div style="border: 1px solid black; height: 20px; margin-bottom: 5px;"></div><div style="border: 1px solid black; padding: 5px;"><p>VM2 only</p><p>VM2 and VM4 only</p><p>VM2, VM3, and VM4 only</p><p>VM2, VM3, VM4, and VM5</p></div></div>
VM4:	<div style="border: 1px solid black; padding: 5px;"><div style="border: 1px solid black; height: 20px; margin-bottom: 5px;"></div><div style="border: 1px solid black; padding: 5px;"><p>VM3 only</p><p>VM1 and VM3 only</p><p>VM1, VM2, and VM3 only</p><p>VM1, VM2, VM3, and VM5</p></div></div>

Answer Area

VM1:

VM2 only

VM2 and VM4 only

VM2, VM3, and VM4 only

VM2, VM3, VM4, and VM5

Correct Answer:

VM4:

VM3 only

VM1 and VM3 only

VM1, VM2, and VM3 only

VM1, VM2, VM3, and VM5

rAyLeE29 5 days, 12 hours ago

"before NSG10 and NSG11 are created" is the keyword?
upvoted 1 times

SJHCI 1 week, 1 day ago

For me as peering description:

- Vm 2,3,4
- VM 1,2,3

upvoted 4 times

samir111 1 week, 1 day ago

hmm, I think both of the answers are wrong.

VM1: (VNET1- Peered with VNET2/VNET3) Meaning VM1 can ping VM2,VM3 and VM4

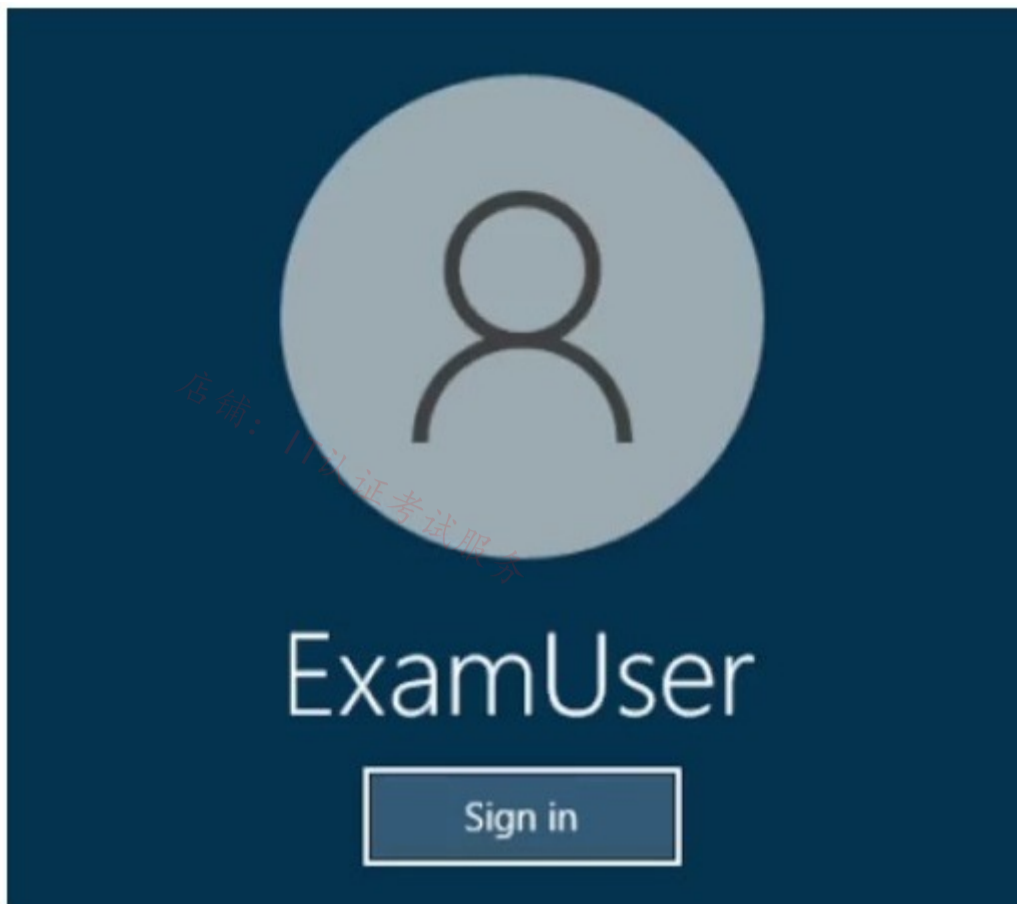
VM4: (VNET 3 - Peered with VNET/2 and VNET1) meaning VM4 can ping VM3 . VM2 and VM1.

NSG only has custom rule to allow RDP connection, meaning rest are default rules, allowing VNET to VNET Connectivity.
upvoted 1 times

rishabr019 1 week, 3 days ago

Correct answer. Vm 2,3,4 and vm3 onlu
upvoted 2 times

SIMULATION -



Username and password -

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx -

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678 -

You plan to deploy a VPN gateway and an ExpressRoute gateway to VNET2.

You need to prepare VNET2 to ensure that you can deploy the gateways.

To complete this task, sign in to the Azure portal.

Correct Answer:

Configure ExpressRoute and Site-to-Site coexisting connections using the Azure portal

Step 1: In the Azure portal, search for and select virtual networks.

Step 2: On the Virtual networks page, select the virtual network you want to add a subnet to. Select the VNET2 virtual network

Step 3: On the virtual network page, select Subnets from the left navigation.

Step 4: On the Subnets page, select + Subnet.

Step 5: On the Add subnet screen, enter or select values for the subnet settings.

You can configure the following settings for a subnet:

* Name - The name must be unique within the virtual network.

* Subnet address range - The range must be unique within the address space and can't overlap with other subnet address ranges in the virtual network. You must specify the address space by using Classless Inter-Domain Routing (CIDR) notation.

The Gateway Subnet must be /27 or a shorter prefix (such as /26 or /25).

Specify: 10.0.0.0/27

Step 6: Select Save.

Reference:

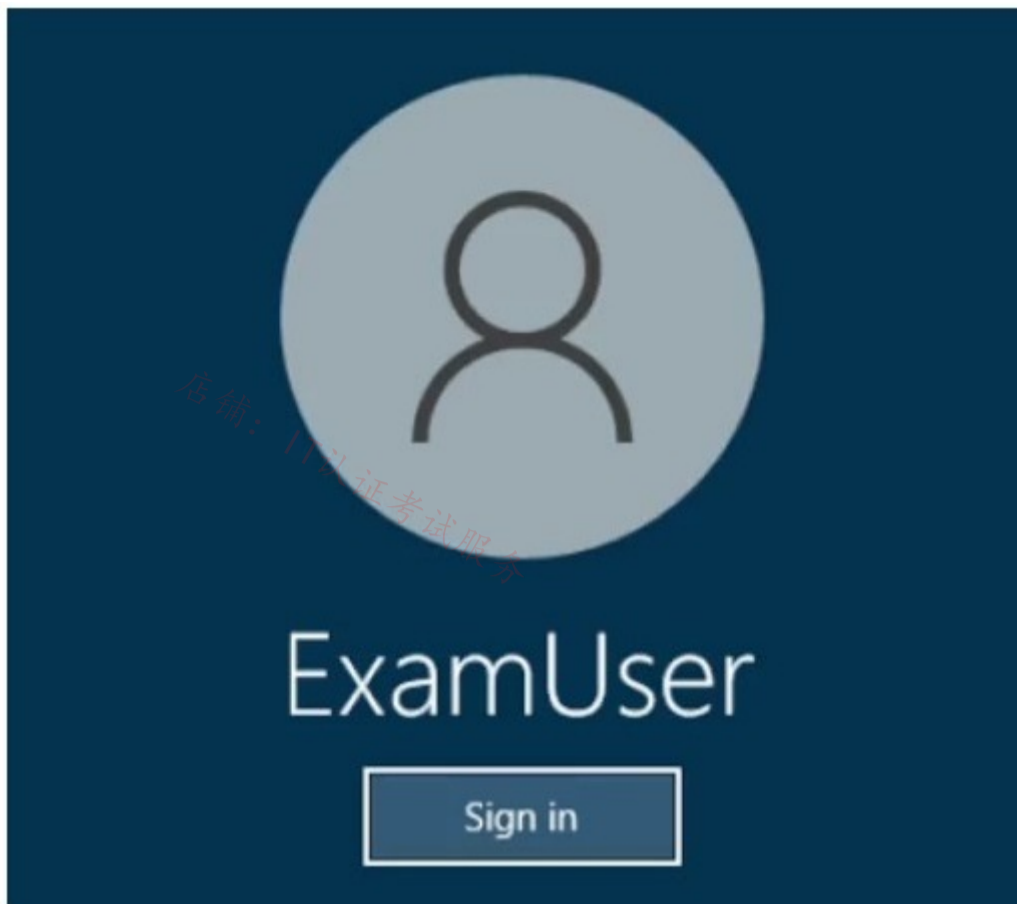
<https://learn.microsoft.com/en-us/azure/expressroute/how-to-configure-coexisting-gateway-portal>

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-subnet>

店铺: IT认证考试服务

店铺: IT认证考试服务

SIMULATION -



Username and password -

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx -

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678 -

You plan to manage the public DNS records for a domain named fabrikam.com by using an Azure solution.

You need to ensure that www.fabrikam.com resolves to 131.107.2.50.

To complete this task, sign in to the Azure portal.

Correct Answer:

Create an Azure DNS zone [already done] and record using the Azure portal

Create a DNS record

DNS records are created for your domain inside the DNS zone. A new address record, known as an 'A' record, is created to resolve a host name to an IPv4 address.

To create an 'A' record

Step 1: In the Azure portal, under All resources, open the fabrikam.com DNS zone. You can enter fabrikam.com in the Filter by name box to find it more easily.

Step 2: In the Add a record set window, enter or select the following values:

Step 3: At the top of the fabrikam.com DNS zone page, select + Record set.

Name: Type www. This record name is the host name that you want to resolve to the specified IP address.

Type: Select A. 'A' records are the most common, but there are other record types for mail servers ('MX'), IP v6 addresses ('AAAA'), and so on.

TTL: Type 1. Time-to-live of the DNS request specifies how long DNS servers and clients can cache a response.

TTL unit: Select Hours. The time unit for the TTL entry is specified here.

IP address: Type 131.107.2.50. This value is the IP address that the record name resolves to. In a real-world scenario, you would enter the public IP address for your web server.

Step 4: Select OK to create the A record.

Reference:

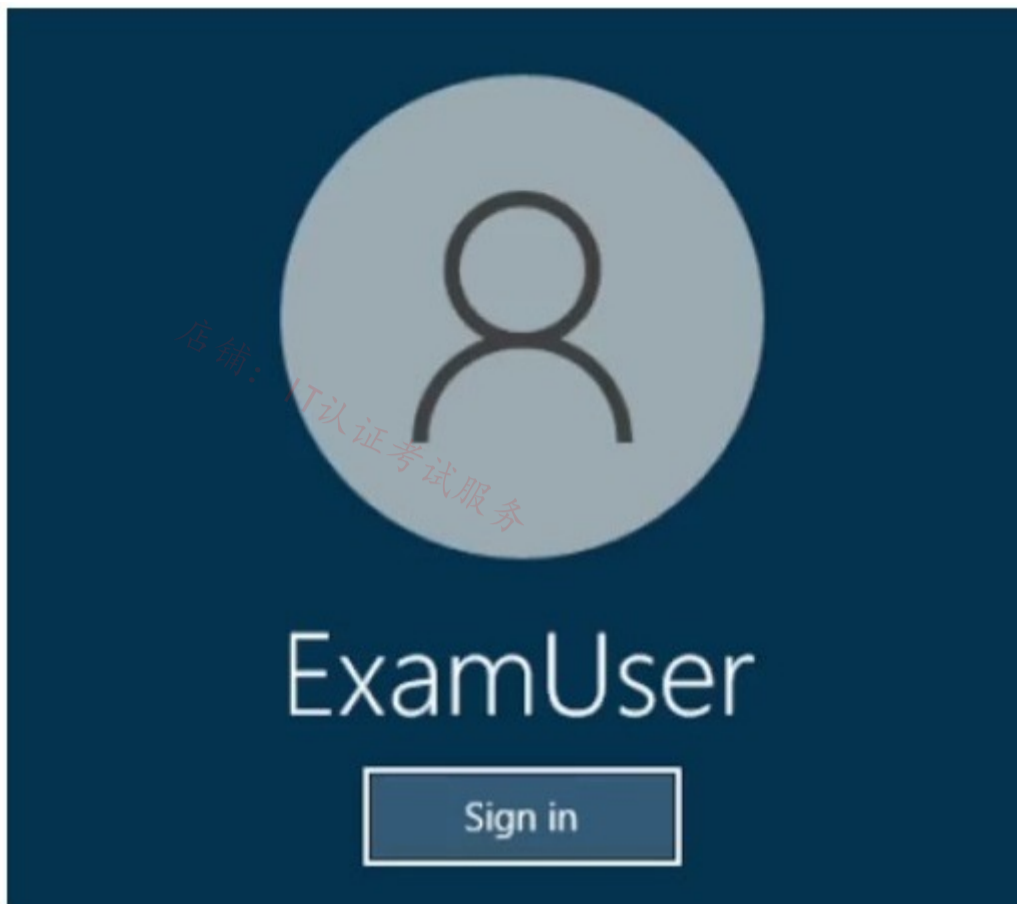
<https://learn.microsoft.com/en-us/azure/dns/dns-getstarted-portal>

店铺: IT认证考试服务

店铺: IT认证考试服务

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You plan to configure a VPN tunnel for VNET2.

You need to ensure that all internet traffic from subnet2-1 is routed through an on-premises firewall before reaching the destination. The solution must be achieved without using dynamic routing protocols.

To complete this task, sign in to the Azure portal.

Correct Answer:

Route network traffic with a route table using the Azure portal

Azure routes traffic between all subnets within a virtual network, by default. You can create your own routes to override Azure's default routing. Custom routes are helpful when, for example, you want to route traffic between subnets through a network virtual appliance (NVA) (or a Firewall).

Send Traffic from Azure Firewall to Internet

Even if the Azure Firewall is created with support for Forced Tunneling, you do not have to add a Route Table here at all. The default behavior will provide outbound connectivity to Internet just like a regular firewall.

Phase 1: Create a route table

In this section, create a route table to define the route of the traffic through the NVA virtual machine. The route table is associated to the subnet-1 subnet where the vm-public virtual machine is deployed.

Step 1: In the search box at the top of the portal, enter Route table. Select Route tables in the search results.

Step 2: Select + Create.

Step 3: In Create Route table enter or select the following information:
* Details omitted. *

Step 4: Select Review + create.

Step 5: Select Create.

Phase 2: Create a route

In this section, create a route in the route table that you created in the previous steps.

Step 1: In the search box at the top of the portal, enter Route table. Select Route tables in the search results.

Step 2: Select route-table-public.

Step 3: In Settings select Routes.

Step 4: Select + Add in Routes.

Step 5: Enter or select the following information in Add route:

Route name: to-firewall.

Destination type: Select IP Addresses.

Destination IP addresses/CIDR ranges Enter 0.0.0.0/0

Use 0.0.0.0/0 for any unmatched routes.

Next hop type: Select Virtual appliance.

Next hop address: Enter the IP address of the Firewall.

This is the IP address you of the Firewall.

Step 6: Select Add.

Step 7: Select Subnets in Settings.

Step 8: Select + Associate.

Step 9: Enter or select the following information in Associate subnet:

Setting Value

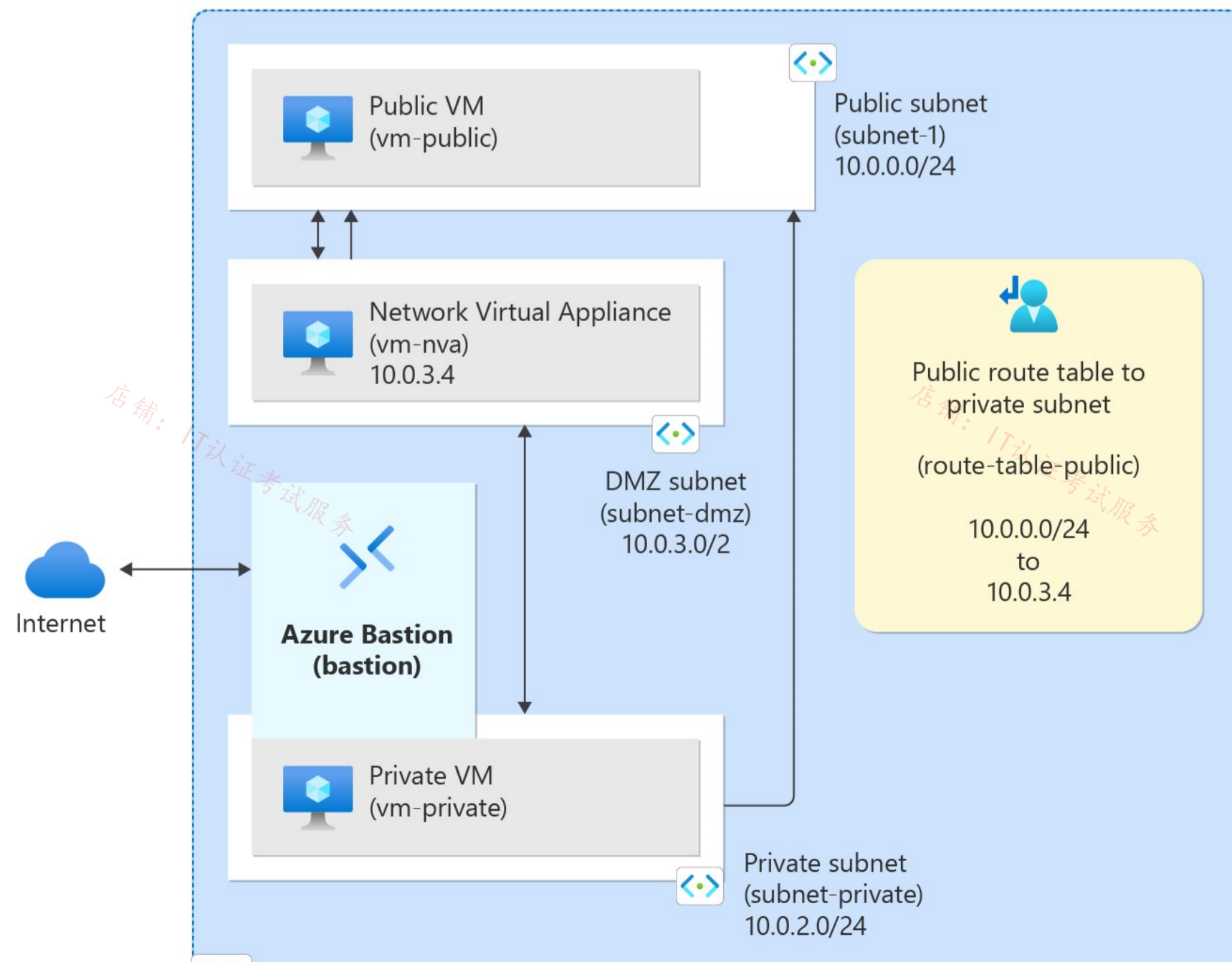
Virtual network: Select VNET2

Subnet: Select subnet2-1.

Step 10: Select OK.

Note: Route network traffic with a route table using the Azure portal

Azure routes traffic between all subnets within a virtual network, by default. You can create your own routes to override Azure's default routing. Custom routes are helpful when, for example, you want to route traffic between subnets through a network virtual appliance (NVA).





Virtual Network
(vnet-1)
10.0.0.0/16

Reference:

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

<https://learn.microsoft.com/en-us/answers/questions/1356750/internet-routing-via-azure-firewall>

店铺：IT认证考试服务

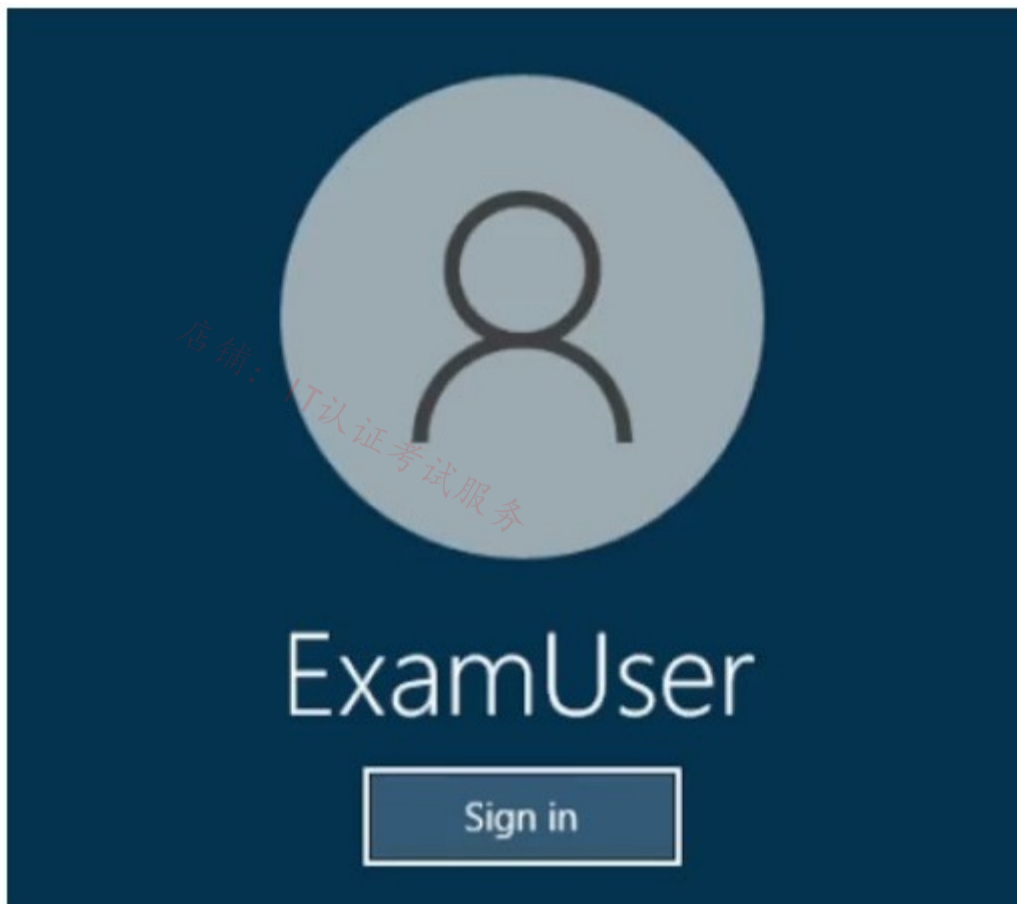
店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You plan to deploy two DNS servers to subnet2-1. Each server will host a DNS zone for fabrikam.com. The DNS zones will contain records from the on-premises network only. The IP address of the DNS servers will be 10.2.1.4 and 10.2.1.5.

You need to ensure that virtual machines on VNET2 can resolve the names of the on-premises servers in fabrikam.com.

To complete this task, sign in to the Azure portal.

Correct Answer:**Azure DNS Private Resolver**

The Azure DNS Private Resolver is a service that can resolve on-premises DNS queries for Azure DNS private zones. Previously, it was necessary to deploy a VM-based custom DNS resolver, or use non-Microsoft DNS, DHCP, and IPAM (DDI) solutions to perform this function.

Create a DNS resolver inside the virtual network

Step 1: In the Azure portal, search for DNS Private Resolvers.

Step 2: Select DNS Private Resolvers, select Create, and then on the Basics tab for Create a DNS Private Resolver enter the following:

Subscription

Resource group:

Name: Enter a name for your DNS resolver (ex: mydnsresolver).

Region: Choose the region you used for the VNET2 virtual network.

Virtual Network: Select VNET2.

Don't create the DNS resolver yet.

[Home](#) > [DNS private resolvers](#) >

Create a DNS private resolver

[Basics](#) [Inbound Endpoints](#) [Outbound Endpoints](#) [Ruleset](#) [Tags](#) [Review + Create](#)

Azure DNS private resolver bridges on-premises DNS namespaces with private DNS zones hosted on Azure DNS without the burden of deploying VM-based custom DNS servers. You can resolve DNS queries from on-premises networks and do conditional forwarding to on-premises DNS zones. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

Resource group * ⓘ [Create new](#)

Instance details

Private resolver is a regional service. Only virtual networks and rulesets in the same region can use this private resolver.

Name *

Region *

ⓘ DNS private resolver and virtual network must exist in the same location, so the region selected here will affect the available virtual networks for selection.

Virtual Network

Select a virtual network for your private resolver and endpoints. [Learn more](#)

Virtual Network * ⓘ

Add rules to the forwarding ruleset

Add two new conditional forwarding rules to the ruleset.

Step 3: On the myruleset | Rules page, select Add, and enter the following rule data:

Rule Name: Internal

Domain Name: internal.fabrikam.com. (fabrikam.com domain in the question)

Rule State: Enabled

Under Destination IP address enter 10.2.1.4, and then select Add.

Question has the IP address of the DNS servers will be 10.2.1.4 and 10.2.1.5.

Step 4: On the mvruleset | Rules page, select Add, and enter the following rule data:

Rule Name: Internal
Domain Name: internal.fabrikam.com. (fabrikam.com domain in the question)
Rule State: Enabled
Under Destination IP address enter 10.2.1.5, and then select Add.

Reference:
<https://learn.microsoft.com/en-us/azure/dns/dns-private-resolver-get-started-portal>

Topic 3 - Question Set 3

店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 Azure application gateway that has Azure Web Application Firewall (WAF) enabled.

You configure the application gateway to direct traffic to the URL of the application gateway.

You attempt to access the URL and receive an HTTP 403 error. You view the diagnostics log and discover the following error.

```
{
  "timeStamp": "2021-06-02T18:13:45+00:00",
  "resourceID": "/SUBSCRIPTIONS/489f2hht-se7y-987v-g571-463hw3679512/RESOURCEGROUPS/RG1/PROVIDERS/MICROSOFT.NETWORK/APPLICATIONGATEWAYS/AGW1",
  "operationName": "ApplicationGatewayFirewall",
  "category": "ApplicationGatewayFirewallLog",
  "properties": {
    "instanceId": "appgw_0",
    "clientIp": "137.135.10.24",
    "clientPort": "",
    "requestUri": "/login",
    "ruleSetType": "OWASP_CRS",
    "ruleSetVersion": "3.0.0",
    "ruleId": "920300",
    "message": "Request Missing an Accept Header",
    "action": "Matched",
    "site": "Global",
    "details": {
      "message": "Warning. Match of \\\"pm AppleWebKit Android\\\" against \\\"REQUEST_HEADER:User-Agent\\\" required. ",
      "data": "",
      "file": "rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf",
      "line": "1247"
    },
    "hostname": "appl.contoso.com",
    "transactionId": "f7546159yhjk7wal14568if5131t68h7",
    "policyId": "default",
    "policyScope": "Global",
    "policyScopeName": "Global",
  }
}
```

You need to ensure that the URL is accessible through the application gateway from any IP address.

Solution: You configure a custom cookie and an exclusion rule.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

The log shows that WAF rule with ruleId 920300 was triggered. Instead we should disable the WAF rule that has a ruleId 920300.

Reference:

<https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/web-application-firewall-troubleshoot>

Community vote distribution

B (100%)

 **OrangeSG** 2 months, 1 week ago

Selected Answer: B

The log shows that WAF rule with ruleId 920300 was triggered.

Fixing false positives, you can do a few things to stop this from blocking your traffic:

- Use an exclusion list
- Disable the rule.

So we should disable the WAF rule that has a ruleId 920300.

<https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/web-application-firewall-troubleshoot#fixing-false-positives>

upvoted 1 times

 **khanda** 9 months, 2 weeks ago

Selected Answer: B

Correct, disable the matched rule. False positive.

upvoted 2 times

 **Rajan395** 12 months ago

correct

upvoted 1 times

 **sshera** 1 year ago

in exam 4jan23

upvoted 3 times

 **fisherx001** 1 year, 2 months ago

correct

upvoted 1 times

 **Shereenassaf984** 1 year, 4 months ago

correct

upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT -

You have an Azure subscription that contains the route tables and routes shown in the following table.

Route table name	Route name	Prefix	Destination
RT1	Default Route	0.0.0.0/0	VirtualNetworkGateway
RT2	Default Route	0.0.0.0/0	Internet

The subscription contains the subnets shown in the following table.

Name	Prefix	Route table	Virtual network
Subnet1	10.10.1.0/24	RT1	Vnet1
Subnet2	10.10.2.0/24	RT2	Vnet1
GatewaySubnet	10.10.3.0/24	None	Vnet1

The subscription contains the virtual machines shown in the following table.

Name	IP address
VM1	10.10.1.5
VM2	10.10.2.5

The subscription contains the local network gateways shown in the following table.

Name	Prefix	Default site
New York	10.9.0.0/16	Yes
Seattle	10.8.0.0/16	No

There is a Site-to-Site VPN connection to each local network gateway.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Traffic from VM2 to the internet is routed through the New-York Site-to-Site VPN connection	<input type="radio"/>	<input type="radio"/>
Traffic from VM1 to VM2 is routed through the New-York Site-to-Site VPN connection	<input type="radio"/>	<input type="radio"/>
Traffic from VM1 to the internet is routed through the New-York Site-to-Site VPN connection	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
Traffic from VM2 to the internet is routed through the New-York Site-to-Site VPN connection	<input type="radio"/>	<input checked="" type="radio"/>
Traffic from VM1 to VM2 is routed through the New-York Site-to-Site VPN connection	<input type="radio"/>	<input checked="" type="radio"/>
Traffic from VM1 to the internet is routed through the New-York Site-to-Site VPN connection	<input checked="" type="radio"/>	<input type="radio"/>

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview>

🗨️ **jellybiscuit** Highly Voted 1 year, 3 months ago

The answers depend on some assumptions.
Is there actually a vpn gateway sitting in that gateway subnet?
If so, is it configured for BGP? If so, then...

N - all outbound traffic from VM2 is sent to the internet
N - by default, subnets within a vnet can communicate. (I'm assuming that a NSG isn't blocking)
Y - all outbound traffic from VM1 is sent to the VPN gateway

BGP eliminates the need for a local azure route table.
upvoted 34 times

🗨️ **Ajdlfasudfo** 1 year, 1 month ago

VPN: You can, optionally use BGP. For details, see BGP with site-to-site VPN connections.

There is no mentioning of BGP so you can't simply assume we have it set up
<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview#border-gateway-protocol>
upvoted 1 times

🗨️ **kimalto452** Highly Voted 1 year, 4 months ago

incorrect, the answer is NYY
upvoted 25 times

🗨️ **aklas** 8 months, 1 week ago

No you're wrong. Given answer is correct. The subnets are in the same VNet so there is a local route between them which is more specific than 0.0.0.0
upvoted 8 times

🗨️ **CristianM99** 6 months ago

Aklas explanation is correct. The answer is NNY
upvoted 3 times

🗨️ **Lazylinux** Most Recent 6 months ago

Given answer is correct

N- all outbound traffic from VM2 is sent to the internet by default as use route table RT2

N - Since both subnets are part of the same vNET1 hence communicate directly with each other

Y - Since VM1 uses RT1 and RT1 has VPNGWY as its default GWY then VM1 uses this for its internet access
upvoted 3 times

🗨️ **occupatissimo** 9 months ago

NNY
Third answer look at: <https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-forced-tunneling-rm>.
upvoted 2 times

🗨️ **khanda** 9 months, 2 weeks ago

Correct answer: NNY
Check comments
upvoted 1 times

🗨️ **DerekKey** 1 year ago

No | No | Yes
Yes -> Forced tunneling is carried out by using a virtual private network (VPN) tunnel; this tunnel requires a default site, a local gateway where all the Azure Internet-bound traffic is redirected.
upvoted 6 times

🗨️ **NoeHdzMII** 1 year, 1 month ago

Correct answer
N - all outbound traffic from VM2 is sent to the internet by default
N - the effective route table show the all the the subnet on the same VNET as a more specific one than the default route and Gateway routes. So subnets within a vnet can communicate can communicate directly.
Y - all outbound traffic from VM1 is sent to the VPN gateway
upvoted 3 times

🗨️ **Takloy** 1 year, 1 month ago

By New York Site-to-site- VPN Connection, I assume whenever the traffic hits the VPN Gateway from the default route in Route1. Am I right? so my answer is NYY
upvoted 1 times

🗨️ **Edzor** 1 year, 3 months ago

Given answer is correct, since New York local gateway is the default site (forced tunneling) to the VPN <https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-forced-tunneling-rm>
(GatewayDefaultSite)
upvoted 3 times

🗨️ **DeepMoon** 1 year, 4 months ago

Given answers are wrong.

Don't think too hard in trying to draw a logical network diagram in your head.

Simply realize NY is 10.9.0.0 (not on any of the route tables).
So nothing is routed through the NY. All answers are

Q1: No

Q2: No

Q3: No

upvoted 11 times

🗨️ **[Removed]** 1 year, 4 months ago

I agree, there is no default route towards NY

upvoted 3 times

🗨️ **DeepMoon** 1 year, 4 months ago

I have no idea of creating a logical diagram of this network. Can someone help me out here?
Where is NY & Seattle relative to subnet1 & subnet 2.

My drawing would be

```
| Vnet1- boundary subnet1(vm1) | subnet2 (vm2) vnet1-boundary |
```

Which way is internet?

Which way is VirtualNetworkGateway?

Which way is NY

Which way is Seattle?

upvoted 2 times

🗨️ **AdityaGupta** 1 year, 4 months ago

Given answers are correct.

upvoted 5 times

🗨️ **tkcltoh** 1 year, 4 months ago

default route is 0.0.0.0/0 internet. RT1 route is UDR therefore VM1 to VM2 is communicates via VPN

upvoted 1 times

🗨️ **Prutser2** 1 year, 3 months ago

from subnet1 to subnet 2 (vm1 to VM2), uses intra vnet, as its a longer match, would not choose default gateway

upvoted 3 times

🗨️ **RollinDeep** 1 year, 4 months ago

NNY. VM1 to VM2 are routed within Vnet1. RT1 and RT2 define default routes.

upvoted 5 times

🗨️ **Cristoicach91** 1 year, 4 months ago

correct

upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

You have an Azure subscription that contains the public IP addresses shown in the following table.

Name	IP version	SKU	IP address assignment
IP1	IPv4	Basic	Static
IP2	IPv4	Basic	Dynamic
IP3	IPv4	Standard	Static
IP4	IPv6	Basic	Dynamic
IP5	IPv6	Standard	Static

You plan to deploy a NAT gateway named NAT1.

Which public IP addresses can be used as the public IP address for NAT1?

- A. IP3 only
- B. IP5 only
- C. IP2 and IP4 only
- D. IP1, IP3 and IP5 only
- E. IP3 and IP5 only

Correct Answer: A

Only static IPv4 addresses in the Standard SKU are supported. IPv6 doesn't support NAT.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-overview>

Community vote distribution

A (100%)

 **WorkHardBeProud** Highly Voted 2 years, 3 months ago

<https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-overview#limitations>
upvoted 9 times

 **crawfish** 2 years, 3 months ago

Answer is correct. Per the link, NAT cannot be associated to an IPv6 Public IP address or IPv6 Public IP Prefix. However, it can be associated to a dual stack subnet.
upvoted 21 times

 **Lazylinux** Most Recent 6 months ago

Selected Answer: A

Answer A
as per Microsoft

NAT gateway is compatible with standard SKU public IP addresses or public IP prefix resources or a combination of both.

Basic SKU resources, such as basic load balancer or basic public IPs aren't compatible with NAT gateway. NAT gateway can't be used with subnets where basic SKU resources exist. Basic load balancer and basic public IP can be upgraded to standard to work with a NAT gateway
upvoted 2 times

 **Webfacat33** 1 year, 1 month ago

Selected Answer: A

NAT doesn't support ipv6
upvoted 3 times

 **jellybiscuit** 1 year, 3 months ago

Selected Answer: A

This page confirms you can use standard SKU only
<https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-overview#limitations>

This page confirms that the address must be static, and that IPv6 is not supported
<https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-addresses#at-a-glance>
upvoted 4 times

 **sandeepmalik** 1 year, 3 months ago

IP3 only.....as NAT gateway is compatible with Standard SKU for IPv4 only
A NAT gateway can't be associated to an IPv6 public IP address or IPv6 public IP prefix
In today exam Oct 2nd 2022

upvoted 2 times

 **AdityaGupta** 1 year, 4 months ago

Selected Answer: A

NAT gateway is compatible with standard SKU public IP addresses or public IP prefix resources or a combination of both. You can use a public IP prefix directly or distribute the public IP addresses of the prefix across multiple NAT gateway resources. The NAT gateway will groom all traffic to the range of IP addresses of the prefix.

Basic resources, such as basic load balancer or basic public IPs aren't compatible with Virtual Network NAT. Basic resources must be placed on a subnet not associated to a NAT gateway. Basic load balancer and basic public IP can be upgraded to standard to work with a NAT gateway

upvoted 2 times

 **Alessandro365** 1 year, 4 months ago

Selected Answer: A

IP3 only (standard/IPv4)

upvoted 1 times

 **jeffangel28** 1 year, 5 months ago

Selected Answer: A

IP3 only.

Ref: <https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-overview#nat-gateway-and-basic-sku-resources>

upvoted 2 times

 **zerocool114** 1 year, 6 months ago

on exam today

upvoted 1 times

 **Fearless90** 1 year, 7 months ago

Selected Answer: A

A. IP3 only

upvoted 3 times

 **Fearless90** 1 year, 7 months ago

<https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-overview#virtual-network-nat-basics>

Virtual Network NAT basics

A NAT gateway can't be associated to an IPv6 public IP address or IPv6 public IP prefix. It can be associated to a dual stack subnet but will only be able to direct outbound traffic with an IPv4 address.

upvoted 1 times

 **Fearless90** 1 year, 7 months ago

<https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-overview#virtual-network-nat-basics>

Virtual Network NAT basics

Basic resources, such as basic load balancer or basic public IPs aren't compatible with Virtual Network NAT. Basic resources must be placed on a subnet not associated to a NAT gateway. Basic load balancer and basic public IP can be upgraded to standard to work with a NAT gateway

- To upgrade a basic load balancer to standard, see Upgrade a public basic Azure Load Balancer.
- To upgrade a basic public IP to standard, see Upgrade a public IP address.

upvoted 1 times

 **Fearless90** 1 year, 7 months ago

<https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-overview#virtual-network-nat-basics>

Virtual Network NAT basics

Virtual Network NAT is compatible with standard SKU public IP addresses or public IP prefix resources or a combination of both. You can use a public IP prefix directly or distribute the public IP addresses of the prefix across multiple NAT gateway resources. The NAT gateway will groom all traffic to the range of IP addresses of the prefix.

upvoted 1 times

 **unclegrandfather** 1 year, 7 months ago

Appeared on exam 6/28/22

upvoted 1 times

 **kogunribido** 1 year, 7 months ago

Appeared on exam 6/27/2022

upvoted 1 times

 **milan92stankovic** 1 year, 8 months ago

Selected Answer: A

Only Standard Static IPv4 can be used. The answer is correct.

upvoted 1 times

 **Edward1** 1 year, 9 months ago

Is correct:

*Basic resources, such as basic load balancer or basic public IPs aren't compatible with Virtual Network NAT. Basic resources must be placed on a subnet not associated to a NAT gateway. Basic load balancer and basic public IP can be upgraded to standard to work with a NAT gateway

*A NAT gateway can't be associated to an IPv6 public IP address or IPv6 public IP prefix. It can be associated to a dual stack subnet

upvoted 4 times

🗨️ **bmulvIT** 1 year, 11 months ago

on exam 3/3/2022

upvoted 1 times

🗨️ **rockethack** 1 year, 11 months ago

This question was on the exam on 18th Feb 2022.

upvoted 1 times

🗨️ **d0bermann** 1 year, 11 months ago

Selected Answer: A

A. IP3 only [std sku & ipv4]

upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

You have an Azure application gateway named AGW1 that has a routing rule named Rule1. Rule 1 directs traffic for <http://www.contoso.com> to a backend pool named Pool1. Pool1 targets an Azure virtual machine scale set named VMSS1.

You deploy another virtual machine scale set named VMSS2.

You need to configure AGW1 to direct all traffic for <http://www.adatum.com> to VMSS2.

The solution must ensure that requests to <http://www.contoso.com> continue to be directed to Pool1.

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

NOTE: Each correct selection is worth one point.

- A. Add a backend pool.
- B. Modify an HTTP setting.
- C. Add an HTTP setting.
- D. Add a listener.
- E. Add a rule.

Correct Answer: ADE

Reference:

<https://docs.microsoft.com/en-us/azure/application-gateway/configuration-overview>

Community vote distribution

ADE (100%)

 **RickMorais** Highly Voted 2 years, 3 months ago

Correct

You need a backend for VMSS2, a listener for the site adatum.com and a rule to redirect the request from the listener to backend VMSS2
upvoted 71 times

 **jeffangel28** 1 year, 5 months ago

Right!

upvoted 1 times

 **AidenYoukhana** 2 years ago

THANKS!

upvoted 1 times

 **crawfish** 2 years, 3 months ago

perfect explanation

upvoted 3 times

 **JoMa** 2 years, 1 month ago

simple and perfect explanation

upvoted 2 times

 **Lazylinux** Most Recent 6 months ago

Selected Answer: ADE

Answer correct

you don't have to modify or add HTTP setting because you can use the same existing with new backend pool

upvoted 1 times

 **Rajan395** 12 months ago

correct answer!

upvoted 1 times

 **TJ001** 1 year ago

HTTP setting can be common(if the same type of setting) across rules is important understand...


upvoted 1 times

 **AdityaGupta** 1 year, 4 months ago

Selected Answer: ADE

Correct Answer, you don't have to modify or add HTTP setting.

upvoted 1 times

 **tartarus23** 1 year, 6 months ago

Selected Answer: ADE

A. Add a backend pool. | D. Add a listener. | E. Add a rule.

VMSS2 is newly created and would need a backend pool. AGW needs to listen to HTTP traffic and forward the HTTP requests based on the rules for VMSS1 Pool1 or VMSS2 Pool2 as per the question.

upvoted 3 times

  **rockethack** 1 year, 11 months ago

This question was on the exam on 18th Feb 2022.

upvoted 1 times

  **d0bermannn** 1 year, 11 months ago

Selected Answer: ADE

ADE is correct

upvoted 2 times

  **Kimimoto** 1 year, 11 months ago

Appeared in exam on 11/Feb/2022

upvoted 1 times

  **KranthiChaitanya** 2 years ago

Came on exam 28/Jan/22

upvoted 1 times

  **Contactfornitish** 2 years ago

Appeared in exam on 17/01/2022

upvoted 1 times

  **Pravda** 2 years ago

Variation on exam 1/6/2022

upvoted 3 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT -

You have an Azure Traffic Manager parent profile named TM1. TM1 has two child profiles named TM2 and TM3.

TM1 uses the performance traffic-routing method and has the endpoints shown in the following table.

Name	Location
App1	North Europe
App2	East US
App3	Central US
TM2	West Europe
TM3	West US

TM2 uses the weighted traffic-routing method with MinChildEndpoint = 2 and has the endpoints shown in the following table.

Name	Location	Weight
App4	West Europe	99
App5	West Europe	1

TM3 uses priority traffic-routing method and has the endpoints shown in the following table.

Name	Location
App6	West US
App2	East US

The App2, App4, and App6 endpoints have a degraded monitoring status.

To which endpoint is traffic directed? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point

Hot Area:

Answer Area

Traffic from West Europe:

<input type="checkbox"/>	▼
<input type="checkbox"/>	App1
<input type="checkbox"/>	App2
<input type="checkbox"/>	App4
<input type="checkbox"/>	App5

Traffic from West US:

<input type="checkbox"/>	▼
<input type="checkbox"/>	App1
<input type="checkbox"/>	App2
<input type="checkbox"/>	App3
<input type="checkbox"/>	App6

Answer Area

Traffic from West Europe:

	▼
App1	
App2	
App4	
App5	

Correct Answer:

Traffic from West US:

	▼
App1	
App2	
App3	
App6	

Reference:

<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-nested-profiles>

 **crawfish** Highly Voted 2 years, 3 months ago

Traffic from West Europe:

Based on TM1 table, West Europe will trigger TM2. However, as the MinChildEndpoint is set to 2, and App4 is degraded (down), the entire TM2 will not be considered available.

This goes back to the origin TM1 that uses performance traffic-routing method, which means the closest location is App1 and naturally be the next best performance instance.

Hence, Answer = App1

Traffic from West US:

Based on TM1 table, West US will trigger TM3. However, both App2 and App6 were degraded (down), so none of them can be considered.

This goes back to the original TM1 that uses performance traffic-routing method, from TM1, the other 2 US locations would be App2 and App3.

But App2 we know it's already degraded (unavailable), hence the only option would be App3.

Answer = App3

upvoted 221 times

 **macka2005** 4 months ago

Great explanation, thanks

upvoted 1 times

 **CiscoTerminator** 5 months, 3 weeks ago

Spot on my friend. Initially missed the minChildEndpoints =2 but got to you same answer. Thanks for the detailed explanation.

upvoted 1 times

 **leotoronto123** 2 years ago

MinChildEndpoint:

Gets or sets the minimum number of endpoints that must be available in the child profile in order for the parent profile to be considered available. Only applicable to endpoint of type 'NestedEndpoints'.

my question is here the value is 2. should it consider App5 before going to parent and considering APP1?

upvoted 2 times

 **CiscoTerminator** 5 months, 2 weeks ago

Minimum healthy endpoints should be 2 so since App4 is down, this is not healthy so App5 is NOT considered.

upvoted 1 times

 **JohnnyChimpo** 9 months ago

Thanks for explaining this

upvoted 1 times

 **JennyHuang36** Highly Voted 11 months, 1 week ago

In exam Feb, 2023

upvoted 5 times

 **Rajan395** Most Recent 12 months ago

correct answer

upvoted 2 times

 **sshera** 1 year ago

in exam 4jan23

upvoted 2 times

- Andersonalm 1 year, 2 months ago
Correct!
upvoted 1 times
- Stanley3427 1 year, 7 months ago
App5 and App3 is correct
upvoted 1 times
- geuser 1 year, 2 months ago
it cannot be App5 because MinChildEndpoint = 2 not 1 (which is default).
upvoted 2 times
- bebop 1 year, 3 months ago
How come?
upvoted 1 times
- bmulvIT 1 year, 11 months ago
On exam today 3/3/2022
upvoted 2 times
- rockethack 1 year, 11 months ago
This question was on the exam on 18th Feb 2022.
upvoted 2 times
- Kimimoto 1 year, 11 months ago
Appeared in exam on 11/Feb/2022
upvoted 1 times
- KranthiChaitanya 2 years ago
Came on exam 28/Jan/22
upvoted 2 times
- sallymaher 2 years ago
i though the TM doesn't have a location and it is a global service , how come they mentioned locations for the TMs !!!!
upvoted 2 times
- Contactfornitish 2 years ago
Appeared in exam on 17/01/2022
upvoted 1 times
- Pravda 2 years ago
Not on exam 1/6/2022
upvoted 2 times
- aftab7500 2 years, 1 month ago
Nested Traffic Manager profiles
<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-nested-profiles>
upvoted 1 times
- Bharat 2 years, 3 months ago
Well explained in the provided link. Answers are correct
upvoted 4 times
- slieksl 2 years, 3 months ago
It should be App5 and App3.
upvoted 3 times
- Roman_Rabodzey 2 years, 3 months ago
There is traffic-routing method with MinChildEndpoint = 2. The parameter determines the minimum number of available endpoints in the child profile. So the parent profile considers the entire child profile to be unavailable and directs traffic to the other endpoints.
upvoted 14 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 Azure application gateway that has Azure Web Application Firewall (WAF) enabled.

You configure the application gateway to direct traffic to the URL of the application gateway.

You attempt to access the URL and receive an HTTP 403 error. You view the diagnostics log and discover the following error.

```
{
  "timeStamp": "2021-06-02T18:13:45+00:00",
  "resourceID": "/SUBSCRIPTIONS/489f2hht-se7y-987v-g571-463hw3679512/RESOURCEGROUPS/RG1/PROVIDERS/MICROSOFT.NETWORK/APPLICATIONGATEWAYS/AGW1",
  "operationName": "ApplicationGatewayFirewall",
  "category": "ApplicationGatewayFirewallLog",
  "properties": {
    "instanceId": "appgw_0",
    "clientIp": "137.135.10.24",
    "clientPort": "",
    "requestUri": "/login",
    "ruleSetType": "OWASP_CRS",
    "ruleSetVersion": "3.0.0",
    "ruleId": "920300",
    "message": "Request Missing an Accept Header",
    "action": "Matched",
    "site": "Global",
    "details": {
      "message": "Warning. Match of \\\"pm AppleWebKit Android\\\" against \\\"REQUEST_HEADER:User-Agent\\\" required. ",
      "data": "",
      "file": "rules\\REQUEST-920-PROTOCOL-ENFORCEMENT.conf",
      "line": "1247"
    },
    "hostname": "appl.contoso.com",
    "transactionId": "f7546159yhjk7wall14568if5131t68h7",
    "policyId": "default",
    "policyScope": "Global",
    "policyScopeName": "Global",
  }
}
```

You need to ensure that the URL is accessible through the application gateway from any IP address.

Solution: You add a rewrite rule for the host header.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

The log shows that WAF rule with ruleId 920300 was triggered. Instead we should disable the WAF rule that has a ruleId 920300.

Reference:

<https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/web-application-firewall-troubleshoot>

Community vote distribution

B (100%)

Supreem 3 months, 1 week ago

In exam 10/18/2023
upvoted 2 times

jakubklapka 4 months ago

In exam Sep, 2023
upvoted 1 times

Rajan395 12 months ago

correct answer!
upvoted 4 times

caliph_noman 1 year ago

Selected Answer: B

correct
upvoted 1 times

sshera 1 year ago

in exam 4jan23

upvoted 4 times

 **Andersonalm** 1 year, 2 months ago

Correct!

upvoted 3 times

 **ghmymnvhvtlkwiz** 1 year, 2 months ago

sdfsdfs

upvoted 4 times

店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

HOTSPOT -

You have an Azure Front Door instance that provides access to a web app. The web app uses a hostname of www.contoso.com.

You have the routing rules shown in the following table.

Name	Path
RuleA	/abc/def
RuleB	/ab
RuleC	/*
RuleD	/abc/*

Which rule will apply to each incoming request? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point

Hot Area:

Answer Area

www.contoso.com/abc/def

- RuleA
- RuleB
- RuleC
- RuleD

www.contoso.com/default.htm

- RuleA
- RuleB
- RuleC
- RuleD

www.contoso.com/abc/def/default.htm

- RuleA
- RuleB
- RuleC
- RuleD

Answer Area

www.contoso.com/abc/def

- RuleA
- RuleB
- RuleC
- RuleD

www.contoso.com/default.htm

- RuleA
- RuleB
- RuleC
- RuleD

Correct Answer:

www.contoso.com/abc/def/default.htm

- RuleA
- RuleB
- RuleC
- RuleD

Reference:

<https://docs.microsoft.com/en-us/azure/frontdoor/front-door-route-matching>

🗄️ 👤 **Pravda** Highly Voted 2 years, 1 month ago

Look for any routing rule with an exact match on the Path

If no exact match Paths, look for routing rules with a wildcard Path that matches

If no routing rules are found with a matching Path, then reject the request and return a 400: Bad Request error HTTP response.

upvoted 33 times

🗄️ 👤 **y0eri** 1 week ago

<https://docs.microsoft.com/en-us/azure/frontdoor/standard-premium/concept-route#path-matching>

upvoted 1 times

🗄️ 👤 **hc007** 1 month ago

Great explanation. to complete it I would add " if more than one rule with wildcard Paths matches, use the most specific (detailed) path matched.

upvoted 1 times

🗄️ 👤 **Sarvajanik** Highly Voted 2 years, 2 months ago

Longest match is the correct answer.

upvoted 8 times

🗄️ 👤 **Murad01** Most Recent 1 month, 3 weeks ago

Appeared on Exam November - 2023

upvoted 1 times

🗄️ 👤 **Lazylinux** 6 months ago

Answer is correct

looks for exact match IF NOT then Wildcard path match otherwise Bad request

upvoted 1 times

🗄️ 👤 **Rajan395** 12 months ago

correct answer

upvoted 1 times

🗄️ 👤 **sshera** 1 year ago

in exam 4jan23

upvoted 6 times

🗄️ 👤 **Andersonalm** 1 year, 2 months ago

Correct answer

upvoted 1 times

🗄️ 👤 **naidu** 1 year, 4 months ago

Correct Answer

upvoted 1 times

🗄️ 👤 **jeffangel28** 1 year, 5 months ago

Right!

upvoted 1 times

🗄️ 👤 **rockethack** 1 year, 11 months ago

This question was on the exam on 18th Feb 2022.

upvoted 1 times

🗄️ 👤 **Kimimoto** 1 year, 11 months ago

Appeared in exam on 11/Feb/2022

upvoted 1 times

🗄️ 👤 **sleekdunga** 1 year, 11 months ago

RuleA/RuleC & RuleD

upvoted 6 times

🗄️ 👤 **KranthiChaitanya** 2 years ago

Came on exam 28/Jan/22

upvoted 1 times

🗄️ 👤 **Contactfornitish** 2 years ago

Appeared in exam on 17/01/2022

upvoted 1 times

🗄️ 👤 **Pravda** 2 years ago

Not on exam 1/6/2022

upvoted 1 times

🗄️ 👤 **AidenYoukhana** 2 years ago

CORRECT ANSWER.

upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

 **teamaws** 2 years, 2 months ago

correct, <https://docs.microsoft.com/en-us/azure/frontdoor/standard-premium/concept-route#path-matching>

upvoted 3 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 Azure application gateway that has Azure Web Application Firewall (WAF) enabled.

You configure the application gateway to direct traffic to the URL of the application gateway.

You attempt to access the URL and receive an HTTP 403 error. You view the diagnostics log and discover the following error.

```
{
  "timeStamp": "2021-06-02T18:13:45+00:00",
  "resourceId": "/SUBSCRIPTIONS/489f2hht-se7y-987v-g571-463hw3679512/RESOURCEGROUPS/RG1/PROVIDERS/MICROSOFT.NETWORK/APPLICATIONGATEWAYS/AGW1",
  "operationName": "ApplicationGatewayFirewall",
  "category": "ApplicationGatewayFirewallLog",
  "properties": {
    "instanceId": "appgw_0",
    "clientIp": "137.135.10.24",
    "clientPort": "",
    "requestUri": "/login",
    "ruleSetType": "OWASP_CRS",
    "ruleSetVersion": "3.0.0",
    "ruleId": "920300",
    "message": "Request Missing an Accept Header",
    "action": "Matched",
    "site": "Global",
    "details": {
      "message": "Warning. Match of \\\"pm AppleWebKit Android\\\" against \\\"REQUEST_HEADER:User-Agent\\\" required. ",
      "data": "",
      "file": "rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf",
      "line": "1247"
    },
    "hostname": "appl.contoso.com",
    "transactionId": "f7546159ylhjk7wall14568if5131t68h7",
    "policyId": "default",
    "policyScope": "Global",
    "popolicyScopeName": "Global",
  }
}
```

You need to ensure that the URL is accessible through the application gateway.

Solution: You disable the WAF rule that has a ruleId 920300.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

The log shows that WAF rule with ruleId 920300 was triggered. We should disable the WAF rule that has a ruleId 920300.

Reference:

<https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/web-application-firewall-troubleshoot>

Community vote distribution

A (100%)

 **AidenYoukhana** Highly Voted 2 years ago

Selected Answer: A

CORRECT ANSWER

upvoted 9 times

 **Rajan395** Most Recent 12 months ago

correct answer

upvoted 1 times

 **sshera** 1 year ago

in exam 4jan23

upvoted 3 times

 **Fearless90** 1 year, 7 months ago

Selected Answer: A

A. Yes

disable the WAF rule that has a ruleId 920300

<https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-diagnostics#firewall-log>

Value

action

Description

Action taken on the request. Available values are Blocked and Allowed (for custom rules), Matched (when a rule matches a part of the request), and Detected and Blocked (these are both for mandatory rules, depending on if the WAF is in detection or prevention mode).

upvoted 1 times

🗨️ 👤 **samers** 1 year, 8 months ago

Matched for blocking that can be disabled ,while blocking for rules that can't be disabled "builtin"

upvoted 1 times

🗨️ 👤 **sleekdunga** 1 year, 11 months ago

A correct Answer. Disabling the WAF Rule implies not match required for " specified header string"

upvoted 3 times

🗨️ 👤 **Contactforntish** 2 years ago

Appeared in exam on 17/01/2022

upvoted 2 times

🗨️ 👤 **Pravda** 2 years ago

Not on exam 1/6/2022

upvoted 2 times

🗨️ 👤 **cooksiecooks** 2 years, 3 months ago

To be more precise, the action should be stated as "Blocked" rather "Matched" for accuracy purposes.

upvoted 4 times

🗨️ 👤 **WorkHardBeProud** 2 years, 3 months ago

No - the action is well stated. The action is Blocked when it reaches the max anomaly count and trigger the non-disabled rule, from that rule you will see action "Blocked"

upvoted 9 times

店铺: IT认证考试服务

店铺: IT认证考试服务

You have an Azure subscription that contains an Azure App Service app. The app uses a URL of <https://www.contoso.com>. You need to use a custom domain on Azure Front Door for www.contoso.com. The custom domain must use a certificate from an allowed certification authority (CA).

What should you include in the solution?

- A. an enterprise application in Azure Active Directory (Azure AD)
- B. Active Directory Certificate Services (AD CS)
- C. Azure Key Vault
- D. Azure Application Gateway

Correct Answer: C

Reference:

<https://docs.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain-https>

Community vote distribution

C (100%)

 **teamaws** Highly Voted 2 years, 2 months ago

Correct, use Key Vault with your own certificate

<https://docs.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain-https#option-2-use-your-own-certificate>

upvoted 9 times

 **walkwolf3** 2 years, 2 months ago

Your own certificate means the certificate is issued by a CA.

upvoted 5 times

 **AdityaGupta** Highly Voted 1 year, 4 months ago

Selected Answer: C

The correct answer is C, but the explanation is - you must create a complete certificate chain with an allowed certificate authority (CA) that is part of the Microsoft Trusted CA List. And Azure Key Vault allows you to store your certificates securely. Azure Front Door uses this secure mechanism to get your certificate (Self Signed or CA Provided) and it requires a few extra steps.

<https://docs.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain-https#option-2-use-your-own-certificate>

upvoted 6 times

 **Lazylinux** Most Recent 6 months ago

Selected Answer: C

C is correct and how can i get this one WRONG!! no way considering i just finished 20 of them at work!!

upvoted 1 times

 **Jamesat** 1 year, 5 months ago

Selected Answer: C

Keyvault is the correct answers as noted in the official docs

<https://docs.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain-https>

upvoted 1 times

 **zerocool114** 1 year, 6 months ago

on exam today

upvoted 2 times

 **unclegrandfather** 1 year, 7 months ago

Appeared on exam 6/28/22

upvoted 2 times

 **kogunribido** 1 year, 7 months ago

Appeared on exam 6/27/2022

upvoted 1 times

 **dObermannn** 1 year, 11 months ago

Selected Answer: C

C. Azure Key Vault

upvoted 3 times

🗄️ 👤 **rockethack** 1 year, 11 months ago

This question was on the exam on 18th Feb 2022.
upvoted 2 times

🗄️ 👤 **rockethack** 1 year, 11 months ago

Azure Key Vault is the correct answer
upvoted 1 times

🗄️ 👤 **Ben_Dover2** 1 year, 12 months ago

Selected Answer: C

Azure Key Vault is the correct answer
upvoted 3 times

🗄️ 👤 **KranthiChaitanya** 2 years ago

Came on exam 28/Jan/22
upvoted 1 times

🗄️ 👤 **Pravda** 2 years ago

on exam 1/6/2022 - Order is different.
upvoted 2 times

🗄️ 👤 **Pravda** 2 years ago

Option 2
<https://docs.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain-https>
upvoted 1 times

🗄️ 👤 **AidenYoukhana** 2 years ago

AZURE KEY VAULT.
upvoted 1 times

🗄️ 👤 **crawfish** 2 years, 3 months ago

C - Azure Key Vault is the correct answer.

<https://docs.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain-https>
upvoted 3 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

You have an Azure application gateway for a web app named App1. The application gateway allows end-to-end encryption. You configure the listener for HTTPS by uploading an enterprise-signed certificate. You need to ensure that the application gateway can provide end-to-end encryption for App1. What should you do?

- A. Increase the Unhealthy threshold setting in the custom probe.
- B. Enable the SSL profile to the listener.
- C. Set Listener type to Multi site.
- D. Upload the public key certificate to the HTTP settings.

Correct Answer: D

Reference:

<https://docs.microsoft.com/en-us/azure/application-gateway/end-to-end-ssl-portal>

Community vote distribution

D (100%)

 **Eitant** Highly Voted 2 years ago

Selected Answer: D

The certificate is an enterprise certificate and not a public certificate so you must upload the root certificate to the Application Gateway.

There is no typo, it's HTTP settings.

<https://docs.microsoft.com/en-us/azure/application-gateway/self-signed-certificates#upload-the-root-certificate-to-application-gateways-http-settings>

upvoted 28 times

 **derrp** 1 year, 6 months ago

For anyone doing any last minute cramming for this exam, you've likely encountered this question several times now. I immediately remember this top-voted comment above from Eitant. (Thanks dude). Pointing out that it's "HTTP settings" not being a typo - even though we're actually dealing with HTTPS helps me to remember the answer. This is for the Enterprise generated cert whereas the other version of this question uses a legitimate Certificate Authority (CA) Good luck, ya'll.

upvoted 21 times

 **daemon101** 6 months, 2 weeks ago

I'm not sure if this question still appears on the exam this year (2023) because it's now called Backend settings.

upvoted 1 times

 **Lazylinux** 6 months ago

NO you are WRONG!! it is still called HTTPS Settings, you are mixing https settings with backend settings both are different

upvoted 1 times

 **teamaws** Highly Voted 2 years, 2 months ago

Think there's a typo in answer D, should be HTTPS settings.

Under HTTPS Settings:

Choose a certificate - Select Upload a certificate.

<https://docs.microsoft.com/en-us/azure/application-gateway/create-ssl-portal#configuration-tab>

upvoted 12 times

 **Lazylinux** Most Recent 6 months ago

Selected Answer: D

There are the following settings for Https settings and NOT http as it is not secure port 80 hence don't need cert - so for https port 443 it is as per below

Https Settings

Choose a certificate (you can choose upload file or key vault if set up and preferably use key vault to manage certs)

Upload a certificate Choose a certificate from Key Vault

Cert name (here you can call it anything you like even Bill Gates!!)

PFX certificate file - if you are uploading and NOT using key vault

Password - is password for the PFX file

upvoted 1 times

 **Rajan395** 12 months ago

correct answer

upvoted 1 times

🗨️ **AdityaGupta** 1 year, 4 months ago

Selected Answer: D

You need to upload .pfx file in Http Setting.
upvoted 1 times

🗨️ **naidu** 1 year, 4 months ago

D is the right answer
upvoted 1 times

🗨️ **kogunribido** 1 year, 7 months ago

Appeared on exam 6/27/2022
upvoted 2 times

🗨️ **Edward1** 1 year, 9 months ago

Selected Answer: D

The Answer is correct.

To create a new application gateway with end-to-end TLS encryption, you'll need to first enable TLS termination while creating a new application gateway. This action enables TLS encryption for communication between the client and application gateway. Then, you'll need to put on the Safe Recipients list the certificates for the back-end servers in the HTTP settings. This configuration enables TLS encryption for communication between the application gateway and the back-end servers. That accomplishes end-to-end TLS encryption.

upvoted 4 times

🗨️ **d0bermann** 1 year, 11 months ago

Selected Answer: D

D. Upload the public key certificate to the HTTP settings
upvoted 1 times

🗨️ **rockethack** 1 year, 11 months ago

This question was on the exam on 18th Feb 2022.
upvoted 1 times

🗨️ **viva6516** 1 year, 11 months ago

To ensure that the application gateway provide end-to-end encryption, SSL must be enabled

Answer - B

upvoted 2 times

🗨️ **KranthiChaitanya** 2 years ago

Came on exam 28/Jan/22
upvoted 1 times

🗨️ **Pravda** 2 years ago

Not on exam 1/6/2022
upvoted 2 times

🗨️ **[Removed]** 2 years, 1 month ago

little confused, documentation says first enable TLS and then upload cert to listener. Is option B incorrect because it says enable SSL instead of TLS?

upvoted 2 times

🗨️ **Pravda** 2 years, 1 month ago

Web page does say to use HTTPS

<https://docs.microsoft.com/en-us/azure/application-gateway/self-signed-certificates#upload-the-root-certificate-to-application-gateways-http-settings>

upvoted 2 times

🗨️ **prepper666** 2 years, 2 months ago

Correct as described here: <https://docs.microsoft.com/en-us/azure/application-gateway/self-signed-certificates>. There is no need to upload if using a well-known certificate (public)

upvoted 5 times

🗨️ **WorkHardBeProud** 2 years, 3 months ago

Perfect !

Since the cx is using an enterprise cert which is not a public certificate that can check publicly, he needs to upload the root cert(.cer) on the HTTPS settings to help the AppGW recognize App1 in the backend.

upvoted 6 times

HOTSPOT -

You have an Azure virtual network named Vnet1 that contains two subnets named Subnet1 and Subnet2.

You have the NAT gateway shown in the NATgateway1 exhibit.

NATgateway1
NAT gateway

» [Delete](#) [Refresh](#)

^ **Essentials** [JSON View](#)

Resource group (change)	: RG1
Location	: North Europe (Zone 1)
Subscription (change)	: Subscription1
Subscription ID	: 489f2hht-se7y-987v-g571-463hw3679512
Virtual network	: Vnet1
Subnets	: 1
Public IP addresses	: 0
Public IP prefixes	: 1
Tags (change)	: Click here to add tags

You have the virtual machine shown in the VM1 exhibit.

VM1
Virtual machine

» [Connect](#) [Start](#) [Restart](#) [Stop](#) [Capture](#) [Delete](#) [Refresh](#)

^ **Essentials**

Resource group (change)	RG1	Operating system	Windows
Status	Running	Size	Standard B1s (1 vcpu, 1 GiB memory)
Location	North Europe (Zone 2)	Public IP address	
Subscription (change)	Subscription1	Virtual network/subnet	Vnet1/Subnet1
Subscription ID	489f2hht-se7y-987v-g571-463hw3679512	DNS name	
Availability zone	2		
Tags (change)	Click here to add tags		

Subnet1 is configured as shown in the Subnet1 exhibit.

Subnet1

Vnet1

Name

Subnet1

Subnet address range * ⓘ

10.100.1.0 – 10.100.1.255 (251 + 5 Azure reserved addresses)

Add IPv6 address space ⓘ

NAT gateway ⓘ

Network security group

Route table

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ

SUBNET DELEGATION

Delegate subnets to a service ⓘ

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
VM1 can communicate outbound by using NATgateway1	<input type="radio"/>	<input type="radio"/>
The virtual machines in Subnet2 communicate outbound by using NATgateway1	<input type="radio"/>	<input type="radio"/>
All the virtual machines that use NATgateway1 to connect to the internet use the same public IP address	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
VM1 can communicate outbound by using NATgateway1	<input type="radio"/>	<input checked="" type="radio"/>
The virtual machines in Subnet2 communicate outbound by using NATgateway1	<input checked="" type="radio"/>	<input type="radio"/>
All the virtual machines that use NATgateway1 to connect to the internet use the same public IP address	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: No -

VM1 is in Zone2 whereas the NAT Gateway is in Zone1. The VM would need to be in the same zone as the NAT Gateway to be able to use it. Therefore, VM1 cannot use the NAT gateway.

Box 2: Yes -

NATgateway1 is configured in the settings for Subnet2.

Box 3: No -

The NAT gateway does not have a single public IP address, it has an IP prefix which means more than one IP address. The VMs that use the NAT Gateway can use different public IP addresses contained within the IP prefix.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource>

 **AdityaGupta** Highly Voted 1 year, 4 months ago

Correct Answer: - YNN

1) NAT gateway can provide outbound connectivity for virtual machines from other availability zones different from itself. The virtual machine's subnet needs to be configured to the NAT gateway resource to provide outbound connectivity. Additionally, multiple subnets can be configured to the same NAT gateway resource.

While virtual machines in subnets from different availability zones can all be configured to a single zonal NAT gateway resource, this configuration doesn't provide the most effective method for ensuring zone-resiliency against zonal outages.

2) Subnet2 is not configured with NatGateway, refer exhibit 1, Nat Gateway is associated with only 1 subnet. In exhibit 2 it shows that Subnet 1 is associated with that Nat Gateway.

3) In exhibit 1 it shows that NAT Gateway is configured with Public IP Prefix, and outbound connection can use any Public from that prefix. It is NOT necessary to use same (one) Public IP.

upvoted 72 times

 **_cloudio_** 3 months, 4 weeks ago

Can VM1 in Subnet1 communicate outbound when no Route Table is configured?

upvoted 1 times

 **rac_sp** 11 months ago

your answers are top !

upvoted 1 times

 **jellybiscuit** Highly Voted 1 year, 3 months ago

NNN

N - The nat gateway *could have been* created to support multiple zones, but it was not. A gateway supporting all zones does not show the zone in the location field.

VM1 is located in a different zone and as a result, cannot use Natgateway1.

N - Subnet2 is not configured to use Natgateway1.

--- The screenshot of vnet1 shows that it is using Natgateway1.

--- The screenshot of NATgateway1 shows a Subnet count of 1.

--- If Subnet2 was configured to use the gateway, the Subnet count would be at least two.

N - The gateway is using a public IP prefix (instead of a single public ip address) so communication will happen over various outbound addresses.

I know we hear "tested in the lab" all the time. I actually did. I built two gateways... one in a zone, one without. I built a vnet and two subnets, one configured with the natgateway and one without.

upvoted 8 times

 **jellybiscuit** 1 year, 3 months ago

Changing my answer to YNN - sorry

<https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-availability-zones#zonal>

I was misreading this documentation - or rather, not reading far enough down.

While it says this: "When NAT gateway is deployed to a specific zone, it will provide outbound connectivity to the internet explicitly from that zone."

It also says this:

"NAT gateway can provide outbound connectivity for virtual machines from other availability zones different from itself."

Seems to contradict itself.

upvoted 15 times

 **Goofer** 1 year ago

<https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-availability-zones#single-zonal-nat-gateway-resource-for-zone-spanning-resources>

upvoted 2 times

 **sapien45** 1 year, 3 months ago

No contradiction here. YNN

It says that a ZONAL NAT gateway provides internet connectivity FROM a single zone.

It does not say TO a single zone. VMs in others zones can use that ZONAL nat gateway.

<https://azurecomcdn.azureedge.net/mediahandler/acomblog/media/Default/blog/809936d8-a658-465b-9085-f4bbae9b7e33.png>

YNN

upvoted 4 times

Bill831231 1 year, 3 months ago

seems there are two types of NAT GW deployment, zonal or regional
upvoted 1 times

Murad01 Most Recent 1 month, 3 weeks ago

Appeared on Exam November - 2023
upvoted 1 times

Lazylinux 6 months ago

YNN

1- Y - Based on this From MS

Zonal: You can place your NAT gateway resource in a specific zone for a region. When NAT gateway is deployed to a specific zone, it will provide outbound connectivity to the internet explicitly from that zone. The public IP address or prefix configured to NAT gateway must match the same zone. NAT gateway resources with public IP addresses from a different zone, zone-redundancy or with no zone aren't allowed.

NAT gateway can provide outbound connectivity for virtual machines from other availability zones different from itself. The virtual machine's subnet needs to be configured to the NAT gateway resource to provide outbound connectivity. Additionally, multiple subnets can be configured to the same NAT gateway resource.

see next post run out of buffer!!

upvoted 1 times

Lazylinux 6 months ago

continued

2- N - Subnet 2 is not associated with NATgateway1

3- N - Considering that Public IP prefixes are of CIDR /28-31 and from the question Prefix 1 /28 = 16 IPs /29 = 8 IPs /30 = 4 IPs and smallest /31 = 2 IPs

Implies CIDR /31 has 2 IP addresses available and hence outbound connection can be from any of them

upvoted 1 times

MightyMonarch74 10 months ago

YNN - Confirmed via lab

upvoted 2 times

sapien45 1 year, 4 months ago

YNN

If not Zonal NAT would have been deployed, multiple subnets can be configured to the same NAT gateway resource.

<https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource>

upvoted 3 times

sapien45 1 year, 3 months ago

NNN then as VM1 is not in the same zone as the zonal NATGTWAY

upvoted 1 times

BlackZeros 1 year, 4 months ago

Answer should be YNY.

Minimum number of PIP you need for Nat Gateway is 1 and maximum is 16.

It will work just like your home router where multiple devices are using same IP to go out. it is not one to one ratio. If Subnet1 has 50 VMs and you can only have 16 IP addresses in Nat gateway then there will be a problem (ip exhaustion) which is not the case here.

Nat Gateways can be assigned to multiple Subnets

<https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/faq#can-virtual-network-nat-gateway-be-attached-to-multiple-subnets>

upvoted 3 times

MrHabanero 1 year, 4 months ago

YNN

NAT GW is attached only to subnet1

upvoted 3 times

charlesr1700 1 year, 4 months ago

YNN

Agree with Tonys link, under the Zonal header it clearly states

'NAT gateway can provide outbound connectivity for virtual machines from other availability zones different from itself'

upvoted 1 times

TonyOmar 1 year, 4 months ago

YNN

for part 1 you can use NATgateway1 while your VM in different zone

check: <https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-availability-zones>

upvoted 2 times

zenithcsa1 1 year, 4 months ago

NNN

Only Subnet1 is connected to NATgateway1.


upvoted 2 times

zenithcsa1 1 year, 4 months ago

YNN

tested) VM in zone3 can use a NATGW in zone2. It does support outbound connectivity, while it does not guarantee availability from zone-failure.

upvoted 6 times

 **Cristoicach91** 1 year, 4 months ago

NNN. VM and NAT gate are in different zones. Subnet 2 is not using NAT gateway. NAT gateway uses a public prefix.

upvoted 3 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

You have an Azure application gateway named AppGW1 that balances requests to a web app named App1. You need to modify the server variables in the response header of App1. What should you configure on AppGW1?

- A. HTTP settings
- B. rewrites
- C. rules
- D. listeners

Correct Answer: B

Reference:

<https://docs.microsoft.com/en-us/azure/application-gateway/rewrite-http-headers-url>

Community vote distribution

B (100%)

Sarvajanik Highly Voted 2 years, 2 months ago

Application Gateway allows you to add, remove, or update HTTP request and response headers while the request and response packets move between the client and back-end pools.

Its correct

upvoted 18 times

derrp Highly Voted 1 year, 6 months ago

Cramming for this exam next week. Already seen this question countless times. As soon as I see anything that involves messing around with editing headers, I immediately think Rewrites. Hope this helps.

upvoted 15 times

iwikneerg 1 year, 5 months ago

This is the best way to approach the more confusing questions because Microsoft can only rewrite their questions so many ways :)

upvoted 6 times

drprepper_ 10 months, 3 weeks ago

Hahaha excellent, going to remember this answer now.

upvoted 1 times

Lazylinux Most Recent 6 months ago

Selected Answer: B

B is Honey and as per others comments

upvoted 1 times

Rajan395 12 months ago

correct answer

upvoted 1 times

AdityaGupta 1 year, 4 months ago

Selected Answer: B

Correct answer is B > Rewrites.

upvoted 1 times

rac_sp 1 year, 6 months ago

Selected Answer: B

rewrite

upvoted 1 times

Edward1 1 year, 9 months ago

Selected Answer: B

The Answer is correct

You use rewrite actions to specify the URL, request headers or response headers that you want to rewrite and the new value to which you intend to rewrite them to.

upvoted 2 times

dObermannn 1 year, 11 months ago

Selected Answer: B

B. rewrites

upvoted 1 times

🗨️ **rockethack** 1 year, 11 months ago

This question was on the exam on 18th Feb 2022.

upvoted 1 times

🗨️ **Ben_Dover2** 1 year, 11 months ago

Selected Answer: B

Rewriters for sure !

upvoted 2 times

🗨️ **Joshalom** 1 year, 11 months ago

on exam 6/2/2022

upvoted 1 times

🗨️ **Pravda** 2 years ago

on exam 1/6/2022

upvoted 3 times

🗨️ **AidenYoukhana** 2 years ago

REWRITES.

upvoted 1 times

🗨️ **Pravda** 2 years, 1 month ago

Question on exam 11/2021

upvoted 2 times

🗨️ **Aathithyan** 2 years, 2 months ago

Answer is correct

upvoted 3 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

You have an Azure Virtual Desktop deployment that has 500 session hosts.

All outbound traffic to the internet uses a NAT gateway.

During peak business hours, some users report that they cannot access internet resources. In Azure Monitor, you discover many failed SNAT connections.

You need to increase the available SNAT connections.

What should you do?

- A. Bind the NAT gateway to another subnet.
- B. Add a public IP address.
- C. Deploy Azure Standard Load Balancer that has outbound rules.

Correct Answer: B

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource>

Community vote distribution

B (85%)

A (15%)

 **gme999** Highly Voted 2 years, 3 months ago

Correct. Evaluate if SNAT port exhaustion should be mitigated with additional IP addresses assigned to NAT gateway resource.

<https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/troubleshoot-nat#snat-exhaustion>

upvoted 21 times

 **Ajdlfasudfo** 1 year, 1 month ago

the url changed to <https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/troubleshoot-nat-connectivity>

upvoted 3 times

 **leotoronto123** 2 years ago

Correct Answer is B.

Evaluate if SNAT port exhaustion should be mitigated with additional IP addresses assigned to NAT gateway resource.

upvoted 4 times

 **Lazylinux** Most Recent 6 months ago

Selected Answer: B

B is Honey!! Just modify the IP address Prefixes CIDR ranges from /28 - /31

/28 = 16 IPs /29 = 8 IPs /30 = 4IPs and /31 (smallest possible) = 2IPs

upvoted 2 times

 **wooyourdaddy** 10 months, 3 weeks ago

Selected Answer: B

The first scenario in the table at this link.

<https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/troubleshoot-nat-connectivity#nat-gateway-not-scaled-out-enough>

Scenario

You're experiencing contention for SNAT ports and SNAT port exhaustion during periods of high usage.

Evidence:

You run the following metrics in Azure Monitor: Total SNAT Connection Count: "Sum" aggregation shows high connection volume. For SNAT Connection Count, "Failed" connection state shows transient or persistent failures over time. Dropped Packets: "Sum" aggregation shows packets dropping consistent with high connection volume and connection failures.

Mitigation:

Add more public IP addresses or public IP prefixes as need (assign up to 16 IP addresses in total to your NAT gateway). This addition will provide more SNAT port inventory and allow you to scale your scenario further.

upvoted 3 times

 **samir111** 11 months, 2 weeks ago

Selected Answer: B

The answer is B

upvoted 1 times

 **Rajan395** 12 months ago

correct answer

upvoted 1 times

🗨️ **sapien45** 1 year, 4 months ago

Selected Answer: B

<https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/troubleshoot-nat-connectivity>

Add more public IP addresses or public IP prefixes as need (assign up to 16 IP addresses in total to your NAT gateway). This addition will provide more SNAT port inventory and allow you to scale your scenario further.

upvoted 1 times

🗨️ **AdityaGupta** 1 year, 4 months ago

Selected Answer: B

Correct Answer is B

upvoted 1 times

🗨️ **iwikneerg** 1 year, 5 months ago

<https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/troubleshoot-nat#outbound-connectivity-not-scaled-out-enough>

Determine if you can add more public IP addresses or public IP prefixes. This addition will allow for up to 16 IP addresses in total to your NAT gateway. This addition will provide more inventory for available SNAT ports (64,000 per IP address) and allow you to scale your scenario further.

upvoted 1 times

🗨️ **zerocool114** 1 year, 6 months ago

on exam today, correct answer

upvoted 1 times

🗨️ **Fearless90** 1 year, 7 months ago

Selected Answer: B

B. Add a public IP address. > Do this first since 500 session hosts

A. Bind the NAT gateway to another subnet.

upvoted 1 times

🗨️ **Fearless90** 1 year, 7 months ago

<https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/troubleshoot-nat#snat-exhaustion-due-to-nat-gateway-configuration>
SNAT exhaustion due to NAT gateway configuration

Common SNAT exhaustion issues with NAT gateway typically have to do with the configurations on the NAT gateway. Common SNAT exhaustion issues include:

- Outbound connectivity on NAT gateway not scaled out enough.
- NAT gateway's configurable TCP idle timeout timer is set higher than the default value of 4 minutes.

upvoted 2 times

🗨️ **Fearless90** 1 year, 7 months ago

<https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/troubleshoot-nat#snat-exhaustion-due-to-nat-gateway-configuration>
Outbound connectivity not scaled out enough

Each public IP address provides 64,512 SNAT ports to subnets attached to NAT gateway. From those available SNAT ports, NAT gateway can support up to 50,000 concurrent connections to the same destination endpoint. If outbound connections are dropping because SNAT ports are being exhausted, then NAT gateway may not be scaled out enough to handle the workload. More public IP addresses may need to be added to NAT gateway in order to provide more SNAT ports for outbound connectivity.

upvoted 2 times

🗨️ **Fearless90** 1 year, 7 months ago

<https://docs.microsoft.com/en-us/azure/load-balancer/troubleshoot-outbound-connection#configure-an-individual-public-ip-on-vm>

Configure an individual public IP on VM

For smaller scale deployments, you can consider assigning a public IP to a VM. If a public IP is assigned to a VM, all ports provided by the public IP are available to the VM. Unlike with a load balancer or a NAT gateway, the ports are only accessible to the single VM associated with the IP address.

We highly recommend considering utilizing NAT gateway instead, as assigning individual public IP addresses isn't a scalable solution.

upvoted 2 times

🗨️ **milan92stankovic** 1 year, 8 months ago

Selected Answer: B

B is the correct answer.

upvoted 2 times

🗨️ **d3j4n** 1 year, 7 months ago

Pozdravi Radu Manojlovic brat moj !

upvoted 5 times

🗨️ **Edward1** 1 year, 9 months ago

Selected Answer: B

B is Correct

Azure Firewall proporciona 2496 puertos SNAT por dirección IP pública configurada por instancia de conjunto de escalado de máquina virtual de back-end (mínimo de 2 instancias) y puede asociar hasta 250 direcciones IP públicas . Una mejor opción para escalar los puertos SNAT salientes es usar una NAT de Azure Virtual Network como puerta de enlace NAT. Proporciona 64 000 puertos SNAT por dirección IP pública y admite hasta 16 direcciones IP públicas, proporcionando efectivamente hasta 1 024 000 puertos SNAT salientes.

upvoted 4 times

🗨️ **mohamed1999** 1 year, 10 months ago

Selected Answer: B

Answer is B

Outbound connectivity not scaled out enough

Each public IP address provides 64,512 SNAT ports to subnets attached to NAT gateway. From those available SNAT ports, NAT gateway can support up to 50,000 concurrent connections to the same destination endpoint. If outbound connections are dropping because SNAT ports are being exhausted, then NAT gateway may not be scaled out enough to handle the workload. More public IP addresses may need to be added to NAT gateway in order to provide more SNAT ports for outbound connectivity.

upvoted 3 times

🗨️ **Kiwi28** 1 year, 10 months ago

Selected Answer: A

Hi all, I think answer is A, because of what is says here - <https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-outbound-connections#:~:text=The%20frontend%20IPs%20of%20a,load%20balancer's%20public%20IP%20address.>

Basically answer A is saying assing to a subnet, meaning bigger subnet, to increase number of available IP addresses.

Answer B says assing public IP address - not sure how this will help, as NAT gateway is already used and as such must have a public IP assigned.

upvoted 1 times

🗨️ **rockethack** 1 year, 11 months ago

This question was on the exam on 18th Feb 2022.

upvoted 1 times

🗨️ **dObermannn** 1 year, 11 months ago

Selected Answer: B

B. Add a public IP address

upvoted 1 times

🗨️ **AckeyGraham** 1 year, 11 months ago

Selected Answer: A

than out of ports

upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

You have an Azure subscription that contains the public IPv4 addresses shown in the following table.

Name	SKU	IP address assignment	Location
IP1	Basic	Static	West US
IP2	Basic	Dynamic	West US
IP3	Standard	Static	West US
IP4	Basic	Static	West US 2
IP5	Standard	Static	West US 2

You plan to create a load balancer named LB1 that will have the following settings:

- ☞ Name: LB1
- ☞ Location: West US
- ☞ Type: Public
- ☞ SKU: Standard

Which public IPv4 addresses can be used by LB1?

- A. IP1, IP3, IP4, and IP5 only
- B. IP3 only
- C. IP1 and IP3 only
- D. IP2 only
- E. IP1, IP2, IP3, IP4, and IP5
- F. IP3 and IP5 only

Correct Answer: F

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-public-ip-address>

Community vote distribution

B (95%)

5%

🗳️ **Cristoicach91** Highly Voted 1 year, 4 months ago

Selected Answer: B

Must match SKU and Region.

upvoted 27 times

🗳️ **Villaran** Highly Voted 1 year, 5 months ago

Selected Answer: B

I think it's B. IP3 only. Must match SKU and Location

upvoted 14 times

🗳️ **Lazylinux** Most Recent 6 months ago

Selected Answer: B

B is Honey and as per others comments SKU and region for IP MUST be same as LB

upvoted 2 times

🗳️ **mrgreat** 10 months ago

LB1 can use IP3 only.

Explanation:

The load balancer LB1 requires a public IP address that meets the following criteria:

Type: Public

SKU: Standard

Location: West US

Among the five public IP addresses listed in the table, only IP3 meets all these criteria.

IP1 and IP4 are located in West US and have a Basic SKU, so they cannot be used for a Standard SKU load balancer in West US.

IP2 is located in West US and has a Basic SKU, but it is a dynamic IP address, which is not supported for a load balancer.

IP5 is located in West US 2 and has a Standard SKU, but it cannot be used for a load balancer in West US.

Therefore, the only public IP address that can be used by LB1 is IP3, which has a Standard SKU, a static assignment, and is located in West US.

upvoted 3 times

🗳️ **RAN_L** 10 months, 1 week ago

Selected Answer: F

When creating a load balancer in Azure, you need to specify a public IP address to use as the frontend of the load balancer. The public IP address must be of the same SKU as the load balancer, and it can be either static or dynamic.

In this scenario, the load balancer that needs to be created is named LB1 and has the following settings:

Location: West US

Type: Public

SKU: Standard

Therefore, you can use the following public IPv4 addresses for LB1:

IP3: Standard SKU and static IP assignment, located in West US

IP5: Standard SKU and static IP assignment, located in West US 2

IP1, IP2, and IP4 are not suitable for LB1 because they have a Basic SKU, and LB1 requires a Standard SKU. Additionally, IP2 has a dynamic IP address assignment, which is not recommended for use with a load balancer.

upvoted 1 times

 **Apptech** 10 months, 2 weeks ago


Selected Answer: F

It is in Preview ... but possible

Azure Standard Load Balancer supports cross-region load balancing enabling geo-redundant High Availability scenarios

<https://learn.microsoft.com/en-us/azure/load-balancer/cross-region-overview>

upvoted 2 times

 **zcheny** 4 months, 3 weeks ago

Tested in Azure lab, you cannot assign other region's ip to a cross-region load balancing.

upvoted 2 times

 **sridot** 11 months ago

Standard Load Balancer - Equipped for load-balancing network layer traffic when high performance and ultra-low latency is needed. Routes traffic within => and across regions <=, and to availability zones for high resiliency.

<https://learn.microsoft.com/en-us/azure/load-balancer/skus>

upvoted 1 times

 **mVic** 11 months, 2 weeks ago

Selected Answer: B

Must match SKU and Region

upvoted 2 times

 **Gabaky** 11 months, 3 weeks ago

Correct Answer is F - because Standard SKU Load Balancer routes traffic within and across regions, and to Availability Zones for high resiliency.

upvoted 3 times

 **daemon101** 6 months, 2 weeks ago

The thing is, the question didn't mention that the Load balancer and IP5 are using Global tier. Therefore, I would not assume. I would still go for IP3 only.

upvoted 2 times

 **pear77777** 10 months ago

Right. Standard LB supports the Global tier for Public LBs enabling cross-region load balancing

upvoted 1 times

 **Madball** 1 year ago

Selected Answer: B

I have tested this in my lab and the correct answer is B, IP3 only.

upvoted 1 times

 **TJ001** 1 year ago


match the SKU and region Answer B

upvoted 1 times

 **sshera** 1 year ago

in exam 4jan23

upvoted 2 times

 **nikolas1234397** 1 year, 1 month ago

Selected Answer: B

Must match SKU and Region

upvoted 1 times

 **abdulmoiz** 1 year, 1 month ago

Public can't treat as static , should be IP3 only

upvoted 1 times

 **jellybiscuit** 1 year, 3 months ago

Selected Answer: B

I am only able to add public IP addresses from the same region to the load balancers I create.
upvoted 1 times

 **AdityaGupta** 1 year, 4 months ago

Selected Answer: B

Must match SKU and Region.
upvoted 3 times

 **Alessandro365** 1 year, 4 months ago

Selected Answer: B

IP3 only
upvoted 3 times

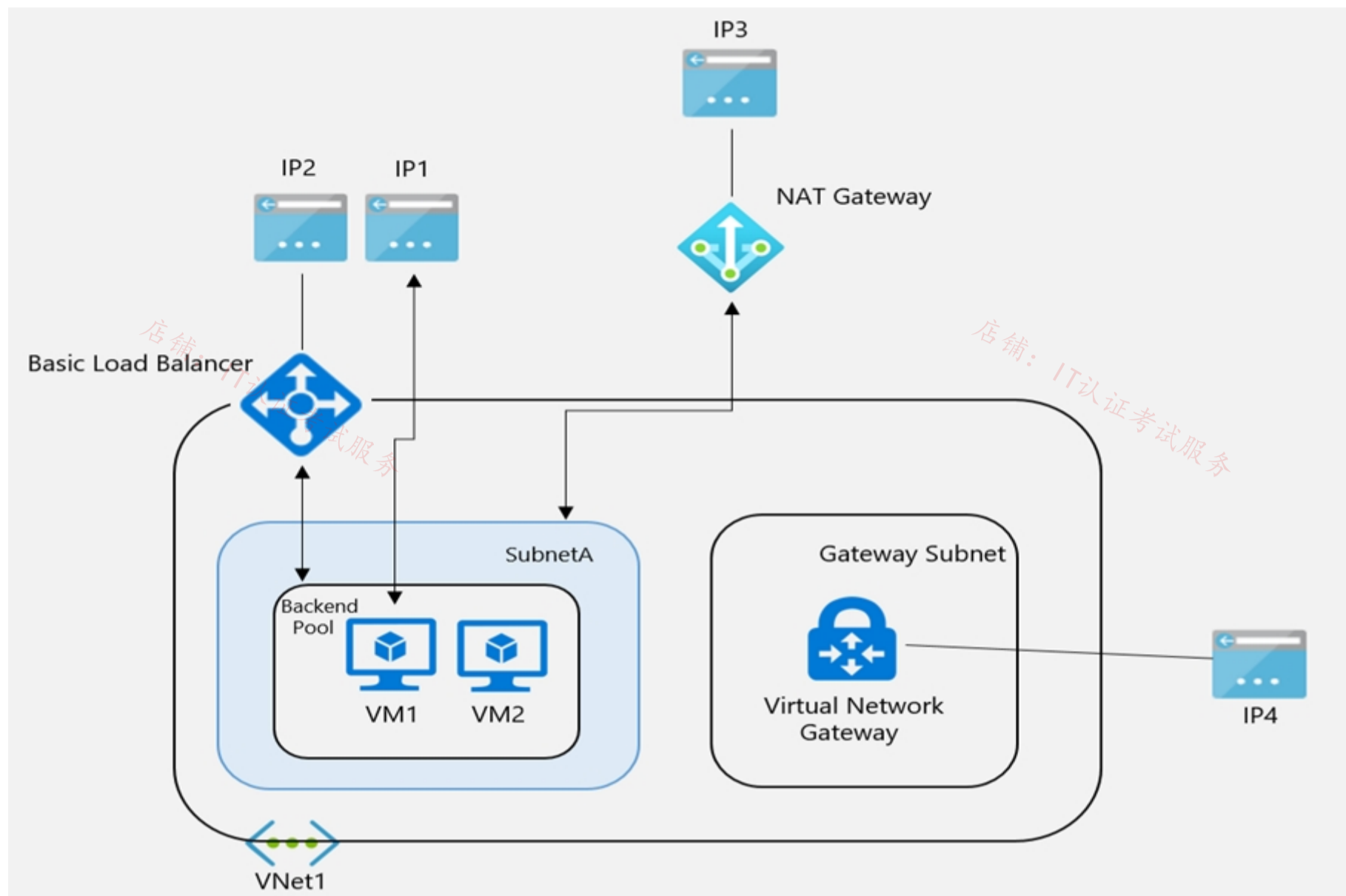
店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

You have the Azure environment shown in the exhibit.



VM1 is a virtual machine that has an instance-level public IP address (ILPIP).

Basic Load Balancer uses a public IP address. VM1 and VM2 are in the backend pool.

NAT Gateway uses a public IP address named IP3 that is associated to SubnetA.

VNet1 has a virtual network gateway that has a public IP address named IP4.

When initiating outbound traffic to the internet from VM1, which public address is used?

- A. IP1
- B. IP2
- C. IP3
- D. IP4

Correct Answer: A

Community vote distribution

C (94%)

4%

christianpageqc Highly Voted 2 years, 3 months ago

According to this article correct answer would be NAT Gateway (IP3)

<https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource#nat-and-vm-with-instance-level-public-ip>
upvoted 95 times

js_orozco 7 months, 3 weeks ago

That's right! From top to bottom preference: NAT Gateway Public IP > Backend Standard LB (with defined outbound rules) > Backed Basic Public LB > VM IL Public IP.

upvoted 1 times

christianpageqc 2 years, 3 months ago

More this <https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource#nat-and-vm-with-instance-level-public-ip-and-public-load-balancer>


Anyway the article says "On a subnet with a NAT gateway, all outbound to Internet scenarios are superseded by the NAT gateway"

upvoted 33 times

nkhan19 1 year, 12 months ago

the key is "superseded" ONLY if the traffic goes via LB else , ILPIP is prioritized.

upvoted 2 times

  **vunder** 1 year, 9 months ago

No, the article says " When NAT gateway is configured to subnets, all previous outbound configurations, such as Load balancer or instance-level public IPs (IL PIPs) are superseded and NAT gateway directs all outbound traffic to the internet. " So the correct answer is C: Ref: <https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource#connect-to-the-internet-with-nat-gateway>

upvoted 18 times

  **pear7777** 10 months ago

Another benefit of Instance-Level Public IP Address is that it is used as the Outgoing IP address of the VM when connecting to external endpoints. Since a PIP uniquely identifies a VM the receiver can easily whitelist or identify the source of the traffic. For scenarios requiring large number of outbound connections such as Web crawler, it is recommended that the VMs uses Instance-Level public IPs so that it has dedicated outbound IP for Source Network Address Translation (SNAT)

upvoted 1 times

  **Takloy** 2 years ago

This is the only explanation I need. Thanks!

upvoted 1 times

  **Bharat** 2 years, 3 months ago

I believe that you are correct.

upvoted 5 times

  **northgaterebel** Highly Voted 2 years, 2 months ago

Selected Answer: C

<https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource#nat-and-vm-with-instance-level-public-ip-and-public-load-balancer>

upvoted 13 times

  **voldemort123** Most Recent 3 months, 3 weeks ago

<https://learn.microsoft.com/en-us/azure/nat-gateway/nat-gateway-design>

"In the presence of other outbound configurations within a virtual network, such as a load balancer or instance-level public IPs (IL PIPs), the NAT gateway takes precedence for outbound connectivity"

IP3 is correct

upvoted 1 times

  **Az700crasher** 4 months, 2 weeks ago

According to Microsoft Learn, when a NAT gateway is attached to a subnet within a virtual network, the NAT gateway assumes the subnet's default next hop type for all outbound traffic directed to the internet. No extra routing configurations are required. NAT Gateway doesn't provide unsolicited inbound connections from the internet 12.

NAT gateway takes precedence over other outbound connectivity methods, including Load balancer, instance-level public IP addresses, and Azure Firewall. When NAT gateway is configured to a virtual network where a different outbound connectivity method already exists, NAT gateway takes over all outbound traffic moving forward 1.

I hope this helps!

upvoted 2 times

  **azure_dori** 5 months, 1 week ago

Selected Answer: C

C is the correct answer. <https://learn.microsoft.com/en-us/azure/nat-gateway/nat-gateway-design#connect-to-the-internet-with-a-nat-gateway>

upvoted 1 times

  **Lazylinux** 6 months ago

Selected Answer: C

I C

As per MS guidelines for outbound connections

NAT gateway takes precedence over other outbound connectivity methods, including Load balancer, instance-level public IP addresses, and Azure Firewall.

upvoted 1 times

  **Kipruto** 10 months ago

"In the presence of other outbound configurations within a virtual network, such as Load balancer or instance-level public IPs (IL PIPs), NAT gateway takes precedence for outbound connectivity. All new outbound initiated and return traffic starts using NAT gateway. There's no down time on outbound connectivity after adding NAT gateway to a subnet with existing outbound configurations." so correct answer is NAT Gateway (IP3)

upvoted 1 times

  **RockyAnil** 10 months, 1 week ago

Selected Answer: C

NAT takes precedence

upvoted 1 times



 **AzureLearner01** 10 months, 3 weeks ago

I think this question or scenario is not right. You can't add a NAT gateway to a subnet that have a load balancer with basic sku. Tried this in a lab and i needed to change the loadbalancer to standard sku with standard ip and not basic.

upvoted 1 times

  **GiorgioLDN** 11 months ago

Selected Answer: C

See the "NAT and VM with an instance-level public IP" section at:

<https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource#nat-and-vm-with-instance-level-public-ip>

upvoted 1 times

  **JennyHuang36** 11 months, 1 week ago

In exam Feb, 2023

upvoted 2 times

  **Rajan395** 12 months ago

correct answer

upvoted 1 times

  **TJ001** 1 year ago

IP3.. NAT gateway is priority

upvoted 1 times

  **zukako** 1 year ago

IP3 is correct. NAT Gateway is most prioritised.

upvoted 1 times

  **Nicolas_UY** 1 year, 1 month ago

Selected Answer: C

<https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource>

Any outbound configuration from a load-balancing rule or outbound rules is superseded by NAT gateway. The VM will also use NAT gateway for outbound. Inbound originated isn't affected. The question is for outbound, inbound will use ILPIP



upvoted 1 times

  **Nicolas_UY** 1 year, 1 month ago

Selected Answer: A

When initiating outbound traffic from VM1, the instance-level public IP address (ILPIP) of VM1 would be used. This is because the ILPIP is the public IP address associated specifically with VM1, and would be used for outbound traffic originating from that virtual machine. The public IP address associated with the Basic Load Balancer and the NAT Gateway, as well as the public IP address associated with the virtual network gateway, would not be used for outbound traffic originating from VM1.

upvoted 1 times

  **winy** 1 year, 2 months ago

Based on below

<https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource#nat-and-vm-with-an-instance-level-public-ip-and-a-standard-public-load-balancer>

"Any outbound configuration from a load-balancing rule or outbound rules is superseded by NAT gateway."

upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

You are configuring two network virtual appliances (NVAs) in an Azure virtual network. The NVAs will be used to inspect all the traffic within the virtual network.

You need to provide high availability for the NVAs. The solution must minimize administrative effort.

What should you include in the solution?

- A. Azure Standard Load Balancer
- B. Azure Application Gateway
- C. Azure Traffic Manager
- D. Azure Front Door

Correct Answer: A

Reference:

<https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/dmz/nva-ha?tabs=cli>

Community vote distribution

A (100%)

 **derrp** Highly Voted 1 year, 6 months ago

The solution must minimize administrative effort.

When it comes to the simplest solution, do you really want to be configuring a CDN (Azure Front Door), Azure Traffic Manager - with all those profiles and child profiles as we saw from the other convoluted question on this exam, or even an Azure Application Gateway (Whatever that is) Or do you want to stick with the tried and true method of just creating a Load Balancer and be done with it? Gentlemen, I think answer is obvious: Load Balancer. Hope this helps you to remember!

upvoted 16 times

 **sapien45** 1 year, 3 months ago

Your response is a lot of things ... but obvious is not one of them.

Obvious answers comes with Azure links This design uses two Azure Load Balancers to expose a cluster of NVAs to the rest of the network:

<https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/dmz/nva-ha?tabs=cli>

upvoted 7 times

 **Prutser2** 1 year, 3 months ago

id have to agree with the ever so friendly sapien45

upvoted 4 times

 **Lazylinux** Most Recent 6 months ago

Selected Answer: A

A is correct, NVA in availability set and STD LB

upvoted 1 times

 **Rajan395** 12 months ago

A is the correct answer

upvoted 1 times

 **Nicolas_UY** 1 year, 1 month ago

Selected Answer: A

To provide high availability for the NVAs and minimize administrative effort, you should include an Azure Standard Load Balancer in the solution.

The Azure Standard Load Balancer is a load balancing service that distributes incoming traffic across multiple VMs or appliances, such as the NVAs in this case. It uses a health probe to monitor the health of the VMs or appliances, and only directs traffic to healthy instances. This ensures that traffic is always directed to a healthy NVA, providing high availability for the NVAs.

Using a Standard Load Balancer also minimizes administrative effort, as it automatically distributes traffic and monitors the health of the VMs or appliances. There is no need to manually configure or manage the load balancing process.

Therefore, the correct answer is A: Azure Standard Load Balancer.


upvoted 4 times

 **AdityaGupta** 1 year, 4 months ago

Selected Answer: A

Standard load balancer is correct answer, when it comes to minimizing the efforts.

upvoted 2 times

 **naidu** 1 year, 4 months ago

A is correct.

upvoted 1 times

🗨️ **Jamesat** 1 year, 5 months ago

Selected Answer: A

Agree. Load balancer would be the simplest solution.

Also with the NVA you would be using Transport Layer addressing not Application Layer. So a standard Load Balancer would be best.

upvoted 2 times

🗨️ **Lazylinux** 6 months ago

Totally incorrect your comment regarding layer 4 - NVA can be layer 7, 3 and 4 here is comment from MS

There are many examples of NVAs, such as network firewalls, Layer-4 reverse-proxies, IPsec VPN endpoints, web-based reverse-proxies with web application firewall functionality, Internet proxies to restrict which Internet pages can be accessed from Azure, Layer-7 load balancers, and many others.

read here

<https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/dmz/nva-ha>

upvoted 1 times

🗨️ **PRABHU1993** 1 year, 5 months ago

How to get access to all questions

upvoted 1 times

🗨️ **zerocool114** 1 year, 6 months ago

on exam today

upvoted 2 times

🗨️ **unclegrandfather** 1 year, 7 months ago

Appeared on exam 6/28/22

upvoted 2 times

🗨️ **lasmus** 1 year, 8 months ago

Selected Answer: A

I think A is the correct one

upvoted 2 times

🗨️ **rockethack** 1 year, 11 months ago

This question was on the exam on 18th Feb 2022.

upvoted 2 times

🗨️ **dObermannn** 1 year, 11 months ago

Selected Answer: A

A. Azure Standard Load Balancer

upvoted 1 times

🗨️ **Kimimoto** 1 year, 11 months ago

Appeared in exam on 11/Feb/2022

upvoted 1 times

🗨️ **Contactfornitish** 2 years ago

Appeared in exam on 17/01/2022

upvoted 1 times

🗨️ **Pravda** 2 years ago

Variation on exam 1/6/2022

upvoted 3 times

🗨️ **AidenYoukhana** 2 years ago

CORRECT ANSWER: AZURE STANDARD LOAD BALANCER.

Reference: <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/dmz/nva-ha?tabs=cli>

upvoted 1 times

You have five virtual machines that run Windows Server. Each virtual machine hosts a different web app.

You plan to use an Azure application gateway to provide access to each web app by using a hostname of `www.contoso.com` and a different URL path for each web app, for example: `https://www.contoso.com/app1`.

You need to control the flow of traffic based on the URL path.

What should you configure?

- A. HTTP settings
- B. listeners
- C. rules
- D. rewrites

Correct Answer: C


Reference:


<https://docs.microsoft.com/en-us/azure/application-gateway/url-route-overview>


Community vote distribution


C (100%)


 **prepper666** Highly Voted 2 years, 2 months ago
URL path rules for routing to /app1 and /app2 etc.
upvoted 9 times


 **JMGENZOR** Highly Voted 2 years, 2 months ago
Selected Answer: C
Correct!
upvoted 9 times

 **Opala79** Most Recent 2 months, 3 weeks ago
The correct option is the B-Listeners option, in the listener you will configure which url the Application Gateway will "listen to"
upvoted 1 times

 **Lazylinux** 6 months ago
Selected Answer: C
I C
Rules manage URL path routing
upvoted 1 times

 **js_orozco** 7 months, 3 weeks ago
Correct! Only 1 path-rule is needed (associated with the 5 backend pools).
<https://learn.microsoft.com/en-us/azure/application-gateway/configuration-request-routing-rules#rule-type>
upvoted 1 times


 **Abid9** 11 months ago
Correct
upvoted 1 times

 **Nicolas_UY** 1 year, 1 month ago
Selected Answer: C
To control the flow of traffic based on the URL path, you should configure rules in the Azure application gateway.

Rules in an Azure application gateway define how incoming traffic is routed to the backend pool or target. Each rule consists of a listener, which specifies the protocol, port, and hostname to listen for, and a backend pool or target, which specifies the destination for traffic that matches the listener's criteria.

In this case, you can create a rule for each web app, specifying the hostname `www.contoso.com` and the URL path for the web app (e.g. /app1, /app2, etc.) as the listener criteria, and the corresponding virtual machine hosting the web app as the backend pool or target. This will allow you to control the flow of traffic based on the URL path, directing traffic to the appropriate virtual machine for each web app.

Therefore, the correct answer is C: rules.
upvoted 3 times

 **Prutser2** 1 year, 3 months ago
this question is around Path based routing, which can be configured under Routing Rule, answer C
upvoted 1 times

AdityaGupta 1 year, 4 months ago

Selected Answer: C

URL path rules for routing to /app1 and /app2 etc.
upvoted 1 times

Alessandro365 1 year, 4 months ago

Selected Answer: C

C = rules
upvoted 1 times

Edward1 1 year, 9 months ago

Selected Answer: C

Is Correct.
<https://docs.microsoft.com/en-us/azure/application-gateway/configuration-request-routing-rules>
upvoted 2 times

ronieto 1 year, 10 months ago

Selected Answer: C

C Rules
upvoted 2 times

dObermannn 1 year, 11 months ago

Selected Answer: C

C. rules
upvoted 2 times

rockethack 1 year, 11 months ago

This question was on the exam on 18th Feb 2022.
upvoted 1 times

Vinit_Singh 1 year, 11 months ago

Selected Answer: C

Path based routing can be configured in Routing rules
upvoted 3 times

Contactfornitish 2 years ago

Appeared in exam on 17/01/2022 with variation
upvoted 1 times

Pravda 2 years ago

on exam 1/6/2022
upvoted 3 times

店铺: IT认证考试服务

店铺: IT认证考试服务

You plan to publish a website that will use an FQDN of `www.contoso.com`. The website will be hosted by using the Azure App Service apps shown in the following table.

Name	FQDN	Location	Public IP address
AS1	As1.contoso.com	East US	131.107.100.1
AS2	As2.contoso.com	West US	131.107.200.1

You plan to use Azure Traffic Manager to manage the routing of traffic for `www.contoso.com` between AS1 and AS2.

You create a Traffic Manager profile named `TMprofile1`. `TMprofile1` uses the weighted traffic-routing method.

You need to ensure that Traffic Manager routes traffic for `www.contoso.com`.

Which DNS record should you create?

- A. two A records that map `www.contoso.com` to `131.107.100.1` and `131.107.200.1`
- B. a CNAME record that maps `www.contoso.com` to `TMprofile1.azurefd.net`
- C. a CNAME record that maps `www.contoso.com` to `TMprofile1.trafficmanager.net`
- D. a TXT record that contains a string of `as1.contoso.com` and `as2.contoso.com` in the details

Correct Answer: C

Reference:

<https://docs.microsoft.com/en-us/azure/traffic-manager/quickstart-create-traffic-manager-profile> <https://docs.microsoft.com/en-us/azure/app-service/configure-domain-traffic-manager>

Community vote distribution

C (100%)

 **Nicolas_UY** Highly Voted 1 year, 1 month ago

Selected Answer: C

To ensure that Traffic Manager routes traffic for `www.contoso.com`, you should create a CNAME record that maps `www.contoso.com` to `TMprofile1.trafficmanager.net`.

A CNAME (Canonical Name) record is a type of DNS record that maps a hostname to another hostname, rather than an IP address. When a client sends a request for the hostname specified in the CNAME record, the DNS server responds with the IP address of the target hostname.

In this case, you can create a CNAME record that maps `www.contoso.com` to `TMprofile1.trafficmanager.net`, which is the hostname of the Traffic Manager profile. This will allow clients to access the website using the hostname `www.contoso.com`, while Traffic Manager handles the routing of traffic between AS1 and AS2 based on the configured traffic-routing method.

Therefore, the correct answer is C: a CNAME record that maps `www.contoso.com` to `TMprofile1.trafficmanager.net`.

upvoted 10 times

 **jellybiscuit** Highly Voted 1 year, 3 months ago

Selected Answer: C

Correct

`azurefd.net` = Front Door

`trafficmanager.net` = Traffic Manager

upvoted 6 times

 **Murad01** Most Recent 1 month, 3 weeks ago

Appeared on Exam November- 2023

upvoted 1 times

 **Lazylinux** 6 months ago

Selected Answer: C

I C the answer

upvoted 1 times

 **CarlosBarrero** 1 year, 3 months ago

<https://vceguide.com/microsoft/az-700-designing-and-implementing-microsoft-azure-networking-solutions/>

upvoted 2 times

 **Alessandro365** 1 year, 4 months ago

Selected Answer: C

C is correct

upvoted 1 times

 **jilguens** 1 year, 4 months ago

Selected Answer: C

correct


upvoted 2 times

 **jilguens** 1 year, 4 months ago

Selected Answer: C

Correct

upvoted 2 times

 **naidu** 1 year, 4 months ago

correct

upvoted 2 times

 **Cristoicach91** 1 year, 4 months ago

correct

upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 Azure application gateway that has Azure Web Application Firewall (WAF) enabled.

You configure the application gateway to direct traffic to the URL of the application gateway.

You attempt to access the URL and receive an HTTP 403 error. You view the diagnostics log and discover the following error.

```
{
  "timeStamp": "2021-06-02T18:13:45+00:00",
  "resourceID": "/SUBSCRIPTIONS/489f2hht-se7y-987v-g571-463hw3679512/RESOURCEGROUPS/RG1/PROVIDERS/MICROSOFT.NETWORK/APPLICATIONGATEWAYS/AGW1",
  "operationName": "ApplicationGatewayFirewall",
  "category": "ApplicationGatewayFirewallLog",
  "properties": {
    "instanceId": "appgw_0",
    "clientIp": "137.135.10.24",
    "clientPort": "",
    "requestUri": "/login",
    "ruleSetType": "OWASP_CRS",
    "ruleSetVersion": "3.0.0",
    "ruleId": "920300",
    "message": "Request Missing an Accept Header",
    "action": "Matched",
    "site": "Global",
    "details": {
      "message": "Warning. Match of '\\\\\"pm AppleWebKit Android\\\\\"' against '\\\\\"REQUEST_HEADER:User-Agent\\\\\"' required. ",
      "data": "",
      "file": "rules\\REQUEST-920-PROTOCOL-ENFORCEMENT.conf",
      "line": "1247"
    },
    "hostname": "appl.contoso.com",
    "transactionId": "f7546159yhjk7wal14568if5131t68h7",
    "policyId": "default",
    "policyScope": "Global",
    "policyScopeName": "Global",
  }
}
```

You need to ensure that the URL is accessible through the application gateway from any IP address.

Solution: You create a WAF policy exclusion for request headers that contain 137.135.10.24.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

The log shows that WAF rule with ruleId 920300 was triggered. Instead we should disable the WAF rule that has a ruleId 920300.

Reference:

<https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/web-application-firewall-troubleshoot>

Community vote distribution

B (100%)

 **flurgen248** 10 months, 2 weeks ago

Selected Answer: B

<https://learn.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-monitor?pivots=front-door-standard-premium#waf-logs>

Client IP is the IP address of the client that made the request. If there was an X-Forwarded-For header in the request, the client IP address is taken from that header field instead.

There wasn't an X-Forwarded-For header, so it is your IP address. Creating a WAF exclusion would allow you to connect, but that is not the goal. Any connections from a different IP would still get the 403 error.

The answer is No.
upvoted 1 times

 **daemon101** 6 months, 2 weeks ago

Agree. The requirement is "You need to ensure that the URL is accessible through the application gateway from any IP address".
upvoted 1 times


 **Nicolas_UY** 1 year, 1 month ago

Selected Answer: B

B. No

Creating a WAF policy exclusion for request headers that contain 137.135.10.24 will not ensure that the URL is accessible through the application gateway from any IP address. Instead, you should check the WAF rules and policy settings to ensure that the IP address or range of IP addresses from which you are trying to access the URL is not being blocked by the WAF. You may also need to check the access control lists (ACLs) and network security groups (NSGs) associated with the application gateway to ensure that traffic from the desired IP addresses is allowed.

upvoted 2 times

 **DeepMoon** 1 year, 4 months ago

Given Answer is Correct:

Disabling a client IP for missing an Accept Header is definitely not the answer.

upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT -

Your company has 10 instances of a web service. Each instance is hosted in a different Azure region and is accessible through a public endpoint.

The development department at the company is creating an application named App1. Every 10 minutes, App1 will use a list of endpoints and connect to the first available endpoint.

You plan to use Azure Traffic Manager to maintain the list of endpoints.

You need to configure a Traffic Manager profile that will minimize the impact of DNS caching.

What should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Traffic Manager algorithm:

	▼
Geographic	
Multivalued	
Priority	
Subnet	

Endpoint type:

	▼
Azure endpoint	
External endpoint	
Nested endpoint	

Answer Area

Traffic Manager algorithm:

	▼
Geographic	
Multivalued	
Priority	
Subnet	

Correct Answer:

Endpoint type:

	▼
Azure endpoint	
External endpoint	
Nested endpoint	

Reference:

<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods> <https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-endpoint-types>

🗨️ **VonKellus** Highly Voted 1 year, 9 months ago

The Multivalue traffic-routing method allows you to get multiple healthy endpoints in a single DNS query response. This configuration enables the caller to do client-side retries with other endpoints in case a returned endpoint being unresponsive. This pattern can increase the availability of a service and reduce the latency associated with a new DNS query to obtain a healthy endpoint. MultiValue routing method works only if all the endpoints of type 'External' and are specified as IPv4 or IPv6 addresses. When a query is received for this profile, all healthy endpoints are returned and are subject to a configurable maximum return count.

upvoted 23 times

🗨️ **Bon_** 1 year, 5 months ago

Your statement is correct.

We know it's external endpoint due to the key word "...accessible through a public endpoint"

<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-configure-multivalue-routing-method#add-traffic-manager-endpoint>

"At this time adding endpoints using IPv4 or IPv6 addresses is supported only for endpoints of type External and hence MultiValue routing is also supported only for such endpoints." Therefore the other endpoints including Azure endpoint are not an option. Simple process of elimination.

upvoted 3 times

🗨️ **wmohsen** Highly Voted 1 year, 9 months ago

Has to be Azure endpoints?

<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-endpoint-types>

upvoted 8 times

🗨️ **pinpin06** 1 year, 9 months ago

- Azure endpoints are used for services hosted in Azure.
- External endpoints are used for services hosted outside Azure, either on-premises or with a different hosting provider.
- Nested endpoints are used to combine Traffic Manager profiles to create more flexible traffic-routing schemes to support the needs of larger, more complex deployments.

as per the following I assume we are talking about azure endpoints, not external endpoints

upvoted 7 times

🗨️ **Dean208** 1 year, 7 months ago

I have tested it in the Azure Portal. If you try to use Azure endpoint you get error ..."MultiValue profiles cannot have endpoint with domain names, Azure endpoints or nested endpoints as targets"

upvoted 6 times

🗨️ **Lazylinux** Most Recent 2 months, 2 weeks ago

Given answer is correct

Multivalue Routing traffic as per

<https://learn.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods>

External Endpoint as per

<https://learn.microsoft.com/en-us/azure/traffic-manager/traffic-manager-endpoint-types>

upvoted 1 times

🗨️ **bakamon** 8 months ago

:: Multivalue

:: External endpoint

sidhi baat no bakwas

upvoted 3 times

🗨️ **sapien45** 1 year, 4 months ago

The Multivalue traffic-routing method allows you to get multiple healthy endpoints in a single DNS query response. This configuration enables the caller to do client-side retries with other endpoints in case a returned endpoint being unresponsive. This pattern can increase the availability of a service and reduce the latency associated with a new DNS query to obtain a healthy endpoint. MultiValue routing method works only if all the endpoints of type 'External' and are specified as IPv4 or IPv6 addresses.

<https://learn.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods>

upvoted 2 times

🗨️ **1particle** 1 year, 5 months ago

Multivalue and External Endpoint

<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-configure-multivalue-routing-method#add-traffic-manager-endpoints>

upvoted 3 times

🗨️ **Fearless90** 1 year, 7 months ago

Traffic Manager algorithm > Multivalue

Endpoint type > External endpoint

minimize the impact of DNS caching

upvoted 4 times

🗨️ **Fearless90** 1 year, 7 months ago

<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods#multivalue-traffic-routing-method>

Multivalue traffic-routing method

The Multivalue traffic-routing method allows you to get multiple healthy endpoints in a single DNS query response. This configuration enables the caller to do client-side retries with other endpoints in case a returned endpoint being unresponsive. This pattern can increase the

availability of a service and reduce the latency associated with a new DNS query to obtain a healthy endpoint. MultiValue routing method works only if all the endpoints of type 'External' and are specified as IPv4 or IPv6 addresses. When a query is received for this profile, all healthy endpoints are returned and are subject to a configurable maximum return count.

upvoted 1 times

🗨️ 👤 **unclegrandfather** 1 year, 7 months ago

Appeared on exam Jun/28/22

upvoted 2 times

🗨️ 👤 **kogunribido** 1 year, 7 months ago

Appeared on exam 6/27/2022

upvoted 1 times

🗨️ 👤 **milan92stankovic** 1 year, 8 months ago

I think the answer is correct.

Multivalued is the only option that will return the list of the endpoints, which is the requirement. However, you cannot use Azure endpoints with a multivalued routing algorithm and also you are reaching out to all the WebApps from the "outside".

upvoted 5 times

🗨️ 👤 **Whatsamattr81** 1 year, 8 months ago

Has to be multi value which only seems to work with external (and not azure endpoints)

upvoted 3 times

🗨️ 👤 **RVR** 1 year, 8 months ago

The catch is that " minimize the impact of DNS caching" and when we select Multivalued it clearly says "MultiValue routing method works only if all the endpoints of type 'External' and are specified as IPv4 or IPv6 addresses"

upvoted 5 times

🗨️ 👤 **jkklm** 1 year, 9 months ago

Endpoint : Azure endpoint

<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-endpoint-types#:~:text=Azure%20endpoints%20are%20used%20for,with%20a%20different%20hosting%20provider.>

upvoted 2 times

🗨️ 👤 **Kay04** 1 year, 9 months ago

i think it has to be azure end point, as the services are hosted in Azure

Azure endpoints are used for services hosted in Azure.

External endpoints are used for IPv4/IPv6 addresses, FQDNs, or for services hosted outside Azure. These services can either be on-premises or with a different hosting provider.

Nested endpoints are used to combine Traffic Manager profiles to create more flexible traffic-routing schemes to support the needs of larger, more complex deployments.

upvoted 2 times

🗨️ 👤 **anwar1** 1 year, 8 months ago

"Instances are hosted in Azure but are accessible via public endpoints". Hence External endpoints.

upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

DRAG DROP -

You have an Azure Front Door instance named FrontDoor1.

You deploy two instances of an Azure web app to different Azure regions.

You plan to provide access to the web app through FrontDoor1 by using the name app1.contoso.com.

You need to ensure that FrontDoor1 is the entry point for requests that use app1.contoso.com.

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.

Select and Place:

Actions

- Add a custom domain to FrontDoor1.
- Add a PTR record to DNS.
- Add a rules engine configuration to FrontDoor1.
- Add a routing rule to FrontDoor1.
- Add a CNAME record to DNS.

>

<

Answer Area

- ↑
- ↓

Correct Answer:

Actions

-
- Add a PTR record to DNS.
- Add a rules engine configuration to FrontDoor1.
-
-

>

<

Answer Area

- Add a CNAME record to DNS.
- Add a custom domain to FrontDoor1.
- Add a routing rule to FrontDoor1.

Reference:

- <https://docs.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain#associate-the-custom-domain-with-your-front-door>
- <https://docs.microsoft.com/en-us/azure/frontdoor/quickstart-create-front-door>

- tartarus23** Highly Voted 1 year, 6 months ago

 1. Add a CNAME record to DNS
 2. Add a custom domain to FrontDoor1
 3. Add a routing rule to FrontDoor1

Cname record to DNS for frontdoor to verify and then you can add the custom domain followed by the routing rule to app1.contoso.com

upvoted 25 times
- jkklm** Highly Voted 1 year, 9 months ago

above is correct as done in labs

upvoted 6 times
- jkklm** 1 year, 9 months ago

add cname to dns ==> add them externally eg in godaddy

upvoted 4 times
- Lazylinux** Most Recent 2 months, 2 weeks ago

Given answer is correct and sequence/steps is correct

upvoted 1 times
- Skankhunt** 12 months ago

I agree answer is correct, however wouldn't it be better to structure the sequence:

- 1) Add a custom domain to FrontDoor1
- 2) Add a routing rule to FrontDoor1
- 3) Add a CNAME record to public DNS

That way as soon as traffic is routed to FrontDoor1 it's already configured and running.

Or we could just say it takes some time for the new public DNS record to properly propagate, which gives the admin enough time to configure FrontDoor1

upvoted 1 times

  **Skankhunt** 12 months ago

LoL never mind, the next question explains why DNS record should be step1 xD

upvoted 4 times

  **zerocool114** 1 year, 6 months ago



on exam today

upvoted 4 times

  **Whatsamattr81** 1 year, 8 months ago

cname for your custom domain to the given name for your front door instance, assign that custom domain to front door, tell front door where to route to

upvoted 3 times

  **HTD** 1 year, 9 months ago

Custom rule , routing and then CNAME should be the order.

upvoted 3 times

  **alexbic1890** 1 year, 8 months ago

The answer is correct.

"Before you can use a custom domain with your Front Door, you must first create a canonical name (CNAME) record with your domain provider to point to your Front Door's default frontend host... After Front Door verifies the CNAME record that you create, traffic addressed to the source custom domain ... is routed to the specified destination Front Door default frontend host..."

From: <https://docs.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain>

upvoted 4 times

  **examlearner** 1 year, 8 months ago

Hi do you have contributor access ?

upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

You have a website that uses an FQDN of `www.contoso.com`. The DNS record for `www.contoso.com` resolves to an on-premises web server. You plan to migrate the website to an Azure web app named `Web1`. The website on `Web1` will be published by using an Azure Front Door instance named `ContosoFD1`. You build the website on `Web1`. You plan to configure `ContosoFD1` to publish the website for testing. When you attempt to configure a custom domain for `www.contoso.com` on `ContosoFD1`, you receive the error message shown in the exhibit. (Click the Exhibit tab.)

Add a custom domain

Add a custom domain to your Front Door. Create a DNS mapping from your custom domain to the Front Door `azurefd.net` frontend host with your DNS provider. [Learn more](#)

Frontend host end

ContosoFD1.azurefd.net

Custom host name *

www.contoso.com

✘ A CNAME record for `www.contoso.com` that points to `ContosoFD1.azurefd.net` could not be found. Before you can associate a domain with this Front Door, you need to create a CNAME record with your DNS provider for `'www.contoso.com'` that points to `'ContosoFD1.azurefd.net'`.

You need to test the website and `ContosoFD1` without affecting user access to the on-premises web server. Which record should you create in the `contoso.com` DNS domain?

- A. a CNAME record that maps `afdverify.www.contoso.com` to `ContosoFD1.azurefd.net`
- B. a CNAME record that maps `www.contoso.com` to `ContosoFD1.azurefd.net`
- C. a CNAME record that maps `afdverify.www.contoso.com` to `afdverify.ContosoFD1.azurefd.net`
- D. a CNAME record that maps `www.contoso.com` to `Web1.contoso.com`

Correct Answer: C

Reference:

<https://docs.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain#map-the-temporary-afdverify-subdomain>

Community vote distribution

C (94%)

6%

pinpin06 Highly Voted 1 year, 9 months ago

Selected Answer: C

response C: "You need to test the website and `ContosoFD1` without affecting user access to the on-premises web server." `afdverify` permits to do it without impact.

upvoted 5 times

Murad01 Most Recent 1 month, 3 weeks ago

Appeared on Exam November -2023

upvoted 1 times

Lazylinux 5 months, 3 weeks ago

Selected Answer: C

I C is the answer as per link below

<https://learn.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain>

upvoted 1 times

JennyHuang36 11 months, 1 week ago

In exam Feb,2023

upvoted 4 times

🗨️ **DeepMoon** 1 year, 4 months ago

Production site www.contoso.com is mapped to on-prem server.
Future production site would map www.contoso.com to ContosoFD1.azurefd.net, which then would point to Azure WebApp named web1.
Before you can do this you need to test while current production (on-prem) server and its current DNS mapping untouched.
Your test site afdverify.www.contoso.com is mapped to afdverify.contosofd1.azurefd.net which is pointing to Azure WebApp.
Now when you send all your DNS traffic to afdverify.www.contoso.com it ends in Azure Web App that is being tested.

upvoted 3 times

🗨️ **Mike2020** 1 year, 5 months ago

Selected Answer: C

Answer is correct. This is to map the custom domain while registering to the Azure portal without affecting Web traffic traffic ...

With this method, users can access your domain without interruption while the DNS mapping occurs.

<https://docs.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain#map-the-temporary-afdverify-subdomain%20Community%20vote%20distribution>

upvoted 4 times

🗨️ **whiteherondance** 1 year, 9 months ago

Selected Answer: C

"...You need to test the website and ContosoFD1 *without affecting user access to the on-premises web server.*"

Answer is C - read the provided document in the answer, it explains why. B would interrupt user access to on-prem server.

upvoted 3 times

🗨️ **frks** 1 year, 9 months ago

Selected Answer: C

Ignore my previous comment. New domain -> create cname directly, existing production domain --> afdverify

upvoted 2 times

🗨️ **frks** 1 year, 9 months ago

Selected Answer: B

afdverify is useless in this scenario

upvoted 1 times

🗨️ **Ochman** 1 year, 9 months ago

The answer is B

upvoted 1 times

🗨️ **HTD** 1 year, 9 months ago

As per microsoft document reference this is a correct answer.

upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

You have the Azure load balancer shown in the Load Balancer exhibit.

LB2
Load balancer

Move Delete Refresh

Essentials [JSON View](#)

Resource group (change)
RG1

Location
North Europe

Subscription (change)
Subscription1

Subscription ID
169d1bba-ba4c-471c-b513-092eb7063265

SKU
Standard

Tags (change)
[Click here to add tags](#)

Backend pool
LB2-BEP1 (2 virtual machines)

Load balancing rule
-

Health probe
-

NAT rules
0 inbound

Public IP address
20.82.214.15 (LB2-IP1)

LB2 has the backend pools shown in the Backend Pools exhibit.

LB2 | Backend pools
Load balancer

Add Refresh

Filter by name...

Backend pool == all Resource Name == all Resource Status == all IP address == all
Network interface == all Availability zone == all

Group by Backend pool

Backend pool	Resource Name	Resource Status	IP address	Network interface	Availability zone
LB2-BEP1	VMSS1 (instance 2)	Running	10.0.0.6	RG1-vnet-nic01	
LB2-BEP1	VMSS1 (instance 3)	Running	10.0.0.7	RG1-vnet-nic01	

You need to ensure that LB2 distributes traffic to all the members of VMSS1.

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

NOTE: Each correct selection is worth one point.

- A. Add a network interface to VMSS1.
- B. Add a load balancing rule.
- C. Configure a health probe.

D. Add a public IP address to each member of VMSS1.

Correct Answer: BC

Reference:

<https://docs.microsoft.com/en-us/azure/load-balancer/quickstart-load-balancer-standard-public-portal?tabs=option-1-create-load-balancer-standard>

Community vote distribution

BC (100%)

 **HTD** Highly Voted 1 year, 9 months ago

This is correct. Health Probe and a rule is missing in the configuration.
upvoted 6 times


 **Lazylinux** Most Recent 5 months, 3 weeks ago

Selected Answer: BC

BC- Yes load Bal rule and health probe needed
upvoted 1 times

 **JennyHuang36** 11 months, 1 week ago

In exam Feb, 2023
upvoted 4 times

 **staffo** 11 months, 2 weeks ago

Should it not be A and B? You need to assign different NIC's to machines for it to work.
I don't think C is needed. The question does not reference anything about distributing to healthy servers only, just distributing the traffic evenly.
upvoted 1 times

 **TJ001** 1 year ago

Typical configuration...BC correct
upvoted 2 times

 **vivikar** 1 year ago

Answer: BC
B - configure the load balancing rule, which maps the frontend IP with backend Pool.
C - monitor the Backend pools
upvoted 4 times

 **DeepMoon** 1 year, 1 month ago

Can anybody explain why BC is correct. Instead of just religiously repeating the mantra 'it is correct'.
Any reference docs?
upvoted 1 times

 **[Removed]** 1 year ago

You have an explanation in the docs posted in the answer, which says:
During the creation of the load balancer, you'll configure:
Frontend IP address
Backend pool
Inbound load-balancing rules
Health probe
upvoted 1 times

 **Alessandro365** 1 year, 4 months ago


Selected Answer: BC

BC is correct
upvoted 3 times

 **jilguens** 1 year, 4 months ago


Selected Answer: BC

correct
upvoted 1 times

 **Hermi** 1 year, 6 months ago

Selected Answer: BC

Correct
upvoted 2 times

 **d3j4n** 1 year, 7 months ago

Correct !
upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

You have an Azure subscription that contains the following resources:

- ☞ A virtual network named Vnet1
- ☞ Two subnets named subnet1 and AzureFirewallSubnet
- ☞ A public Azure Firewall named FW1
- ☞ A route table named RT1 that is associated to Subnet 1
- ☞ A rule routing of 0.0.0.0/0 to FW1 in RT1

After deploying 10 servers that run Windows Server to Subnet 1, you discover that none of the virtual machines were activated.

You need to ensure that the virtual machines can be activated.

What should you do?

- A. On FW1, configure a DNAT rule for port 1688.
- B. Deploy an application security group that allows outbound traffic to 1688.
- C. On FW1, create an outbound network rule that allows traffic to the Azure Key Management Service (KMS).
- D. On FW1, create an outbound service tag rule for Azure Cloud.

Correct Answer: C

Cause -

The Azure Windows VMs need to connect to the Azure KMS server for Windows activation. The activation requires that the activation request come from an Azure public IP address.

To resolve this problem, use the Azure custom route to route activation traffic to the Azure KMS server.

Reference:

<https://docs.microsoft.com/en-us/troubleshoot/azure/virtual-machines/custom-routes-enable-kms-activation>

Community vote distribution

C (100%)

🗳️ 👤 **Lazylinux** 5 months, 3 weeks ago

Selected Answer: C

I C the answer

Azure uses different endpoints for KMS (Key Management Services) activation depending on the cloud region where the VM resides. When using this troubleshooting guide, use the appropriate KMS endpoint that applies to your region.

Azure public cloud regions: kms.core.windows.net:1688 or azkms.core.windows.net:1688

Azure China 21Vianet national cloud regions: kms.core.chinacloudapi.cn:1688 or azkms.core.chinacloudapi.cn:1688

Azure Germany national cloud regions: kms.core.cloudapi.de:1688

Azure US Gov national cloud regions: kms.core.usgovcloudapi.net:1688

upvoted 2 times

🗳️ 👤 **TJ001** 1 year ago

Correct Answer C

upvoted 1 times

🗳️ 👤 **MariusFlorea99** 1 year, 3 months ago

Correct answer C - one of the main causes of activation failure is firewall blocking outbound access to kms.core.windows.net:1688 (Azure KMS)

upvoted 1 times

🗳️ 👤 **sapien45** 1 year, 4 months ago

Selected Answer: C

Understanding Azure KMS endpoints for Windows product activation of Azure Virtual Machines

Azure uses different endpoints for KMS (Key Management Services) activation depending on the cloud region where the VM resides

<https://learn.microsoft.com/en-us/troubleshoot/azure/virtual-machines/troubleshoot-activation-problems>

upvoted 2 times

🗳️ 👤 **BlackZeros** 1 year, 4 months ago

Selected Answer: C

C seems correct

upvoted 1 times

 **Alessandro365** 1 year, 4 months ago

Selected Answer: C

C is correct

upvoted 1 times

店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

You have an Azure Front Door instance that has a single frontend named Frontend1 and an Azure Web Application Firewall (WAF) policy named Policy1. Policy1 redirects requests that have a header containing "string1" to <https://www.contoso.com/redirect1>. Policy1 is associated to Frontend1.

You need to configure additional redirection settings. Requests to Frontend1 that have a header containing "string2" must be redirected to <https://www.contoso.com/redirect2>.

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

NOTE: Each correct selection is worth one point.

- A. Create a custom rule.
- B. Create a policy.
- C. Create a frontend host.
- D. Configure a managed rule.
- E. Add a custom rule to Policy1.
- F. Create an association.

Correct Answer: CEF

E: A WAF policy consists of two types of security rules:
custom rules that are authored by the customer.

managed rule sets that are a collection of Azure-managed pre-configured set of rules.

You can create a fully customized policy that meets your specific application protection requirements by combining managed and custom rules.

A web application delivered by Front Door can have only one WAF policy associated with it at a time.

CF: We create a frontend host and associate it with the Policy.

In the Association tab of the Create a WAF policy page, select + Associate a Front Door profile, enter the following settings, and then select Add:

Associate a Front door profile ×

Front door profiles can be added and removed after a WAF policy is created.

Front door profile * ⓘ

contosoafd ▼

Domain

Multiple domains can be associated with a front door profile. Select those you want your WAF policy to apply to.

Domain *

contosoafd1 ▼

Add
Cancel

Reference:

<https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/afds-overview> <https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-create-portal>

Community vote distribution

ABF (60%)

AEF (23%)

Other

 **Villaran** Highly Voted 1 year, 4 months ago

Selected Answer: ABF

I think the order is:

- B. Create a policy.
- A. Create a custom rule.
- F. Create an association.

upvoted 23 times

  **siddique12345** 2 months, 1 week ago

CEF is correct. One frontend host can have only one WAF policy associated. One WAF policy can be associated with multiple Frontend host. Tested in my lab.

upvoted 1 times

  **wooyourdaddy** Highly Voted  10 months ago

Selected Answer: AEF

At this link:

<https://learn.microsoft.com/en-us/azure/web-application-firewall/afds/afds-overview#waf-policy-and-rules>

It states:

A web application delivered by Front Door can have only one WAF policy associated with it at a time.

Since the question states "Policy1 is associated to Frontend1.", this eliminates option B.

The question also states: "Requests to Frontend1 that have a header containing "string2" must be redirected to https://www.contoso.com/redirect2.", which tells us that we don't need a new frontend. So option C is eliminated.

At the above link, it also states: "managed rule sets that are a collection of Azure-managed pre-configured set of rules." Since we are targeting a specific value of "string2", this option would be eliminated.

That leaves us with only AEF as possible answers.

upvoted 9 times

  **Apptech** 9 months, 2 weeks ago

If we use existing Policy1 instead of creating a new one, we can assume that it has already an association to Frontend1. So F is no possible answer.

upvoted 2 times

  **ironbornson** 3 months, 3 weeks ago

From the question: "Policy1 is associated to Frontend1".

I am missing something?

upvoted 1 times

  **ironbornson** 3 months, 2 weeks ago

Sorry, ignore my comment. I missread yours. Admin please delete my coment and the previous answer. Thx

upvoted 1 times

  **Lazylinux** Most Recent  2 months, 1 week ago

Selected Answer: ABC

The following points apply

- You can ONLY apply one WAF policy per AFD domain (Endpoint)
- WAF Policy can ONLY have ONE redirection that is configured at the Policy settings and hence if you have two different redirections which is the case in this question than you will need two different WAF policies
- Independent Association Action is NOT needed here as when you create WAF policy it will require you to chose the appropriate Endpoint (Domain and hence you are associating the WAF policy) [Note: any Endpoint that already has WAF policy applied to it will NOT be present and hence New Endpoint-Domain is required]

upvoted 1 times

  **Lazylinux** 2 months, 1 week ago

Following on from previous

- Within the Policy you create custom rule with the appropriate re-direction settings - such as Match rule type, Priority, condition IF match type => choose String => Match variable "RequestHeader", Header name, Operation IS, Operator CONTAINS, Transformation => Lower Case, Match value "string2", THEN => Redirect Traffic (this setting is taken from Policy Settings which is Global to the policy) Once Done click OK and SAVE
- Associations can be check from the Associations option under settings and as I said is automatically once the Policy is created, if you need add new one then first you need NEW DOMAIN as the existing once will be grayed out if already associated with WAF policy

upvoted 2 times

  **Lazylinux** 2 months, 1 week ago

Following on from previous

- The ONLY thing that was NOT mentioned in the question and is Definitely NEEDED is the ROUTING RULE (ROUTES), because when you create NEW Endpoint (Domain) you need routing rule to be associated with it. However you can still use the same backend (origin group) and the origin (Backend instance)

- Option D – NOT at all

upvoted 1 times

  **Lazylinux** 2 months, 1 week ago

- Option E - Yes you can add custom rule and configure accordingly for STRING2, however the re-redirect Option is Global to the policy and done via Policy settings and since we already have one i.e. STRING1, the it will redirect to (https://www.contoso.com/redirect1.) and NOT as per requirement (https://www.contoso.com/redirect2)
- Option F – this is NOT required as this is done by default then you first create WAF Policy, it will force you to associate with Endpoint (Domain)

Therefore Based on the above and been tested I would chose ABC which I can see no one else chose!!

upvoted 1 times

  **roshingr** 7 months, 3 weeks ago

The three actions you should perform to configure the additional redirection settings are:

A. Create a custom rule: This custom rule will define the condition for redirecting requests that have a header containing "string2" to the desired URL. Custom rules allow you to define specific behavior based on your requirements.

E. Add a custom rule to Policy1: Once you have created the custom rule, you need to add it to Policy1. This ensures that the new rule is part of the policy and will be applied to the incoming requests.

F. Create an association: To apply the updated Policy1 to Frontend1, you need to create an association between the policy and the frontend. This ensures that the policy is enforced for requests coming through Frontend1.

So, the correct actions to configure the additional redirection settings would be:

- A. Create a custom rule.
- E. Add a custom rule to Policy1.
- F. Create an association.

upvoted 5 times

  **GBAU** 3 months ago

In the question "Policy1 is associated to Frontend1", so F does not apply.

upvoted 1 times

  **hal01** 9 months, 2 weeks ago

Selected Answer: ABE

To configure additional redirection settings to redirect requests to Frontend1 that have a header containing "string2" to <https://www.contoso.com/redirect2>, you should perform the following three actions:

B. Create a policy: If you haven't created a policy already, create a new Azure Web Application Firewall (WAF) policy named Policy1.

A. Create a custom rule: Create a custom rule in Policy1 to redirect requests that have a header containing "string2" to <https://www.contoso.com/redirect2>.

E. Add a custom rule to Policy1: Add the custom rule created in the previous step to Policy1.

The other options listed are not required for this scenario:

C. Create a frontend host: A frontend host is not required since Frontend1 already exists.

D. Configure a managed rule: Managed rules are not required for this scenario.

F. Create an association: An association is not required since Policy1 is already associated with Frontend1.

upvoted 3 times

  **_fvt** 9 months, 3 weeks ago

Not C - You need to use Frontend 1

Not D - Not sure what it is, probably microsoft WAF policy managed rules which will no helps in our case

Not E - You cannot have two different redirect URLs in the same WAF policy, even in different rules (tested in lab)

F - you cannot create an association to the same route which would likely needs be /* there as asked in this scenario, so you are blocker with only 1 WAF policy...

You can create a policy and a custom rule but not associate it...

I think this question is outdated, WAF policies are not meant to be used for redirect. Normally for this you just a create a Frond Door rule set with all your conditions and rediects and that's it.

upvoted 2 times

  **mrgreat** 10 months ago

To configure additional redirection settings, you should perform the following three actions:

A. Create a custom rule that matches requests with a header containing "string2".

E. Add a custom rule to Policy1 that redirects requests that match the custom rule to <https://www.contoso.com/redirect2>.

F. Create an association between Frontend1 and Policy1.

Therefore, the correct answer is: A, E, F.

upvoted 2 times

  **breakpoint0815** 10 months ago

Selected Answer: AEF

You already have a Policy1, no need to create a new one (= not B)

You already have a Frontend Host, Frontend1 (= Not C)


You need to deploy a custom rule (=Not D)

upvoted 2 times

  **Apptech** 9 months, 2 weeks ago

For Policy1 we also have an association to Frontend1 ...

upvoted 2 times

  **Apptech** 10 months, 2 weeks ago

The text clearly says:

1. Requests to Frontend1 that have a header containing "string2" must be redirected
2. Frontend1 already has a policy assigned.

Because of the fact that you cannot add more than 1 policy to frontend1 it makes no sense to create a second policy.

For that reason my vote is CEF

upvoted 1 times

  **Apptech** 9 months, 2 weeks ago

I have to add that option F don't make sense in that scenario because Policy 1 must have an association to Frontend1

upvoted 1 times

  **DeepMoon** 1 year ago

<https://learn.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-create-portal>>

This link clearly states the 3 steps.

1. Create a WAF policy
2. Associate it with a frontend host
3. Configure WAF rules

So answers are C. E .F.

upvoted 1 times

  **jotajotajeje** 1 year, 2 months ago

Selected Answer: ABF

the question itself makes no sense as already have the policy1 created hence the available options tends you to do the all process again.

B. Create a policy.

A. Create a custom rule.

F. Create an association.

But if you already have the policy created would be just to Create a custom rule, as you are already using the same domain...

upvoted 2 times

  **Ajdlfasudfo** 1 year, 1 month ago

this is incorrect. You can only define one redirect URL per policy. That's why you need a new policy.

upvoted 3 times

  **Prutser2** 1 year, 3 months ago

Selected Answer: CEF

i tend to agree with provided answer: cef, first of all we need a new front end to allow the redirected traffic to, the new front end is www.contoso.com/redirect2.

question clearly stated a redirect when hitting frontend1, and policy1, so policy1 needs changing: add custom rule to policy 1. then finally associate

upvoted 4 times

  **BlackZeros** 1 year, 4 months ago

Selected Answer: ABF

ABF seems to be the right answer after reading the documents provided by the answer.

upvoted 4 times

  **A_A_AB** 1 year, 4 months ago

Agree with Villaran. ABF

The current answers are non-sense

upvoted 1 times

  **zenithcsa1** 1 year, 4 months ago

Is it really possible to set 2 redirection rules for one frontend(endpoint) without using rules engine configuration? As I understand, WAF policy is mapped with only one frontend and can have only one Redirect URL which is shown in 'Policy settings' blade. Could anyone help with explanation?

upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

You have 10 Azure App Service instances. Each instance hosts the same web app. Each instance is in a different Azure region. You need to configure Azure Traffic Manager to direct users to the instance that has the lowest latency. Which routing method should you use?

- A. geographic
- B. weighted
- C. priority
- D. performance

Correct Answer: D

Select Performance routing when you have endpoints in different geographic locations and you want end users to use the "closest" endpoint for the lowest network latency.

Reference:

<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods>

Community vote distribution

D (100%)

 **Lazylinux** 5 months, 3 weeks ago

Selected Answer: D

D is answer
upvoted 1 times

 **BlackZeros** 1 year, 4 months ago

Selected Answer: D

D is right
upvoted 1 times

 **A_A_AB** 1 year, 4 months ago

Selected Answer: D

Select Performance routing when you have endpoints in different geographic locations and you want end users to use the "closest" endpoint for the lowest network latency.

Select Geographic routing to direct users to specific endpoints (Azure, External, or Nested) based on where their DNS queries originate from geographically. With this routing method, it enables you to be in compliance with scenarios such as data sovereignty mandates, localization of content & user experience and measuring traffic from different regions.

upvoted 2 times

 **Alessandro365** 1 year, 4 months ago

Selected Answer: D

D is correct
upvoted 1 times

 **jilguens** 1 year, 4 months ago

Selected Answer: D

correct
upvoted 2 times

Your company has offices in London, Tokyo, and New York.

The company has a web app named App1 that has the Azure Traffic Manager profile shown in the following table.

Parameter	Value	Azure region
DNS Name	app1.trafficmanager.net	Not applicable
Endpoint	app1-asia.azurewebsites.net	East Asia
Endpoint	app1-na.azurewebsites.net	East US
Endpoint	app1-na.azurewebsites.net	UK South
Routing method	Geographic	Not applicable

In Asia, you plan to deploy an additional endpoint that will host an updated version of App1.

You need to route 10 percent of the traffic from the Tokyo office to the new endpoint during testing.

What should you configure in Traffic Manager?

- A. two profiles and five endpoints
- B. two profiles and four endpoints
- C. three profiles and four endpoints
- D. one profile and five endpoints

Correct Answer: B

Need two profiles. Add one Child profile using Weighted routing. One additional trial endpoint, to the existing three, for the Child Profile is needed.

Note 1: Each Traffic Manager profile specifies a single traffic-routing method. However, there are scenarios that require more sophisticated traffic routing than the routing provided by a single Traffic Manager profile. You can nest Traffic Manager profiles to combine the benefits of more than one traffic-routing method.

Note 2: Weighted routing: Select Weighted routing when you want to distribute traffic across a set of endpoints based on their weight. Set the weight the same to distribute evenly across all endpoints.

Reference:

<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-nested-profiles> <https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods>

Community vote distribution

B (80%)

A (20%)

 **sapien45** Highly Voted 1 year, 4 months ago

Selected Answer: B

You cannot combine both 'Weighted' and 'Geographic' traffic-routing in a single profile.

The parent profile still uses the Geographic traffic-routing method and child profile uses the Weighted traffic-routing method. This 'child' profile act as an endpoint to the 'parent' profile.

upvoted 6 times

 **[Removed]** 1 year ago

This is why I wonder whether they do not count this child profile as a "fifth" endpoint. This is said in the documentation: "To create a nested profile, you add a 'child' profile as an endpoint to a 'parent' profile."

upvoted 2 times

 **daemon101** 6 months, 2 weeks ago

Initially, there are only 3 endpoints with 1 TM profile using Geographic routing-method. However, you need to deploy 10% of traffic to Tokyo which requires Weighted TM routing-method. When you create a Child TM, it is considered as endpoint. Therefore, 3 endpoints + 1 endpoint (child TM) is equal to 4 endpoints. 1 Parent TM Profile + 1 Child Profile is equal to 2 Profiles.

B is the correct answer. 2 Profiles and 4 endpoints

upvoted 4 times

 **Rododendron2** 1 month, 1 week ago

Nope, you need additional endpoint , the Tokyo one. You can hardly load balance 10% of traffic in Child profile to 1 endpoint if you have there just single endpoint :-)

upvoted 1 times

 **CiscoTerminator** 5 months, 1 week ago

thanks for the explanation mate

upvoted 1 times

🗄️ 👤 **Prutser2** Highly Voted 1 year, 3 months ago

Selected Answer: B

you will need to add the updated server to the list so you end up with 4 nodes,
for Japan, you will need a Traffic profile, with routing geographic and inside that a weighted group with two server, so answer B
upvoted 5 times

🗄️ 👤 **GBAU** Most Recent 3 months ago

Selected Answer: A

A. two profiles and five endpoints

1x Parent Geographic Profile:

3x Endpoints:

-East US

-UK South

-East Asia Nested Endpoint*

*A nested endpoint is still an endpoint, created by using the "Add" button in the settings/Endpoints of the TM Profile. The type of endpoint is just 'Nested endpoint' instead of Azure Endpoint or External Endpoint.

1x Asia Child Weighted Endpoint (to be nested)

2x Endpoints

-Existing Tokyo office Endpoint

-New Endpoint in Asia

3+2=5

upvoted 3 times

🗄️ 👤 **Lazylinux** 4 months, 2 weeks ago

Selected Answer: B

B is Honey

2 profiles Geographic for parents and Weighted for child, parent 3 endpoints and child profile 1 endpoint

upvoted 1 times

🗄️ 👤 **vivikar** 1 year ago

For Asia: 3 Endpoints: 1+1+1(Nested Endpoint with 2 Child endpoint using Weight method)

Another regions has 2 Endpoints,

So 2 profiles(Nested and geographic) and 5 Endpoints

upvoted 1 times

🗄️ 👤 **vivikar** 1 year ago

Sorry, Ignore my comment.. Nested endpoint is wrong, it should be profile.. So 2 and 2 is answer

upvoted 1 times

🗄️ 👤 **OliwerCiecwierz** 10 months, 3 weeks ago

That's not even a listed answer so we will ignore your comments, don't worry

upvoted 7 times

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT -

You configure a route table named RT1 that has the routes shown in the following table.

Name	Prefix	Next hop type	Next hop IP address
Route1	0.0.0.0/0	Network virtual appliance (NVA)	192.168.0.4
Route2	10.0.0.0/24	Network virtual appliance (NVA)	192.168.0.4

You have an Azure virtual network named Vnet1 that has the subnets shown in the following table.

Name	Prefix	Route table
DMZ	192.168.0.0/24	None
FrontEnd	192.168.1.0/24	RT1
BackEnd	192.168.2.0/24	None

You have the resources shown in the following table.

Name	IP address	Type
NVA1	192.168.0.4	NVA
VM1	192.168.1.4	Virtual machine
VM2	192.168.2.4	Virtual machine

Vnet1 connects to an ExpressRoute circuit. The on-premises router advertises the following routes:

- ⇒ 0.0.0.0/0
- ⇒ 10.0.0.0/16

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Internet traffic from NVA1 is routed to the on-premises network.	<input type="radio"/>	<input type="radio"/>
Traffic from VM2 to the on-premises network is routed through NVA1.	<input type="radio"/>	<input type="radio"/>
Traffic from VM1 is routed to VM2 through NVA1.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
Internet traffic from NVA1 is routed to the on-premises network.	<input checked="" type="radio"/>	<input type="radio"/>
Traffic from VM2 to the on-premises network is routed through NVA1.	<input type="radio"/>	<input checked="" type="radio"/>
Traffic from VM1 is routed to VM2 through NVA1.	<input checked="" type="radio"/>	<input type="radio"/>

Box 1: Yes -

NVA1 with IP (NVA-network virtual appliance) 192.168.0.4 is on the DMZ subnet. It will use route 10.0.0.0/16 to the on-premises network.

Box 2: No -

VM2 has IP address 192.168.2.4 and is on the BackEnd subnet. VM2 will not use the RT1 route table, and will not reach the on-premises network through NVA1.

Box 3: Yes -

VM1 with IP address 192.168.1.4 is on the FrontEnd subnet, and will use the RT1 routing table. It will use Route2 and Next Hop IP address 192.168.0.4, IP address of NVA1, to reach VM2.

 **Cristoicach91** Highly Voted 1 year, 4 months ago

YNN. Route 0.0.0.0/0 is advertised to NVA from on-prem. VM2 learns route 10.0.0.0/16 from on-prem. VM1 and VM2 are in different subnets, but same virtual network, there is a system route that is a better match than the one in the route table.

upvoted 31 times

  **prabhjot** 1 week, 3 days ago

The last and is N (as RT will over ride the System route) as RT is applied on the VM1 via the subnet

upvoted 1 times

  **sapien45** 1 year, 3 months ago

Perfect Answer.

Both below answers are based on not reading :

ONLY if If multiple routes contain the SAME address prefix, UDR prevails

upvoted 2 times

  **Chricrown** 1 year, 4 months ago

YNY .. Box 3 is yes as it is using the UDR (RT1) which points to the NVA as its default gateway. UDR gets higher priority.

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview>

upvoted 9 times

  **mav3r1ck** 1 year, 4 months ago

Agree.

If multiple routes contain the same address prefix, Azure selects the route type, based on the following priority:

- User-defined route
- BGP route
- System route

upvoted 3 times

  **Lrrr_FromOmicronPersei8** 1 year, 2 months ago

Well no, you get a longer prefix system-generated route with a next-hop type VnetLocal, therefore YNN.

upvoted 7 times

  **daemon101** 6 months, 1 week ago

Agree. This means if you only create a custom default route pointing to NVA, the inter-subnet (subnets within one vnet) communication will never go through the NVA.

upvoted 1 times

  **jellybiscuit** Highly Voted 1 year, 3 months ago

YNY

UDRs exist for a reason: to override the default behavior of Azure routing

- It is correct that there is a default route that would allow VM1 to communicate with VM2
- that route is superseded by the UDR
- Someone has intentionally decided that all outbound traffic from the frontend subnet should pass through the NVA (firewall).

It is important to know that the other routes exist and in what order they are used

- 1) User-defined
- 2) BGP
- 3) system/default

Just remember that if they show you a route table, it is a UDR and is always in-use.

If you want to see the full list of routes, find it by looking at Effective Routes from the portal.

upvoted 9 times

  **mickeysonix** 1 year, 1 month ago

Thought similar, but Azure uses the longest prefix match algorithm and only after that it uses UDRs. So VNet2 has a system defined route of longer prefix than BGP ones and UDRs and therefore traffic is direct.

upvoted 1 times

  **Prutser2** 1 year, 3 months ago

not always, there is still the mechanism of the longest match, for instance in box 3, even though there is a UDR, the longest match is still the route that dictates that subnets within the same vnet can flow.

upvoted 2 times

  **Lazylinux** Most Recent 4 months, 2 weeks ago

YNN is my answer for 3rd it is on same vnet and there is no overriding route in the NVA and hence default route will take place i.e. internal GWY and hence direct traffic

upvoted 3 times

  **azure_dori** 5 months ago

My 2 cents are:

YNY

The third question is No, because VM1 and VM2 are in different subnets and Route1 means that the traffic between the subnets of Vnet1 goes through NVA1. Only if VM1 and VM2 are in the same subnet => the traffic between them flows directly.

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview#routing-example>

upvoted 1 times

  **azure_dori** 5 months ago

I mean "The third question is" Yes, of course. Sorry for the typo.

upvoted 1 times

🗨️ **crypto700** 9 months ago

YNN, VM1 will get to VM2 without NVA because they are in the same Vnet.

upvoted 4 times

🗨️ **AzureLearner01** 10 months, 3 weeks ago

My answer is Yes, No, No. I think Q1 and Q2 are obvious. but Q3 is not. UDR will overwrite the system route but only if you create a specific route not the default route 0.0.0.0/0. The default route 0.0.0.0/0 would not overwrite the system route, so next Hop is the internal GW from the subnet and not the nva. To verify this theory i've created a UDR that routes traffic from the subnet of VM1 to the subnet of VM2 over the NVA. Traffic from VM1 will go over the nva to VM2 even if they are in the same VNet.

upvoted 4 times

🗨️ **Hajji** 11 months, 1 week ago

YNY

When you create a route table and associate it to a subnet, the table's routes are combined with the subnet's default routes. If there are conflicting route assignments, user-defined routes will override the default routes.

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview>

upvoted 1 times

🗨️ **ejml** 1 year ago

Default routes of the one subnet are the address space of the its virtual network and virtual networks peered. In the worst case, when both routes (UDR and System Route) UDR has higher priority. Answer is YNY

upvoted 2 times

🗨️ **eVo3000** 1 year ago

YNN

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview#how-azure-selects-a-route>

"When outbound traffic is sent from a subnet, Azure selects a route based on the destination IP address, using the longest prefix match algorithm[...]If multiple routes contain the same address prefix, Azure selects the route type, based on the following priority:

1.User-defined route

2.BGP route

3.System route

In our case, we do not take the default route

upvoted 6 times

🗨️ **GBAU** 3 months ago

Important omission to the above details from that page:

Note

System routes for traffic related to virtual network, virtual network peerings, or virtual network service endpoints, are preferred routes, even if BGP routes are more specific.

upvoted 1 times

🗨️ **jotajotajeje** 1 year, 2 months ago

YNN.

1-Route 0.0.0.0/0 is advertised to NVA from on-prem and it doesn't have routing table.

2-VM2 has no routing table hence it will go via the 0.0.0.0/0 advertised via BGP from the on premises router that has more priority that system route 0.0.0.0/0 to internet via Azure network

3-VM1 and VM2 are in different subnets, but same virtual network, there is a system route in every subnet/VM interface that has the network and mask of the entire VNET where the subnet is, therefore as it has the prefix length bigger than the default route it will prefer going directly from VM to VM.

upvoted 3 times

🗨️ **JWYANG** 1 year, 3 months ago

YNY

Azure automatically added this route for all subnets within Virtual-network-1, because 10.0.0.0/16 is the only address range defined in the address space for the virtual network. If the user-defined route in route ID2 weren't created, traffic sent to any address between 10.0.0.1 and 10.0.255.254 would be routed within the virtual network, because the prefix is longer than 0.0.0.0/0, and not within the address prefixes of any of the other routes. Azure automatically changed the state from Active to Invalid, when ID2, a user-defined route, was added, since it has the same prefix as the default route, and user-defined routes override default routes. The state of this route is still Active for Subnet2, because the route table that user-defined route, ID2 is in, isn't associated to Subnet2.

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview#routing-example>

upvoted 2 times

🗨️ **mickeysonix** 1 year, 1 month ago

Thought similar, but Azure uses the longest prefix match algorithm and only after that it uses UDRs. So VNet2 has a system defined route of longer prefix than BGP ones and UDRs and therefore traffic is direct.

upvoted 2 times

🗨️ **DeepMoon** 1 year, 4 months ago

Given Answers are incorrect.

Correct Answers

Q1: Yes. Why?

Because On-Prem router advertises 0.0.0.0/0 route to the NVA through a Express Route. We are not told NVA has any other route.

Q2: Yes. Why?

Because VM2 is on backend subnet (192.168.2.0/24) it has no UDR. But NVA1 is advertising all the routes on its table (that includes what it learned from On-Prem) to the all of VNet1. NVA1 knows how to get to 10.0.0/16 network via On-Prem router.

Q3:No. Why?

Because VM1 & VM2 are in VNET1. Azure by default knows how to route traffic between its subnets without needing a UDR's.
upvoted 1 times

🗨️ **sapien45** 1 year, 4 months ago

YNN.

Read the link in its entirety ! Especially the implementation example.

The very same routes are being displayed.

Route ID1 is not invalidated by route ID12 because the prefix is longer than 0.0.0.0/0

upvoted 2 times

🗨️ **andry79** 1 year, 4 months ago

Tested in lab, is YNN

upvoted 6 times

🗨️ **Fule** 1 year, 4 months ago

I will go with YNY.

"Azure automatically creates system routes and assigns the routes to each subnet in a virtual network. You can't create system routes, nor can you remove system routes, but you can override some system routes with custom routes." so basically means custom routes is a better match than the system, which is somehow logical, you want to manipulate with system routes in some scenario.

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview>

upvoted 2 times

🗨️ **Kafura** 9 months, 2 weeks ago

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview#:~:text=When%20you%20create%20a%20route%20table%20and%20associate%20it%20to%20a%20subnet%2C%20the%20table%27s%20routes%20are%20combined%20with%20the%20subnet%27s%20default%20routes.%20If%20there%20are%20conflicting%20route%20assignments%2C%20user%2Ddefined%20routes%20will%20override%20the%20default%20routes.>

overview#:~:text=When%20you%20create%20a%20route%20table%20and%20associate%20it%20to%20a%20subnet%2C%20the%20table%27s%20routes%20are%20combined%20with%20the%20subnet%27s%20default%20routes.%20If%20there%20are%20conflicting%20route%20assignments%2C%20user%2Ddefined%20routes%20will%20override%20the%20default%20routes.

upvoted 1 times

🗨️ **zenithcsa1** 1 year, 4 months ago

YNN

Box 3 : When communicating from VM1 to VM2, the Next-hop Type becomes VirtualNetwork due to the longest prefix. So UDR routes(0.0.0.0/0 - > NVA) are not used.

upvoted 7 times

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT -

You have an Azure subscription. The subscription contains virtual machines that host websites as shown in the following table.

Name	Public host name	Location
VM1	site1.us.contoso.com	East US
VM2	site1.uk.contoso.com	UK West
VM3	site2.us.contoso.com	East US
VM4	site2.uk.contoso.com	UK West
VM5	site2.japan.contoso.com	Japan West

You have the Azure Traffic Manager profiles shown in the following table.

Name	Routing method	DNS name	Hosted on
Tm1	Performance	site1.contoso.com	VM1 and VM2
Tm2	Priority	site2.contoso.com	VM3, VM4, and VM5

You have the endpoints shown in the following table.

Name	Traffic Manager profile	Azure endpoint	Routing method parameter	Status
Ep1	Tm1	VM1	1	Degraded
Ep2	Tm1	VM2	2	Online
Ep3	Tm2	VM3	1	CheckingEndpoint
Ep4	Tm2	VM4	2	Online
Ep5	Tm2	VM5	3	Online

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Statements	Yes	No
A user that requests site1.contoso.com from the East US Azure region will connect to site1.us.contoso.com.	<input type="radio"/>	<input type="radio"/>
A user that requests site2.contoso.com from the East US Azure region will connect to site2.uk.contoso.com.	<input type="radio"/>	<input type="radio"/>
A user that requests site2.contoso.com from the Japan East Azure region will connect to site2.japan.contoso.com.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Statements	Yes	No
A user that requests site1.contoso.com from the East US Azure region will connect to site1.us.contoso.com.	<input type="radio"/>	<input checked="" type="radio"/>
A user that requests site2.contoso.com from the East US Azure region will connect to site2.uk.contoso.com.	<input type="radio"/>	<input checked="" type="radio"/>
A user that requests site2.contoso.com from the Japan East Azure region will connect to site2.japan.contoso.com.	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: No -

VM1, which is hosting site1.contoso.com, is located in East US. The VM1 endpoint status is degraded. Endpoint monitoring health checks are failing. The endpoint isn't included in DNS responses and doesn't receive traffic.

When an endpoint has a Degraded status, it's no longer returned in response to DNS queries. Instead, an alternative endpoint is chosen and returned. The traffic- routing method configured in the profile determines how the alternative endpoint is chosen.

Priority. Endpoints form a prioritized list. The first available endpoint on the list is always returned. If an endpoint status is Degraded, then the next available endpoint is returned.

The user will connect to site2.us.contoso.com instead.

Box 2: No -

VM3, which is hosting site2.contoso.com, is located in in East US. The VM3 endpoint status is CheckingEndpoint. The endpoint is monitored, but the results of the first probe haven't been received yet. CheckingEndpoint is a temporary state that usually occurs immediately after adding or enabling an endpoint in the profile. An endpoint in this state is included in DNS responses and can receive traffic.

User will connect to site2.contoso.com, not to site2.uk.contoso.com

Box 3: No -

VM3, which is hosting site2.contoso.com, is located in in East US. The VM1 endpoint status is CheckingEndpoint, which is OK (see above).

User will connect to site2.contoso.com, not to site2.japan.contoso.com

Reference:

<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-monitoring>

 **jellybiscuit** Highly Voted 1 year, 3 months ago

Correct.

N - site1.uk.contoso.com is the only site1 host online

N - In a priority routing method, lower numbers are chosen first. Traffic Manager will send traffic to endpoints with the "Checking Endpoint" status - so it's going to site2.us

N - same reason as Q2

upvoted 17 times

 **bleemster** 1 year, 2 months ago

Can you back this up? "checking endpoint" will still receive traffic? I cant find anything to validate this. All i read is that when you add it you get this status while its checking the endpoint (fitting status really) and when its available traffic will then be sent there.

upvoted 3 times

 **wiki715** 1 year, 1 month ago

"Checking Endpoint" status == "An endpoint in this state is included in DNS responses and can receive traffic."

(At least according to <https://learn.microsoft.com/en-us/azure/traffic-manager/traffic-manager-monitoring#endpoint-monitor-status>)

upvoted 2 times

 **CiscoTerminator** 5 months, 2 weeks ago

Thanks for the link but not sure if its "safe" to send traffic to an endpoint being checked. What if status turns to degraded?

upvoted 1 times

 **davidkerr7** Highly Voted 1 year, 3 months ago

N - Choose the closest VM1, but it's degraded so choose the next closest VM2 UK [site1.uk.contoso]

Y - Choose in order, VM3 but its checking, so choose VM4 UK [site2.uk.contoso]

N - (Same) Choose in order, VM3 but its checking, so choose VM4 UK

upvoted 10 times

 **samir111** Most Recent 1 week, 1 day ago

You are welcome, NNN

The endpoint is monitored, but the results of the first probe haven't been received yet. CheckingEndpoint is a temporary state that usually occurs immediately after adding or enabling an endpoint in the profile. An endpoint in this state is included in DNS responses and can receive traffic.

upvoted 1 times

 **toto74500** 3 weeks, 3 days ago

NYN

For 2nd Question :Yes because "checkingendpoint" status means:

The endpoint is monitored, but the results of the first probe haven't been received yet. CheckingEndpoint is a temporary state that usually occurs immediately after adding or enabling an endpoint in the profile. An endpoint in this state is included in DNS responses and can receive traffic.

<https://learn.microsoft.com/en-us/azure/traffic-manager/traffic-manager-monitoring>

upvoted 2 times

 **Lazylinux** 4 months, 2 weeks ago

I would say NNN based on the following links

<https://learn.microsoft.com/en-us/azure/traffic-manager/traffic-manager-monitoring>

<https://learn.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods>

upvoted 1 times

 **TJ001** 1 year ago

NNN is right...

upvoted 3 times

 **Ajdlfasudfo0** 1 year, 1 month ago

N,N,N actually,

the last one as you can see here: <https://learn.microsoft.com/en-us/azure/traffic-manager/traffic-manager-monitoring#endpoint-monitor-status>

The endpoint is monitored, but the results of the first probe haven't been received yet. CheckingEndpoint is a temporary state that usually occurs immediately after adding or enabling an endpoint in the profile. An endpoint in this state is included in DNS responses and can receive traffic.

upvoted 3 times

🗨️ 👤 **geuser** 1 year, 2 months ago

N,N,N

<https://learn.microsoft.com/en-us/azure/traffic-manager/traffic-manager-monitoring#endpoint-monitor-status>

CheckingEndpoint means The endpoint is monitored, but the results of the first probe haven't been received yet. CheckingEndpoint is a temporary state that usually occurs immediately after adding or enabling an endpoint in the profile. An endpoint in this state is included in DNS responses and CAN receive traffic.

upvoted 1 times

🗨️ 👤 **roshingrg** 7 months, 1 week ago

If an endpoint is in the CheckingEndpoint state, then requests will be routed to the next endpoint in the Traffic Manager profile. This is because the endpoint is not yet considered healthy, and Traffic Manager does not want to send traffic to an endpoint that may not be able to handle it.

upvoted 2 times

🗨️ 👤 **GohanF2** 1 year, 2 months ago

1. VM1 is degraded . The traffic profile is "performance" which it will be using the closest endpoint to the region.

In this case will connect to VM which is in site1.uk.contonso.com . Answer is: No.

2. VM3 is in checkingEndpoint which is not ready for connectivity. The routing method is "priority"; which means will select the Endpoint with the lowest priority digit. We still have VM4 and VM5 which are online.

VM4 the public site is: site2.uk.contonso.com . Answer is : Yes.

3. Same scenario the profile is "Priority" in this case, the VM with the lowest priority is VM4 which is in UK West: site2.uk.contonso.com. Answer is: No.

NO

YES

NO

upvoted 6 times

🗨️ 👤 **Goofer** 1 year ago

The endpoint is monitored, but the results of the first probe haven't been received yet. CheckingEndpoint is a temporary state that usually occurs immediately after adding or enabling an endpoint in the profile. An endpoint in this state is included in DNS responses and can receive traffic.

upvoted 3 times

🗨️ 👤 **Azuriste** 1 year, 3 months ago

For Me NNY

upvoted 5 times

店铺: IT认证考试服务

店铺: IT认证考试服务

You have an Azure application gateway configured for a single website that is available at <https://www.contoso.com>.

The application gateway contains one backend pool and one rule. The backend pool contains two backend servers. Each backend server has an additional website that is available on port 8080.

You need to ensure that if port 8080 is unavailable on a backend server, all the traffic for <https://www.contoso.com> is redirected to the other backend server.

What should you do?

- A. Create a health probe
- B. Add a new rule
- C. Change the port on the listener
- D. Add a new listener

Correct Answer: A

By default, Azure Application Gateway probes backend servers to check their health status and to check whether they're ready to serve requests. Users can also create custom probes to mention the host name, the path to be probed, and the status codes to be accepted as Healthy. In each case, if the backend server doesn't respond successfully, Application Gateway marks the server as Unhealthy and stops forwarding requests to the server. After the server starts responding successfully, Application Gateway resumes forwarding the requests. Note: The default probe request is sent in the format of `<protocol>://127.0.0.1:<port>/`. For example, `http://127.0.0.1:80` for an http probe on port 80. Only HTTP status codes of 200 through 399 are considered healthy. The protocol and destination port are inherited from the HTTP settings. If you want Application Gateway to probe on a different protocol, host name, or path and to recognize a different status code as Healthy, configure a custom probe and associate it with the HTTP settings.

Reference:

<https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-backend-health-troubleshooting>

Community vote distribution

A (100%)

 **BlackZeros** Highly Voted 1 year, 4 months ago

Selected Answer: A

Create Health Probe to monitor the port and server health
upvoted 6 times

 **rehanalam** Most Recent 6 months, 3 weeks ago

I am facing hard time to understand the problem and how Custom health probe is a solution
upvoted 1 times

 **JennyHuang36** 11 months, 1 week ago

In exam Feb, 2023
upvoted 1 times

 **omgMerrick** 11 months, 2 weeks ago

Selected Answer: A

Option A appears correct.

By default, the health probe checks port 80 for HTTP traffic. However, you can configure the health probe to check other ports, such as port 8080 in this case. If the application gateway determines that a backend server is unavailable, it can automatically redirect traffic to the other available backend server.

upvoted 2 times

You have an Azure subscription that contains the following resources:

- A virtual network named Vnet1
- Two subnets named subnet1 and AzureFirewallSubnet
- A public Azure Firewall named FW1
- A route table named RT1 that is associated to Subnet1
- A rule routing of 0.0.0.0/0 to FW1 in RT1

After deploying 10 servers that run Windows Server to Subnet1, you discover that none of the virtual machines were activated.

You need to ensure that the virtual machines can be activated.

What should you do?

- A. On FW1, create an outbound service tag rule for AzureCloud.
- B. Add an internet route to RT1 for the Azure Key Management Service (KMS).
- C. On FW1, configure a DNAT rule for port 1688.
- D. Deploy an Azure Standard Load Balancer that has an outbound NAT rule.

Correct Answer: B

Community vote distribution

B (100%)

 **Murad01** 1 month, 3 weeks ago

Not again this question, repeated 9 times already
upvoted 1 times

 **flurgen248** 10 months, 2 weeks ago

Selected Answer: B

Correct Answer is B.

A: AzureCloud is the wrong tag. Apparently would need to be AzurePlatformLKM-Windows licensing or key management service.
<https://learn.microsoft.com/en-us/azure/virtual-network/service-tags-overview#available-service-tags>

B: Something is blocking access to KMS, so a route should fix that.
<https://learn.microsoft.com/en-us/troubleshoot/azure/virtual-machines/troubleshoot-activation-problems#cause>

C: DNAT rules are inbound only.

D: A Nat rule wouldn't work, for reasons.
<https://learn.microsoft.com/en-us/azure/load-balancer/outbound-rules>
upvoted 3 times

 **tester2023** 12 months ago

The article below is a simiar scenario and it points out you need a route (in our case FW or Route Table) that will route traffic to the Microsoft KMS service on port 1688.

<https://learn.microsoft.com/en-us/troubleshoot/azure/virtual-machines/custom-routes-enable-kms-activation>
upvoted 2 times

 **TJ001** 1 year ago

There are two options ...
1) Add specific outbound rule for KMS in the FW as there is already default route points FW
2) Add specific address prefix route in route table so it can by pass default route to FW

In this case the chosen Answer - B looks correct
upvoted 4 times

 **NoeHdzMII** 1 year ago

Correct answer C.
"DNAT rules implicitly add a corresponding network rule to allow the translated traffic."

<https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-dnat>

upvoted 1 times

 **alfonzo47** 1 year ago

i think that DNAT is only for inbound rules. In this case the windows VMs will try to reach the KMS server (outbound traffic) hence i would go with option B even tho there is no service tag for KMS that can be chosen...

upvoted 1 times

店铺：IT认证考试服务

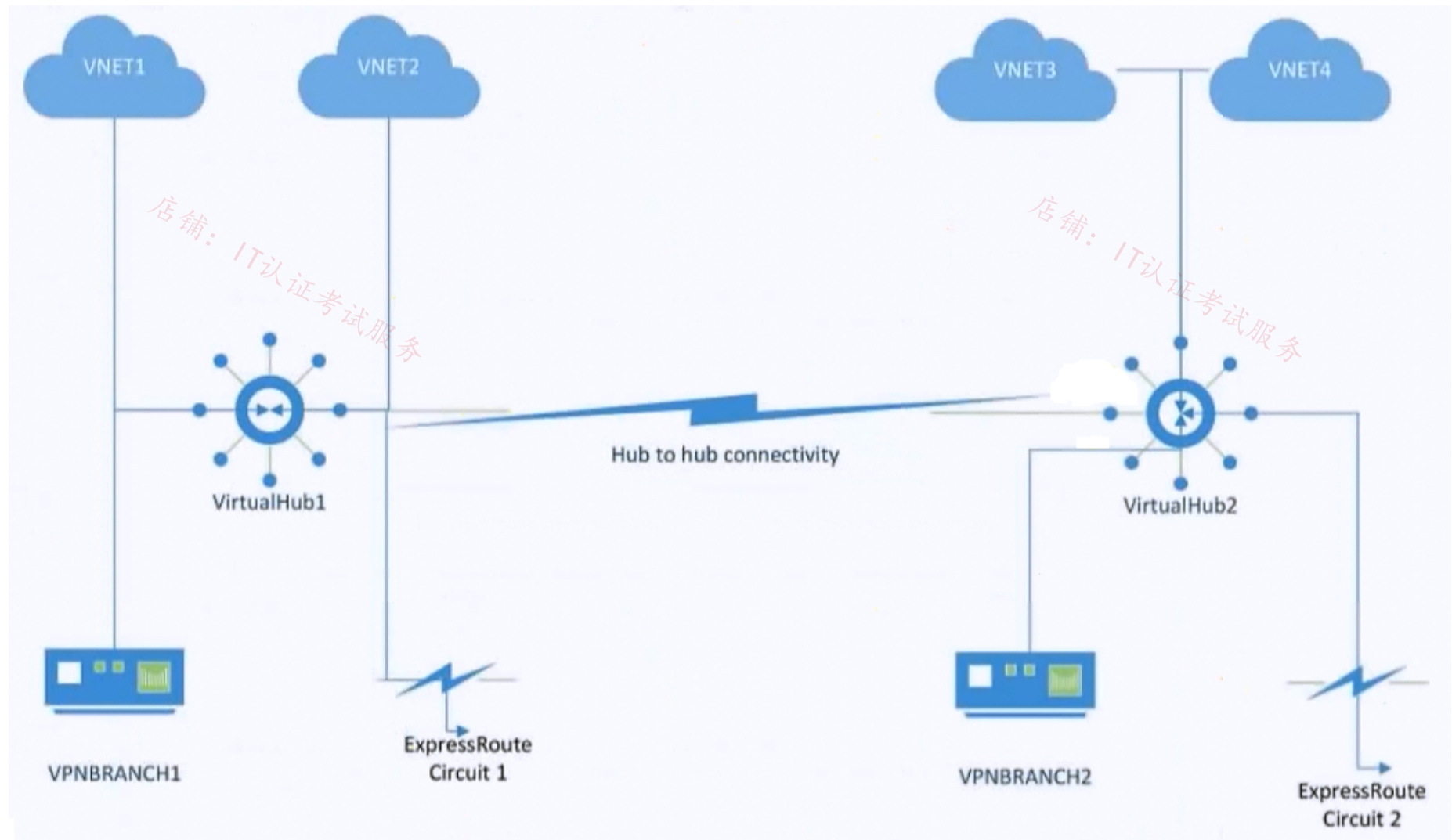
店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

You have an Azure subscription.

You plan to implement Azure Virtual WAN as shown in the following exhibit.



What is the minimum number of route tables that you should create?

- A. 1
- B. 2
- C. 4
- D. 6

Correct Answer: B

Community vote distribution

B (100%)

DeepMoon (Highly Voted) 1 year ago

Standard Virtual WAN is enabled due to the presence of a router in every virtual hub. This router is instantiated when the virtual hub is first created.

If it has a router. Then it needs a routing table. Therefore two hubs. Two routing tables.

upvoted 8 times

Salem2020s 1 year ago

can you please explain more? why dont we add routing tables for each Vnet as well?

upvoted 3 times

DeepMoon 1 year ago

<https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about>

upvoted 1 times

MrBlueSky (Highly Voted) 9 months, 3 weeks ago

Question is flawed because VWAN creates its own routes. Yes you would technically need at least two route tables, but the question asks about creating them. You wouldn't need to create these since it will create the routes on its own

upvoted 7 times

CiscoTerminator 5 months, 2 weeks ago

exactly what I read and understood!

upvoted 1 times

 **Lazylinux** Most Recent 4 months, 2 weeks ago

Selected Answer: B

B is Honey as per this link
<https://learn.microsoft.com/en-us/azure/virtual-wan/about-virtual-hub-routing>
upvoted 1 times

 **flurgen248** 10 months, 2 weeks ago

Selected Answer: B

The given answer is correct. The minimum number of route tables you can have for this setup is 2.

By default, all connections are associated to a Default route table in a virtual hub. Each virtual hub has its own Default route table, which can be edited to add a static route(s). Routes added statically take precedence over dynamically learned routes for the same prefixes.

<https://learn.microsoft.com/en-us/azure/virtual-wan/about-virtual-hub-routing#association>
upvoted 2 times

 **wooyourdaddy** 10 months, 3 weeks ago

Selected Answer: B

Assuming the VNETs are using Hub virtual network connections, then each connection is associated to one route table. Associating a connection to a route table allows the traffic to be sent to the destination indicated as routes in the route table. The routing configuration of the connection will show the associated route table. Multiple connections can be associated to the same route table. All VPN, ExpressRoute, and User VPN connections are associated to the same (default) route table.

By default, all connections are associated to a Default route table in a virtual hub. Each virtual hub has its own Default route table, which can be edited to add a static route(s). Routes added statically take precedence over dynamically learned routes for the same prefixes.

Source: <https://learn.microsoft.com/en-us/azure/virtual-wan/about-virtual-hub-routing#association>

As there is no indication in the question that connections were pointed to any specific route table, we would assume they would get added to the Default route table in each virtual hub. So 2 route tables total.

upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

You have an internal Basic Azure Load Balancer named LB1 that has two frontend IP addresses. The backend pool of LB1 contains two Azure virtual machines named VM1 and VM2.

You need to configure the rules on LB1 as shown in the following table.

Rule	Frontend IP address	Protocol	ILB1 port	Destination	VM port
1	65.52.0.1	TCP	80	IP address of the NIC of VM1 and VM2	80
2	65.52.0.2	TCP	80	IP address of the NIC of VM1 and VM2	80

What should you do for each rule?

- A. Enable Floating IP.
- B. Disable Floating IP.
- C. Set Session persistence to Enabled.
- D. Set Session persistence to Disabled.

Correct Answer: A

Community vote distribution

A (100%)

 **TJ001** Highly Voted 1 year ago

Correct Answer

<https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-multivip-overview#rule-type-2-backend-port-reuse-by-using-floating-ip>

If you want to reuse same port for both load balancing rules then Floating IP needs to be enabled

upvoted 6 times

 **omgMerrick** Most Recent 11 months, 2 weeks ago

Selected Answer: A

Answer is correct, Enable floating IP.

<https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-floating-ip#floating-ip>

upvoted 4 times

Your company has 40 branch offices that are linked by using a Software-Defined Wide Area Network (SD-WAN). The SD-WAN uses BGP.

You have an Azure subscription that contains 20 virtual networks configured as a hub and spoke topology. The topology contains a hub virtual network named Vnet1.

The virtual networks connect to the SD-WAN by using a network virtual appliance (NVA) in Vnet1.

You need to ensure that BGP route advertisements will propagate between the virtual networks and the SD-WAN. The solution must minimize administrative effort.

What should you implement?

- A. An Azure VPN Gateway that has BGP enabled
- B. a NAT gateway
- C. Azure Traffic Manager
- D. Azure Route Server

Correct Answer: D

 **DeepMoon** Highly Voted 1 year ago

<https://learn.microsoft.com/en-us/azure/route-server/overview>

Azure Route Server is a fully managed service and is configured with high availability.

Azure Route Server simplifies dynamic routing between your network virtual appliance (NVA) and your virtual network.

When BGP Peering is set up with this, it eliminates the need to manually update routes across all connected networks.

upvoted 14 times

 **occupatissimo** 8 months, 2 weeks ago

Virtual gateway

A route server propagate to a sdn existing inside a vnet, here the sdn is outside

upvoted 2 times

 **ironbornson** 5 months, 1 week ago

Hub virtual network centralized route management to route traffic to the hub works with

User Defined Routes, not with BGP: <https://learn.microsoft.com/en-us/azure/firewall-manager/vhubs-and-vnets#comparison>

upvoted 1 times

 **TJ001** 1 year ago

Agree with the answer

upvoted 3 times

 **Murad01** Most Recent 1 month, 3 weeks ago

Appeared on Exam November - 2023

upvoted 1 times

HOTSPOT

-

You have an Azure load balancer that has the following configurations:

- Name: LB1
- Location: East US 2
- SKU: Standard
- Private IP address: 10.3.0.7
- Load balancing rule: rule1 (Tcp/80)
- Health probe: probe1 (Http:80)
- NAT rules: 0 inbound

The backend pool of LB1 has the following configurations:

- Name: backend1
- Virtual network: Vnet2
- Backend pool configuration: NIC
- IP version: IPv4
- Virtual machines: VM1, VM2, VM3

You have an Azure virtual machine named VM4 that has the following network configurations:

- Network interface: vm4981
- Virtual network/subnet: Vnet3/Subnet3
- NIC private IP address: 10.4.0.4
- Accelerated networking: Enabled

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
To add VM4 to LB1, you must create a new backend pool.	<input type="radio"/>	<input type="radio"/>
VM1 is connected to Vnet2.	<input type="radio"/>	<input type="radio"/>
Connections to HTTPS://10.3.0.7 will be load balanced between VM1, VM2, and VM3.	<input type="radio"/>	<input type="radio"/>

Answer Area

Statements	Yes	No
To add VM4 to LB1, you must create a new backend pool.	<input type="radio"/>	<input checked="" type="radio"/>
VM1 is connected to Vnet2.	<input checked="" type="radio"/>	<input type="radio"/>
Connections to HTTPS://10.3.0.7 will be load balanced between VM1, VM2, and VM3.	<input type="radio"/>	<input checked="" type="radio"/>

Correct Answer:

🗨️ **MightyMonarch74** Highly Voted 10 months ago

N - Tested in lab and confirmed once 1 backend pool has been configured you cannot add another backend pool on a different VNET, the original VNET is always selected.

Y - VM1 is on VNET2

N - rule 1 is TCP/80, not 443 (HTTPS)

upvoted 16 times

🗨️ **jorgesoma** 2 months, 3 weeks ago

Correct

upvoted 3 times

🗨️ **Goofer** Highly Voted 1 year ago

Y - VM4 is in another Vnet. A backend pool can only contain resources from one virtual network.

Y - Backend pool Virtual Network is Vnet2. VM1 is in Vnet2

N - Load balancing rule: rule1 (Tcp/80) is HTTP not HTTPS

upvoted 15 times

🗨️ **c2e9cb4** 3 weeks, 2 days ago

N for question #1 ==> tested in lab

upvoted 1 times

🗨️ **ironbornson** 5 months ago

damm ppl voting this comment...PEOPLE!

"The backend resources must be in the same virtual network as the load balancer for IP based LBs", How in the hell you want to add a new backendpool if the VM4 is in a different VNET than the original Backendpool!! ""think mark think!!!"

<https://learn.microsoft.com/en-us/azure/load-balancer/backend-pool-management#limitations>

upvoted 8 times

🗨️ **asdasd123123iu** 6 months ago

Y - VM4 is in another Vnet. A backend pool can only contain resources from one virtual network. - In that case adding additional pool didn't help, new lb in VM4 must be created.

upvoted 2 times

🗨️ **asdasd123123iu** 6 months ago

I mean vnet where VM4 is located.

upvoted 1 times

🗨️ **Lazylinux** Most Recent 4 months, 2 weeks ago

NYN

N - multiple backend pools, mix of IP backend pool or NIC backend pool, but they must be in the same VNET as the Loadbalancer and it's not possible to change this VNet once LB is created and deployed

Y - both in samebackendpool in vnet2

N - LB rule is for port 80 and NOT 443

upvoted 3 times

🗨️ **aBAN** 7 months ago

YYN

- The backend resources must be in the same virtual network as the load balancer for IP based LBs

- You can configure IP based and NIC based backend pools for the same load balancer. You can't create a single backend pool that mixes backed addresses targeted by NIC and IP addresses within the same pool.

<https://learn.microsoft.com/en-us/azure/load-balancer/backend-pool-management#limitations>

upvoted 1 times

🗨️ **_fvt** 9 months, 3 weeks ago

N - you can have multiple backend pools, mix of IP backend pool or NIC backend pool, but they must be in the same VNET than the Loadbalancer (in fact same vnet than the first frontend IP chosen at deployment: then you can't create another Frontend IP in a different VNet or remove all frontend IP; So it's not possible to change this VNet once LB is deployed). Backend pools must be in the same VNet than the Frontend IP. So in facts a Loadbalancer cannot span multiple vnets. (all tested in lab) (may change with cross-region load balancer which is still in preview <https://learn.microsoft.com/fr-fr/azure/load-balancer/cross-region-overview>)

Y - Loadbalancer backend pool is in VNet2 so following the explanations above, all the VMS in the pool are in VNet 2. So VM1 which is in this backend pool is in VNet2.

N - Load Balancing rule is set for port 80 wich is the default HTTP port. HTTPS is 443. so HTTPS connections will not be handled by this Loadbalancer.

upvoted 3 times

🗨️ **wooyourdaddy** 9 months, 4 weeks ago

The first answer is no because VM4 exists in VNET3/Subnet3, so it can never be added to LB1, even as a 2nd backend pool. We can see the LB has a private address, meaning it is an internal LB. When you create the ILB, it assigns the FE configuration to a VNET/Subnet of your choosing. When you go to the backend pool page, the Virtual Network is always hardcoded to the VNET your FE is assigned to. When you click on "+ Add a backend pool", you get the Add backend pool page, which states:

IP configurations

IP configurations associated to virtual machines and virtual machine scale sets must be in same location as the load balancer and be in the same virtual network.

The answer to question 1 also confirms that the 2nd answer is Yes, as the VMs need to be in the same VNET as the LB Virtual Network which the question defines as VNET2.

The 3rd answer is no, because the inbound rule is for HTTP (Port 80) only. No HTTPS (Port 443).

upvoted 4 times

🗨️ **Apptech** 10 months, 1 week ago

NYN is the correct answer:

It is important to note that the backend pool configuration for backend1 is set to "NIC", which means that the load balancer is configured to load balance traffic between the network interfaces associated with the virtual machines (VMs) in the backend pool.

In order to add VM4 to LB1, you would need to create a new NIC for VM4 that is associated with a subnet in the same virtual network as the existing backend pool, Vnet2. This would allow LB1 to load balance traffic between the NICs associated with all the VMs in the backend pool, including VM4.

upvoted 2 times

🗨️ **AzureLearner01** 10 months, 1 week ago

Provided answer is correct. NYN. 1. You cant add the vm to the loadbalancer because

IP configurations associated to virtual machines and virtual machine scale sets must be in same location as the load balancer and be in the same virtual network.

2. True because of the previous sentence

3. No https is not in the rule

upvoted 2 times

🗨️ **flurgen248** 10 months, 2 weeks ago

I think it's N Y N.

1. It says the backend pool is NIC based, and I can't find anything saying that resources in a NIC based backend pool have to be in the same VNET. If it were IP-based, that is directly stated in this link: <https://learn.microsoft.com/en-us/azure/load-balancer/backend-pool-management#limitations>

I assume that link would say if it were also a requirement for NIC based backend pools.

2. VM1 is in the backend pool, which is assigned to VNET2.

3. rule1 is on port 80, which is HTTP. HTTPS requires port 443.

upvoted 1 times

🗨️ **flurgen248** 10 months, 2 weeks ago

Maybe it's YYN. There's just so little information about NIC based backend pools that I can't find proof one way or the other.

upvoted 1 times

🗨️ **Ayokun** 11 months, 1 week ago

Y Y N

1) A VM on a different Vnet cannot be added on a backend LB on VNET2 | VM4 on VNET 3

2) VM1 is connected in VNET 2

3) Watch out the rule is on "HTTP" = 80 port not on "HTTPS" = 443

upvoted 4 times

🗨️ **omgMerrick** 11 months, 2 weeks ago

Yes Yes No.

To add VM4 to LB1, you must create a new backend pool.

Yes. In order to add VM4 to LB1, you must create a new backend pool that includes VM4's network interface (vm4981) in Vnet3/Subnet3.

VM1 is connected to VNET2.

Yes. VM1 is a part of the backend pool "backend1" which is associated with the virtual network Vnet2.

Connections to <https://10.3.0.7> will be load balanced between VM1, VM2, and VM3.

No. The load balancing rule "rule1" is configured to load balance traffic on TCP port 80, not HTTPS (TCP port 443). Therefore, connections to <https://10.3.0.7> will not be load balanced by LB1.

upvoted 4 times

🗨️ **GeorgeMilev91** 1 year ago

Backend hosts have to be in the same vnet - <https://stackoverflow.com/questions/66529619/can-azure-internal-loadbalancer-have-backends-belonging-to-different-subnets-in>

upvoted 3 times

🗨️ **alfonzo47** 1 year ago

N Y N - Backend resources must be in the same virtual network as the load balancer for IP based load balancers <https://learn.microsoft.com/en-us/azure/load-balancer/backend-pool-management#limitations>.

1, Since Vms in the current backed pool are in Vnet2 we can assume that load balancer is also in vnet2. Hence vms from Vnet3 cant be added as backend resources = N.

2, VM must be in the same vnet as load balancers backend pool so it must be in vnet2 = Y.

3, Https defaults to port 443 and there is not load balancing rule for port 443 = N

upvoted 3 times

🗨️ **TJ001** 1 year ago

so 1. is Y not N !

upvoted 5 times



🗨️ **NoeHdzMII** 1 year ago

A backend pool can only contain resources from one virtual network.
HTTPS is using port tcp 443

upvoted 3 times

  **eVo3000** 1 year ago

I think we need to create a new backend pool
upvoted 3 times

  **tester2023** 12 months ago

Disagree.

The question shows "Backend pool configuration: NIC" for the existing pool, which means any new VMs added by NIC must be from the same vNet.

If we create a new backend pool that is IP-based, Microsoft states, "The backend resources must be in the same virtual network as the load balancer for IP based LBs"

Reference:

<https://learn.microsoft.com/en-us/azure/load-balancer/backend-pool-management#limitations>

upvoted 2 times

  **tester2023** 12 months ago

Creating a new backend pool will not allow you to add a VM that is on a different vNet.
upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

DRAG DROP

Your company, named Contoso, Ltd., has an Azure subscription that contains the resources shown in the following table.

Name	Type	Location	Description
App1us	Azure App Service	East US	A website for the United States office of Contoso
App1uk	Azure App Service	UK West	A website for the United Kingdom office of Contoso
St1us	Storage account	East US	Contains images for the United States website
St1uk	Storage account	UK West	Contains images for the United Kingdom website

You plan to deploy Azure Front Door. The solution must meet the following requirements:

- Requests to a URL of `https://contoso.azurefd.net/uk` must be routed to App1uk.
- Requests to a URL of `https://contoso.azurefd.net/us` must be routed to App1us.
- Requests to a URL of `https://contoso.azurefd.net/images` must be routed to the storage account closest to the user.

What is the minimum number of backend pools and routing rules you should create? To answer, drag the appropriate number to the correct components. Each number 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.

NOTE: Each correct selection is worth one point.

Number

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

Answer Area

Backend pools:

Routing rules:

Answer Area

Correct Answer: Backend pools:
Routing rules:

 **tester2023** Highly Voted 11 months, 3 weeks ago

3 Backend Pools | 3 Rules

I believe this is a Classic Front Door question. The first reference link provides an overview of classic routing. The questions shows we have a single frontend (`contoso.azurefd.net`) and there are three paths - `/uk`, `/us`, and `/images`.

The second link shows the three paths would each be a separate rule.

Regarding the number of backend pools, the question states, "...must be routed to [App1uk or App1us]" for the two App Services. The third link does not indicate there is a way to route traffic to a specific app service based on location. However, if we put each app service in its own backend pool, we can have the path rule route to the correct App Service everytime. The Latency routing logic is fine for storage accounts, but not the App Services based on the question requirements.


References

<https://learn.microsoft.com/en-us/azure/frontdoor/front-door-routing-architecture? pivots=front-door-classic>

<https://learn.microsoft.com/en-us/azure/frontdoor/front-door-route-matching? pivots=front-door-classic#frontend-host-matching>

<https://learn.microsoft.com/en-us/azure/frontdoor/routing-methods>

upvoted 17 times

 **Kafura** 9 months, 2 weeks ago

I agree

upvoted 1 times

 **Mbrigaldino97** Highly Voted 1 year ago

correct answer should be 2 and 2.

You have 1 Frontend, which is contoso.com, this is one frontend with a custom domain and not App Service as origin!

You then create 2 Backend Pools, (1 for the App Services, one for both Storage Accounts) and 2 routing rules -> 1 routing rule containing both entries for the App Services (/uk and /us) and 1 for the Storage Accounts (/images). The latter one will be configured to route by latency (default)

<https://learn.microsoft.com/en-us/azure/frontdoor/create-front-door-portal>

<https://learn.microsoft.com/en-us/azure/frontdoor/front-door-route-matching? pivots=front-door-standard-premium#frontend-host-matching>

The App Service Routing Rules specifies the precise paths, the Storage Account routing rule

upvoted 7 times

 **TJ001** 1 year ago

for storage account yes ...it will be one pool containing two storage accounts... but for app service it should be separate as the routing is totally path based ...so 3 ,3

upvoted 7 times

 **roshingrg** Most Recent 7 months, 2 weeks ago

To meet the requirements mentioned, you would need to create the following backend pools and routing rules:

Backend pools:

Backend pool for App1uk: This backend pool will include the App1uk Azure App Service.

Backend pool for App1us: This backend pool will include the App1us Azure App Service.

Backend pool for the storage account closest to the user: This backend pool will include the storage account in the location closest to the user.

Routing rules:

Routing rule for <https://contoso.azurefd.net/uk>: This routing rule will route requests to the App1uk backend pool when the URL is <https://contoso.azurefd.net/uk>.

Routing rule for <https://contoso.azurefd.net/us>: This routing rule will route requests to the App1us backend pool when the URL is <https://contoso.azurefd.net/us>.

Routing rule for <https://contoso.azurefd.net/images>: This routing rule will route requests to the backend pool for the storage account closest to the user when the URL is <https://contoso.azurefd.net/images>.

Therefore, the minimum number of backend pools to create is 3, and the minimum number of routing rules to create is also 3.

upvoted 4 times

 **Cabelen** 10 months ago

2 and 2, 2 different websites required each one requires 1 backend pool and 1 rules.

upvoted 1 times

 **Apptech** 10 months, 1 week ago

Agree to 3 backend pools and 3 Rules. Check this video on minute 4:37: <https://www.bing.com/videos/search?q=azure+front+door+%22latency%22+traffic-routing&view=detail&mid=DB458D3377D5DDEBD61DDB458D3377D5DDEBD61D&&FORM=VRD GAR&ru=%2Fvideos%2Fsearch%3Fq%3Dazure%2520front%2520door%2520%2522latency%2522%2520traffic-routing%26qs%3Dn%26form%3DQBVR%26%3D%2525eIhren%2520Suchverlauf%2520verwalten%2525E%26sp%3D-1%26lq%3D0%26pq%3Dazure%2520front%2520door%2520%2522latency%2522%2520traffic-routing%26sc%3D10-42%26sk%3D%26cvid%3D2EA1718352724A27AAB92A15B0444F7B%26ghsh%3D0%26ghacc%3D0%26ghpl%3D>

[q=azure+front+door+%22latency%22+traffic-routing&view=detail&mid=DB458D3377D5DDEBD61DDB458D3377D5DDEBD61D&&FORM=VRD GAR&ru=%2Fvideos%2Fsearch%3Fq%3Dazure%2520front%2520door%2520%2522latency%2522%2520traffic-routing%26qs%3Dn%26form%3DQBVR%26%3D%2525eIhren%2520Suchverlauf%2520verwalten%2525E%26sp%3D-1%26lq%3D0%26pq%3Dazure%2520front%2520door%2520%2522latency%2522%2520traffic-routing%26sc%3D10-42%26sk%3D%26cvid%3D2EA1718352724A27AAB92A15B0444F7B%26ghsh%3D0%26ghacc%3D0%26ghpl%3D](https://www.bing.com/videos/search?q=azure+front+door+%22latency%22+traffic-routing&view=detail&mid=DB458D3377D5DDEBD61DDB458D3377D5DDEBD61D&&FORM=VRD GAR&ru=%2Fvideos%2Fsearch%3Fq%3Dazure%2520front%2520door%2520%2522latency%2522%2520traffic-routing%26qs%3Dn%26form%3DQBVR%26%3D%2525eIhren%2520Suchverlauf%2520verwalten%2525E%26sp%3D-1%26lq%3D0%26pq%3Dazure%2520front%2520door%2520%2522latency%2522%2520traffic-routing%26sc%3D10-42%26sk%3D%26cvid%3D2EA1718352724A27AAB92A15B0444F7B%26ghsh%3D0%26ghacc%3D0%26ghpl%3D)

[routing%26qs%3Dn%26form%3DQBVR%26%3D%2525eIhren%2520Suchverlauf%2520verwalten%2525E%26sp%3D-1%26lq%3D0%26pq%3Dazure%2520front%2520door%2520%2522latency%2522%2520traffic-routing%26sc%3D10-42%26sk%3D%26cvid%3D2EA1718352724A27AAB92A15B0444F7B%26ghsh%3D0%26ghacc%3D0%26ghpl%3D](https://www.bing.com/videos/search?q=azure+front+door+%22latency%22+traffic-routing&view=detail&mid=DB458D3377D5DDEBD61DDB458D3377D5DDEBD61D&&FORM=VRD GAR&ru=%2Fvideos%2Fsearch%3Fq%3Dazure%2520front%2520door%2520%2522latency%2522%2520traffic-routing%26qs%3Dn%26form%3DQBVR%26%3D%2525eIhren%2520Suchverlauf%2520verwalten%2525E%26sp%3D-1%26lq%3D0%26pq%3Dazure%2520front%2520door%2520%2522latency%2522%2520traffic-routing%26sc%3D10-42%26sk%3D%26cvid%3D2EA1718352724A27AAB92A15B0444F7B%26ghsh%3D0%26ghacc%3D0%26ghpl%3D)

[1%26lq%3D0%26pq%3Dazure%2520front%2520door%2520%2522latency%2522%2520traffic-routing%26sc%3D10-42%26sk%3D%26cvid%3D2EA1718352724A27AAB92A15B0444F7B%26ghsh%3D0%26ghacc%3D0%26ghpl%3D](https://www.bing.com/videos/search?q=azure+front+door+%22latency%22+traffic-routing&view=detail&mid=DB458D3377D5DDEBD61DDB458D3377D5DDEBD61D&&FORM=VRD GAR&ru=%2Fvideos%2Fsearch%3Fq%3Dazure%2520front%2520door%2520%2522latency%2522%2520traffic-routing%26qs%3Dn%26form%3DQBVR%26%3D%2525eIhren%2520Suchverlauf%2520verwalten%2525E%26sp%3D-1%26lq%3D0%26pq%3Dazure%2520front%2520door%2520%2522latency%2522%2520traffic-routing%26sc%3D10-42%26sk%3D%26cvid%3D2EA1718352724A27AAB92A15B0444F7B%26ghsh%3D0%26ghacc%3D0%26ghpl%3D)

[42%26sk%3D%26cvid%3D2EA1718352724A27AAB92A15B0444F7B%26ghsh%3D0%26ghacc%3D0%26ghpl%3D](https://www.bing.com/videos/search?q=azure+front+door+%22latency%22+traffic-routing&view=detail&mid=DB458D3377D5DDEBD61DDB458D3377D5DDEBD61D&&FORM=VRD GAR&ru=%2Fvideos%2Fsearch%3Fq%3Dazure%2520front%2520door%2520%2522latency%2522%2520traffic-routing%26qs%3Dn%26form%3DQBVR%26%3D%2525eIhren%2520Suchverlauf%2520verwalten%2525E%26sp%3D-1%26lq%3D0%26pq%3Dazure%2520front%2520door%2520%2522latency%2522%2520traffic-routing%26sc%3D10-42%26sk%3D%26cvid%3D2EA1718352724A27AAB92A15B0444F7B%26ghsh%3D0%26ghacc%3D0%26ghpl%3D)

[You can see that a rule maps a frontend host \(in our case contoso.azurefd.net\) and a matching URL path to a specific backend pool. So, it is a 1:1 relation. Each URL needs 1 backend pool. We have three URLs. /uk, /us, /images. Backend Pool for uk contains 1 backend, same for us. Backend pool for images contains 2 backends. within the routing rule you can define routing method](https://www.bing.com/videos/search?q=azure+front+door+%22latency%22+traffic-routing&view=detail&mid=DB458D3377D5DDEBD61DDB458D3377D5DDEBD61D&&FORM=VRD GAR&ru=%2Fvideos%2Fsearch%3Fq%3Dazure%2520front%2520door%2520%2522latency%2522%2520traffic-routing%26qs%3Dn%26form%3DQBVR%26%3D%2525eIhren%2520Suchverlauf%2520verwalten%2525E%26sp%3D-1%26lq%3D0%26pq%3Dazure%2520front%2520door%2520%2522latency%2522%2520traffic-routing%26sc%3D10-42%26sk%3D%26cvid%3D2EA1718352724A27AAB92A15B0444F7B%26ghsh%3D0%26ghacc%3D0%26ghpl%3D)

[You can see that a rule maps a frontend host \(in our case contoso.azurefd.net\) and a matching URL path to a specific backend pool. So, it is a 1:1 relation. Each URL needs 1 backend pool. We have three URLs. /uk, /us, /images. Backend Pool for uk contains 1 backend, same for us. Backend pool for images contains 2 backends. within the routing rule you can define routing method](https://www.bing.com/videos/search?q=azure+front+door+%22latency%22+traffic-routing&view=detail&mid=DB458D3377D5DDEBD61DDB458D3377D5DDEBD61D&&FORM=VRD GAR&ru=%2Fvideos%2Fsearch%3Fq%3Dazure%2520front%2520door%2520%2522latency%2522%2520traffic-routing%26qs%3Dn%26form%3DQBVR%26%3D%2525eIhren%2520Suchverlauf%2520verwalten%2525E%26sp%3D-1%26lq%3D0%26pq%3Dazure%2520front%2520door%2520%2522latency%2522%2520traffic-routing%26sc%3D10-42%26sk%3D%26cvid%3D2EA1718352724A27AAB92A15B0444F7B%26ghsh%3D0%26ghacc%3D0%26ghpl%3D)

[Backend Pool for uk contains 1 backend, same for us. Backend pool for images contains 2 backends. within the routing rule you can define routing method](https://www.bing.com/videos/search?q=azure+front+door+%22latency%22+traffic-routing&view=detail&mid=DB458D3377D5DDEBD61DDB458D3377D5DDEBD61D&&FORM=VRD GAR&ru=%2Fvideos%2Fsearch%3Fq%3Dazure%2520front%2520door%2520%2522latency%2522%2520traffic-routing%26qs%3Dn%26form%3DQBVR%26%3D%2525eIhren%2520Suchverlauf%2520verwalten%2525E%26sp%3D-1%26lq%3D0%26pq%3Dazure%2520front%2520door%2520%2522latency%2522%2520traffic-routing%26sc%3D10-42%26sk%3D%26cvid%3D2EA1718352724A27AAB92A15B0444F7B%26ghsh%3D0%26ghacc%3D0%26ghpl%3D)

[Backend Pool for uk contains 1 backend, same for us. Backend pool for images contains 2 backends. within the routing rule you can define routing method](https://www.bing.com/videos/search?q=azure+front+door+%22latency%22+traffic-routing&view=detail&mid=DB458D3377D5DDEBD61DDB458D3377D5DDEBD61D&&FORM=VRD GAR&ru=%2Fvideos%2Fsearch%3Fq%3Dazure%2520front%2520door%2520%2522latency%2522%2520traffic-routing%26qs%3Dn%26form%3DQBVR%26%3D%2525eIhren%2520Suchverlauf%2520verwalten%2525E%26sp%3D-1%26lq%3D0%26pq%3Dazure%2520front%2520door%2520%2522latency%2522%2520traffic-routing%26sc%3D10-42%26sk%3D%26cvid%3D2EA1718352724A27AAB92A15B0444F7B%26ghsh%3D0%26ghacc%3D0%26ghpl%3D)

[Backend Pool for uk contains 1 backend, same for us. Backend pool for images contains 2 backends. within the routing rule you can define routing method](https://www.bing.com/videos/search?q=azure+front+door+%22latency%22+traffic-routing&view=detail&mid=DB458D3377D5DDEBD61DDB458D3377D5DDEBD61D&&FORM=VRD GAR&ru=%2Fvideos%2Fsearch%3Fq%3Dazure%2520front%2520door%2520%2522latency%2522%2520traffic-routing%26qs%3Dn%26form%3DQBVR%26%3D%2525eIhren%2520Suchverlauf%2520verwalten%2525E%26sp%3D-1%26lq%3D0%26pq%3Dazure%2520front%2520door%2520%2522latency%2522%2520traffic-routing%26sc%3D10-42%26sk%3D%26cvid%3D2EA1718352724A27AAB92A15B0444F7B%26ghsh%3D0%26ghacc%3D0%26ghpl%3D)

upvoted 1 times

 **saad_SEIU** 10 months, 1 week ago

I asked ChatGPT, answer is 3 rules and 4 backend pools and I think that is correct.

The backend pools would be:

App1uk pool - contains the backend instances for the UK app

App1us pool - contains the backend instances for the US app

StorageAccountUK pool - contains the backend instance for the storage account storing images for users in the UK

StorageAccountUS pool - contains the backend instance for the storage account storing images for users in the US

The routing rules would be:

Route requests to <https://contoso.azurefd.net/uk> to the App1uk backend pool.

Route requests to <https://contoso.azurefd.net/us> to the App1us backend pool.

Route requests to <https://contoso.azurefd.net/images> to the appropriate backend pool based on the geographic location of the user.

- a. If the user is located in the UK, route the request to the StorageAccountUK pool.
- b. If the user is located in the US, route the request to the StorageAccountUS pool.

So, you would need three routing rules and four backend pools to meet the requirements you specified.
upvoted 1 times

  **DeepMoon** 1 year ago

Each URL is a separate 'edge front end' on Azure Front Door. with its own Routing Rule and its own backend pool.
<https://learn.microsoft.com/en-us/azure/frontdoor/quickstart-create-front-door>
upvoted 2 times

  **DeepMoon** 1 year ago

But correcting myself there are 3 frontends here; each frontend with a rule will require 3 rules.
upvoted 6 times

  **TJ001** 1 year ago

I agree with this 3 urls needed 3 rules...
upvoted 5 times

  **TJ001** 1 year ago

it is called origin groups and not backend poolfrontend is called endpoint...
upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT

-

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

Name	Location
RG1	East US
RG2	UK West

You have the virtual networks shown in the following table.

Name	Location	Subnet	Resource group
Vnet1	East US	Sb1	RG1
Vnet1	East US	Sb2	RG1
Vnet2	West US	Sb3	RG2
Vnet2	West US	Sb4	RG2

Vnet1 contains two virtual machines named VM1 and VM2. Vnet2 contains two virtual machines named VM3 and VM4.

You have the network security groups (NSGs) shown in the following table that include only default rules.

Name	Associated to
Nsg1	Sb1
Nsg2	Network interface of VM2
Nsg3	Network interface of VM3
Nsg4	Sb4

You have the Azure load balancers shown in the following table.

Name	Resource group	Location	Type	Backend pool	Virtual machine	Rule
Lb1	RG1	East US	Public	Vnet1	VM1	Protocol: TCP Port: 80 Backend port: 80
Lb2	RG2	West US	Internal	Vnet2	VM3	Protocol: TCP Port: 1433 Backend port: 1433

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements	Yes	No
VM2 can be added to the backend pool of Lb2.	<input type="radio"/>	<input type="radio"/>
VM4 can access VM3 via port 1433 by using the frontend address of Lb2.	<input type="radio"/>	<input type="radio"/>
VM1 can be accessed via port 80 from the internet by using the frontend address of Lb1.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Statements	Yes	No
VM2 can be added to the backend pool of Lb2.	<input type="radio"/>	<input checked="" type="radio"/>
VM4 can access VM3 via port 1433 by using the frontend address of Lb2.	<input checked="" type="radio"/>	<input type="radio"/>
VM1 can be accessed via port 80 from the internet by using the frontend address of Lb1.	<input checked="" type="radio"/>	<input type="radio"/>

NoeHdzMII Highly Voted 1 year ago

- 1. NO. A backend pool can only contain resources from one virtual network. VM2 (VNet1) VM3 (VNet2)
 - 2. YES. using the frontend Ip address.
 - 3. NO. the default NSGs are blocking any ingress internet traffic
- upvoted 14 times

Goofer 1 year ago

- 3. YES. NSG is Blocking ingress internet traffic but not traffic from the load balancer. (AllowAzureLoadBalancerInBound)
- upvoted 9 times

bp_a_user 3 months, 1 week ago

No.
We have a NSG assigned to it and the question is about if traffic from the internet is blocked or not. By default, NSG blocks traffic from the internet

upvoted 1 times

tftfk 8 months ago

- 3. YES.

Inbound default Security Rules:

AllowVNetInbound: Allows inbound traffic from within the virtual network.
AllowAzureLoadBalancerInbound: Allows inbound traffic from Azure Load Balancer.
DenyAllInbound: Denies all inbound traffic from any source.

so as Goofer said NSG is Blocking ingress internet traffic but not traffic from the load balancer.

upvoted 3 times

Ditka 6 months, 1 week ago

*AllowAzureLoadBalancerInbound: Allows Azure LB Health probe ONLY

<https://learn.microsoft.com/en-us/azure/virtual-network/service-tags-overview>

upvoted 3 times

Lazylinux 4 months, 3 weeks ago

Rubbish and you have NO idea what you talking about
read here nothing to do with health probes, beside health probes are internal backend mechanism!!

<https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview>

upvoted 1 times

JohnnyChimpo 8 months, 2 weeks ago

- 3 is YES - Default NSG rules all have a AllowAzureLoadBalancerInbound rule
- upvoted 2 times

occupatissimo 8 months ago

that's for LB probes, not for client traffic

upvoted 3 times

 **SaadKhamis** 9 months ago

3. Tested in the lab and confirmed answer to be NO.
A rule for port 80 must be added to the NSG to be able to reach VM1 using port 80.

upvoted 7 times

 **Madball** 11 months, 4 weeks ago

Completely agree with this.

upvoted 1 times

 **sotec** Most Recent 1 month, 2 weeks ago

What NSG is linked to VM1?
Is the VM1 in the subnet1 or subnet2?
The NSG is working in subnet1 or subnet2?

upvoted 2 times

 **_Cris** 4 months, 1 week ago

appears on exam, 19 Sept 2023

upvoted 3 times

 **Lazylinux** 4 months, 3 weeks ago

No YES YES for sure..all seem to agree on 1 and 2 but not 3..here is why 3 is YES - as per some others comments All incoming traffic from Load Public Balancer are Allowed via service tags which are logical collection of IP address from Azure, think logic!! it is Azure trusted service, why would they BLOCK it!! read further here

<https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview>

upvoted 3 times

 **magnem66** 4 months, 2 weeks ago

Here's the reason they block it by default.

<https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-overview>

The relevant section is "Secure by default"

3 is NO.

upvoted 3 times

 **occupatissimo** 8 months, 2 weeks ago

3. always start learning from overview: <https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-overview>

Standard -> Standard load balancers and standard public IP addresses are closed to inbound connections unless opened by Network Security Groups.

Basic -> open to the internet by default

In this case SKU is missing

upvoted 1 times

 **azure_dori** 5 months, 1 week ago

You're absolutely right. The third question is NO. I deduce that the LB SKU is Standard, because for Basic the backend pool can only be a scale/availability set.

upvoted 2 times

 **occupatissimo** 8 months, 2 weeks ago


however basic is never for production so 3 is N

upvoted 2 times

 **Tasli6** 7 months ago


Yes, but there is a rule allowing port 80 on the LB1 therefore its open.

upvoted 1 times

 **sierra1784** 8 months, 3 weeks ago

3. NO - When you create NSGs to filter traffic coming through an Azure Load Balancer, the source port and address range applied are from the originating computer, not the load balancer frontend.

upvoted 2 times

 **flurgen248** 9 months ago

1. No - It's in another VNET and would need another backend pool

2. Yes - It's in the same VNET, so default rules allow it.

3. No -

Virtual machines in load-balanced pools: The source port and address range applied are from the originating computer, not the load balancer. The destination port and address range are for the destination computer, not the load balancer.

<https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#azure-platform-considerations>

So the NSG would still block traffic internet traffic, because the Source IP isn't from the load balancer.

upvoted 2 times

 **hal01** 9 months, 2 weeks ago

NO,YES,No

NO, VM2 in not in the VNET 2 so it's an another network and cannot be add to the backend pool

YES, because they can use the public ip address

NO, because the the network security groups (NSGs) include only default rules

upvoted 2 times

  **_fvt** 9 months, 3 weeks ago

N - VM2 is not in the same VNet and cannot be added to the backend pool
Y - VM4 is in the same VNet than Lb2 so it can access his fronted IP therefore access VM3 through it
Y - VM1 is in Lb1 backend pool. Lb1 is a public LB and rule specify port 80

NSGs should not be an issue there because it's specified that they have default rules only. These default rules allow Inbound Loadbalancers traffic; VNet to VNet traffic (inbound and outbound); and outbound internet access.

<https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview>

upvoted 1 times

  **_fvt** 9 months, 3 weeks ago

After further reading, the 3rd should be "No": Azure Load Balancer is not an App Gateway / a Reverse Proxy and doesn't replace the client IP address.

<https://stackoverflow.com/questions/59541796/how-to-restrict-direct-access-from-internet-to-azure-public-loadbalancer-backend>
"for example, client1 send a request to backend via LB front IP, it will generate a flow source client1, source port, protocol, destination LB IP, destination port. When hitting the load balancer, with Inbound NAT rules, it will change to source client1, source port, protocol, destination VM IP, dest port but the source IP for incoming traffic does not change, the NSG rule still is evaluated with the same source IP in the inbound rules. with LB or not, it will work the same for a client for NSG rules."

upvoted 4 times

  **alkorkin** 1 year ago

3. Will be YES just in case we have Basic LB. Standard requires NSG in order to explicitly open access from the Internet

upvoted 2 times

  **DeepMoon** 1 year ago

1. No - Lb2 is a ILB in US West. VM2 is in East US. ILB cannot use cross region load balancing.

<https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-basic-upgrade-guidance#basic-load-balancer-sku-vs-standard-load-balancer-sku>

2. Yes- VM3 is connected to Lb2 and backend port 1433

3. Yes - Port 80 is opened on Lb1.

upvoted 3 times

  **TJ001** 1 year ago

3- port is defined in LB1 but not in the default NSG attached

upvoted 1 times

  **TJ001** 1 year ago

my bad ...did not watch that the load balancer is a public so 3. YES

upvoted 2 times

  **magnem66** 4 months, 1 week ago

You were right the first time. Port 80 needs to be open on the NSG.



So 3 is NO.

upvoted 2 times

  **DeepMoon** 1 year ago

Box 1 : can be Yes depending on the load balancer SKU being basic or standard. That is currently not given. So you cannot definitively answer this question.

upvoted 1 times

  **tester2023** 12 months ago

The issue isn't SKU-related. The issue with adding the VM is that it is on a different vNet than the LB, which isn't allowed.

upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

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

Name	Type	Description
App1	Azure App Service	A web app
Gateway1	Azure Application Gateway	includes an SSL certificate that has a subject name of *.contoso.com

Gateway1 provides access to App1 by using a URL of https://app1.contoso.com.

You create a new web app named App2.

You need to configure Gateway1 to enable access to App2 by using a URL of https://app2.contoso.com. The solution must minimize administrative effort.

What should you configure on Gateway1?

- A. a backend pool and a routing rule
- B. a listener and a routing rule
- C. a listener, a backend pool, and a routing rule
- D. a listener and a backend pool

Correct Answer: B

Community vote distribution

C (62%)

A (38%)

 **energie** Highly Voted 11 months, 2 weeks ago

Selected Answer: C

You can't use the same backend pool.
upvoted 7 times

 **daemon101** Highly Voted 6 months, 1 week ago


Selected Answer: A

Since we have a wildcard certificate *.contoso.com, we can just use the same listener with multi-site. Hence, i would go for add a rule and backend pool.

Using a wildcard character in the host name, you can match multiple host names in a single listener. For example, *.contoso.com can match with ecom.contoso.com, b2b.contoso.com and customer1.b2b.contoso.com and so on.

<https://learn.microsoft.com/en-us/azure/application-gateway/multiple-site-overview#wildcard-host-names-in-listener>

upvoted 6 times

 **Lazylinux** 1 month, 3 weeks ago

Totally incorrect and i cant believe 4 people voted this answer- here is why you wrong for sure and ANSWER is for sure C

1- You need to know the routing rule and the listener go in ratio 1-1 i.e. for every rule there MUST be 1 listener and vice versa and NO listener can be associated with more than 1 rule and vice versa - simple proof of this go to your Azure subscription if you have one!!! try from scratch create a rule and routing rule and associate them then try to create another rule - when you try to select listener for the rule it will Prompt you with error message and goes like this "There is NO unassociated listener, please create listener first!!"

2- The multi site option which is by the way ONLY available in App GWY V2 is to be used when you have Domain with multiple sub-domains that you want to point to the same backend pool then you use it as opposed to App GWY V1 where you have to create multiple rules and listeners!!

upvoted 1 times

 **PandaTuga** 1 month, 2 weeks ago

Perhaps you should invest on your knowledge instead of criticizing the ones who knows
upvoted 1 times

 **GBAU** Most Recent 3 months ago

Selected Answer: C

What should you CONFIGURE on Gateway1?

Configure a listener to listen for app2.contoso.com

Configure a backend pool to add App2

Configure a routing rule to direct traffic for app2.contoso.com to go to App2.

Configuring can mean Changing or Creating, it is still configuring.

upvoted 1 times

🗨️ 👤 **Lazylinux** 4 months, 2 weeks ago

Selected Answer: C

I C for sure

it is different FQDN and hence routing rule is required which includes both backend and listener and because both URL are different app1 and app2 then backend is different as for the cert it is wild card and hence can be used for both app1 and app2 urls

upvoted 1 times

🗨️ 👤 **Lazylinux** 1 month, 3 weeks ago

further add to my explanation since some people are confused and as per below

Remember the 2 points below

1- You need to know the routing rule and the listener go in ratio 1-1 i.e. for every rule there MUST be 1 listener and vice versa and NO listener can be associated with more than 1 rule and vice versa - simple proof of this go to your Azure subscription if you have one!!! try from scratch create a rule and routing rule and associate them then try to create another rule - when you try to select listener for the rule it will Prompt you with error message and goes like this "There is NO unassociated listener, please create listener first!!"

2- The multi site option which is by the way ONLY available in App GWY V2 is to be used when you have Domain with multiple sub-domains that you want to point to the same backend pool then you use it as opposed to App GWY V1 where you have to create multiple rules and listeners!!

upvoted 2 times

🗨️ 👤 **7e13aa4** 6 months ago

Selected Answer: A

we can use listener with multi-site.

upvoted 4 times

🗨️ 👤 **roshingrg** 7 months, 2 weeks ago

In order to enable access to App2 through Gateway1 with the URL <https://app2.contoso.com>, you need to configure the following components:

Listener: A listener is responsible for handling incoming traffic and directing it to the appropriate backend pool based on the defined routing rules. In this case, you need to configure a new listener on Gateway1 to handle requests for the URL <https://app2.contoso.com>.

Backend Pool: A backend pool is a collection of resources that can serve the incoming requests. In this scenario, you need to create a new backend pool specifically for App2, which will contain the necessary resources (in this case, the web app App2).

Routing Rule: A routing rule determines how the incoming requests should be forwarded to the appropriate backend pool. In this case, you need to create a routing rule that matches requests for the URL <https://app2.contoso.com> and directs them to the backend pool associated with App2.

By configuring a listener, a backend pool, and a routing rule, you can ensure that Gateway1 routes the incoming requests for <https://app2.contoso.com> to the correct backend pool (App2), thus enabling access to App2 through the specified URL.

upvoted 3 times

🗨️ 👤 **_fvt** 9 months, 3 weeks ago

Selected Answer: C

You will have to use a multi site listener to be able to listen on the same (HTTPS) for specific host only, then you will create a routing rule to a NEW back-end pool (you don't want to balance the traffic between the two app service but separate it for each listener)

upvoted 1 times

🗨️ 👤 **MightyMonarch74** 10 months ago

backend pool and rule

upvoted 2 times

🗨️ 👤 **harshit101** 11 months, 2 weeks ago

Selected Answer: C

Backend pool also needed

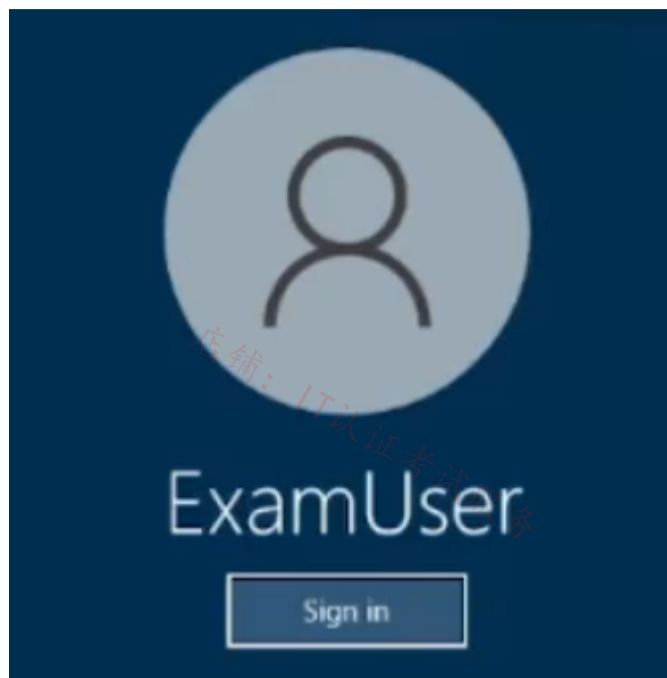
upvoted 6 times

店铺: IT认证考试服务

店铺: IT认证考试服务

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You plan to deploy a firewall to subnet1-2. The firewall will have an IP address of 10.1.2.4.

You need to ensure that traffic from subnet1-1 to the IP address range of 192.168.10.0/24 is routed through the firewall that will be deployed to subnet 1-2. The solution must be achieved without using dynamic routing protocol.

To complete this task, sign in to the Azure portal.

Correct Answer:

Custom routes, User-defined

You can create custom, or user-defined (static), routes in Azure to override Azure's default system routes, or to add more routes to a subnet's route table. In Azure, you create a route table, then associate the route table to zero or more virtual network subnets. Each subnet can have zero or one route table associated to it.

Create a route table (Skip Step 1 to Step 4 if route table already present=

Step 1: From the Azure portal menu, select + Create a resource > Networking > Route table, or search for Route table in the portal search box.

Step 2: Select Create.

Step 3: On the Basics tab of Create route table, enter or select information:

Home > New > Route table >

Create Route table

Basics Tags Review + create

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ Contoso Subscription

Resource group * ⓘ myResourceGroup
[Create new](#)

Instance details

Region * ⓘ East US

Name * ⓘ myRouteTablePublic

Propagate gateway routes * ⓘ Yes No

[Review + create](#) < Previous Next : Tags >

Step 4: Select the Review + create tab, or select the blue Review + create button at the bottom of the page.

Create a route

In this section, you'll create a route in the route table that you created in the previous steps.

Step 5: Select Go to resource or Search for myRouteTablePublic (The route table you created earlier) in the portal search box.

Step 6: In the myRouteTablePublic page, select Routes from the Settings section.

Step 7: In the Routes page, select the + Add button.

Step 8: In Add route, enter or select this information:

Route name: SomeName

Address prefix destination: Select IP Addresses.

Destination IP addresses/CIDR ranges: Enter 192.168.10.0/24 - The address range of to be routed from.

Next hop type: Select Virtual appliance.

Next hop address: Enter 10.1.2.4 (The address of the firewall in the sbunet1-2 subnet).

Reference:

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview>

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

upvoted 13 times

店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

You have two Azure virtual networks in the East US Azure region as shown in the following table.

Name	IP address space
Vnet1	192.168.0.0/20
Vnet2	10.0.0.0/20

The virtual networks are peered to one another. Each virtual network contains four subnets.

You plan to deploy a virtual machine named VM1 that will inspect and route traffic between all the subnets on both the virtual networks.

What is the minimum number of IP addresses that you must assign to VM1?

- A. 1
- B. 2
- C. 4
- D. 8

Correct Answer: B

Community vote distribution

A (100%)

 **jonav94** Highly Voted 9 months ago

Selected Answer: A

I think it must be 1, both vnets are peered so we don't need to add an IP from each vnet.

upvoted 5 times

 **Lazylinux** Most Recent 4 months, 2 weeks ago

Selected Answer: A

A is the answer

This is really typical silly MS question nothing but confusing!!

If vNET networks are peered then both networks can communicate free with each other via the Microsoft Backbone NOT gateway and the only way to control resource access from one Vnet to another is via NSG. The only time you will need a Gateway is when you have on-Prem access requirements from Peered vNETS than ONLY one vNET can have gateway and other uses it as transit point to on-prem.

Also all subnets within the same vNET can communicate free with each other


So having 1 VM inspect and route traffic between all the subnets on both the virtual networks DOES NOT MAKE SENSE but anyway it requires 1 IP but if the vNETs were NOT peered then the VM acts as router and in that case 2 IPs

upvoted 3 times

 **y0eri** 3 days, 5 hours ago

You can associate multiple NICs on a VM to multiple subnets, but those subnets must all reside in the same virtual network (vNet).

upvoted 1 times

 **Kipper_2022** 8 months, 1 week ago

Selected Answer: A

agree with Jonav94

upvoted 1 times

 **_fvt** 9 months, 3 weeks ago

Selected Answer: A

<https://learn.microsoft.com/en-us/azure/firewall/firewall-faq#can-azure-firewall-forward-and-filter-network-traffic-between-subnets-in-the-same-virtual-network-or-peered-virtual-networks>

Can Azure Firewall forward and filter network traffic between subnets in the same virtual network or peered virtual networks?

Yes. However, configuring the UDRs to redirect traffic between subnets in the same VNET requires additional attention. While using the VNET address range as a target prefix for the UDR is sufficient, this also routes all traffic from one machine to another machine in the same subnet through the Azure Firewall instance. To avoid this, include a route for the subnet in the UDR with a next hop type of VNET. Managing these routes might be cumbersome and prone to error. The recommended method for internal network segmentation is to use Network Security Groups, which don't require UDRs.

upvoted 4 times

MrBlueSky 9 months, 3 weeks ago

This link and answer are completely irrelevant to the question being asked.

The question asks about setting up a VM to perform this traffic inspection, not an Azure Firewall. The VM would function as a Network Virtual Appliance (NVA). NVAs are frequently configured as Firewalls using third party OS (Barracuda, Palo Alto, Cisco, etc), but this doesn't make it an Azure Firewall.

This should be easily doable with a single IP on the NIC attached to the VM that will be configured as an NVA.

Answer = 1

upvoted 8 times

Question #41

Topic 3

You have an Azure subscription that contains the following resources:

- A virtual network named Vnet1
- Two subnets named subnet1 and AzureFirewallSubnet
- A public Azure Firewall named FW1
- A route table named RT1 that is associated to Subnet1
- A rule routing of 0.0.0.0/0 to FW1 in RT1

After deploying 10 servers that run Windows Server to Subnet1, you discover that none of the virtual machines were activated.

You need to ensure that the virtual machines can be activated.

What should you do?

- A. On FW1, configure a DNAT rule for port 1688
- B. Deploy a NAT gateway.
- C. Add an internet route to RT1 for the Azure Key Management Service (KMS).
- D. To Subnet1, associate a network security group (NSG) that allows outbound access to port 1688.

Correct Answer: C

Community vote distribution

C (100%)

Ditka 6 months, 1 week ago

Same question, different answer. The answer to Topic 3, Q24 states to add a rule to FW1 to allow outbound traffic to the Azure KMS. Both will accomplish the goal, but bypassing your FW should not be best practice. An "Internet" route sends the traffic directly to the Azure Internet service which is always accessible by default or with "Internet" routes.

upvoted 1 times

makkelijzat 6 months, 3 weeks ago

Selected Answer: C

Same question, same answer...

upvoted 1 times

You have an on-premises network.

You have an Azure subscription that includes a virtual network named VNet1 and a private Azure Kubernetes Service (AKS) cluster named AKS1. VNet1 is connected to your on-premises environment via an Azure ExpressRoute circuit. AKS1 is connected to VNet1.

You need to implement an off-cluster ingress controller for AKS1. The solution must provide connectivity from the on-premises environment to containerized workloads hosted on AKS1.

Which Azure service should you use?

- A. Azure Application Gateway
- B. Azure Front Door
- C. Azure Traffic Manager
- D. Azure Load Balancer

Correct Answer: A

Community vote distribution

A (100%)


 **Lazylinux** 4 months, 2 weeks ago

Selected Answer: A

A is correct as per

<https://learn.microsoft.com/en-us/azure/application-gateway/tutorial-ingress-controller-add-on-existing>

upvoted 2 times

 **flurgen248** 9 months ago


Selected Answer: A

Answer is A.

The Application Gateway Ingress Controller (AGIC) is a Kubernetes application, which makes it possible for Azure Kubernetes Service (AKS) customers to leverage Azure's native Application Gateway L7 load-balancer to expose cloud software to the Internet.

<https://learn.microsoft.com/en-us/azure/application-gateway/ingress-controller-overview>

upvoted 1 times

 **Ben_88** 7 months, 2 weeks ago

But AGIC is within the K8s cluster , question ask for a an ingress controller outside the cluster . would go with D

upvoted 1 times

 **Apptech** 9 months, 1 week ago

A is correct. reference: <https://learn.microsoft.com/en-us/azure/application-gateway/ingress-controller-overview>

upvoted 1 times

 **seth_saurabh84** 9 months, 3 weeks ago

Why not D? AKS by default uses a standard load balancer for ingress. App Gateway will mean we are pointing towards AGIC which is not what the questions mentions.

upvoted 1 times

 **Marcoos** 7 months, 2 weeks ago

A load balancer will only do layer 4. Ingress controllers, if i remember correctly, will operate on layer 7 in the vast majority of cases. You need layer 7 functionality to do the type of ingress that's asked for.

upvoted 1 times

 **25max** 9 months, 3 weeks ago

The LB is in front of a service and does not provide ingress controller solution for the cluster only for the service that type is LoadBalancer.

upvoted 3 times

HOTSPOT

-

You are planning an Azure Front Door deployment that will contain the resources shown in the following table.

Name	Type
ASP93	App Service plan
Webapp93.azurewebsites.net	App Service
FD93.azurefd.net	Front Door

Users will connect to the App Service through Front Door by using a URL of <https://www.fabrikam.com>.

You obtain a certificate for the host name of www.fabrikam.com.

You need to configure a DNS record for www.fabrikam.com and upload the certificate to Azure.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Upload the certificate to:

▼

- A certificate in Active Directory Certificate Services (AD CS)
- A custom rule in Azure Web Application Firewall (WAF)
- An enterprise application in Azure AD
- A secret in Azure Key Vault

Set the DNS record target to:

▼

- ASP93
- fabrikam.com
- FD93.azurefd.net
- Webapp93.azurewebsites.net

Answer Area

Upload the certificate to:

▼

- A certificate in Active Directory Certificate Services (AD CS)
- A custom rule in Azure Web Application Firewall (WAF)
- An enterprise application in Azure AD
- A secret in Azure Key Vault**

Correct Answer:

Set the DNS record target to:

▼

- ASP93
- fabrikam.com
- FD93.azurefd.net**
- Webapp93.azurewebsites.net

 **MrBlueSky** Highly Voted 9 months, 3 weeks ago

Answer listed is correct: A Secret in Azure Key Vault + FD93.azurefd.net

Source: <https://learn.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain-https>
upvoted 13 times

 **Murad01** Most Recent 1 month, 3 weeks ago

Appeared on Exam November - 2023
upvoted 2 times

HOTSPOT

-

You have an Azure subscription that contains an app named App1. App1 is hosted on the Azure App Service instances shown in the following table.

Name	Location
AppSrv1	East US
AppSrv2	East US
AppSrv3	North Europe
AppSrv4	North Europe

You need to implement Azure Traffic Manager to meet the following requirements:

- App1 traffic must be assigned equally to each App Service instance in each Azure region.
- App1 traffic from North Europe must be routed to the App1 instances in the North Europe region.
- App1 traffic from North America must be routed to the App1 instances in the East US Azure region.
- If an App Service instance fails, all the traffic for that instance must be routed to the remaining instances in the same region.

How should you configure the Traffic Manager profiles? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Minimum number of Traffic Manager profiles required:

- 1
- 2
- 3
- 4

Routing method for the traffic in each region:

- Geographic
- Performance
- Priority
- Weighted

Answer Area

Minimum number of Traffic Manager profiles required:

- 1
- 2
- 3
- 4

Correct Answer:

Routing method for the traffic in each region:

- Geographic
- Performance
- Priority
- Weighted

 **manny72** Highly Voted 9 months, 2 weeks ago

One parent profile configured with geographical routing method, 2 child profiles configured with weighted routing method.

So:

3 minimum profiles

Weighted (the question is the routing method in each region)


upvoted 32 times

  **khksoma** 8 months, 4 weeks ago

I agree

It says - App1 traffic must be assigned equally to each App Service instance in each Azure region. So shouldn't it be weighted? Parent profile will have Geographic routing method, once it hits the child profiles in each region the traffic should be split equally between the instances(50/50).

upvoted 3 times

  **nazir_tpbf** 5 months, 3 weeks ago

bravo manny72

upvoted 1 times

  **daemon101** 6 months, 1 week ago



good catch for routing method in each region.

upvoted 2 times

  **stack120566** Highly Voted 9 months, 4 weeks ago



one parent profile configured for 'performance' and 2 child profiles configured for 'priority' each child profile configured on having 2 nodes.

upvoted 5 times

  **nazir_tpbf** 5 months, 3 weeks ago

priority will not distribute load equally as requested

upvoted 1 times

  **Ditka** 6 months, 1 week ago

It doesn't say go to the fastest one, it says go to a specific one. Only Geo will accomplish that.

upvoted 1 times

  **Murad01** Most Recent 1 month, 3 weeks ago

I think given answer is correct

upvoted 1 times

  **Apptech** 7 months, 4 weeks ago

Based on this description I would say Performance routing is correct and not the geographical routing: "Performance: Select Performance routing when you have endpoints in different geographic locations and you want end users to use the "closest" endpoint for the lowest network latency. Geographic: Select Geographic routing to direct users to specific endpoints (Azure, External, or Nested) based on where their DNS queries originate from geographically. With this routing method, it enables you to be in compliance with scenarios such as data sovereignty mandates, localization of content & user experience and measuring traffic from different regions." --> <https://learn.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods>

My conclusion:

1 parent profile T1 with performance routing

2 child profiles TM2 (North EU) and TM3 (EAST US) with weighted routing (50/50) and minChildEndpoint=1

upvoted 4 times

  **Apptech** 7 months, 4 weeks ago

in addition: we also have to think which method (geographic / performance) is better to route equally between the instances when requests originate from other regions that North Europe and East US

upvoted 1 times

  **occupatissimo** 8 months, 4 weeks ago

1) App1 traffic must be assigned equally to each App Service instance in each Azure region. -> weight method (look at the word assigned equally)

2) App1 traffic from North Europe must be routed to the App1 instances in the North Europe region. App1 traffic from North America must be routed to the App1 instances in the East US Azure region. -> geographic method in a child profile (look at the word "traffic from")

3) If an App Service instance fails, all the traffic for that instance must be routed to the remaining instances in the same region. -> in the child profile set MinChildEndpoints = 1

so 2 profiles and geographic method inside the region

upvoted 1 times

  **occupatissimo** 8 months, 2 weeks ago

sorry, i was absolutely drunk.

parent profile can be only geographic (if weighted could be EU request sent to US and viceversa)



then we have two location so we need a weighted child profile each one

total 3 profile (1 parent and 2 child) end weighted inside the region

MinChildEndpoints = 1 remain

problem here is how is build the question, be careful and read well !!

upvoted 3 times

  **crypto700** 9 months ago



the Given Answer is correct

Two profiles

Traffic Manager Profile 1 - Performance Routing method to distribute the traffic equally to each App Service instance in each Azure region.

Traffic Manager Profile 2 - Geographic Routing method

upvoted 2 times

  **crypto700** 9 months ago

I have read the questions again.. it seems we need 3 profiles (1 Parent profile with Geographical routing method + 2 Child for each region with Weighted method)
i think the right answers
3 Profile and Weighted for Each Region
upvoted 6 times

🗨️ 👤 **_fvt** 9 months, 3 weeks ago

I have difficulties understanding how it should be done with 2 or 3 profiles...

I would have created 4 profiles instead:

- TM_Parent : Geographical
- > World => TM_Child_All (AS1 AS2 AS3 AS4 / weighted 50-50)
- > NorthEurope => TM_Child_NE (AS3 AS4 / weighted 50-50)
- > NorthAmerica => TM_Child_EUS (AS1 AS2 / weighted 50-50)

So TM profiles: TM_Parent, TM_Child_All, TM_Child_NE, TM_Child_EUS

upvoted 2 times

🗨️ 👤 **flurgen248** 9 months ago

It doesn't need to be split evenly across all 4 app service instances, just across the instances in each listed region. You don't need the "World" profile TM_Child_All.

upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

You have an Azure subscription that contains the Azure App Service web apps shown in the following table.

Name	Location	Description
App1eu	West Europe	Production app service for a URL of https://www.fabrikam.com
App1us	East US	Standby app service for a URL of https://www.fabrikam.com

You need to deploy Azure Traffic Manager. The solution must meet the following requirements:

- Traffic to <https://www.fabrikam.com> must be directed to App1eu.
- If App1eu becomes unresponsive, all the traffic to <https://www.fabrikam.com> must be directed to App1us.

You need to implement Traffic Manager to meet the requirements.

Which two resources should you create? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. a Traffic Manager profile that uses the priority routing method
- B. a Traffic Manager profile that uses the geographic routing method
- C. a CNAME record in a DNS domain named fabrikam.com
- D. a TXT record in a DNS domain named fabricam.com
- E. a real user measurements key in Traffic Manager

Correct Answer: AC

Community vote distribution

AC (100%)


 **_fvt** Highly Voted 9 months, 3 weeks ago

Selected Answer: AC

Priority to force all traffic to active instance
DNS CName on your registrar to the Traffic manager DNS Name
upvoted 7 times

 **Zeppoonstream** 9 months, 1 week ago

but cant you also use a txt entry for varification?
upvoted 1 times

 **Ditka** 6 months, 1 week ago

Yes, you could, but that is not related to the question. Zone verification would be if you were starting to manage your own public DNS records in Azure public DNS. The question doesn't mention how the zone is managed, it only requires a record to be created.
upvoted 1 times

 **Zeppoonstream** 9 months, 1 week ago

i just checked the documentation. he is correct.
upvoted 1 times

HOTSPOT

-

You have an Azure subscription that contains an app named App1. App1 is deployed to the Azure App Service apps shown in the following table.

Name	Location	Worker instances
App1-East	East US 1	4
App1-West	West US 1	4

You need to publish App1 by using Azure Front Door. The solution must ensure that all the requests to App1 are load balanced between all the available worker instances.

What is the minimum number of origin groups and origins that you should configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Origin groups:

Origins:

Answer Area

Correct Answer:

Origin groups:

Origins:

 **sierra1784** Highly Voted 8 months, 3 weeks ago

1 group: Multi-region active/active deployment: Create a single origin group. Within that origin group, create an origin for each of the App Service apps.
2 origins: Your App Service app might be configured to scale out across worker instances, but from Front Door's perspective there's a single origin.

<https://learn.microsoft.com/en-us/azure/frontdoor/front-door-faq>
upvoted 10 times

 **Lazylinux** Most Recent 4 months, 2 weeks ago

This is bit tricky because of the workers, however workers are just instance that power single App i.e. highly localized availability not be mixed with Zonal availability.

Origin group was formally known as backend pool and origin backend target. So really there is ONLY one backendpool/Origin group is required and in the Origin Group there should be two origins/backend targets, so the answer is 1 and 2

upvoted 2 times

 **Lazylinux** 4 months, 2 weeks ago

Forgot to add the following from MS doco

For example, suppose you host an application on Azure App Service. The way that you configure Front Door depends on how many application instances you deploy:

Single-region deployment: Create a single origin group. Within that origin group, create a single origin to represent the App Service app. Your App Service app might be configured to scale out across worker instances, but from Front Door's perspective there's a single origin.

Multi-region active/passive deployment: Create a single origin group. Within that origin group, create an origin for each of the App Service apps. Configure each origin's priority to ensure that the primary application has a higher priority than the secondary application.

Multi-region active/active deployment: Create a single origin group. Within that origin group, create an origin for each of the App Service apps. Configure each origin's priority to be the same. Configure each origin's weight to set the proportion of requests that should go to that origin.

upvoted 1 times

 **occupatissimo** 8 months, 3 weeks ago

Define the origin group as a logical grouping of your application instances that receives the same traffic and responds with an expected behavior, then add the origins to this group.

So 1 group and 2 origins

<https://learn.microsoft.com/en-us/azure/frontdoor/origin?pivot=front-door-standard-premium>

upvoted 4 times

店铺: IT认证考试服务

店铺: IT认证考试服务

You have an Azure subscription that contains the following resources:

- A virtual network named Vnet1
- Two subnets named subnet1 and AzureFirewallSubnet
- A public Azure Firewall named FW1
- A route table named RT1 that is associated to Subnet1
- A rule routing of 0.0.0.0/0 to FW1 in RT1

After deploying 10 servers that run Windows Server to Subnet1, you discover that none of the virtual machines were activated.

You need to ensure that the virtual machines can be activated.

What should you do?

- A. On FW1, configure a DNAT rule for port 1688.
- B. On FW1, create an outbound network rule that allows traffic to the Azure Key Management Service (KMS).
- C. Deploy an application security group that allows outbound traffic to 1688.
- D. Deploy an Azure Standard Load Balancer that has an outbound NAT rule.

Correct Answer: B

Community vote distribution

B (100%)

Murad01 1 month, 3 weeks ago

I almost punch my screen when I see this question repeated 7 times
upvoted 1 times

Lazylinux 4 months, 2 weeks ago

Selected Answer: B

Too many repetitive questions - this is 3rd time this question repeated.... Gap filling!!
upvoted 2 times

ryuhei 6 months, 3 weeks ago

Selected Answer: B

Why put several questions with the same content?
upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

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

You deploy an instance of Azure Application Gateway v2 named AppGw1 to Subnet1. You create a network security group (NSG) named NSG1 and link NSG1 to Subnet1.

You need to ensure that AppGw1 will only load balance traffic that originates from VNet1. The solution must minimize the impact on the functionality of AppGw1.

What should you add to NSG1?

- A. an outbound rule that has a priority of 4096 and blocks all internet traffic
- B. an inbound rule that has a priority of 4096 and blocks all internet traffic
- C. an inbound rule that has a priority of 100 and blocks all internet traffic
- D. an outbound rule that has a priority 100 and blocks all internet traffic

Correct Answer: B

Community vote distribution

B (100%)

 **Lazylinux** Highly Voted 4 months, 2 weeks ago

Selected Answer: B

B is Honey

The given answer is correct, read more here

<https://learn.microsoft.com/en-us/azure/application-gateway/application-gateway-faq>

the part =>How do I use Application Gateway V2 with only private frontend IP address? Dont worry about the private the principal remains same for the public IP - pay attention to the images of NSG rules.

Also as handy note, remember this

classic good firewall rule practice. General rules should be low priority, and specific rules should be high priority. The more general, the lower. The more specific, the higher. The most general rule we have in firewalls is "block everything we don't allow"; in other words, we are creating a white list of exceptions with the previously mentioned rules. So port 4096 is correct

upvoted 8 times

 **Velidot100** 3 months, 3 weeks ago

Thank you for elaborating. At first, I thought priority number 100 was the correct answer. But your explanations makes sense.

upvoted 2 times

 **Bigfatdavey** Highly Voted 4 months, 3 weeks ago

should be an inbound rule that has a priority of 100 and blocks all internet traffic

upvoted 5 times

 **Lazylinux** 4 months, 2 weeks ago

WRONG if so will block legitimate traffic - Golden rule use low Priority number for specific custom rule and high number like 4096 for General custom rule to avoid blocking legitimate traffic

upvoted 2 times

 **Webesciaki** Most Recent 3 weeks, 6 days ago

Selected Answer: B

explanation IMHO is:

1) we need to allow "GatewayManager" service tag which is diff per region but in general it is public IP range.

Internet service tag - "The address range includes the Azure-owned public IP address space so we would block GatewayManager if we left block Internet on 100

upvoted 1 times

 **Webesciaki** 2 weeks, 6 days ago

actually that needs update:

"Network security groups associated to an Application Gateway subnet no longer require inbound rules for GatewayManager, and they don't require outbound access to the Internet. The only required rule is Allow inbound from AzureLoadBalancer to ensure health probes can reach the gateway"

<https://learn.microsoft.com/en-us/azure/application-gateway/application-gateway-private-deployment?tabs=portal#network-security-group-control>

upvoted 1 times

 **Tyler** 4 months, 3 weeks ago

4096 is right. if the rule has 100, then it blocks everything, even you have allowed rule after it, that rule will not work.

upvoted 2 times

Question #49

Topic 3

You plan to implement an Azure virtual network that will contain 10 virtual subnets. The subnets will use IPv6 addresses. Each subnet will host up to 200 load-balanced virtual machines.

You need to recommend a load balancing solution for the virtual network. The solution must meet the following requirements:

- The virtual machines and the load balancer must be accessible only from the virtual network.
- Costs must be minimized.

What should you include in the recommendation?

- A. Basic Azure Load Balancer
- B. Azure Application Gateway v1
- C. Azure Standard Load Balancer
- D. Azure Application Gateway v2

Correct Answer: C

Community vote distribution

C (100%)

 **toto74500** 1 month ago

C Azure Standard LB because secure by default , closed to inbound flows unless allowed by an NSG group. Internal traffic from VNet to the internal LB is allowed

upvoted 1 times

 **Lazylinux** 4 months, 2 weeks ago

Selected Answer: C

I C

You need LB at layer 4 and can support ipv6 and hence STD LB

upvoted 2 times

 **GBAU** 3 months ago

Basic LB supports IP6

<https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-ipv6-overview>

However MS never let us learn to deploy a "Basic" anything so no doubt their answer is Standard, not to mention on September 30, 2025, Basic Load Balancer will be retired.

upvoted 2 times

 **loopback00** 1 month, 1 week ago

> load balancer must be accessible only from the virtual network therefore you need standard lb.

upvoted 1 times

You have an Azure subscription that contains the following resources:

- A virtual network named Vnet1
- Two subnets named subnet1 and AzureFirewallSubnet
- A public Azure Firewall named FW1
- A route table named RT1 that is associated to Subnet1
- A rule routing of 0.0.0.0/0 to FW1 in RT1

After deploying 10 servers that run Windows Server to Subnet1, you discover that none of the virtual machines were activated.

You need to ensure that the virtual machines can be activated.

What should you do?

- A. On FW1, configure a DNAT rule for port 1688.
- B. Deploy an application security group that allows outbound traffic to 1688.
- C. Add an internet route to RT1 for the Azure Key Management Service (KMS).
- D. Deploy an Azure Standard Load Balancer that has an outbound NAT rule.

Correct Answer: C

Community vote distribution

C (100%)

 **voldemort123** Highly Voted 4 months ago

This question is repeated so many times after the paywall page. Not the expectation for contributor access.
upvoted 5 times

 **Murad01** Most Recent 1 month, 3 weeks ago

This answer will remain in my mind forever, I hope I face this question in the real exam, so worth it to remember.
upvoted 1 times

 **Anguis34** 3 months, 3 weeks ago

I'm definitely not gonna forget this answer.
upvoted 2 times

 **Lazylinux** 4 months, 2 weeks ago

Selected Answer: C

I C
Given answer is correct
upvoted 1 times

HOTSPOT

-

You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Subnet	Peered with
VNet1	Subnet11, Subnet12	VNet2
VNet2	Subnet21	VNet1

The subscription contains the virtual machines shown in the following table.

Name	Connected to	Availability set
VM1	Subnet11	AS1
VM2	Subnet11	AS1
VM3	Subnet12	None
VM4	Subnet21	None

You create a load balancer named LB1 that has the following configurations:

- SKU: Basic
- Type: Internal
- Subnet: Subnet12
- Virtual network: VNet1

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
LB1 can balance requests between VM1 and VM2.	<input type="radio"/>	<input type="radio"/>
LB1 can balance requests between VM2 and VM3.	<input type="radio"/>	<input type="radio"/>
LB1 can balance requests between VM3 and VM4.	<input type="radio"/>	<input type="radio"/>

Answer Area

Statements	Yes	No
LB1 can balance requests between VM1 and VM2.	<input checked="" type="radio"/>	<input type="radio"/>
LB1 can balance requests between VM2 and VM3.	<input checked="" type="radio"/>	<input type="radio"/>
LB1 can balance requests between VM3 and VM4.	<input type="radio"/>	<input checked="" type="radio"/>

Correct Answer:


 **Murad01** 1 month, 3 weeks ago

I think the correct answer is YNN, VM3 and VM4 are not in the same Vnet and Scale set
upvoted 2 times

 **Lazylinux** 4 months, 2 weeks ago

Definitely YNN

Basic LB needs vms to be in Avail set or VM scale set and in same vnet where LB is deployed but STD LB can load balance single VMs by adding single vms to backend pool but they also MUST be n same vNET where the LB is deployed
upvoted 4 times

 **glatovi** 4 months, 3 weeks ago

I think it's NNN.

ILB is on subnet12 and not subnet11

upvoted 2 times

 **Lazylinux** 3 weeks, 3 days ago

Sorry you are INCORRECT - Definitely YNN - you can try do the following as i had done, i created vnet01 (any region u like), then i created subnet1 and subnet2 in vnet01 then i created internal LB01 in subnet1 and VM01 (scale set) in subnet2, then i was able to add VM01 to backendpool of LB01 and from another vm i was able to access VM01 port 80 and via LB01 hence yes you can add vm from different subnet, BUT thing to remember is that VM MUST be in the same VNET and region as the load balancer, this is the ONLY restriction to backendpool
upvoted 1 times

 **goooru** 4 months, 1 week ago

@glatovi you right

upvoted 1 times

 **Acaer** 4 months, 3 weeks ago

YNN

Basic Load Balancer Backend pool

Virtual machines in a single availability set or virtual machine scale set

<https://learn.microsoft.com/en-us/azure/load-balancer/skus>

1. Y

VM1 and VM2 are in the same availability set

2. N

VM3 is not in AS1

3. N

VM3 and 4 are not in an availability or scale set

upvoted 1 times

 **Acaer** 4 months, 2 weeks ago

Basic Load Balancer can balance requests between Subnets but not VNETs.

It can only be used for exactly 1 VM(not a good idea), 1 Availability Set or 1 Scale Set

When you create a Basic LB with frontend IP in Subnet2 you can pick the AS1 VM's from Subnet1

This makes answer 1 YES

In Portal:

When you choose 1 single VM or 1 AS VM or 1 Scale Set VM, all other VM's which are not part of the Set wont be pickable anymore.

So when you pick VM1 for the pool, only VM2 will be left to be picked for the pool.

If you pick VM3 for the pool, no other VM will be available to be used.

This makes answer 2 NO

Like i have said in the beginning, you cant balance between VNet's and also the VM's are not in any AS anyways.

This makes answer 3 NO

upvoted 5 times

HOTSPOT

-

You have an Azure subscription. The subscription contains an Azure application gateway that has the following configurations:

- Name: AppGW1
- Tier: Standard V2
- Autoscaling: Disabled

You create an Azure AD user named User1.

You need to ensure that User1 can change the tier of AppGW1. The solution must use the principle of least privilege.

Which role should you assign to User1, and to which tiers can AppGW1 be changed? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Role:

- Cloud Device Administrator
- Network Contributor
- Owner
- User Access Administrator

Tiers:

- Standard only
- WAF only
- WAF V2 only
- Standard and WAF only
- Standard, WAF, and WAF V2

Answer Area**Correct Answer:**

Role:

- Cloud Device Administrator
- Network Contributor**
- Owner
- User Access Administrator

Tiers:

- Standard only
- WAF only
- WAF V2 only**
- Standard and WAF only
- Standard, WAF, and WAF V2

 **Lazylinux** Highly Voted 4 months, 2 weeks ago

Given answer is correct
upvoted 5 times

You have an Azure subscription that contains the following resources:

- A virtual network named Vnet1
- Two subnets named subnet1 and AzureFirewallSubnet
- A public Azure Firewall named FW1
- A route table named RT1 that is associated to Subnet1
- A rule routing of 0.0.0.0/0 to FW1 in RT1

After deploying 10 servers that run Windows Server to Subnet1, you discover that none of the virtual machines were activated.

You need to ensure that the virtual machines can be activated.

What should you do?

- A. On FW1, create an outbound service tag rule for AzureCloud.
- B. Deploy an Azure Standard Load Balancer that has an outbound NAT rule.
- C. On FW1, create an outbound network rule that allows traffic to the Azure Key Management Service (KMS).
- D. To Subnet1, associate a network security group (NSG) that allows outbound access to port 1688.

Correct Answer: C

Community vote distribution

C (100%)

Murad01 1 month, 3 weeks ago

Please not again this question
upvoted 1 times

voldemort123 4 months ago

again this?
upvoted 4 times

Lazylinux 4 months, 2 weeks ago

Selected Answer: C

I C is correct
This question been repeated so many times, there si also another version of it with route table
upvoted 3 times

jorgesoma 2 months, 3 weeks ago

repeated.
upvoted 1 times

You have an Azure subscription that contains the following resources:

- A virtual network named Vnet1
- Two subnets named subnet1 and AzureFirewallSubnet
- A public Azure Firewall named FW1
- A route table named RT1 that is associated to Subnet1
- A rule routing of 0.0.0.0/0 to FW1 in RT1

After deploying 10 servers that run Windows Server to Subnet1, you discover that none of the virtual machine operating systems were activated.

You need to ensure that the virtual machines can be activated.

What should you do?

- A. To Subnet1, associate a network security group (NSG) that allows outbound access to port 1688.
- B. On FW1, create an outbound network rule that allows traffic to the Azure Key Management Service (KMS).
- C. Deploy a NAT gateway.
- D. Deploy an application security group that allows outbound traffic to 1688.

Correct Answer: B

- Murad01** 1 month, 3 weeks ago
This question repeated number of times already
upvoted 1 times
- jorgesoma** 2 months, 3 weeks ago
repeated a lot of times...
upvoted 1 times

DRAG DROP

-

You have an Azure subscription.

You plan to deploy Azure Front Door with Azure Web Application Firewall (WAF).

You plan to implement custom rules and managed rules that meet the following requirements:

- Block malicious bots.
- Throttle client IP addresses that exceed 100 connections per minute.

You need to identify which Front Door SKU to configure, and which type of rule to configure for each requirement. The solution must minimize administrative effort and costs.

What should you identify? To answer, drag the appropriate options to the correct targets. Each option 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.

NOTE: Each correct selection is worth one point.

Options

A custom rule

A managed rule

Classic

Premium

Standard

Answer Area

SKU:

Option

Block malicious bots:

Option

Throttle client IP addresses:

Option


Answer Area

Correct Answer:


SKU: Premium

Block malicious bots: A managed rule

Throttle client IP addresses: A custom rule

 **jorgesoma** 2 months, 2 weeks ago

I think it's correct
upvoted 1 times

 **jorgesoma** 2 months, 2 weeks ago

It's correct. SKU Standard doesn't have bot protection. Only Premium SKU.
upvoted 1 times

HOTSPOT

-

You have an Azure application gateway.

You need to create a rewrite rule that will remove the origin port from the HTTP header of incoming requests that are being forwarded to the backend pool.

How should you configure each setting? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Common header:

Via
X-Forwarded-For
X-Forwarded-Host

Header value:

add_x_forwarded_for_proxy
client_port
host**Answer Area**

Common header:

Via
X-Forwarded-For
X-Forwarded-Host**Correct Answer:**

Header value:

add_x_forwarded_for_proxy
client_port
host

 **jorgesoma** Highly Voted 2 months, 3 weeks ago

The X-Forwarded-For client request header field with the client_ip variable (see explanation later in this table) appended to it in the format IP1, IP2, IP3, and so on. If the X-Forwarded-For field isn't in the client request header, the add_x_forwarded_for_proxy variable is equal to the \$client_ip variable. This variable is particularly useful when you want to rewrite the X-Forwarded-For header set by Application Gateway so that the header contains only the IP address without the port information.

<https://learn.microsoft.com/en-us/azure/application-gateway/rewrite-http-headers-url>
upvoted 5 times

You have an Azure subscription that contains the following resources:

- A virtual network named Vnet1
- Two subnets named subnet1 and AzureFirewallSubnet
- A public Azure Firewall named FW1
- A route table named RT1 that is associated to Subnet1
- A rule routing of 0.0.0.0/0 to FW1 in RT1


After deploying 10 servers that run Windows Server to Subnet1, you discover that none of the virtual machine operating systems were activated.

You need to ensure that the virtual machines can be activated.

What should you do?

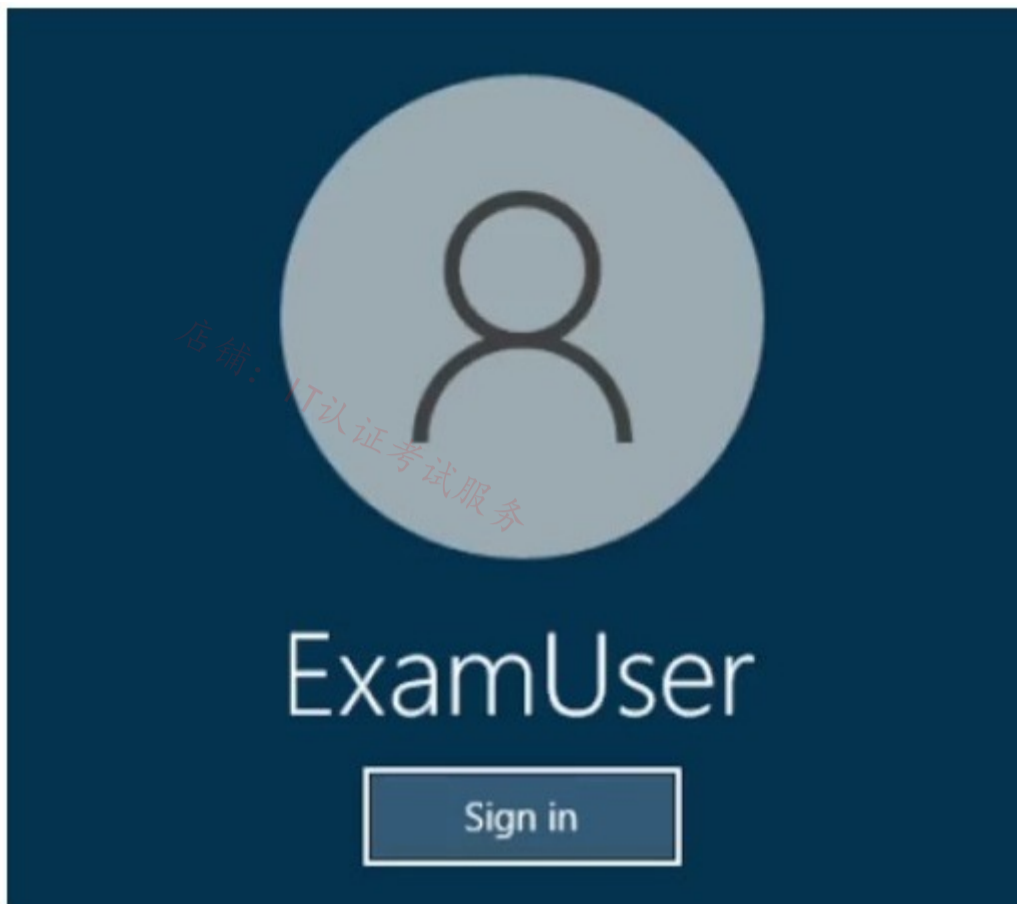
- A. On FW1, create an outbound service tag rule for AzureCloud.
- B. On FW1, create an outbound network rule that allows traffic to the Azure Key Management Service (KMS).
- C. To Subnet1, associate a network security group (NSG) that allows outbound access to port 1688.
- D. Deploy an application security group that allows outbound traffic to 1688.

Correct Answer: B

 **jungle_mungle** 1 month, 2 weeks ago
again :)
upvoted 1 times

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You need to ensure that traffic to host.fabrikam.com is directed to the Traffic Manager profile.

To complete this task, sign in to the Azure portal.

Correct Answer:

Manage an Azure Traffic Manager profile

Traffic Manager profiles use traffic-routing methods to control the distribution of traffic to your cloud services or website endpoints.

Add Traffic Manager endpoint

Step 1: In the portal's search bar, search for the Traffic Manager. Select the profile in the results that are displayed.

Step 2: In Traffic Manager profile, in the Settings section, select Endpoints > Add.

Step 3: Enter or select the following information. Accept the defaults for the other settings, and then select OK.

Setting Value

Type: Enter the Azure endpoint.

Name: Enter myEndpoint.

Target resource type: Select Host name.

Target resource: host.fabrikam.com

Weight Enter 100.

店铺: IT认证考试服务

Topic 4 - Question Set 4

Reference:

<https://learn.microsoft.com/en-us/azure/traffic-manager/tutorial-traffic-manager-weighted-endpoint-routing>

店铺: IT认证考试服务

店铺: IT认证考试服务

You have an Azure virtual machine named VM1.
 You need to capture all the network traffic of VM1 by using Azure Network Watcher.
 To which locations can the capture be written?

- A. blob storage only
- B. blob storage, a file path on VM1, and a premium storage account
- C. a file path on VM1 only
- D. blob storage and a file path on VM1 only
- E. blob storage and a premium storage account only
- F. a premium storage account only

Correct Answer: D

Once your packet capture session has completed, the capture file is uploaded to blob storage or to a local file on the virtual machine. The storage location of the packet capture is defined during creation of the packet capture.

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-packet-capture-manage-portal>

Community vote distribution

D (88%)

13%

 **GohanF2** Highly Voted 1 year, 2 months ago

It's correct.

To blob storage account or to VM's valid path.

Storage account or file: Select Storage account, File, or both. If you select File, the capture is written to a path within the virtual machine.

Local file path: The local path on the virtual machine where the packet capture will be saved (valid only when File is selected). The path must be a valid path. If you are using a Linux virtual machine, the path must start with /var/captures.


Storage accounts: Select an existing storage account, if you selected Storage account. This option is only available if you selected Storage.
 upvoted 8 times

 **Lazylinux** Most Recent 4 months, 2 weeks ago

Selected Answer: D

Given answer is correct

Capture location Select Storage account, File, or Both.
 upvoted 1 times

 **JennyHuang36** 11 months, 1 week ago

In exam Feb, 2023

upvoted 2 times

 **TJ001** 1 year ago

Correct Answer is D

upvoted 2 times

 **TJ001** 1 year ago

<https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-packet-capture-manage-portal>

upvoted 2 times

 **Prutser2** 1 year, 3 months ago

Selected Answer: D

as stated

upvoted 1 times

 **jellybiscuit** 1 year, 3 months ago

Selected Answer: D

It seems illogical to me that you couldn't write to blockblob storage, but M\$ says it's a no-go.
 So only blob storage or file path on the VM that is being captured.

<https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-packet-capture-manage-portal>

upvoted 1 times

🗨️ **Alessandro365** 1 year, 4 months ago

Selected Answer: D

D is correct.

de acordo com o doc: "Storage account or file: Select Storage account, File, or both. If you select File, the capture is written to a path within the virtual machine."

<https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-packet-capture-manage-portal>

upvoted 1 times

🗨️ **leonidagolfre** 1 year, 4 months ago

Selected Answer: D

According to the doc:

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-packet-capture-manage-portal>

"Storage account or file: Select Storage account, File, or both. If you select File, the capture is written to a path within the virtual machine."

So D is the correct one.

upvoted 3 times

🗨️ **gr4** 1 year, 4 months ago

Selected Answer: A

I would say only blob storage

SA doesn't have to premium one

upvoted 1 times

🗨️ **Chiscrown** 1 year, 4 months ago

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-packet-capture-manage-portal>

Premium storage accounts are currently not supported for storing packet captures

Answer: D

upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

You have an Azure virtual network that contains the subnets shown in the following table.

Name	IP address space
AzureFirewallSubnet	192.168.1.0/24
Subnet2	192.168.2.0/24

You deploy an Azure firewall to AzureFirewallSubnet. You route all traffic from Subnet2 through the firewall.

You need to ensure that all the hosts on Subnet2 can access an external site located at https://*.contoso.com.

What should you do?

- A. In a firewall policy, create a DNAT rule.
- B. Create a network security group (NSG) and associate the NSG to Subnet2.
- C. In a firewall policy, create a network rule.
- D. In a firewall policy, create an application rule.

Correct Answer: D

Reference:


<https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal>

Community vote distribution

D (100%)

 **izidorf** Highly Voted 2 years, 2 months ago

Network rule is based on port Ivank23. Application rules are based in FQDN. The answer is correct, I suppose.
upvoted 29 times

 **Bbb78** 11 months, 3 weeks ago

you can use FQDN in the network rules, network rules are processed before AppRules and if there is a DENY on the outbound traffic in the NETWORK rule - adding to the APPRule will not help
upvoted 1 times

 **mammoot** 11 months, 1 week ago

According to this, you can NOT use FQDN in a network rule
<https://learn.microsoft.com/en-us/azure/firewall/policy-rule-sets#network-rules>
upvoted 3 times

 **Pravda** Highly Voted 2 years ago

D - FQDN
Application rules that define fully qualified domain names (FQDNs) that can be accessed from a subnet.
Network rules that define source address, protocol, destination port, and destination address.
upvoted 16 times

 **leotoronto123** 2 years ago


thanks!
upvoted 2 times

 **Lazylinux** Most Recent 4 months, 1 week ago

Selected Answer: D

Given answer is correct

<https://learn.microsoft.com/en-us/azure/firewall/policy-rule-sets>
upvoted 2 times

 **tester2023** 12 months ago

DNAT - use a DNAT rule when you want a public IP address to be translated into a private IP address.
Network - use a network rule when you want to filter traffic based on IP addresses, any ports, and any protocols
Application - use an application rule when you want to filter traffic based on fully qualified domain names (FQDNs), URLs, and HTTP/HTTPS protocols

<https://learn.microsoft.com/en-us/azure/firewall/policy-rule-sets#rule-types>
upvoted 2 times

 **wiki715** 1 year, 1 month ago

Selected Answer: D

as explained here: <https://learn.microsoft.com/en-us/azure/firewall/policy-rule-sets>
Application rules

Application rules allow or deny outbound and east-west traffic based on the application layer (L7). You can use an application rule when you want to filter traffic based on fully qualified domain names (FQDNs), URLs, and HTTP/HTTPS protocols.

upvoted 1 times

🗄️ 👤 **Syldana** 1 year, 3 months ago

Selected Answer: D

The requirement mentions the HTTP URL so it can only be done through FQDN application rules

upvoted 2 times

🗄️ 👤 **lobs_wort** 1 year, 6 months ago

Selected Answer: D

In exam 22-July-2022.

upvoted 2 times

🗄️ 👤 **tartarus23** 1 year, 6 months ago

D. In a firewall policy, create an application rule.

The requirement mentions the HTTP URL so it can only be done through FQDN application rules

upvoted 1 times

🗄️ 👤 **Sixfun** 1 year, 8 months ago

Selected Answer: D

It is correct answer.

upvoted 1 times

🗄️ 👤 **HTD** 1 year, 9 months ago

in order words allow https (ssl) traffic thru. APPID and also http .

upvoted 1 times

🗄️ 👤 **Kimimoto** 1 year, 11 months ago

Appeared in exam on 11/Feb/2022

upvoted 1 times

🗄️ 👤 **Contactfornitish** 2 years ago

Appeared in exam on 17/01/2022

upvoted 1 times

🗄️ 👤 **aftab7500** 2 years, 1 month ago

Correct:

Application rules that define fully qualified domain names (FQDNs) that can be accessed from a subnet.

Network rules that define source address, protocol, destination port, and destination address.

upvoted 3 times

🗄️ 👤 **Ivank23** 2 years, 2 months ago

Is this not supposed to be C. the network rule?

upvoted 1 times

🗄️ 👤 **Eitant** 2 years ago

No. A scenario, contoso.com changed the domain IP address. With networking rule you will have to modify the rules.

upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

You have an Azure Web Application Firewall (WAF) policy in prevention mode that is associated to an Azure Front Door instance. You need to configure the policy to meet the following requirements:

- ☞ Log all connections from Australia.
- ☞ Deny all connections from New Zealand.
- ☞ Deny all further connections from a network of 131.107.100.0/24 if there are more than 100 connections during one minute.

What is the minimum number of objects you should create?

- A. three custom rules that each has one condition
- B. one custom rule that has three conditions
- C. one custom rule that has one condition
- D. one rule that has two conditions and another rule that has one condition

Correct Answer: A

Reference:

<https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/afds-overview>

Community vote distribution

A (100%)

🗳️ 👤 **walkwolf3** Highly Voted 2 years, 2 months ago

Answer is correct since all 3 requirements have different conditions and actions.
upvoted 13 times

🗳️ 👤 **pinchocr** 1 year, 7 months ago

actions are the same for two of them (block)
upvoted 1 times

🗳️ 👤 **jeepTango123456** 1 year, 5 months ago

<https://techcommunity.microsoft.com/t5/azure-network-security-blog/azure-waf-custom-rule-samples-and-use-cases/ba-p/2033020>
"Another concept to make use of in constructing effective Custom Rules is compound conditions. Rules can be created with a single condition, or you can add multiple conditions that must be satisfied to constitute a match. When adding multiple conditions, they are added as an AND statement, so all conditions must be met for the Action to take place. If you need to construct a rule with OR logic, it is best to create multiple rules with the same Action."
so three rules are needed
upvoted 6 times

🗳️ 👤 **Jamesat** Highly Voted 1 year, 5 months ago

Selected Answer: A

I would go with A as you would need 3 separate rules for this.

Rule 1 - Match rule, condition match Australia, action Log
Rule 2 - Match rule, condition match New Zealand action Deny
Rule 3 - Rate Limit rule, condition match IP range and rate, action Deny
upvoted 11 times

🗳️ 👤 **GBAU** Most Recent 3 months ago

Selected Answer: A

Deny all traffic from NZ? Harsh
upvoted 2 times

🗳️ 👤 **Lazylinux** 4 months, 1 week ago

Selected Answer: A

Definitely A as per given answer

three custom rules that each has one condition, as NOTE you cannot and another different condition but you can add AND IF condition into the custom rule and hence means if you did use AND IF then both conditions MUST be met in order for the custom rule to be effective but in this scenario the conditions are NOT related at all

1 x Geo - Log Australia
1 x Geo - New Zealand BLOCKED
1 x Rate Limit - limit specific IP
upvoted 6 times

🗳️ 👤 **polinoma** 9 months, 2 weeks ago

The answer should be B, because we are looking for a "minimum number of objects you should create"

Answer A not covering this rule.

You could create three custom rules, one to log all connections from Australia, another to deny all connections from New Zealand, and a third to deny further connections from a network of 131.107.100.0/24 if there are more than 100 connections during one minute.

However, this approach requires creating three custom rules instead of one, which increases the number of objects to manage, so it is not the most efficient solution.

upvoted 1 times

 **MightyMonarch74** 10 months ago

three custom rules that each has one condition

1 x Geographic - Log Australia

1 x Geographic - Block New Zealand

1 x Rate Limit - limit specific IP

upvoted 2 times

 **GohanF2** 1 year, 2 months ago

Answers are correct.

upvoted 1 times

 **jellybiscuit** 1 year, 3 months ago

Selected Answer: A

A

The three conditions

- from australia


- from new zealand

- from 131.107.100.0

They are not related and not additive, so you need three rules.

When you add multiple conditions they come with a "and if". There is no "or" option. You have to get "or" with a new rule.

upvoted 4 times

 **Cristoicach91** 1 year, 4 months ago

Selected Answer: A


You need 3 rules because you can either allow/deny/log

upvoted 4 times

 **lobs_wort** 1 year, 6 months ago

In exam on 21-July-2022.

upvoted 1 times

 **cypher9** 1 year, 6 months ago

A rule is made of a match condition, a priority, and an action.

Action types supported are: ALLOW, BLOCK, LOG, and REDIRECT.

3 different conditions = 3 custom rules

upvoted 2 times

 **armand10** 1 year, 7 months ago

D correct since each custom rule is mapped only to one action (log,allow, deny).

upvoted 2 times

 **Kannanthalaiappan** 1 year, 10 months ago

Ans D ??

one rule type "match" with first two conditions, another rule type "Rate limit" with last condition.

upvoted 5 times

 **Prutser2** 1 year, 3 months ago

that would require a Boolean OR statement, which is not available under the condition, its on IF which can be combined with AND IF

upvoted 1 times

 **pinchocr** 1 year, 7 months ago

You can only give one action "Deny" or "Allow" per rule. Not sure if you can use one rule for block traffic from one region AND per number of request. The other rule would contain the Allow traffic from first region

upvoted 1 times

 **nitinkumarmca** 1 year, 11 months ago

Selected Answer: A

Correct answer is A

upvoted 3 times

 **Contactfornitish** 2 years ago

Appeared in exam on 17/01/2022

upvoted 1 times



 **Pravda** 2 years ago

Variation on exam 1/6/2022
upvoted 3 times

 **gme999** 2 years, 3 months ago

Correct
upvoted 3 times

Question #4

Topic 4

You have an Azure subscription that contains multiple virtual machines in the West US Azure region.

You need to use Traffic Analytics.

Which two resources should you create? Each correct answer presents part of the solution. (Choose two.)

NOTE: Each correct answer selection is worth one point.

- A. an Azure Monitor workbook
- B. a Log Analytics workspace
- C. a storage account
- D. an Azure Sentinel workspace
- E. an Azure Monitor data collection rule

Correct Answer: BC

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics>

Community vote distribution

BC (100%)

 **sapien45** Highly Voted 1 year, 3 months ago

Selected Answer: BC

Traffic Analytics requires the following prerequisites:

A Network Watcher enabled subscription.

Network Security Group (NSG) flow logs enabled for the NSGs you want to monitor.

An Azure Storage account, to store raw flow logs.

An Azure Log Analytics workspace, with read and write access.

upvoted 8 times

 **gr4** Highly Voted 1 year, 4 months ago

Selected Answer: BC

This is correct

<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics-faq#what-are-the-prerequisites-to-use-traffic-analytics->

upvoted 7 times

 **Lazylinux** Most Recent 4 months, 1 week ago

Selected Answer: BC

Given answer is correct

upvoted 1 times

HOTSPOT -

You have an Azure subscription that contains the virtual machines shown in the following table.

Name	Connected to
VM1	Vnet1/Subnet1
VM2	Vnet1/Subnet2

Subnet1 and Subnet2 are associated to a network security group (NSG) named NSG1 that has the following outbound rule:

- ☞ Priority: 100
- ☞ Port: Any
- ☞ Protocol: Any
- ☞ Source: Any
- ☞ Destination: Storage
- ☞ Action: Deny

You create a private endpoint that has the following settings:

- ☞ Name: Private1
- ☞ Resource type: Microsoft.Storage/storageAccounts
- ☞ Resource: storage1
- ☞ Target sub-resource: blob
- ☞ Virtual network: Vnet1
- ☞ Subnet: Subnet1

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
From VM2, you can create a container in storage1	<input type="radio"/>	<input type="radio"/>
From VM1, you can upload data to a blob storage container in storage1	<input type="radio"/>	<input type="radio"/>
From VM2, you can upload data to a blob storage container in storage1	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
From VM2, you can create a container in storage1	<input type="radio"/>	<input checked="" type="radio"/>
From VM1, you can upload data to a blob storage container in storage1	<input checked="" type="radio"/>	<input type="radio"/>
From VM2, you can upload data to a blob storage container in storage1	<input type="radio"/>	<input checked="" type="radio"/>

Reference:

<https://docs.microsoft.com/en-us/azure/private-link/disable-private-endpoint-network-policy>

WorkHardBeProud Highly Voted 2 years, 3 months ago

Correct!

Service Tag "storage" represents Azure Storage Accounts and can only be applied on the Outbound direction.

Here the NSG is denying the access to any Storage account (direction is Outbound, read well) and it is applied on the Subnet level not on the NIC level.

No - VM2 being on the subnet 2 not on subnet 1 will be deny

Yes - VM1 and Private 1 are in the same subnet so VM1 will have access

NO - VM2 has been denied the access by the NSG



upvoted 49 times

  **Pamban** 2 years, 1 month ago

Wrong. Lab tested. answer is YES YES YES


There is no block between subnets.

upvoted 20 times

  **waqas** 2 years, 1 month ago



You are wrong. Answer must be NYN. When u configure Private Endpoint then you always mention the Vnet alongwith Subnet. Here Subnet1 is selected for Private endpoint deployment not Subnet2. So According to this article <https://docs.microsoft.com/en-us/azure/storage/common/storage-private-endpoints#network-security-group-rules-for-subnets-with-private-endpoints> "NSG rules applied to the subnet hosting the private endpoint are not applied to the private endpoint". So VM1 would use private endpoint without any NSG filtering. Whereas Subnet2 will use NSG which has a Deny action. There is no linkage of Subnet 2 Subnet communication as the only subnet configured to Private Endpoint is Subnet1. Thats why the answer is NYN.

upvoted 25 times

  **MikeB19** 2 years ago

The nsg in subnet 2 applies to the public IP address of the storage account. In this case the private end point provides a private IP address on subnet 1. And since subnet 1 and 2 are in the same vnet all traffic is routed between the subnets by default. The nsg has no relevance in this scenario. Therefore y y y



upvoted 12 times

  **Fule** 1 year, 4 months ago

ok, it's important to note that security rules in an NSG associated to a subnet can affect connectivity between VMs within it. So, we have that in production, we blocked certain VMs, and Azure resources with NSG, and we have only one VNet with a bunch of subnets, some subnets cant talk with others.

<https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#intra-subnet-traffic>

upvoted 1 times

  **Fule** 1 year, 4 months ago

ahh now i am a bit confused,

"Private endpoints don't support network policies such as Network Security Groups (NSGs) or Azure Firewall, so security rules won't apply to them. User-defined routes (UDR) are bypassed by traffic coming from private endpoints. User-defined routes can be used to override traffic destined for the private endpoint." i mean than i would say YYY

upvoted 4 times

  **leotoronto123** 2 years ago



thanks Waqas ..

upvoted 1 times

  **Prutser2** 1 year, 3 months ago

your lab azure or aws?

upvoted 2 times

  **Pradh** 1 year, 3 months ago

Stop fooling and confusing people. Answer is NYN

upvoted 6 times

  **christianpageqc** Highly Voted  2 years, 3 months ago

According to this article <https://docs.microsoft.com/en-us/azure/storage/common/storage-private-endpoints#network-security-group-rules-for-subnets-with-private-endpoints>

"NSG rules applied to the subnet hosting the private endpoint are not applied to the private endpoint". So VM1 would use private endpoint without any NSG filtering.

upvoted 16 times

  **WorkHardBeProud** 2 years, 3 months ago

Be careful guys it is not the case anymore.

<https://docs.microsoft.com/en-us/azure/private-link/disable-private-endpoint-network-policy>

upvoted 3 times

  **Morgana** 2 years, 3 months ago

NSG for private endpoints are "public preview only" I still think the Answer are YES.YES.YES.

upvoted 14 times

  **AjdIfasudfo0** 1 year, 1 month ago

this feature is now available, but you still have to opt-in manually

upvoted 1 times

  **Roman_Rabodzey** 2 years, 3 months ago

The same is for VM2. There is no rule to deny subnet-to-subnet communication which is open by default. It will have access to a storage account because it uses private endpoint

upvoted 6 times

🗨️ **sapien45** 1 year, 3 months ago

Well answered Sir
upvoted 1 times

🗨️ **srikanth1987** 2 years, 2 months ago

I agree with you @Roman. It's subnet to subnet communication, the source has no idea whether the destination PE belongs to storage or sql or whatever.
upvoted 2 times

🗨️ **RandomUser** 2 years, 3 months ago

That gives us 3 yes. And it makes sense as the Service Tag essentially is just a collection of public IP addresses. And we do not use any of PIPs to connect to the storage.
upvoted 7 times

🗨️ **Bharat** 2 years, 3 months ago

Yes. You are correct.
upvoted 1 times

🗨️ **MostafaNawar** Most Recent 1 week, 5 days ago

1. From VM2, you can create a container in storage1: No

The NSG's outbound rule blocks any traffic from any source to the Storage service, including creating containers. The private endpoint is only for accessing blob storage and doesn't override NSG rules for other storage operations.

2. From VM1, you can upload data to a blob storage container in storage1: Yes

The private endpoint in Subnet1 provides a private IP address for VM1 to access blob storage in storage1. Traffic to the private endpoint bypasses NSG rules, allowing VM1 to upload data to blobs.

3. From VM2, you can upload data to a blob storage container in storage1: No

VM2 is not in the subnet where the private endpoint is configured (Subnet1). It cannot use the private endpoint to bypass the NSG rule, so outbound traffic to storage is still blocked.
upvoted 1 times

🗨️ **Lazylinux** 4 months, 1 week ago

Based on the below im voting NYN and hence given answer is correct

First let's get those facts outlined

Subnet to Subnet communication within the same VNET is allowed by default and would need an explicit NSG rule to restrict and hence The default outbound NSG rule is to allow all VMs to communicate with each other and resources freely on same vNET, however if you create an outbound rule that overrides the default rule by giving it higher priority than the custom rule will override the default rule and this is the case in this scenario and hence communication is blocked to storage

In order to enforce NSG on Private Endpoint – a Network policy MUST be enabled for the vNET specific to NSG, however in this case is NOT mentioned or enabled and hence NSG rules are NOT affecting the private Endpoint

see further info as limit reached

upvoted 6 times

🗨️ **Lazylinux** 4 months, 1 week ago

adding more here

Here snippet from MS article as per below link

Network security groups (NSGs) support for private endpoints is now generally available. This feature enhancement provides you with the ability to enable advanced security controls on traffic destined to a private endpoint. In order to leverage this feature, you will need to set a specific subnet level property, called PrivateEndpointNetworkPolicies, to enabled on the subnet containing private endpoint resources.

See links below

<https://learn.microsoft.com/en-us/azure/private-link/disable-private-endpoint-network-policy?tabs=network-policy-portal>

<https://azure.microsoft.com/en-au/updates/general-availability-of-network-security-groups-support-for-private-endpoints/>

upvoted 4 times

🗨️ **ironbornson** 3 months, 3 weeks ago

Thank you LazyLinux, it looks it's still NYN until they update the question referencing NetworkPolicies feature

upvoted 2 times

🗨️ **heatfan900** 4 months, 2 weeks ago

n, y, n

WHEN CREATING THE PRIVATE ENDPOINT FOR INBOUND ACCESS AGAINST THE STORAGE ACCT SA1, YOU ARE ESSENTIALLY BRINGING THAT SA INTO THE VNET1/SUBNET1 AS PER THE SETTINGS OUTLINED ABOVE. TH

THE NSG IS APPLIED AT THE SUBNET LEVEL, THEREFORE, IT IS NOT APPLIED WHEN CONNECTING FROM A RESOURCE IN SUBNET 1 SUCH AS VM1.

SINCE THERE IS NO PRIVATE ENDPOINT FOR SUBNET AND THE NSG APPLIES TO THAT SUBNET AS WELL THE OUTBOUND TRAFFIC TO SA1 WILL BLOCKED AS PER THE NSG DENY RULE.

upvoted 1 times

🗨️ **mabalon** 4 months, 4 weeks ago

This question seems old. Currently NSGs can be applied on PE subnets:


<https://learn.microsoft.com/en-us/azure/private-link/disable-private-endpoint-network-policy?tabs=network-policy-portal>

upvoted 1 times

🗨️ **Crazysaffer** 8 months, 1 week ago

I thought private endpoints ignores NSG's. Therefore everything should be yes

upvoted 1 times

 **25max** 9 months, 3 weeks ago

<https://learn.microsoft.com/en-us/azure/virtual-network/vnet-integration-for-azure-services>
Using service tags to allow or deny traffic to your Azure resources to and from public IP endpoints.

upvoted 1 times

 **_fvt** 9 months, 3 weeks ago

YYY - Service TAGS are for Public services IP, doesn't contains private endpoints so don't filter any flow to the private endpoint, even on VM NICs or if Network Policies For Private endpoint were enabled for the Subnet where the private endpoint is located.


"<https://learn.microsoft.com/en-us/azure/virtual-network/vnet-integration-for-azure-services>"
<https://learn.microsoft.com/en-us/azure/virtual-network/vnet-integration-for-azure-services>

upvoted 1 times

 **_fvt** 9 months, 3 weeks ago

"Using service tags to allow or deny traffic to your Azure resources to and from public IP endpoints."

upvoted 1 times

 **JennyHuang36** 11 months, 1 week ago

In exam Feb, 2023

upvoted 3 times

 **tzatziki** 12 months ago

...I always wanted to say this... Tested in Lab... And i did just that. All answers are Y. Set the public access level of the containers to blob, did the nsg+rules to the subnets and 2 vms with bastion access and the private endpoint... all test where made with powershell from the vms ... Also pointing out that when the private endpoint was created a note was saying that if i have an nsg on the subnet given, it would be disabled for private endpoints on that subnet... so thats that...

upvoted 7 times

 **TJ001** 1 year ago

will go with yes yes yes...it is very clear private endpoint connections are local and the dns resolution happens to a private IP of the private end point and service tag resolves to public IP wont be applicable here

upvoted 2 times

 **phoenix14** 1 year, 1 month ago

NYN is Correct because. For outbound traffic, Azure processes the rules in a network security group associated to a network interface first, if there's one, and then the rules in a network security group associated to the subnet, if there's one. This includes intra-subnet traffic as well.

upvoted 1 times

 **Takloy** 1 year, 2 months ago

NYN

N - Outbound is Denied so VM2 can't jump to VM1.

Y - Because of the Private Endpoint

N - Same explanation as the first one.

upvoted 1 times

 **daemon101** 6 months, 2 weeks ago

YYY

Outbound NSG rule is filtering Storage service tags that contain public IP addresses of Storage Accounts. The resources that will be impacted by the NSG rules are VM1 and VM2. Furthermore, the Storage Account is enabled with Private Endpoint which means, the Storage Account is no longer using Public IP address and it is not affected by any NSG.

Network traffic between the clients on the VNet and the storage account traverses over the VNet and a private link on the Microsoft backbone network, eliminating exposure from the public internet.

<https://learn.microsoft.com/en-us/azure/storage/common/storage-private-endpoints>

upvoted 1 times

 **Disparate** 1 year, 2 months ago

NYN is correct!

The NSG apply only a VM2 because the private endpoint is only for VM1.

Easy!

upvoted 1 times

 **Prutser2** 1 year, 3 months ago

the answers above are correct, ONLY if it would have stated priavet1 instead of storage1. because as ppl have stated below, storage1 is really accessible through a public ip address. as per usual, these questions are sloppy and badly written

upvoted 1 times

 **sapien45** 1 year, 3 months ago

YYY.

Just tested it

Two VMs in two distincs Subnets, even though the private endpoint is assigned to one subnet , both VMs will have in their Network interface effective routes a destination to the private endpoint, because all traffcis is routed between the subnets by default

upvoted 6 times

 **kira1kira22** 1 month, 1 week ago

"NSG rules applied to the subnet hosting the private endpoint are not applied to the private endpoint".

upvoted 1 times

店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

HOTSPOT -

You have an Azure firewall shown in the following exhibit.

Firewall1
Firewall

>> Delete Lock

Visit Azure Firewall Manager to configure and manage this firewall. →

Essentials

Resource group (change)
RG1

Location
North Europe

Subscription (change)
Subscription1

Subscription ID
489f2hht-se7y-987v-g571-463hw3679512

Virtual network
Vnet1

Firewall policy
FirewallPolicy1

Provisioning state
Succeeded

Tags (change)
Click here to add tags

Firewall sku
Standard

Firewall subnet
AzureFirewallSubnet

Firewall public IP
Firewall-IP1

Firewall private IP
10.100.253.4

Management subnet

Management public IP

Private IP Ranges
Managed by Firewall Policy

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

On Firewall1, forced tunneling [answer choice]

	▼
is enabled already	
cannot be enabled	
is disabled but can be enabled	

On Firewall1, management by Azure Firewall Manager [answer choice]

	▼
is enabled already	
cannot be enabled	
is disabled but can be enabled	

Correct Answer:

Answer Area

On Firewall1, forced tunneling [answer choice]

	▼
is enabled already	
cannot be enabled	
is disabled but can be enabled	

On Firewall1, management by Azure Firewall Manager [answer choice]

	▼
is enabled already	
cannot be enabled	
is disabled but can be enabled	

Box 1:

If forced tunneling was enabled, the Firewall Subnet would be named AzureFirewallManagementSubnet. Forced tunneling can only be enabled during the creation of the firewall. It cannot be enabled after the firewall has been deployed.

Box 2:

The "Visit Azure Firewall Manager to configure and manage this firewall" link in the exhibit shows that the firewall is managed by Azure Firewall Manager.

 **jkklim** Highly Voted 1 year, 9 months ago

from 1st diagram, if you see that Management Subnet and Management IP is empty, it means NO FORCE TUNNELING. And of course, force tunnelling can only be enabled during FW creation
upvoted 17 times

 **Geo13AZ** Highly Voted 2 years ago

The Answer is correct, but the explanation of the first question has a mistake, it says "the Firewall subnet" but it should be "the Management Subnet would be AzureFirewallManagementSubnet". Also, the "Management Public IP" would be "ManagementPublicIP".
<https://azure.microsoft.com/en-us/blog/azure-firewall-forced-tunneling-and-sql-fqdn-filtering-now-generally-available/>
upvoted 13 times

 **Murad01** Most Recent 1 month, 3 weeks ago

Appeared on Exam November - 2023
upvoted 1 times

 **Lazylinux** 4 months, 1 week ago

Given answer is correct and explanation is here
<https://learn.microsoft.com/en-us/azure/firewall/forced-tunneling#forced-tunneling-configuration>
upvoted 1 times

 **BlackZeros** 1 year, 4 months ago

Answer for both is Cannot be Enabled.
"In Forced Tunneling mode, the Azure Firewall service incorporates the Management subnet (AzureFirewallManagementSubnet) for its operational purposes." This is clearly missing in the screenshot.
<https://learn.microsoft.com/en-us/azure/firewall/forced-tunneling>
upvoted 1 times

 **MrBlueSky** 9 months, 2 weeks ago

Wrong.

This AzureFirewallManagementSubnet is not the indicator for if it's being managed by Azure Firewall Manager. The fact that there is a Firewall Policy attached to this is what indicates that Firewall Manager is already in use.

Answers:

1. Cannot be Enabled
2. Already Enabled

upvoted 4 times

 **Contactforitish** 2 years ago

Appeared in exam on 17/01/2022
upvoted 2 times

 **Pravda** 2 years ago

Not on exam 1/6/2022

upvoted 3 times

  **AidenYoukhana** 2 years ago

The answers are correct!

upvoted 1 times

  **Pamban** 2 years, 1 month ago

appeared on exam 5th Dec 2021

upvoted 3 times

  **sadsak** 2 years, 2 months ago

This answer appears to be correct - <https://docs.microsoft.com/en-us/azure/firewall/forced-tunneling#forced-tunneling-configuration>

upvoted 4 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

You have a hybrid environment that uses ExpressRoute to connect an on-premises network and Azure. You need to log the uptime and the latency of the connection periodically by using an Azure virtual machine and an on-premises virtual machine.

What should you use?

- A. Azure Monitor
- B. IP flow verify
- C. Connection Monitor
- D. Azure Internet Analyzer

Correct Answer: C

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/connection-monitor>

Community vote distribution

C (100%)

 **Takloy** Highly Voted 2 years ago

Selected Answer: C

Correct answer is C.

Connection Monitor provides unified, end-to-end connection monitoring in Azure Network Watcher. The Connection Monitor feature supports hybrid and Azure cloud deployments. Network Watcher provides tools to monitor, diagnose, and view connectivity-related metrics for your Azure deployments.

<https://docs.microsoft.com/en-us/azure/network-watcher/connection-monitor-overview>

upvoted 5 times

 **Lazylinux** Most Recent 4 months, 1 week ago

Selected Answer: C

I C is correct as per answer

upvoted 1 times

 **Alessandro365** 1 year, 4 months ago

Selected Answer: C

C is correct

upvoted 1 times

 **unclegrandfather** 1 year, 7 months ago

Appeared on exam Jun/28/22

upvoted 1 times

 **kogunribido** 1 year, 7 months ago


Appeared on exam 6/27/2022

upvoted 1 times

 **jj22222** 1 year, 9 months ago

on test 4.10.2022 Cannot be enabled - forced tunneling on firewall 1 is enabled already - azure firewall manager

upvoted 3 times

 **jj22222** 1 year, 9 months ago

sorry this is for earlier question, this one is connection manager

upvoted 4 times

 **rockethack** 1 year, 11 months ago

This question was on the exam on 18th Feb 2022.

upvoted 1 times

 **nitinkumarmca** 1 year, 11 months ago

Selected Answer: C

Correct

upvoted 1 times

 **Joshalom** 1 year, 11 months ago

on exam 6/2/2022

upvoted 1 times

 **Eitant** 2 years ago

Selected Answer: C

Correct answer

upvoted 1 times

 **Pravda** 2 years ago

on exam 1/6/2022


upvoted 3 times

 **JoMa** 2 years, 1 month ago

Correct

Connection monitor probes the connection every 60 seconds, so you can monitor latency over time

upvoted 1 times

 **Dooa** 2 years, 2 months ago

correcta

upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

You have an Azure subscription that contains the following resources:

- ☞ A virtual network named Vnet1
- ☞ Two subnets named subnet1 and AzureFirewallSubnet
- ☞ A public Azure Firewall named FW1
- ☞ A route table named RT1 that is associated to Subnet1
- ☞ A rule routing of 0.0.0.0/0 to FW1 in RT1

After deploying 10 servers that run Windows Server to Subnet1, you discover that none of the virtual machines were activated.

You need to ensure that the virtual machines can be activated.

What should you do?

- A. On FW1, create an outbound service tag rule for AzureCloud.
- B. On FW1, create an outbound network rule that allows traffic to the Azure Key Management Service (KMS).
- C. Deploy a NAT gateway.
- D. To Subnet1, associate a network security group (NSG) that allows outbound access to port 1688.

Correct Answer: B

Reference:

<https://ryanmangansitblog.com/2020/05/11/firewall-considerations-windows-virtual-desktop-wvd/>

Community vote distribution

B (100%)

voldemort123 Highly Voted 3 months, 3 weeks ago

I will remember this answer even if i want to forget
upvoted 5 times

srs27 Highly Voted 2 years, 1 month ago

This is correct. When you use Force tunneling, then for Windows activation traffic should be allowed for Azure KMS Servers. Either the way mentioned in Option B or you add UDR to point Internet for KMS outbound traffic.
upvoted 5 times

Grafting 2 years ago

where does it mention force tunneling?
upvoted 1 times

hendylaja 1 year, 10 months ago

If forced tunneling was enabled, the Firewall Subnet would be named AzureFirewallManagementSubnet
upvoted 2 times

jellybiscuit 1 year, 3 months ago

I see you learned something from the previous question ;)
upvoted 3 times

[Removed] 1 year ago

Incorrect, there would be 2 FW subnets, one regular one and the second which is management one.
upvoted 1 times

MrBlueSky Most Recent 9 months, 2 weeks ago

Careful, there may be a slightly different worded version of this on the actual exam.
upvoted 1 times

Skankhunt 12 months ago

Déjà vu ^_^
upvoted 3 times

Alessandro365 1 year, 4 months ago

Selected Answer: B

B is correct
upvoted 1 times

unclegrandfather 1 year, 7 months ago

Appeared on exam Jun/28/22
upvoted 1 times

🗨️ **kinder2** 1 year, 7 months ago

Selected Answer: B

the answer "B" is correct.
you should have this rule

```
{  
  "ruleType": "NetworkRule",  
  "name": "azure-to-kms",  
  "ipProtocols": ["TCP"],  
  "sourceAddresses": [  
    "[parameters('envParameters').firewall.properties.baseNetworkPrefix]"  
  ],  
  "sourceIpGroups": [],  
  "destinationAddresses": ["23.102.135.246"],  
  "destinationIpGroups": [],  
  "destinationFqdns": [],  
  "destinationPorts": ["1688"]  
}
```

upvoted 4 times

🗨️ **wsrudmen** 1 year, 8 months ago

Selected Answer: B

Correct!

Azure VM activation issues occur if the Windows VM is not configured by using the appropriate KMS client setup key, or the Windows VM has a connectivity problem to the Azure KMS service.

This link is better:

<https://docs.microsoft.com/en-us/troubleshoot/azure/virtual-machines/troubleshoot-activation-problems>

upvoted 2 times

🗨️ **rockethack** 1 year, 11 months ago

This question was on the exam on 18th Feb 2022.

upvoted 1 times

🗨️ **Kimimoto** 1 year, 11 months ago

Appeared in exam on 11/Feb/2022

upvoted 1 times

🗨️ **Contactfornitish** 2 years ago

Appeared in exam on 17/01/2022

upvoted 1 times

🗨️ **Pravda** 2 years, 1 month ago

KMS is the correct answer.

upvoted 3 times

🗨️ **Bharat** 2 years, 3 months ago

Based on the linked article, it should be D not B, i.e., o Subnet1, associate a network security group (NSG) that allows outbound access to port 1688. Because the Key Management Service Port is 1688.

upvoted 4 times

🗨️ **Bharat** 2 years, 3 months ago

Apologies. The provided answer is correct upon reading the article carefully.

upvoted 9 times

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT -

You have an Azure application gateway named AppGW1 that provides access to the following hosts:

- ☞ www.adatum.com
- ☞ www.contoso.com
- ☞ www.fabrikam.com

AppGW1 has the listeners shown in the following table.

Name	Frontend IP address	Type	Host name
Listen1	Public	Multi site	www.contoso.com
Listen2	Public	Multi site	www.fabrikam.com
Listen3	Public	Multi site	www.adatum.com

You create Azure Web Application Firewall (WAF) policies for AppGW1 as shown in the following table.

Name	Policy mode	Custom rule		
		Priority	Condition	Association
Policy1	Prevention	50	If IP address does contain 131.107.10.15 then deny traffic.	Application gateway: AppGW1
Policy2	Detection	10	If IP address does contain 131.107.10.15 then allow traffic.	HTTP listener: Listen1
Policy3	Prevention	70	If IP address does contain 131.107.10.15 then allow traffic.	HTTP listener: Listen2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
From 131.107.10.15, you can access www.contoso.com	<input type="radio"/>	<input type="radio"/>
From 131.107.10.15, you can access www.fabrikam.com	<input type="radio"/>	<input type="radio"/>
From 131.107.10.15, you can access www.adatum.com	<input type="radio"/>	<input type="radio"/>

Answer Area

	Statements	Yes	No
Correct Answer:	From 131.107.10.15, you can access www.contoso.com	<input checked="" type="radio"/>	<input type="radio"/>
	From 131.107.10.15, you can access www.fabrikam.com	<input checked="" type="radio"/>	<input type="radio"/>
	From 131.107.10.15, you can access www.adatum.com	<input type="radio"/>	<input checked="" type="radio"/>

Reference:
<https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/per-site-policies>

WorkHardBeProud Highly Voted 2 years, 3 months ago



Correct !

Say your application gateway has a global policy applied to it. Then you apply a different policy to a listener on that application gateway. The listener's policy now takes effect for just that listener. The application gateway's global policy still applies to all other listeners and path-based

rules that don't have a specific policy assigned to them.



<https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/policy-overview#per-site-waf-policy>

upvoted 60 times

  **Kafura** 9 months, 2 weeks ago

Say your application gateway has a global policy applied to it. Then you apply a different policy to a listener on that application gateway. The listener's policy now takes effect for just that listener. The application gateway's global policy still applies to all other listeners and path-based rules that don't have a specific policy assigned to them

upvoted 1 times

  **Ilj** 2 years, 1 month ago



correct! global policy only affects the listeners which don't have listener policies applied on them

upvoted 3 times

  **kilosh123** 1 year, 8 months ago

What about the priorities?

upvoted 3 times

  **xavi1** 1 year, 12 months ago

great explanation

upvoted 1 times

  **Morgana** Highly Voted  2 years, 3 months ago

Priority [required]

Determines the rule valuation order. The lower the value, the earlier the evaluation of the rule. The allowable range is from 1-100.

Must be unique across all custom rules. A rule with priority 40 is evaluated before a rule with priority 80.

Priority [required]
Determines the rule valuation order. The lower the value, the earlier the evaluation of the rule. The allowable range is from 1-100.

Must be unique across all custom rules. A rule with priority 40 is evaluated before a rule with priority 80.

So the priority 50 is a Deny, and will not the Connection to listen2 be allowed.



I still go for YES, NO, NO.

upvoted 36 times

  **MightyMonarch74** 10 months ago

YYN - you can ignore the priority column, as these are all separate WAF custom policies assigned to different components of the app gateway, the priorities would come into play if there were multiple custom rules within the same policy

upvoted 1 times

  **izidorf** 2 years, 2 months ago

Agree. As we have Global deny applied with low priority, Listener 2 won't be allowed. YES, NO, NO.

upvoted 8 times

  **blacknurse** 2 years, 2 months ago

If you read this document <https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/policy-overview#per-site-waf-policy> then the answer is Yes, Yes, No. Because the listener's policy takes effect for just listener 2 despite the priority.

upvoted 27 times

  **Murad01** Most Recent  1 month, 3 weeks ago

Appeared on Exam November - 2023

upvoted 1 times

  **Lazylinux** 4 months, 1 week ago

The answer is YYN and here is why as per MS doco

You can apply as many WAF policies as you like to both App gateway or/and listeners and/or path-based routing rule.

- If you want to apply the same policy to all or some listeners than you apply it at the Global level in this case the Application Gateway
- If you want to apply specific policy to certain website than apply to specific listener of that web site and the rest can be applied globally i.e. to application gateway
- This is where you need to pay attention, the Global Policy i.e. policy applied to Application Gateway will only IMPACT /EFFECT the listeners that DO NOT have any specific policy applied to them BUT if a listener has policy applied to it, it will take affect and the Global one will NOT apply to this listener

see next post

upvoted 1 times

  **Lazylinux** 4 months, 1 week ago

Here is snippet from MS Doco

If your Application Gateway has an associated policy, and then you associate a different policy to a listener on that Application Gateway, the listener's policy takes effect, but just for the listener(s) that they're assigned to. The Application Gateway policy still applies to all other listeners that don't have a specific policy assigned to them.

More info here

<https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/create-waf-policy-ag>

upvoted 1 times

  **JennyHuang36** 11 months, 1 week ago

In exam Feb, 2023

upvoted 2 times

  **afhilal** 12 months ago

the answer is correct yes, yes, no
upvoted 1 times

🗨️ **GohanF2** 1 year, 2 months ago

Also, keep in mind the priorities. The lower the integer number in the "priority" field, the highest the priority to be processed. It's like setting up "metrics" in a network; the lower the integer the higher is the priority.
upvoted 1 times

🗨️ **GohanF2** 1 year, 2 months ago

Answer is: YES, NO, NO.
The priority of the policy orders matters.

1. The first one is analyzed by customized rule 1 which is set to allow traffic by default behavior of "Detection mode".
 2. The second goes through the Global Policy attached to the Application Gateway which is set to deny and then stops processing rules.
 3. It's the same as 2. It goes through the global policy rule which is set to deny and then it stops processing policies. The policy 3 its never processed due the global policy that is set to deny.
- upvoted 3 times

🗨️ **wetraining123** 1 year, 5 months ago

The answer is correct.

If your Application Gateway has an associated policy, and then you associated a different policy to a listener on that Application Gateway, the listener's policy will take effect, but just for the listener(s) that they're assigned to. The Application Gateway policy still applies to all other listeners that don't have a specific policy assigned to them.

If you assign a policy to your Application Gateway (or listener) that already has a policy in place, the original policy is overwritten and replaced by the new policy.
upvoted 3 times

🗨️ **Azuriste** 1 year, 5 months ago

For me YES NO NO
upvoted 1 times

🗨️ **lobs_wort** 1 year, 6 months ago

In exam 21-Jul-22.
upvoted 1 times

🗨️ **Payday123** 1 year, 7 months ago

Contoso.com - Y - this policy overrides deny for AppGW1. By default traffic is allowed so even if it is set to Detection only it changes nothing and still does not block the traffic
Fabrikam.com - Y - again this policy overrides deny for AppGW1 and it is set to Prevention and allow
Adatum.com - N - takes policy from AppGW1 so Prevention and deny
upvoted 2 times

🗨️ **Payday123** 1 year, 7 months ago

Priorities does not matter here because every rule is associated with different listener.
upvoted 4 times

🗨️ **Payday123** 1 year, 7 months ago

What is default Action in Application Gateway if none of conditions in rules are matching?
upvoted 1 times

🗨️ **Payday123** 1 year, 7 months ago

I've found it. If there are no custom rules the traffic is scanned by by other global managed rules and allowed.
upvoted 1 times

🗨️ **SCATEST** 1 year, 7 months ago

Policy2 is only in "Detection" mode - so only logging is active but all traffic is allowed: No, Yes, No
upvoted 1 times

🗨️ **d3j4n** 1 year, 7 months ago

N,Y,N Tested in Lab!
upvoted 1 times

🗨️ **sapien45** 1 year, 3 months ago

YYN. Meth Labs do not count
upvoted 2 times

🗨️ **FaceBack** 1 year, 8 months ago

Correct is YYN
Policy 2 is a deny poliy that will deny all access when no such IP is included.
So we are looking at policies 1,3.
upvoted 1 times

🗨️ **RVR** 1 year, 8 months ago

NYN
Policy 2 is in detection mode, so it won't take any action.
upvoted 4 times

店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

You have an Azure virtual network that contains a subnet named Subnet1. Subnet1 is associated to a network security group (NSG) named NSG1. NSG1 blocks all outbound traffic that is not allowed explicitly.

Subnet1 contains virtual machines that must communicate with the Azure Cosmos DB service.

You need to create an outbound security rule in NSG1 to enable the virtual machines to connect to Azure Cosmos DB.

What should you include in the solution?

- A. a service tag
- B. a service endpoint policy
- C. a subnet delegation
- D. an application security group

Correct Answer: A

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/service-tags-overview> <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoint-policies-portal>

Community vote distribution

A (86%)

14%

 **HTD** Highly Voted 1 year, 9 months ago

The ideal option is a Private point, but the question says outbound connection is needed, then adding a rule with a service tag makes sense, also if security is not a concern and cost is needed to be minimum. Else a Private point is a perfect solution here

upvoted 6 times

 **jeffangel28** 1 year, 5 months ago

100% right!

upvoted 1 times

 **tartarus23** Highly Voted 1 year, 6 months ago

Selected Answer: A

A. a service tag

Create a service tag pointing to Azure Cosmos DB to allow the outbound connectivity.

upvoted 5 times

 **Murad01** Most Recent 1 month, 3 weeks ago

Appeared on the Exam November -2023

upvoted 1 times

 **Lazylinux** 4 months, 1 week ago

Selected Answer: B

B is Honey

I cannot believe everyone voted A, I think because everyone is fixated with Service Tags, it would be correct for most Azure services but NOT COSMOS here is why and check the link for yourself

from MS **NSG rules are used to limit connectivity to and from a subnet with virtual network. When you add service endpoint for Azure Cosmos DB to the subnet, there's no need to open outbound connectivity in NSG for your Azure Cosmos DB account.**

<https://learn.microsoft.com/en-us/azure/cosmos-db/how-to-configure-vnet-service-endpoint>

Also check

<https://learn.microsoft.com/en-us/azure/cosmos-db/how-to-configure-vnet-service-endpoint>

upvoted 2 times

 **FN21** 4 months ago

You miss this part in the question "NSG1 blocks all outbound traffic that is not allowed explicitly" :-)

upvoted 1 times

 **Billabongs** 6 months, 1 week ago

Selected Answer: A

Correct Answer

<https://learn.microsoft.com/en-us/azure/virtual-network/service-tags-overview#available-service-tags>

upvoted 1 times

 **JennyHuang36** 11 months, 1 week ago

In exam Feb, 2023

upvoted 1 times

🗳️ 👤 **Alessandro365** 1 year, 4 months ago

Selected Answer: A

A is correct

upvoted 2 times

🗳️ 👤 **zerocool114** 1 year, 6 months ago

on exam today

upvoted 2 times

🗳️ 👤 **unclegrandfather** 1 year, 7 months ago

Appeared on exam Jun/28/22

upvoted 1 times

🗳️ 👤 **VonKellus** 1 year, 10 months ago

why not B. a private endpoint?

upvoted 2 times

🗳️ 👤 **rockethack** 1 year, 11 months ago

This question was on the exam on 18th Feb 2022.

upvoted 1 times

🗳️ 👤 **nitinkumarmca** 1 year, 11 months ago

Selected Answer: A

Service Tags

upvoted 4 times

🗳️ 👤 **Joshalom** 1 year, 11 months ago

on exam 6/2/2022

upvoted 1 times

🗳️ 👤 **Pravda** 2 years ago

on exam 1/6/2022

upvoted 3 times

🗳️ 👤 **Pravda** 2 years, 1 month ago

What is service tag in Azure?

Image result for azure service tags

A service tag represents a group of IP address prefixes from a given Azure service. ... You can use service tags to define network access controls on network security groups or Azure Firewall. Use service tags in place of specific IP addresses when you create security rules.

upvoted 5 times

🗳️ 👤 **SSTan** 2 years, 1 month ago

User defined service tag to enable to connection to Cosmos DB.

upvoted 1 times

🗳️ 👤 **Pravda** 2 years, 1 month ago

You can use service tags to define network access controls on network security groups or Azure Firewall. Use service tags

upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

Your company has offices in Montreal, Seattle, and Paris. The outbound traffic from each office originates from a specific public IP address. You create an Azure Front Door instance named FD1 that has Azure Web Application Firewall (WAF) enabled. You configure a WAF policy named Policy1 that has a rule named Rule1. Rule1 applies a rate limit of 100 requests for traffic that originates from the office in Montreal. You need to apply a rate limit of 100 requests for traffic that originates from each office.

What should you do?

- A. Modify the rate limit threshold of Rule1.
- B. Create two additional associations.
- C. Modify the conditions of Rule1.
- D. Modify the rule type of Rule1.

Correct Answer: C

Community vote distribution

C (88%)

12%

 **Payday123** Highly Voted 1 year, 7 months ago

Selected Answer: C

"Rate limits are applied for each client IP address. If you have multiple clients accessing your Front Door from different IP addresses, they will have their own rate limits applied."

upvoted 11 times

 **pinchocr** Highly Voted 1 year, 7 months ago

Selected Answer: C


It's correct. Lab tested, you can add IP addresses as conditions in the same rule.

upvoted 7 times

 **25max** 9 months, 3 weeks ago

Yes, but in this case the 3 IPs share the 100 request and the task is 100 req/branch so you need 3 rules.

upvoted 1 times

 **25max** 9 months, 3 weeks ago

ignore my comment above, it is IP based and emphasized that the offices has own single

upvoted 1 times

 **bp_a_user** Most Recent 3 months, 1 week ago

"ClientAddr: This is the default option, and it means that each rate limit threshold and mitigation applies independently to every unique source IP address."

Answer C

From here: <https://techcommunity.microsoft.com/t5/azure-network-security-blog/rate-limiting-feature-for-azure-waf-on-application-gateway-now/ba-p/3934957#:~:text=Rate%20limiting%20is%20configured%20using,and%20a%20group%20by%20variable.>

upvoted 1 times


 **Lazylinux** 4 months, 1 week ago

Selected Answer: C

I C is correct!

Correct answer modify condition based on IP address of remote sites, you can also you Geo and rate limit is applied per condition

upvoted 2 times

 **FN21** 4 months ago

Can you add multiple IP address in one condition? As far as I know, additional conditions are added with AND operator not OR. Therefore if that's the case, your rate limit rule will never be matched

upvoted 1 times

 **Lazylinux** 1 month, 3 weeks ago

Thanks for making the comment, however YES you can add multiple IP address in the IF condition, they are added in different rows and you can add as much as you can (im not sure of the limit on IP addresses can be added), so when the policy is checked each IP address is checked and if valid then the policy applies to that IP address and so on. The ONLY exception i.e. if you have IP address 192.168.33.45 rate limit of 50 and other IP 172.16.34.56 rate limit of 100 then definitely in that case you need to create 2 separate rules.

Hope this helps

You can try the above by creating WAF policy which is FREE in Azure tenancy, if this website allows for images be uploaded i would have done so

upvoted 2 times

 **mabalon** 4 months, 4 weeks ago

Selected Answer: C

Answer C.

Tested on LAB. You can add multiple IP on the Same Condition.

I have also tested that the limit is on each ip, not shared. If one IP reach the limit the other IP have its own limit and its able to connect without problem

upvoted 1 times

🗨️ **SaadKhamis** 9 months ago

Selected Answer: C

Just tested in the lab with the following:

```
$IPMatchCondition = New-AzFrontDoorWafMatchConditionObject -MatchVariable RemoteAddr -OperatorProperty IPMatch -NegateCondition $false -MatchValue "20.234.16.25", "20.234.16.26", "20.234.16.27"
$IPAllowRule = New-AzFrontDoorWafCustomRuleObject -Name "IPAllowRule" -RuleType MatchRule -MatchCondition $IPMatchCondition -Action Allow -Priority 10
$IPAllowPolicyExamplePS = New-AzFrontDoorWafPolicy -Name "IPRestrictionExamplePS" -resourceGroupName rg-test -Customrule $IPAllowRule -Mode Detection -EnabledState Enabled
```

I, also, created the rule with one IP address then, manually, was able to add two more IPs.

upvoted 2 times

🗨️ **Darkren4everR** 10 months ago

Option B is Correct

upvoted 1 times

🗨️ **pOOM22** 10 months, 1 week ago

in exam march 23

upvoted 3 times

🗨️ **Sbr82** 10 months, 2 weeks ago

Selected Answer: B

To apply a rate limit of 100 requests for traffic that originates from each office, you should create two additional associations. This is because the current configuration applies a rate limit of 100 requests for traffic that originates from the office in Montreal only. By creating two additional associations, you can apply a rate limit of 100 requests for traffic that originates from each office

upvoted 3 times

🗨️ **TJ001** 1 year ago

When a custom rule is created in WAF policy there is option to add IP address not just on but multiple so 1 rule is sufficient ..all that is needed all the edge IPs from all locations in the one rule

upvoted 1 times

🗨️ **TJ001** 1 year ago

so agree with Answer C

upvoted 1 times

🗨️ **1particle** 1 year, 5 months ago

B

Per this link

<https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-configure-ip-restriction#create-a-waf-policy>

You can add an IP address or range only. You would need to create two additional associations for the other 2 locations.

upvoted 1 times

🗨️ **mdnick** 1 year, 8 months ago

<https://github.com/MicrosoftDocs/azure-docs/issues/32333>, as per the above doc, tried the below. So yes the answer is Modify the condition.

```
$testIPmatches = New-AzFrontDoorWafMatchConditionObject -MatchVariable RemoteAddr -OperatorProperty IPMatch -NegateCondition $true -MatchValue "103.78.18.242", "103.78.18.245"
```

upvoted 4 times

🗨️ **Jorex** 1 year, 8 months ago

Also through the portal it's clearly visible, if you add an IP another text box appears to add another one.

upvoted 3 times

🗨️ **milan92stankovic** 1 year, 8 months ago

That will apply the rate limit of 100 requests in total for all listed IPs.

I haven't tested it yet. If someone has, please teach us :)

upvoted 1 times

🗨️ **JulienYork** 1 year, 8 months ago

Should be B

Create a two additional associations they are individual resources, individual locations.

upvoted 3 times

🗨️ **pinpin06** 1 year, 9 months ago



As per the following link <https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-rate-limit-powershell> and this one

<https://azure.microsoft.com/en-us/resources/templates/front-door-rate-limiting/>

I understand that each rate-limit is for a specific IP address only, I never found anything about a group of IPs, so I would consider the response B : create a two additional associations
upvoted 4 times

  **vunder** 1 year, 9 months ago

I am a bit confused about this line "Your company has offices in Montreal, Seattle, and Paris. The outbound traffic from each office originates from a specific public IP address." so then when you factor in this line "Rate limits are applied for each client IP address. If you have multiple clients accessing your Front Door from different IP addresses, they will have their own rate limits applied." from "<https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-rate-limit-powershell>", I then see why C is correct.
upvoted 4 times

  **lavermil** 1 year, 5 months ago

Agreed! See the note on the link provided above. It says: "Rate limits are applied for each client IP address. If you have multiple clients accessing your Front Door from different IP addresses, they will have their own rate limits applied."
upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

You have an Azure virtual network named Vnet1.

You need to ensure that the virtual machines in Vnet1 can access only the Azure SQL resources in the East US Azure region. The virtual machines must be prevented from accessing any Azure Storage resources.

Which two outbound network security group (NSG) rules should you create? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. a deny rule that has a source of VirtualNetwork and a destination of Sql
- B. an allow rule that has the IP address range of Vnet1 as the source and destination of Sql.EastUS
- C. a deny rule that has a source of VirtualNetwork and a destination of 168.63.129.0/24
- D. a deny rule that has the IP address range of Vnet1 as the source and destination of Storage

Correct Answer: BD

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/service-tags-overview>

Community vote distribution

BD (95%)

5%

 **milan92stankovic** Highly Voted 1 year, 8 months ago

Selected Answer: BD

Correct Answer - B & D
upvoted 9 times

 **pinchocr** Highly Voted 1 year, 7 months ago

Selected Answer: BD

Correct
upvoted 6 times

 **kikocu** Most Recent 1 month, 1 week ago

Storage has nothing to do with SQL. For me the correct answer will be BC. We all agree B is correct. C because the Azure IP DNS resolution (168.63.129.16) is part of that range.
upvoted 1 times

 **Lazylinux** 4 months, 1 week ago

Selected Answer: BD

Have to admit this question is typical MS question i.e. as dumb as can get here is why

- Not much information is given about the vNET
- Yes you can chose AB and answer is correct in terms of meeting the requirement for SQL i.e. stop access to all SQL instances except East USA, however A Deny rule needs to be of lower priority than the E-US rule to avoid blocking access to all SQL instances – example E-US rule priority 100 and block SQL 110 . However this solution doesn't restrict the VMs from accessing the storage as per requirement
- Yes you can chose BD, where B meets the requirement for e-US SQL and D meets the condition to block access to storage, however it doesn't meet the requirement to prevent access to SQL resources in general

If comes in the exam I would RELUCTANTLY chose BD

upvoted 1 times

 **Apptech** 10 months ago

I don't get it. Default outbound rule for NSG is "allow all". For this case for SQL access requirement we would need answers A + B. For storage access prevention we would also need answer D.

If we would assume that outbound default NSG rule is "deny all" we would need allow rule for Sql.East and an allow rule for storage.

So, in none of the scenarios we have a perfect answer option when just choosing 2 answers

upvoted 1 times

 **_fvt** 9 months, 3 weeks ago

"Each correct answer presents part of the solution." the key is here.


So;

B - because you need to allow only VMs to SQL in specific East US region not All SQL (so not A).

D - because as asked you need to deny VMs to all Storage.

And you'll probably will add a deny rule if you had to complete "parts" of the solution.

upvoted 2 times

 **staffo** 11 months, 2 weeks ago

A would work but question only mentions working with VNET1. It does not specifically mention other VNET's. D is more specific.

upvoted 1 times

omgMerrick 11 months, 2 weeks ago

Selected Answer: BD

B & D

Explanation:

Rule B allows traffic from the virtual machines in Vnet1 to the Azure SQL resources in the East US Azure region.

Rule D denies traffic from the virtual machines in Vnet1 to any Azure Storage resources.

Rule A is incorrect because it allows traffic from the virtual machines in Vnet1 to any destination that contains "Sql".

Rule C is incorrect because it denies traffic from the virtual machines in Vnet1 to the Azure instance metadata service, which is not related to the given requirements.

upvoted 3 times

rac_sp 1 year, 6 months ago

Selected Answer: AB

Because Storage is NOT the same as SQL. There are completely different TAGs to SQL and STORAGE.SQL is database, Storage is Storage.

upvoted 1 times

cypher9 1 year, 6 months ago

reference?

upvoted 1 times

cypher9 1 year, 6 months ago

I dont get it, why would you have a deny rule that has a source of VirtualNetwork?

upvoted 1 times

tng69 1 year, 5 months ago

Even if it's not what anyone would do, it is the solution closest to the ideal solution (which would be to set the VM's IP as source)

upvoted 1 times

rac_sp 1 year, 6 months ago

shoud be A and B. Storage Tags is different from SQL(that is a database actually). Also take a look that there is a TAG specifically for SQL which is a completely different resource than a Storage.

upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 Azure subscription that contains the following resources:

- ☞ A virtual network named Vnet1
- ☞ A subnet named Subnet1 in Vnet1
- ☞ A virtual machine named VM1 that connects to Subnet1
- ☞ Three storage accounts named storage1, storage2, and storage3

You need to ensure that VM1 can access storage1. VM1 must be prevented from accessing any other storage accounts.

Solution: You configure the firewall on storage1 to only accept connections from Vnet1.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Community vote distribution

B (100%)

 **Jamesat** Highly Voted 1 year, 5 months ago

Selected Answer: B

Correct.

Setting a firewall setting to only allow access to Storage1 from VM 1 wouldn't stop access to the other 2 storage accounts.

As per requirements, VM1 should only be able to access Storage1. NOT Storage1 should only be accessed from VM1.

upvoted 5 times

 **voldemort123** Most Recent 4 months ago

Service endpoint need to be enabled for storage, only then you can permit/deny in paas firewall.

upvoted 1 times

 **daemon101** 6 months, 2 weeks ago

I think even though you allowed the vnet to SA1 firewall, VM1 won't still be able to access SA1 as it is not mentioned that the service endpoint for storage on subnet1 is enabled.

upvoted 1 times

 **Alessandro365** 1 year, 4 months ago

Selected Answer: B

B is correct.

VM1 can only access storage1, so firewall has to be configured on storage2 and storage3 to block access from VM1

upvoted 2 times

 **Houssemonline** 1 year, 5 months ago

any explanation ? i think A- YES


upvoted 1 times

 **Alessandro365** 1 year, 4 months ago

correct is NO.

VM1 can only access storage1, so firewall has to be configured on storage2 and storage3 to block access from VM1

upvoted 1 times

 **derrp** 1 year, 6 months ago

This solution does not prevent access to Storage2 and Storage3.

upvoted 4 times

 **unclegrandfather** 1 year, 7 months ago

Appeared on exam Jun/28/22

upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 Azure subscription that contains the following resources:

- ☞ A virtual network named Vnet1
- ☞ A subnet named Subnet1 in Vnet1
- ☞ A virtual machine named VM1 that connects to Subnet1
- ☞ Three storage accounts named storage1, storage2, and storage3

You need to ensure that VM1 can access storage1. VM1 must be prevented from accessing any other storage accounts.

Solution: You create a network security group (NSG) and associate the NSG to Subnet1.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Community vote distribution

B (84%)

A (16%)

 **derrp** Highly Voted 1 year, 6 months ago

Assuming the NSG does not magically know what you're trying to do, we can assume the answer is no.
upvoted 32 times

 **tartarus23** Highly Voted 1 year, 6 months ago

Selected Answer: B

B. No

I do not think it meets the goal since the NSG was not specific on what account or access it allowed or denied.
upvoted 12 times

 **omgMerrick** Most Recent 11 months, 2 weeks ago

Selected Answer: B

B. No

This solution does not fully meet the goal.

Although creating a network security group (NSG) and associating it to Subnet1 is a step in the right direction for securing network traffic, simply associating an NSG to a subnet does not restrict outbound traffic from VM1 to the storage accounts.

To ensure that VM1 can access storage1 and is prevented from accessing any other storage accounts, you need to apply a specific set of rules to the NSG. One way to achieve this is by configuring the NSG to allow outbound traffic only to storage1 and deny outbound traffic to all other storage accounts.

So, to fully meet the goal, you need to create an NSG, associate it to Subnet1, and then configure appropriate rules in the NSG to allow traffic from VM1 to storage1 and block traffic to all other storage accounts.

upvoted 4 times

 **TJ001** 1 year ago

NSG wont help...we can define rules to deny/allow access to Storage service or a regional storage service by using service tags...but in this case the VM should access only one storage account... so NSG wont help here... Answer No
upvoted 1 times

 **TJ001** 1 year ago

Creating service endpoint policy is a good idea
upvoted 2 times

 **AzureJobsTillRetire** 1 year ago

Selected Answer: A

Hey guys, I think the answer might be A yes. I had this question in my exam in a group of three YES/NO questions. I passed the exam with a score of 900, which is not very high but enough. I thought that there would be one YES in the three questions, and if that is true, this one is the only one could be YES. We can either assume the NSG does not configure well and give it a NO, or assume the NSG is configured as it should be and give it a YES.

upvoted 2 times

  **wooyourdaddy** 9 months, 4 weeks ago

All of these 3 questions would be a no. The simplest solution to this problem would be to implement a service endpoint for storage on the subnet that VM1 is on and then use a service endpoint policy to limit it to the storage1 resource only.

Source: <https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoint-policies-overview>

upvoted 1 times

  **Aunehwet79** 1 year ago

That's a pretty good score bro

upvoted 4 times

  **GohanF2** 1 year, 2 months ago

it's too vague the solution so the answer is NO.


upvoted 2 times

  **Prutser2** 1 year, 3 months ago

Selected Answer: B

it doesnt stipulate what is in the NSG, so assuming it is empty, in which case it will not do anything

upvoted 2 times

  **BlackZeros** 1 year, 4 months ago

Selected Answer: B

default NSG will allow the traffic to still go out.

upvoted 2 times

  **Alessandro365** 1 year, 4 months ago

Selected Answer: B

No is correct


upvoted 2 times

  **azeem0077** 1 year, 5 months ago

Selected Answer: B

Just adding an NSG won't do any change. So answer is B. Incase if the question also said that outbound and inbound rules are there in the NSG, then the answer may have been A.

upvoted 3 times

  **Jamesat** 1 year, 5 months ago

Selected Answer: B

A NSG would do nothing without Rules.

Also if the Storage Accounts are public then you would need to set a Service Endpoint and then block it. This would affect all the storage accounts.

Without clarity this is cleared a NO.

upvoted 3 times

  **jeffangel28** 1 year, 5 months ago

Selected Answer: B

Correct!, is not only create and associate NSG necessary!

upvoted 3 times



  **hogemax** 1 year, 6 months ago

Selected Answer: B

B. No

This just creates a network security group and associates it to Subnet1. Further configuration is required.

upvoted 7 times

  **rac_sp** 1 year, 6 months ago

extremely abstract the information provided in the question.

upvoted 2 times

  **Swetareddy** 1 year, 6 months ago


It happens only thru service endpoint policies using which u can restrict access to only one storage account.

upvoted 3 times

  **unclegrandfather** 1 year, 7 months ago

Appeared on exam Jun/28/22



upvoted 1 times

  **BenH** 1 year, 8 months ago

Selected Answer: A

I think this will meet the goal.

upvoted 5 times

  **Diazan** 8 months ago

A NSG by itself (with only default rules configured) won't work at all
upvoted 1 times

  **jeffangel28** 1 year, 5 months ago

explain how pls
upvoted 2 times

店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 Azure subscription that contains the following resources:

☞ A virtual network named Vnet1

A subnet named Subnet1 in Vnet1 -

-
- ☞ A virtual machine named VM1 that connects to Subnet1
- ☞ Three storage accounts named storage1, storage2, and storage3

You need to ensure that VM1 can access storage1. VM1 must be prevented from accessing any other storage accounts.

Solution: You create a network security group (NSG). You configure a service tag for Microsoft.Storage and link the tag to Subnet1.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Community vote distribution

B (100%)

🗨️ **Prutser2** Highly Voted 1 year, 3 months ago

Selected Answer: B

the service tag in a blanket rule can only deny all storage or permit all storage, it would have no further granularity
upvoted 7 times

🗨️ **BlackZeros** Most Recent 1 year, 4 months ago

Selected Answer: B

correct
upvoted 1 times

🗨️ **Jamesat** 1 year, 5 months ago

Selected Answer: B

Correct.

I am assuming they mean to create an NSG rule with Storage Service Tag. Not sure whether they are denying access or not, however, this would apply to all Storage Accounts access via public endpoints.

upvoted 3 times

🗨️ **derrp** 1 year, 6 months ago

No. This proposed solution does not mention any means of blocking VM1 from Storage2 and Storage3.

upvoted 1 times

🗨️ **unclegrandfather** 1 year, 7 months ago

Appeared on exam Jun/28/22

upvoted 1 times

You need to use Traffic Analytics to monitor the usage of applications deployed to Azure virtual machines. Which Azure Network Watcher feature should you implement first?

- A. NSG flow logs
- B. IP flow verify
- C. Connection monitor
- D. Packet capture

Correct Answer: A

Network Watcher: A regional service that enables you to monitor and diagnose conditions at a network scenario level in Azure. You can turn NSG flow logs on and off with Network Watcher.

Network security group (NSG) flow logs is a feature of Azure Network Watcher that allows you to log information about IP traffic flowing through an NSG.

Why use NSG Flow Logs?

It is vital to monitor, manage, and know your own network for uncompromised security, compliance, and performance.

Common use cases include Network Monitoring: Identify unknown or undesired traffic. Monitor traffic levels and bandwidth consumption.

Filter flow logs by IP and port to understand application behavior.

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-overview>


Community vote distribution

A (100%)

 **Lazylinux** 4 months, 1 week ago

Selected Answer: A

Given answer is correct as it is one of the requirement for using the Traffic analytics
upvoted 1 times

 **JennyHuang36** 11 months, 1 week ago

In exam Feb, 2023
upvoted 3 times

 **TJ001** 1 year ago

Answer A
Enable NSG Flog Logs. Part of the activity requires the below
Requires a Log Analytics Workspace to enable Traffic Analytics Solution
Storage account is needed to store NSG Flow Logs
upvoted 2 times

 **sapien45** 1 year, 3 months ago

Selected Answer: A

Traffic analytics examines raw NSG flow logs. It then reduces the log volume by aggregating flows that have a common source IP address, destination IP address, destination port, and protocol.
Reduced logs are enhanced with geography, security, and topology information and then stored in a Log Analytics workspace.
upvoted 3 times

 **BlackZeros** 1 year, 4 months ago

<https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics>
NSG Flow Logs are the key component
upvoted 2 times

 **BlackZeros** 1 year, 4 months ago

Selected Answer: A

A seems to be the correct answer.
upvoted 1 times

HOTSPOT -

You have an Azure subscription that contains the virtual machines shown in the following table.

Name	Virtual network	Subnet	Workload
SQL1	VNet1	Subnet1	Microsoft SQL Server 2019
Web1	VNet1	Subnet1	IIS
Web2	VNet1	Subnet2	IIS
SQL2	VNet2	Subnet1	Microsoft SQL Server 2019
Web3	VNet2	Subnet1	IIS
SQL3	VNet2	Subnet2	Microsoft SQL Server 2019

VNet1 and VNet2 are NOT connected to each other.

You need to block traffic from SQL Server 2019 to IIS by using application security groups. The solution must minimize administrative effort. How should you configure the application security groups? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area:

Minimum number of application security groups:

1
2
3
6

Minimum number of application security group assignments:

1
2
3
6

Correct Answer:

Answer Area:

Minimum number of application security groups:

1
2
3
6

Minimum number of application security group assignments:

1
2
3
6

Box 1: 2 -

All network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in.

We need one application security group for each of the two virtual networks.

Box 2: 3 -

One network assignment in VNet1. Two network assignments in VNET2.

Reference:

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

 **keilah123** Highly Voted 10 months, 4 weeks ago

2 ASG and 2 ASG assignments


The question is looking for minimum.

VNET 1:

Create 1 ASG for SQL. Create outbound deny rule and assign to SQL1 Nic

VNET2: Create 1 ASG for IIS. Create inbound deny rule and assign to Web3 Nic

upvoted 10 times

 **Rododendron2** 1 month, 2 weeks ago

Not correct due to not correctly understood Question. Once again - Question is looking for minimum administrative effort, not for minimal number of ASG/assignments.

upvoted 1 times

 **Apptech** 10 months ago

Yes, but question also says: "block traffic from SQL Server 2019 to IIS". With your ASG for IIS you deny any kind of instance / service to access IIS.


upvoted 3 times

 **Ditka** 6 months, 1 week ago

I think it would be:

VNET 2: Create 1 ASG for SQL inbound deny and assign to IIS NIC.

upvoted 1 times

 **ironbornson** 3 months, 3 weeks ago

On SQL Traffic will use a random source port and dst-port 80,443. If you apply an ASG to IIS you will have no way to identify if traffic is coming from SQL or not. The only way to block VM-SQL to VM-IIS is to create a rule blocking ASG for VM-SQL like this:
Direction: outbound, Source:ASG-VM, Dst: (you can put IIS IP or IIS ports), Action: deny

TL;DR: 2 ASG and 3 assignments

upvoted 2 times

 **Ditka** 6 months, 1 week ago

Total 2 ASGs and 2 ASG assignments.

upvoted 1 times

 **Alessandro365** Highly Voted 1 year, 4 months ago

2 ASGs e 3 assignments, answer is correct.

"All network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in."

<https://learn.microsoft.com/en-us/azure/virtual-network/application-security-groups>

the ASG needs to be associated with the network card of the VMs, so there are 3 associations

upvoted 7 times

 **Ayokun** 11 months ago

But being that is requested the configuration of the ASG only on the SQL vm's to minimize administrative effort the answer should be halved:

4 asg = 2 (onlysql)

6 assignments per nic = 3 (only sql)

upvoted 1 times

 **Ayokun** 11 months ago

Hence being the ASG associated per NIC it should be 6 the second answer.

upvoted 1 times

 **Webesciaki** Most Recent 3 weeks, 5 days ago

2 ASG / 3 assignments:

1x ASG for vnet1/sql

1x ASG for vnet2/sql

now assignments:

1) 1st sql server in vnet1

2) 1st sql server in vnet 2

3) 2nd sql server in vnet 2

then subnet level NSGs with inbound rule (source SQL application group -> dst any > deny)

upvoted 2 times

  **occupatissimo** 8 months, 3 weeks ago

2 & 3

key word is "minimize administrative effort", and remember goal is to block sql.

so work only with outbound rule applied to SQL server, when building the rule will have the tcp-80, doesn't matter which destination (use any), for sure IIS server are in.

in this case 2 ASG (1 each vnet) for sql are required and 3 assignment (1 each sql server nic).

upvoted 3 times

  **occupatissimo** 8 months, 2 weeks ago

or think in this way too

communication between vnet is deny due to default rule in nsg, so only to block traffic between subnet in the same vnet. Assuming in the sql subnet the source as any and the dest the ASG necessary is for web server only, tis in each vnet, so 2 ASG in total.

Associate then the three web server nics to them.

upvoted 2 times

  **guchao2000** 10 months, 1 week ago

NSG and ASG can be used in different vnet. Tested.

upvoted 2 times

  **iVath** 10 months, 1 week ago


it's only required : from SQL Server 2019 to IIS. what about these 3 ASG assignments:

(Source=Vnet1/Sub1/SQL, Destination=Vnet1/Sub1/IIS, Access=Deny)

(Source=Vnet2/Sub1/SQL, Destination=Vnet2/Sub1/IIS, Access=Deny)

(Source=Vnet2/Sub2/SQL, Destination=Vnet2/Sub1/IIS, Access=Deny)

upvoted 3 times

  **TJ001** 1 year ago

No of ASGs [ANS 4] - So there are 2 VNETs, 2 types of applications in both VNET one of type IIS and one of type SQL. The best practice is to use ASG assignment for both app types... which means 2 ASGs per VNET = 4 ASGs required. Note ASG cannot reference multiple VNETs

2)No of associations [Ans 6] ? - The assignment is at subnet level, so we could do add either an outbound rule for SQL server subnet or an inbound rule at IIS server subnet or both .. Assume we are adding only one rule (either inbound or outbound) and the question asks minimum no of assignments

- In VNET 1 add an outbound rule for Subnet 1 to deny traffic from SQL ASG to IIS ASG

- In VNET 2 add an inbound rule for Subnet 1 to deny traffic from SQL ASG to IIS ASG

so 1 NSG rule per VNET is sufficient to introduce the control.. To meet this solution the ASG needs to be associated to all the VMs in all VNET ... so total 6 associations is needed (if by 'association' it means attaching ASG to VM NIC)

upvoted 1 times

  **TJ001** 1 year ago

it appears the option does not have an ideal set up and it looks it is only considering attaching ASG to SQL component in which casewe could half the consideration above to conclude the answers as 2 ASG and 3 assignments ...not elegant/scalable approach but will have to go with that

upvoted 4 times

  **Goofer** 1 year ago

I think you must create one ASG for all IIS NIC's and one NSG on all SQL server NICs

In the NSG Block all outgoing traffic to IIS ASG. (You need only to block traffic from SQL Server 2019 to IIS)

1 ASG (for all IIS NICs)

1 NSG (for all SQL NICs)

It's not a pretty solution, but with the least administrative effort

upvoted 3 times

  **Goofer** 1 year ago

If all network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in. You need 2 ASG's

upvoted 1 times

  **mhmyz** 1 year, 1 month ago

2 ASGs

How to make the IIS side (receiving side) an application group,

How to make the SQL side (sending side) an application group

There are two, and both methods create one application group for each VNET, so there are two application groups.

2 Assignments

In VNET1, the IIS side is set as an application group, and transmission to the IIS application group can be suppressed in the transmission traffic of Subnet1 or NIC of SQL1.

In VNET2, the SQL side is set as an application group, and reception to the IIS application group should be suppressed in the reception traffic of Subnet1 or NIC of Web3.

upvoted 4 times

  **Goofer** 1 year ago

How do you block traffic between Web1 and SQL1. They are on the same subnet.

upvoted 2 times

  **palthainon** 10 months, 2 weeks ago

NSG's can be assigned at the NIC level.

upvoted 1 times

  **NoeHdzMII** 1 year, 1 month ago

Confuse answer, the correct answer is to have 2 ASG and 3 associations per VNET, in this case, there are 2 VNETs. Total 4 ASG and 6 associations, one association per VM

upvoted 6 times

  **TJ001** 1 year ago


agree but the options does not have 4 ASG

upvoted 3 times

  **daemon101** 6 months, 2 weeks ago

I also agree. If only vnet1 contains IISs and Vnet2 has SQL then it will only need two ASGs.

upvoted 1 times

  **Prutser2** 1 year, 3 months ago

answer is correct

upvoted 4 times

  **sapien45** 1 year, 3 months ago

By network security group assignement, they mean how many Microsoft SQL servers assigned within an Application security group

upvoted 4 times

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT -

You have an Azure virtual network that contains the subnets shown in the following table.

Name	Address space	Associated network security group (NSG)
Subnet1	10.10.0.0/24	NSG1
Subnet2	10.10.1.0/24	NSG2

In NSG1, you create inbound rules as shown in the following table.

Source	Priority	Port	Action
*	101	80	Allow
*	150	443	Allow
Virtual network	200	*	Deny

NSG2 has only the default rules configured.

You have the Azure virtual machines shown in the following table.

Name	Subnet
VM1	Subnet1
VM2	Subnet1
VM3	Subnet2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
VM3 can connect to port 8080 on VM1.	<input type="radio"/>	<input type="radio"/>
VM1 and VM2 can connect on port 9090.	<input type="radio"/>	<input type="radio"/>
VM1 can connect to VM3 on port 9090.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
VM3 can connect to port 8080 on VM1.	<input checked="" type="radio"/>	<input type="radio"/>
VM1 and VM2 can connect on port 9090.	<input type="radio"/>	<input checked="" type="radio"/>
VM1 can connect to VM3 on port 9090.	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: Yes -

VM3 is Subnet2. NSG2 applies. The default rule will allow communication.

Box 2: No -

VM1 & VM2 is in Subnet1. NSG1 applies. Only traffic on ports 80 and 443 will be allowed. Connection on port 9090 will be denied.

Note: Priority: A number between 100 and 4096. 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. As a result, any rules that exist with lower priorities (higher numbers) that have the same attributes as rules with higher priorities are not processed.

Box 3: No -

VM1 is in Subnet1. NSG1 applies. Only traffic on ports 80 and 443 will be allowed. Connection on port 9090 will be denied.

Reference:

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

🗨️ **Sheriboy** Highly Voted 1 year, 5 months ago

should be N,N, Y

- 1) Inbound rule on subnet1 will deny
 - 2) Inbound rule on subnet2 will deny
 - 3) No rule on VM3 so it would allow connections
- upvoted 74 times

🗨️ **mav3r1ck** 1 year, 4 months ago

Disagree.. Should be N Y Y
upvoted 18 times

🗨️ **daemon101** 6 months, 2 weeks ago

it should be N N Y.

Intra-Subnet traffic - It's important to note that security rules in an NSG associated to a subnet can affect connectivity between VMs within it.

<https://learn.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works#intra-subnet-traffic>

upvoted 4 times

🗨️ **Faridtnx** 1 day, 13 hours ago

if that's the case then NNY is correct answer
upvoted 1 times

🗨️ **Chriscrown** 1 year, 4 months ago

Agree but explanation for #2 is incorrect they are both (VM1 and VM2) in subnet 1 so they are effected by NSG1 attached to subnet 1.
upvoted 9 times

🗨️ **Prutser2** 1 year, 3 months ago

correct intra subnet traffic can be effected by an NSG associated with that subnet as per:
ntra-Subnet traffic

It's important to note that security rules in an NSG associated to a subnet can affect connectivity between VMs within it. By default, virtual machines in the same subnet can communicate based on a default NSG rule allowing intra-subnet traffic. If a rule is added to *NSG1 that denies all inbound and outbound traffic, VM1 and VM2 will no longer be able to communicate with each other.

<https://learn.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works#intra-subnet-traffic> so NNY

upvoted 15 times

🗨️ **AWSAZO** 1 year, 1 month ago

N,N,Y Agree, and I tested it in the LAB using ICMP
upvoted 4 times

🗨️ **EdinaldoJunior1981** 1 year, 1 month ago

N,N,Y correct
upvoted 1 times

🗨️ **charlesr1700** Highly Voted 1 year, 4 months ago

N, inbound rule on subnet one will deny
Y, Communication within the same subnet does not go through an NSG, so nothing blocking
Y, Standard rules do not block vNet to vNet communication unless explicit.
upvoted 25 times

🗨️ **davidkerr7** 1 year, 4 months ago

2) is wrong
"It's important to note that security rules in an NSG associated to a subnet can affect connectivity between VM's within it."
upvoted 9 times

🗨️ **sapien45** 1 year, 3 months ago

<For inbound traffic, Azure processes the rules in a network security group associated to a subnet first, if there's one, and then the rules in a network security group associated to the network interface, if there's one.">

That means NNY,

I recommend you pass AZ-900 Microsoft Azure Fundamentals Certification .

AZ700 is not for you homie.

upvoted 7 times

🗨️ **daemon101** 6 months, 1 week ago

Maybe you are not a modern sapien but a neanderthal due to your behavior. You don't need to mention whether the NSG is bound the interface. Even the NSG is bound to subnet-level, the hosts under the subnet will be impacted by the nsg rules.

<https://learn.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works#intra-subnet-traffic>

upvoted 3 times

🗨️ **WMG** 9 months, 1 week ago

Savage but true..
upvoted 1 times

🗨️ **Stevy_nash** 1 year ago

that was hard =)

upvoted 3 times

  **hogehegohoge** Most Recent 2 months, 3 weeks ago

3) NSG Default inbound rule include DenyAllInBound rule. So this answer is No.

upvoted 1 times

  **GBAU** 3 months ago

N,N,Y

Lab confirmed: Virtual Network 200 * Deny rule blocks both:

-VM1 to VM2

-VM3 to VM1

Remove that rule and connectivity is restored

Good to know, as I had thought the NSG applied to a SN only worked on the ingress and egress of the SN, but it also can work within the SN itself. Maybe I am remembering back to my AWS networking, or just imagining things.

I don't think anyone is disputing VM1->VM3 = Y

upvoted 2 times

  **Lazylinux** 4 months ago

NNY

* Inbound rule on subnet1 will deny

* Inbound rule on subnet2 will deny - remember the scope is the whole vNET

* No rule on VM3 and default rule allows for vNET communication without restrictions

upvoted 1 times

  **Billabongs** 6 months, 1 week ago

NNY

"If you add a rule to NSG1 that denies all inbound and outbound traffic, VM1 and VM2 won't be able to communicate with each other."

<https://learn.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works#intra-subnet-traffic>

upvoted 1 times


  **UR** 6 months, 3 weeks ago

NNY

Ref for #2:

<https://learn.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works#intra-subnet-traffic>

upvoted 1 times

  **Rivaillexd07** 6 months, 3 weeks ago

I think the best answer is N,N,N

the first two are already very clear, about the last one, it is said that the NSG2 has default rules, nothing is said about port 9090 released, so, based on this, access would be denied. Anyone else agree?

upvoted 2 times

  **Rivaillexd07** 6 months, 3 weeks ago

I'm sorry guys I read again the question is the right answer is N,N and Y communication between subnets is released by default, NSG2 is using default rules.

upvoted 1 times

  **ABIYGK** 8 months ago

1. N — VM3 is trying to access VM1 through port 8080 and port 8080 not in allowed port list of NSG1

2. N — VM1 and VM2 tryin to talk with each other. Even though the are on the same subnet the NSG1 deny rule will include port 9090

3. Y — VM1 and VM3 can have connection NSG1 will not affect any outbound connection.

NSG 1 is applied inbound and which means it affect connections that comes Subnet 1 only. The only allowed port is http (80) and https (443) and the rest is blocked. Any connection going out side of Subnet 1 is allowed. VM1 and VM2 will be affected by NSG1 because they are under Subnet1. NG2 will not affect anything because only default rules are configured.

upvoted 1 times

  **ABIYGK** 8 months ago

The answer should be

N

N

Y

upvoted 1 times

  **MrBlueSky** 9 months, 2 weeks ago

I re-created this in a lab and can confirm that the VMs could not communicate with one another even though they are in the same subnet. As others have discussed and provided the link for... NSGs are still used for intra-subnet communication.

Answer is NNY

upvoted 1 times

  **faem** 9 months, 3 weeks ago

I would go with N,N,Y as described,"By default, virtual machines in the same subnet can communicate based on a default NSG rule allowing intra-subnet traffic. If a rule is added to *NSG1 that denies all inbound and outbound traffic, VM1 and VM2 will no longer be able to communicate with

each other." With NSG1 having custom rules, intra-communication is defined by the rules.

upvoted 1 times

🗨️ 👤 **Apptech** 10 months ago

should be NYN

1. Inbound rule on subnet1 will deny

2. By default, virtual machines in the same subnet can communicate based on a default NSG rule allowing intra-subnet traffic.

(<https://learn.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works#intra-subnet-traffic>)

3. VM3 has default rule as the text states. DenyAllInbound is the default vor NSG. See here: <https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview>

upvoted 1 times

🗨️ 👤 **Libaax01** 10 months, 2 weeks ago

VM3, which is part of Subnet 2, can not connect to port 8080 on VM1, because we have inbound rule that denies all ports accept port 80 and 443. so, the answer is No!

VM1 and VM2 are on the same subnet and by default inbound rules within a virtual network are allowed, however we NSG with a lower priority(200) over riding the default allowed rule which is priority 65000. So the Answer is NO!

VM1 is on Subnet 1 and VM3 is on Subnet 2, and outbound communication by default between subnets in the same virtual network is allowed and the question states NSG2 has only the default rules configured. so the answer is YES!

N

N

Y

upvoted 3 times

🗨️ 👤 **samir111** 11 months, 2 weeks ago

It should be N,N, Y

upvoted 2 times

🗨️ 👤 **TJ001** 1 year ago

N,N,Y NSG1 is incomplete there is no reference to Destination...(assumed it is Subnet1)

upvoted 1 times

🗨️ 👤 **Goofer** 1 year ago

<https://www.youtube.com/watch?v=flCoRc1uv9o>

upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

You have the Azure virtual networks shown in the following table.

Name	Resource group	Location
Vnet1	RG1	East US
Vnet2	RG1	UK West
Vnet3	RG1	East US
Vnet4	RG1	UK West

You have the Azure resources shown in the following table.

Name	Type	Virtual network	Resource group	Location
VM1	Virtual machine	Vnet1	RG1	East US
VM2	Virtual machine	Vnet2	RG2	UK West
VM3	Virtual machine	Vnet3	RG3	East US
App1	App Service	Vnet1	RG4	East US
St1	Storage account	Not applicable	RG5	UK West

You need to check latency between the resources by using connection monitors in Azure Network Watcher.

What is the minimum number of connection monitors that you must create?

- A. 1
- B. 2
- C. 3
- D. 4
- E. 5

Correct Answer: C

In the Region UK West region we have one single virtual machine VM2.

There is not anything to monitor here.

In the Region East US region we have two virtual machines VM1 & VM3, and App1.

We can monitor the connections: VM1-VM3, VM1-App1, VM3-App1.

Note: Connection Monitor includes the following entities:

Connection monitor resource: A region-specific Azure resource. All the following entities are properties of a connection monitor resource.

Endpoint: A source or destination that participates in connectivity checks. Examples of endpoints include Azure VMs, on-premises agents, URLs, and IP addresses.

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/connection-monitor-overview>

Community vote distribution

B (62%) C (26%) 9%

 **zenithcsa1** Highly Voted 1 year, 4 months ago

Tested

Source : must be in the same region / VM or VMSS

Target : region doesn't matter / VM, URL, etc.

ConnecitonMonitor1 : VM1, VM3 --> other resources

ConnecitonMonitor2 : VM2 --> other resources

upvoted 5 times

 **daemon101** 6 months, 2 weeks ago

Source and destination (endpoints) can be Vnet and Subnet as well and they're also Azure Resources as well. However, it seems this question refers to only VMs, App Service, and SA when it says resources. Furthermore, I think you forgot to consider the connection monitor between VM1 and VM3.

<https://learn.microsoft.com/en-us/azure/network-watcher/connection-monitor-create-using-portal#before-you-begin>

upvoted 1 times

 **zenithcsa1** 1 year, 4 months ago

I mean 'B'

upvoted 10 times

 **GohanF2** Highly Voted 1 year, 2 months ago

Answer is B.

The Connection Monitor is established per region.

And depending on the region we can connect multiple VMS, VMSS, endpoints and on-premises devices. Since, we have two regions only, we will need to Connection Monitors.

upvoted 5 times

 **Murad01** Most Recent 1 month, 3 weeks ago

Appeared on Exam November -2023

upvoted 2 times

 **Lazylinux** 4 months ago

Selected Answer: B

B Is Honey..

As per MS guidelines

*Region: Select a region for your connection monitor. You can select only the source VMs that are created in this region. Here you see only VMs or Virtual Machine Scale Sets that are bound to the region that you specified when you created the connection monitor. By default, VMs and Virtual Machine Scale Sets are grouped into the subscription that they belong to

* Destination can be anywhere as per this Destinations: You can monitor connectivity to an Azure VM, an on-premises machine, or any endpoint (a public IP, URL, or FQDN) by specifying it as a destination. In a single test group, you can add Azure VMs, on-premises machines, Office 365 URLs, Dynamics 365 URLs, and custom endpoints.

<https://learn.microsoft.com/en-us/azure/network-watcher/connection-monitor-create-using-portal>

upvoted 3 times

 **mabalon** 5 months, 1 week ago

Selected Answer: B

2 in my opinion.

At least two because we have two regions and the as the documentation says "You can select only the source VMs that are created in this region" - we need to measure from East US where is located VM1, VM3 and from UK West where is VM2.

Not more than two because in each one we can play with groups of sources and destinations.

- Connection Monitor 1 from UK West

--- Source VM2

--- Destinations App1 and ST1


- Conection Monitor 2 from East US

--- Source Groups VM1, VM3

--- Destinations App1 and ST1

<https://learn.microsoft.com/en-us/azure/network-watcher/connection-monitor-overview#create-a-connection-monitor-1>

upvoted 1 times

 **mabalon** 4 months, 4 weeks ago

correct link <https://learn.microsoft.com/en-us/azure/network-watcher/connection-monitor-create-using-portal>

upvoted 1 times

 **wooyourdaddy** 10 months ago

Selected Answer: B

At this link:

<https://learn.microsoft.com/en-us/azure/network-watcher/connection-monitor-create-using-portal#create-test-groups-in-a-connection-monitor>

It states as part of the test group creation process:

To choose Azure agents, select the Azure endpoints tab. Here you see only VMs or Virtual Machine Scale Sets that are bound to the region that you specified when you created the connection monitor.

This confirms that you would need 1 connection monitor per region. So the correct answer is B.

upvoted 2 times

 **samir111** 11 months, 1 week ago

Selected Answer: B

Correct: B

upvoted 1 times

 **JennyHuang36** 11 months, 1 week ago

In exam Feb, 2023

upvoted 2 times

 **energie** 11 months, 3 weeks ago

Selected Answer: C

Connection monitor is regional resource but destination VM can be in any region.

upvoted 2 times

aaa112 6 months, 2 weeks ago

Then why C is selected? There are two regions, so must be 2 connection monitors therefore B.
upvoted 1 times

Thanveer 12 months ago

Selected Answer: B

Connection monitor resource is a region-specific Azure resource
upvoted 2 times

caliph_noman 1 year ago

Selected Answer: A

correct
upvoted 1 times

TJ001 1 year ago

will go with B... per region 1 monitor but can add multiple sources and destinations
upvoted 3 times

Nicolas_UY 1 year, 1 month ago

Selected Answer: C

my previous answer was wrong, sorry for the confusion:

In the UK West region, there is only a single virtual machine (VM2). You do not need to create a connection monitor for this resource, as there are no other resources in the region to connect to.

In the East US region, there are two virtual machines (VM1 and VM3) and an App Service (App1). To check the latency between these resources, you would need to create the following connection monitors:

VM1 and VM3: This connection monitor would test the latency between VM1 and VM3 in the East US region.

VM1 and App1: This connection monitor would test the latency between VM1 and App1 in the East US region.

VM3 and App1: This connection monitor would test the latency between VM3 and App1 in the East US region.

Overall, you would need to create a total of three connection monitors to check the latency between all of the resources in the East US region.

upvoted 4 times

Nicolas_UY 1 year, 1 month ago

Selected Answer: D

To check the latency between the resources in the table you provided, you would need to create a minimum of four connection monitors. The correct answer is therefore D.

A connection monitor in Azure Network Watcher is a tool that allows you to continuously test connectivity between two resources. It sends a series of packets to a specified destination at a specified interval, and measures the round-trip time (RTT) of the packets.

In this case, you would need to create at least one connection monitor for each pair of resources that you want to monitor. For example:

VM1 and App1 (located in the same resource group and VNet)

VM2 and St1 (located in different resource groups and VNets)

VM3 and VM1 (located in the same region, but with different resource groups and VNets)

This would require a minimum of four connection monitors to cover all of the resources in the table.

upvoted 1 times

Syldana 1 year, 3 months ago

Selected Answer: B

B is correct
upvoted 2 times

Prutser2 1 year, 3 months ago

Selected Answer: B

each connection monitor can have multiple sources and destinations, but can only be set up in 1 region, because question provides 2 regions, we need 2 separate connection monitors, so B

upvoted 3 times

sapien45 1 year, 3 months ago

Selected Answer: B

Takes a few seconds to try to create a connection monitor in the portal :

Connection Monitor enables you to monitor connectivity in your Azure and hybrid network. Select your preferred subscription and REGION from which monitoring will be performed.

upvoted 1 times

You have an Azure subscription that contains a user named Admin1 and a resource group named RG1.

RG1 contains an Azure Network Watcher instance named NW1.

You need to ensure that Admin1 can place a lock on NW1. The solution must use the principle of least privilege.

Which role should you assign to Admin1?

- A. User Access Administrator
- B. Resource Policy Contributor
- C. Network Contributor
- D. Monitoring Contributor

Correct Answer: A

Community vote distribution

A (71%)

C (29%)

 **chatlisi** Highly Voted 1 year ago

It seems the provided answer to be correct:

"To create or delete management locks, you need access to Microsoft.Authorization/* or Microsoft.Authorization/locks/* actions. Only the Owner and the User Access Administrator built-in roles can create and delete management locks."

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json#who-can-create-or-delete-locks>

* The question is about placing a lock, not about using Network Watcher

upvoted 9 times

 **Aunehwet79** 1 year ago

Yes I have to agree. The Network watcher comment throws us but only owner and user Access Admin can create locks

upvoted 3 times

 **omgMerrick** Highly Voted 11 months, 1 week ago

Selected Answer: A

Well, after reviewing more, I think I was premature in saying the answer was 100% C. I was 100% wrong!! The correct answer is absolutely, 100% A. User Access Administrator

The key to the questions is that we're being asked what permissions are required to place a __lock__ (resource lock) on the Network Watcher resource. To create or delete management locks, you need access to Microsoft.Authorization/* or Microsoft.Authorization/locks/* actions. Only the Owner and the User Access Administrator built-in roles can create and delete management locks. You can create a custom role with the required permissions.

Source:

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json#who-can-create-or-delete-locks>

upvoted 5 times

 **SaadKhamis** Most Recent 9 months ago

Selected Answer: A

Who can create or delete locks

To create or delete management locks, you need access to Microsoft.Authorization/* or Microsoft.Authorization/locks/* actions. Only the Owner and the User Access Administrator built-in roles can create and delete management locks. You can create a custom role with the required permissions.

Network Contributor

Microsoft.Authorization/*/read Read roles and role assignments

upvoted 1 times

 **MrBlueSky** 9 months, 2 weeks ago

This question really has nothing to do with Network Watcher or Azure Networking.

What they want you to know is that you need the User Access Administrator role in order to make changes to create/delete management locks to ANY resource, not just Network Watcher.

I doubt this question would be on the test

upvoted 1 times

 **raj_evergreen** 10 months, 3 weeks ago

A is the correct answer. Network Contributor cannot add lock

upvoted 1 times

🗨️ **Vanja10** 11 months, 1 week ago

Tested. User Access Administrator is right answer.

upvoted 3 times

🗨️ **omgMerrick** 11 months, 1 week ago

Selected Answer: C

The correct answer is 100% C. Network Contributor

To use Network Watcher capabilities, the account you log into Azure with, must be assigned to the Owner, Contributor, or Network contributor built-in roles, or assigned to a custom role that is assigned the actions listed for each Network Watcher capability in the sections that follow.

Source:

<https://learn.microsoft.com/en-us/azure/network-watcher/required-rbac-permissions>

upvoted 1 times

🗨️ **harshit101** 11 months, 1 week ago

Selected Answer: A

A is right answer

upvoted 1 times

🗨️ **samir111** 11 months, 2 weeks ago

Selected Answer: C

C. Network Contributor

upvoted 1 times

🗨️ **samir111** 11 months, 2 weeks ago

Assigning the "User Access Administrator" role to Admin1 would allow them to manage access to all resources in the Azure subscription, including managing role assignments for all users, groups, and service principals. This would be excessive and not in line with the principle of least privilege since Admin1 only needs to be able to place a lock on the Azure Network Watcher instance named NW1.

Assigning the "User Access Administrator" role to Admin1 would provide them with more permissions than necessary and could potentially lead to accidental or intentional misuse of the additional privileges. Therefore, it is not recommended to assign the "User Access Administrator" role to Admin1 for placing a lock on NW1. The "Network Contributor" role would be more appropriate in this scenario.

C. Network Contributor

upvoted 1 times

🗨️ **TJ001** 1 year ago

agree with Answer A

upvoted 1 times

🗨️ **Th3Nk** 1 year ago

Selected Answer: A

Who can create or delete locks:

To create or delete management locks, you need access to Microsoft.Authorization/* or Microsoft.Authorization/locks/* actions. Only the Owner and the User Access Administrator built-in roles can create and delete management locks. You can create a custom role with the required permissions.

Answer: A

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json>

upvoted 3 times

🗨️ **Akodo_Shado** 1 year ago

Selected Answer: C

"To use Network Watcher capabilities, the account you log into Azure with, must be assigned to the Owner, Contributor, or Network contributor built-in roles"

<https://learn.microsoft.com/en-us/azure/network-watcher/required-rbac-permissions>

upvoted 2 times

You have a network security group named NSG1.

You need to enable network security group (NS) flow logs for NSG1. The solution must support retention policies.

What should you create first?

- A. A standard general-purpose v2 Azure Storage account
- B. An Azure Log Analytics workspace
- C. A standard general-purpose v1 Azure Storage account
- D. A premium Block blobs Azure Storage account

Correct Answer: A

Community vote distribution

A (78%)

B (22%)

 **SJHCI** 1 week ago

Selected Answer: A

A for sure.

<https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-overview#how-nsg-flow-logs-work>
"Retention is available only if you use general-purpose v2 storage accounts."

upvoted 1 times

 **ahos** 3 months ago

Selected Answer: A

A for sure!

upvoted 1 times

 **Lazylinux** 4 months ago

Selected Answer: A

Given answer is correct

<https://learn.microsoft.com/en-us/azure/network-watcher/nsg-flow-logging>

upvoted 2 times

 **mabalon** 4 months, 4 weeks ago

Selected Answer: A

Check the note on this link "Retention is available only if you use general-purpose v2 storage accounts."

<https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-overview#how-nsg-flow-logs-work>

upvoted 1 times

 **omgMerrick** 11 months, 1 week ago

Selected Answer: A

A. Standard general-purpose v2 storage account

Read my correction and source:

<https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-portal#enable-nsg-flow-log>

upvoted 3 times

 **omgMerrick** 11 months, 1 week ago

Selected Answer: B

B. An Azure Log Analytics workspace.

To enable network security group (NSG) flow logs for NSG1, you need to create an Azure Log Analytics workspace first. The flow logs can then be sent to the workspace for analysis and monitoring.

After creating the Log Analytics workspace, you can then configure NSG flow logs to be sent to the workspace by specifying the Log Analytics workspace ID and key in the NSG flow log settings. You can also configure retention policies for the logs within the workspace.

upvoted 2 times

 **Lazylinux** 4 months ago

U totally wrong..see here

<https://learn.microsoft.com/en-us/azure/network-watcher/nsg-flow-logging>

upvoted 1 times

🗨️ 👤 **JohnnyChimpo** 9 months ago

If you attempt to enable on any NSG, it only presents the option for storage accounts
upvoted 2 times

🗨️ 👤 **omgMerrick** 11 months, 1 week ago

After further study, I'm changing my answer to A. the standard general-purpose v2 storage account.

It very clearly states that NSG flow logs require a storage account as that is where the log data is actually written. The tutorial on the source link below even states that you should create a standard storage account.

Source:

<https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-portal#enable-nsg-flow-log>

upvoted 2 times

🗨️ 👤 **samir111** 11 months, 2 weeks ago

Selected Answer: B

The correct answer is B
upvoted 1 times

🗨️ 👤 **alkorkin** 1 year ago

Retention is available only if you use General purpose v2 Storage accounts (GPv2).

upvoted 1 times

🗨️ 👤 **TJ001** 1 year ago

Agree with Answer A

upvoted 1 times

🗨️ 👤 **alfonzo47** 1 year ago

Selected Answer: A

The answer is correct as stated right here in documentation: [https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-overview#:~:text=Retention%20is%20available%20only%20if%20you%20use%20General%20purpose%20v2%20Storage%20accounts%20\(GPv2\).](https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-overview#:~:text=Retention%20is%20available%20only%20if%20you%20use%20General%20purpose%20v2%20Storage%20accounts%20(GPv2).)

upvoted 4 times

🗨️ 👤 **Yassine145** 1 year ago

Selected Answer: B

The correct answer is B. An Azure Log Analytics workspace

To enable NS flow logs for NSG1 and support retention policies, you must first create an Azure Log Analytics workspace. Once created, you can configure the NSG1 to send flow logs to the Log Analytics workspace, then you can use the Log Analytics workspace to view and analyze the flow logs data and also set retention policies for the data.

upvoted 1 times

🗨️ 👤 **Lazylinux** 4 months ago

Totally wrong..retention has nothing to do with it as matter of fact it is there when you create NSG FLOW LOGS you will be prompted to put in the retention days..see here

<https://learn.microsoft.com/en-us/azure/network-watcher/nsg-flow-logging>

upvoted 1 times

🗨️ 👤 **TJ001** 1 year ago

No wrong ...when enabling NSG flow log it asks for what storage account and what retention is needed (0 means forever or provide the required no of days upto 365).. Log Analytics workspace is only needed if Traffic Analytics solution needs to be enabled.

upvoted 2 times

🗨️ 👤 **Akodo_Shado** 1 year ago

Selected Answer: A

"Network security group (NSG) flow logs is a feature of Azure Network Watcher that allows you to log information about IP traffic flowing through an NSG. Flow data is sent to Azure Storage accounts from where you can access it as well as export it to any visualization tool, SIEM, or IDS of your choice."

<https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-overview>

upvoted 2 times

You have an Azure subscription that contains the following resources:

- A virtual network named Vnet1
- Two subnets named subnet1 and AzureFirewallSubnet
- A public Azure Firewall named FW1
- A route table named RT1 that is associated to Subnet1
- A rule routing of 0.0.0.0/0 to FW1 in RT1

After deploying 10 servers that run Windows Server to Subnet1, you discover that none of the virtual machines were activated.

You need to ensure that the virtual machines can be activated.

What should you do?

- A. On FW1, create an outbound network rule that allows traffic to the Azure Key Management Service (KMS).
- B. On FW1, create an outbound service tag rule for Azure Cloud.
- C. Deploy a NAT gateway.
- D. Deploy an application security group that allows outbound traffic to 1688.

Correct Answer: A

 **voldemort123** 3 months, 3 weeks ago

i wanna forget this answer :(
upvoted 3 times

 **5aecc64** 2 months, 3 weeks ago

Why Voldemort123?
upvoted 1 times

 **jorgesoma** 2 months, 3 weeks ago

because this question is repeated around 10 times... Please, admin check it. People pay for contributor to get good Q&A
upvoted 3 times

You have an Azure subscription that contains a virtual network named Vnet1. Vnet1 contains a virtual machine named VM1 and an Azure firewall named FW1.

You have an Azure Firewall Policy named FP1 that is associated to FW1.

You need to ensure that RDP requests to the public IP address of FW1 route to VM1.

What should you configure on FP1?

- A. a network rule
- B. URL filtering
- C. a DNAT rule
- D. an application rule

Correct Answer: C

Community vote distribution

C (100%)

 **omgMerrick** Highly Voted 11 months, 1 week ago

Selected Answer: C

C. a DNAT rule

To allow RDP requests to reach VM1 through the public IP of FW1, you need to create a rule that translates the destination IP address of the incoming RDP requests to the private IP address of VM1. This is done through a type of rule called a DNAT rule, which is configured on the Azure Firewall Policy (FP1). Other types of rules, such as network rules, URL filtering, and application rules, are not relevant to this specific scenario.
upvoted 7 times

 **omgMerrick** 11 months, 1 week ago

Source:

<https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-dnat-policy>

upvoted 2 times

 **Lazylinux** Most Recent 4 months ago

Selected Answer: C

I C is correct

DNAT

* External initiated

* Destination IP changed

* destination TCP/UDP

* Scenario = Change Public IP (Firewall IP) to internal - Private IP when packets are coming into local network through firewall

* Order = Before the routing decision outside to inside

* Example = users on the internet accessing Web Server in data Center

upvoted 1 times

 **mVic** 11 months ago

Selected Answer: C

DNAT rule

<https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-dnat-policy>

upvoted 1 times

HOTSPOT

-

You have an Azure application gateway named AppGw1.

You need to create a rewrite rule for AppGw1. The solution must rewrite the URL of requests from `https://www.contoso.com/fashion/shirts` to `https://www.contoso.com/buy.aspx?category=fashion&product=shirts`.

How should you complete the rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

If server variable equals to the pattern `/(.+)/(.+)`

content_type
query_string
uri_path

Set to `buy.aspx` and `category={var_uri_path_1}&product={var_uri_path_2}`

Request Header (Common Header)
Response Header (Common Header)
URL (Both URL path and URL query string)

Correct Answer:

If server variable equals to the pattern `/(.+)/(.+)`

content_type
query_string
uri_path

Set to `buy.aspx` and `category={var_uri_path_1}&product={var_uri_path_2}`

Request Header (Common Header)
Response Header (Common Header)
URL (Both URL path and URL query string)

 **tzatziki** Highly Voted 11 months, 3 weeks ago

Correct... Hey.. New question it seems... Nice to see these are updated! Thank you!

<https://learn.microsoft.com/en-us/azure/application-gateway/rewrite-url-portal#configure-url-rewrite>
upvoted 19 times

 **Lazylinux** Most Recent 3 months, 4 weeks ago

Given answer is correct

More info here regarding both header-basic rule an URI path based rewrites
<https://learn.microsoft.com/en-us/azure/application-gateway/rewrite-http-headers-portal>

<https://learn.microsoft.com/en-us/azure/application-gateway/rewrite-url-portal>
upvoted 2 times

You have an Azure subscription that contains the following resources:

- A virtual network named Vnet1
- Two subnets named subnet1 and AzureFirewallSubnet
- A public Azure Firewall named FW1
- A route table named RT1 that is associated to Subnet1
- A rule routing of 0.0.0.0/0 to FW1 in RT1

After deploying 10 servers that run Windows Server to Subnet1, you discover that none of the virtual machines were activated.

You need to ensure that the virtual machines can be activated.

What should you do?

- A. On FW1, create an outbound network rule that allows traffic to the Azure Key Management Service (KMS).
- B. On FW1, create an outbound service tag rule for Azure Cloud.
- C. Deploy a NAT gateway.
- D. On FW1, configure a DNAT rule for port 1688.

Correct Answer: A

Community vote distribution

A (100%)

 **breakpoint0815** Highly Voted 10 months ago

Why this question/answer appears multiple times??
upvoted 7 times

 **WMG** 9 months, 1 week ago

On the exam it will appear at least 6 times, so better be ready!!
upvoted 7 times

 **meow10** 8 months, 1 week ago

Thats 6 easy points then, Yeeey !!
upvoted 2 times

 **ABIYGK** Highly Voted 8 months, 1 week ago

I think the admin of the page better to check the question and remove the reoccurrence.
upvoted 6 times

 **Lazylinux** Most Recent 3 months, 4 weeks ago

Selected Answer: A

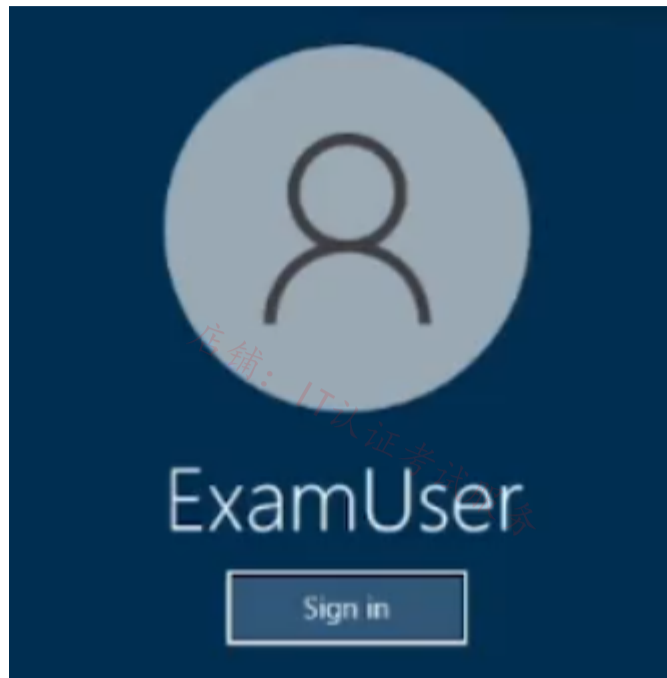
Given answer is correct
upvoted 1 times

 **voldemort123** 4 months ago

wtf, how many times repeated q?
upvoted 1 times

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You need to create an Azure Firewall instance named FW1 that meets the following requirements:

- Has an IP address from the address range of 10.1.255.0/24
- Uses a new Premium firewall policy named FW-policy1
- Routes traffic directly to the internet

To complete this task, sign in to the Azure portal.

Step 1: On the Azure portal menu or from the Home page, select Create a resource.

Step 2: Type firewall in the search box and press Enter.

Step 3: Select Firewall and then select Create.

Step 4: On the Create a Firewall page, use the following table to configure the firewall:

* Name - Enter FW1

* Firewall management - Select Use a Firewall Policy to manage this firewall.

* Firewall policy - Select Add new, and enter FW-policy1.

* Choose a virtual network - Select Create new

Step 4.1: Enter or select the appropriate values:

Subscription - Select your Azure subscription.

Resource group -

Name -

Region -

Correct Answer:

Step 4.2 Select Next: IP addresses.

Step 4.3 For IPv4 Address space, accept the default 10.0.0.0/16.

Step 4.4 Under Subnet, select default.

Subnet name -

For Address range, type 10.1.255.0/24

Step 4.5 Select Save.

Step 4.6 Select Review + create.

Step 4.7: Select Create.

Step 5: Back to the Create a Firewall page:

* Public IP address - Add new

Step 6: Accept the other default values, then select Review + create.

Step 7: Review the summary, and then select Create to create the firewall.

Reference:

<https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal-policy>

<https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal>

 **wooyourdaddy** Highly Voted 10 months, 2 weeks ago

I believe the requirement:

- Routes traffic directly to the internet

Is supposed to indicate that the FW should not use Forced Tunneling.

When you configure a new Azure Firewall, you can route all Internet-bound traffic to a designated next hop instead of going directly to the Internet. For example, you may have a default route advertised via BGP or using User Defined Route (UDR) to force traffic to an on-premises edge firewall or other network virtual appliance (NVA) to process network traffic before it's passed to the Internet.

Source: <https://learn.microsoft.com/en-us/azure/firewall/forced-tunneling>
upvoted 7 times

 **JohnnyChimpo** 8 months, 2 weeks ago

Does that mean that no further configuration is needed since all traffic will be router to the Internet by default?
upvoted 1 times

 **Lazylinux** Most Recent 3 months, 4 weeks ago

- * Create Firewall and ensure no Forced Tunneling enabled
 - * Create Route table and ensure 0.0.0.0/0 as Destination IP addresses/CIDR ranges and the NVA is the firewall Private IP (get it from overview page)
 - * Associate the Route table with subnet in which the FW will direct the traffic to internet on behalf of
- That is all required
upvoted 3 times

 **Aziza_Adam** 11 months, 1 week ago

- 1- create FW with policy (also create vnet using /16 and choose the provided range for the subnet.
- 2- Create Route table

3- Add routing rule that route 0.0.0.0/0 to NVA then give the private IP address of your firewall
upvoted 4 times

🗨️ **ABIYK** 7 months, 4 weeks ago

Route table needs to be associated. Defining a routing table will not do anything. This means routeable could only be associated to a Subnet not a Firewall.
upvoted 1 times

🗨️ **MrBlueSky** 9 months, 2 weeks ago

NVA \neq Azure Firewall

NVAs are frequently Firewalls that are hosted on Azure VMs. This is not the same thing as the actual product called 'Azure Firewall'
upvoted 1 times

🗨️ **tzatziki** 11 months, 3 weeks ago

*Routes traffic directly to the internet

So, in order to achieve this: I made a route pointing to my firewall IP (0.0.0.0 -> Virtual Appliance + IP) and an application rule allowing http / https in the firewall. ... Network rule made no difference as concerned my vm reaching its internet bound traffic.

Used this for reference:

<https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal-policy>

upvoted 4 times

🗨️ **Discussions22** 3 months ago

and what is the destination in app rule? and source 0.0.0.0/0 is not supported also

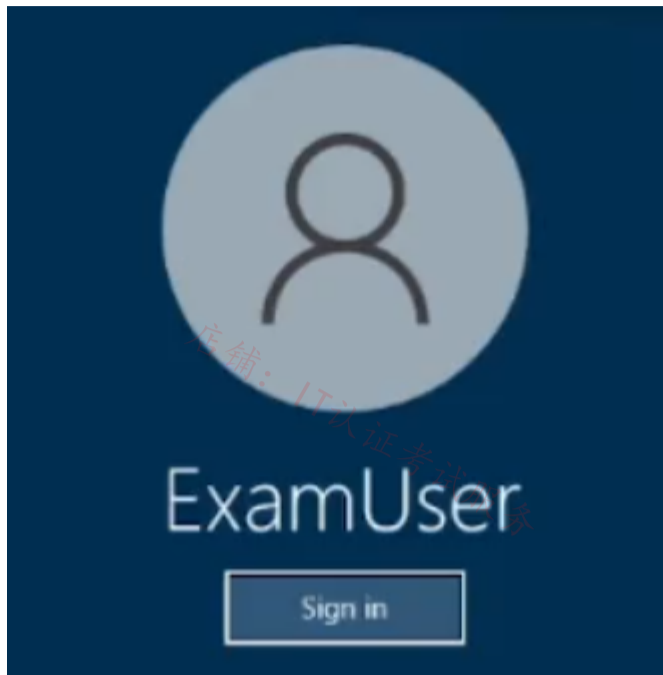
upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You plan to implement an Azure application gateway in the East US Azure region. The application gateway will have Web Application Firewall (WAF) enabled.

You need to create a policy that can be linked to the planned application gateway. The policy must block connections from IP addresses in the 131.107.150.0/24 range. You do NOT need to provision the application gateway to complete this task.

To complete this task, sign in to the Azure portal.

Web Application Firewall Policies contain all the WAF settings and configurations. This includes exclusions, custom rules, managed rules, and so on. These policies are then associated to an application gateway (global), a listener (per-site), or a path-based rule (per-URI) for them to take effect.

Part 1: Create a WAF policy
Create a basic WAF policy with a managed Default Rule Set (DRS) using the Azure portal.

Step 1: On the upper left side of the portal, select Create a resource. Search for WAF, select Web Application Firewall, then select Create.

Step 2: On Create a WAF policy page, Basics tab, enter or select the following information and accept the defaults for the remaining settings:

Policy for - Regional WAF (Application Gateway)

Subscription - Select your subscription name

Resource group - Select your resource group

Policy name - Type a unique name for your WAF policy.

Location: East US

Step 3: On the Association tab, select Add association, then select one of the following settings:

Setting - Value

Application Gateway- Select the application gateway, and then select Add.

HTTP Listener - Select the application gateway, select the listeners, then select Add.

Route Path - Select the application gateway, select the listener, select the routing rule, and then select Add.

Step 4: Select Review + create, then select Create.

Home > WAF policies > Create a WAF policy

Create a WAF policy

Basics Policy settings Managed rules Custom rules Association Tags Review + create

Malicious attacks such as SQL Injection, Cross Site Scripting (XSS), and other OWASP top 10 threats could cause service outage or data loss, and pose a big threat to web application owners. Web Application Firewall (WAF) protects your web applications from common web attacks, keeps your service available and helps you meet compliance requirements.
[Learn more about WAF policy for Front Door](#)
[Learn more about WAF policy for Application Gateway](#)

Project details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Policy for * ⓘ Regional WAF (Application Gateway) ▼

Subscription * ⓘ ANTman ▼

Resource group * ⓘ (New) myPolicy ▼
[Create new](#)

Instance details

Policy name * ⓘ Policy1 ✓

Location * ⓘ (US) West US 2 ▼

Policy state ⓘ Enabled Disabled

Part 2: Configure WAF rule

When you create a WAF policy, by default it is in Detection mode. In Detection mode, WAF doesn't block any requests. Instead, the matching WAF rules are logged in the WAF logs. To see WAF in action, you can change the mode settings to Prevention. In Prevention mode, matching rules defined in the CRS Ruleset you selected are blocked and/or logged in the WAF logs.

Custom rules

Correct Answer: Step 5: To create a custom rule, select Add custom rule under the Custom rules tab. This opens the custom rule configuration page.

Step 6: On the Add custom rule page, use the following test values to create a custom rule:

Setting - Value

Custom rule name - AnyName

Status - Enabled

Rule type- Match

Priority - 100

Match type- IP address

Match variable - SocketAddr (for example)

Operation - Does contain

IP address or range - 131.107.150.0/24

Then Deny traffic

Edit custom rule ×

A custom rule is made up of one or more conditions followed by an action. All custom rules for a WAF policy are match rules. [Learn more about custom rules](#)

Custom rule name *

Status Enabled Disabled

Rule type Match Rate limit

Priority *

Conditions

If 🗑️

Match type ▼

Match variable ▼

Operation
 Does contain Does not contain

IP address or range
 🗑️

+ Add new condition

Then ▼

Step 7: Select Add.

Step 8: Select Next: Association.

Step 9: Select Associate a WAF policy.

Step 10: For WAF policy, select your WAF policy.

Step 11: For Domain, select the domain.

Step 12. Select Add.

Step 13: Select Review + create.

Step 14: After your policy validation passes, select Create.

Reference:

<https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/create-waf-policy-ag>

<https://learn.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-configure-ip-restriction#configure-a-waf-policy-with-the-azure-portal>

GBAU 3 months ago

"You do NOT need to provision the application gateway to complete this task."

So in the exam, is the AP already created in the 'Lab'?

I guess it must be if we have to associate it, but not create it.

upvoted 1 times

Lazylinux 3 months, 4 weeks ago

Create NEW WAF policy

Ensure enabled

Rule Type = Match

condition

if

Match type = IP address

Operation = Does Contain = 131.107.150.0/24

Then => DENY
Click Add and you done
upvoted 2 times

 **Lazylinux** 3 months, 4 weeks ago

Forgot to say last step apply/link it to the application Gateway
upvoted 2 times

 **Billabongs** 6 months, 1 week ago

Create a WAF Custom Rule to block the ip address range.

"you can block all requests from an IP address in the range 192.168.5.0/24. In this rule, the operator is IPMatch, the matchValues is the IP address range (192.168.5.0/24), and the action is to block the traffic."

<https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/custom-waf-rules-overview>

upvoted 1 times

店铺: IT认证考试服务

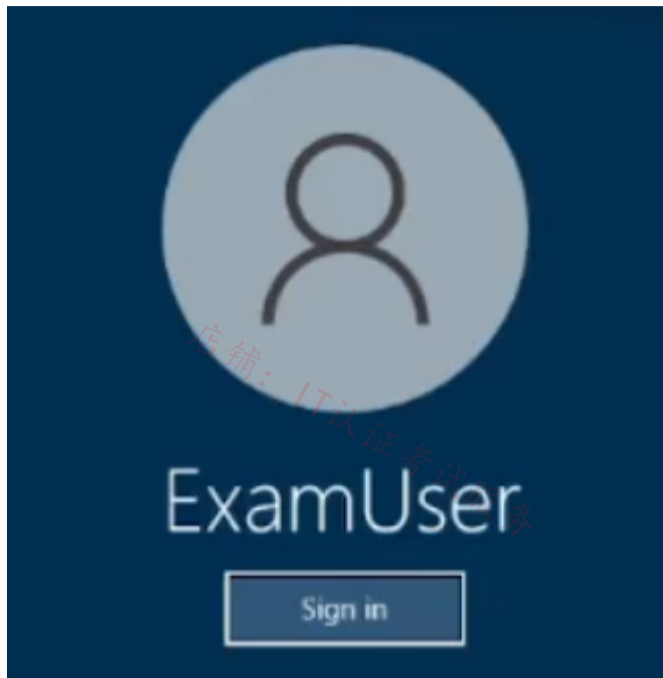
店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You need to configure VNET1 to log all events and metrics. The solution must ensure that you can query the events and metrics directly from the Azure portal by using KQL.

To complete this task, sign in to the Azure portal.

Plan

Stage 1: Determine the resource group of VNET1

Stage 2: In Azure Monitor set up monitoring with the VNET's Resource Group as source, and Log Analytics workspace as destination

Stage 1: Determine the resource group of VNET1

Step 1: In Azure portal locate VNET1 and detect which resource group it is in (here we use XGroup).

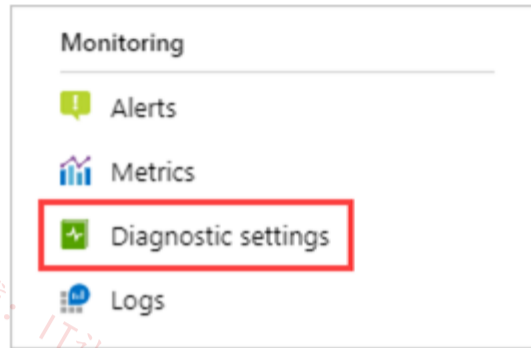
Stage 2: In Azure Monitor set up monitoring with the VNET's Resource Group as source, and Log Analytics workspace as destination

Create diagnostic settings

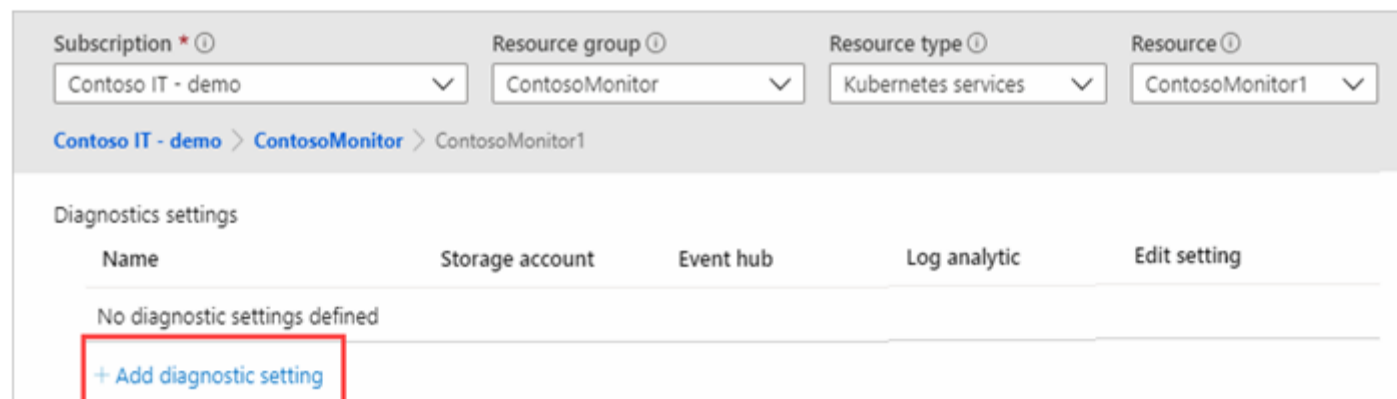
Step 2: You can configure diagnostic settings in the Azure portal either from the Azure Monitor menu or from the menu for the resource (XGroup in our case).

Where you configure diagnostic settings in the Azure portal depends on the resource:

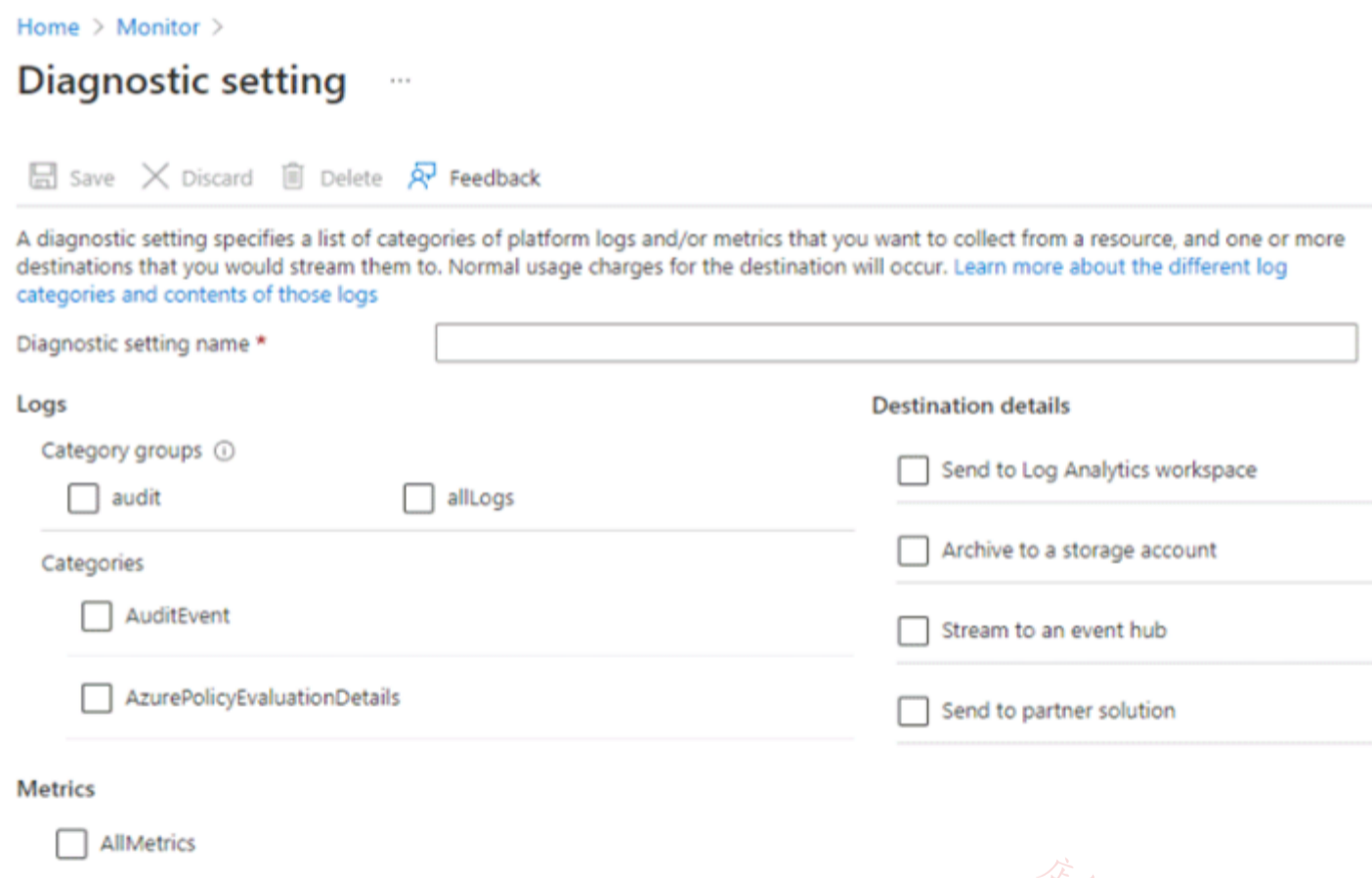
For a single resource, select Diagnostic settings under Monitoring on the resource's menu.



Step 3: If no settings exist on the resource you've selected, you're prompted to create a setting. Select Add diagnostic setting.



Step 4: Give your setting a name if it doesn't already have one.



Correct Answer:

Step 5: Logs and metrics to route: For logs, either choose a category group or select the individual checkboxes for each category of data you want to send to the destinations specified later. The list of categories varies for each Azure service. Select AllMetrics if you want to store metrics in Azure Monitor Logs too.

We do the following:

Categories: Select AuditEvent

Metrics: Select AllMetrics
(to log all events and metrics)

Destination details: Select Send to Log Analytics workspace
(To be able to query using KQL)



A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name *

Logs

Category groups ⓘ

audit allLogs

Categories

AuditEvent

AzurePolicyEvaluationDetails

Destination details

Send to Log Analytics workspace

Archive to a storage account

Stream to an event hub

Send to partner solution

Metrics

AllMetrics

店铺: IT认证考试服务

Step 6: Destination details -skip

Step 7: Select Save.

Note: Azure virtual network collects the same kinds of monitoring data as other Azure resources.

Azure virtual network uses Azure Monitor.

Collection and routing

Platform metrics and the Activity log are collected and stored automatically, but can be routed to other locations by using a diagnostic setting.

Each Azure resource requires its own diagnostic setting, which defines the following criteria:

Sources: The type of metric and log data to send to the destinations defined in the setting. The available types vary by resource type.

Destinations: One or more destinations to send to.

Destinations

Platform logs and metrics can be sent to the destinations listed in the following table.

* Log Analytics workspace

Metrics are converted to log form. This option might not be available for all resource types. Sending them to the Azure Monitor Logs store (which is searchable via Log Analytics) helps you to integrate them into queries, alerts, and visualizations with existing log data.

* Etc.

Reference:

<https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/diagnostic-settings>

<https://learn.microsoft.com/en-us/azure/virtual-network/monitor-virtual-network>

Bbb78 Highly Voted 11 months, 3 weeks ago

This is not clearly explained. The solution would be from the VNET diagnostic settings and send to the Log Analytics workspace from there
upvoted 13 times

JohnnyChimpo Highly Voted 8 months, 1 week ago

The solution shows "Azure Monitor" and it is incorrect. Other resources can be enabled for diagnostic settings in here, however vnets do not appear there for some reason. To configure vnet logging, do so directly from the "diagnostic settings" blade in the vnet itself.
upvoted 6 times

Lazylinux Most Recent 3 months, 4 weeks ago

vNet diagnostic Settings from there you have
* 4 options to send data to - Log analytics workspace or Archive to storage acc or Stream to event hub or send to partner solutions
* tick all logs and Metrics
save and you are done
upvoted 3 times

You have an Azure subscription that contains a virtual network named Vnet1. Vnet1 contains 20 subnets and 500 virtual machines. Each subnet contains a virtual machine that runs network monitoring software.

You have a network security group (NSG) named NSG1 associated to each subnet.

When a new subnet is created in Vnet1 an automated process creates an additional network monitoring virtual machine in the subnet and links the subnet to NSG1.

You need to create an inbound security rule in NSG1 that will allow connections to the network monitoring virtual machines from an IP address of 131.107.1.15. The solution must meet the following requirements:

- Ensure that only the monitoring virtual machines receive a connection from 131.107.1.15.
- Minimize changes to NSG1 when a new subnet is created.

What should you use as the destination in the inbound security rule?

- A. an application security group
- B. a service tag
- C. a virtual network
- D. an IP address

Correct Answer: A

Community vote distribution

A (100%)

  **ckyp** Highly Voted 9 months, 2 weeks ago

Seems to be the right answer. Create an ASG and assign to each monitoring vm. Then in the NSG1, create an allow rule to allow the IP 131.107.1.15 to the ASG.


<https://learn.microsoft.com/en-us/azure/virtual-network/application-security-groups>

upvoted 6 times

  **JackeD** Most Recent 2 months, 2 weeks ago

I dont understand the benefit of an ASG over an ip. An ASG can only be associated to machines within a single subnet and there is only 1 monitoring machine per subnet. Can anyone clarify?

upvoted 1 times

  **JackeD** 2 months, 2 weeks ago

nevermind, ASG cannot be assigned between Vnets but can be between subnets. ASG is the clear answer

upvoted 1 times

  **Lazylinux** 3 months, 4 weeks ago

Selected Answer: A

Given answer is correct - ASG

upvoted 2 times

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

Name	Type	Description
VNet1	Virtual network	Contains a subnet named Subnet1
Subnet1	Virtual subnet	Part of VNet1
NSG1	Network security group (NSG)	Linked to Subnet1
ASG1	Application security group	Not linked

Subnet1 contains three virtual machines that host an app named App1. App1 is accessed by using the SFTP protocol.

From NSG1, you configure an inbound security rule named Rule2 that allows inbound SFTP connections to ASG1.

You need to ensure that the inbound SFTP connections are managed by using ASG1. The solution must minimize administrative effort.

What should you do?

- A. From NSG1, modify the priority of Rule2.
- B. From each virtual machine, associate the network interface to ASG1.
- C. From Subnet1, create a subnet delegation.
- D. From ASG1, modify the role assignments.

Correct Answer: B

Community vote distribution


B (100%)

 **Lazylinux** 3 months, 4 weeks ago

Selected Answer: B

B is Honey

upvoted 2 times

 **crypto700** 8 months, 2 weeks ago

Selected Answer: B

B is correct

upvoted 4 times

店铺: IT认证考试服务

店铺: IT认证考试服务

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

Name	Type	Description
FW1	Azure Firewall Premium	Has a network intrusion detection and prevention system (IDPS) enabled
HP1	Azure Virtual Desktop host pool	All outbound traffic from HP1 to the subscription's resources route through FW1
Server1	Virtual machine	Hosts an application named App1
KV1	Azure Key Vault	None

Users on HP1 connect to App1 by using a URL of <https://app1.contoso.com>.

You need to ensure that the IDPS on FW1 can identify security threats in the connections from HP1 to Server1.

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

NOTE: Each correct selection is worth one point.

- A. Enable TLS inspection for FW1.
- B. Import a server certificate to KV1.
- C. Enable threat intelligence for FW1.
- D. Add an application group to HP1.
- E. Add a secured virtual network to FW1.

Correct Answer: AB

Community vote distribution

AB (100%)

 **_fvt** Highly Voted 9 months, 3 weeks ago

Selected Answer: AB

Seems correct.

<https://learn.microsoft.com/en-us/azure/firewall/premium-certificates>

<https://learn.microsoft.com/en-us/azure/firewall/premium-features#tls-inspection>

upvoted 6 times

 **Lazylinux** Most Recent 3 months, 4 weeks ago

Selected Answer: AB

Given ans is correct

FW needs TLS inspection enable and for TLS inspection to work a cert uploaded to KV need be in place to decrypt encrypted traffic

upvoted 1 times

 **Rob_G** 9 months, 1 week ago

Selected Answer: AB

Correct A & B

The Firewall needs to be able to decrypt the traffic so the IDS can inspect the traffic. To do this TLS inspection needs to be enabled and a copy of the certificate needs to be stored.

upvoted 3 times

HOTSPOT

-

Case Study

-

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

-

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview

-

Contoso, Ltd. is a consulting company that has a main office in San Francisco and a branch office in Dallas.

Contoso recently purchased an Azure subscription and is performing its first pilot project in Azure.

Existing Environment

-

Azure Network Infrastructure

-

Contoso has an Azure Active Directory (Azure AD) tenant named contoso.com.

The Azure subscription contains the virtual networks shown in the following table.

Name	Resource group	IP address space	Location	Peered with
Vnet1	RG1	10.1.0.0/16	West US	Vnet2, Vnet3
Vnet2	RG1	172.16.0.0/16	Central US	Vnet1, Vnet3, Vnet4
Vnet3	RG2	192.168.0.0/16	Central US	Vnet1, Vnet2
Vnet4	RG2	10.10.0.0/16	West US	Vnet2
Vnet5	RG3	10.20.0.0/16	East US	None

Vnet1 contains a virtual network gateway named GW1.

Azure Virtual Machines

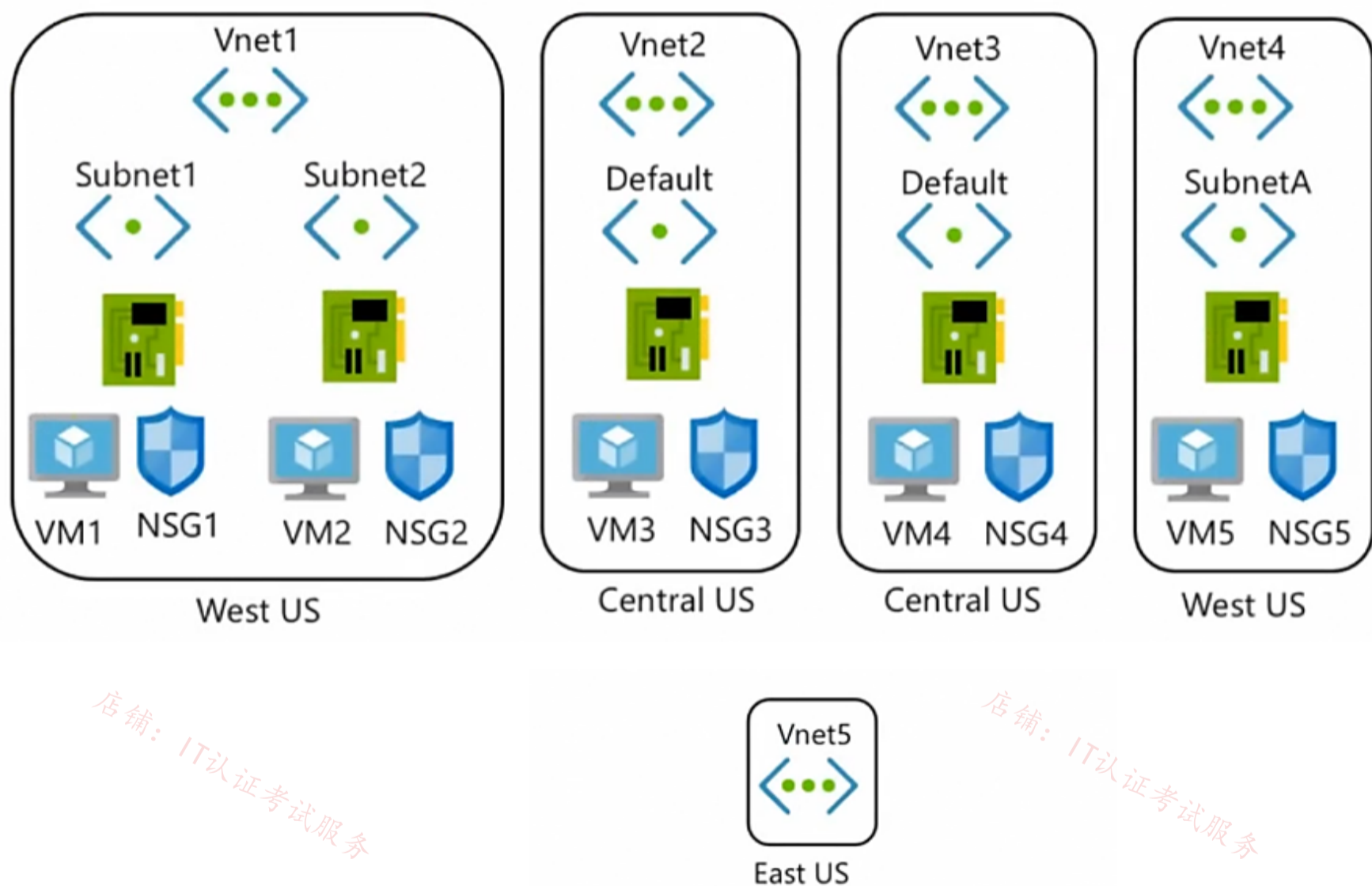
The Azure subscription contains virtual machines that run Windows Server 2019 as shown in the following table.

Name	Location	Connected to	Network security group (NSG)
VM1	West US	Vnet1/Subnet1	NSG1
VM2	West US	Vnet1/Subnet2	NSG2
VM3	Central US	Vnet2/Default	NSG3
VM4	Central US	Vnet3/Default	NSG4
VM5	West US	Vnet4/SubnetA	NSG5

The NSGs are associated to the network interfaces on the virtual machines. Each NSG has one custom security rule that allows RDP connections from the internet. The firewall on each virtual machine allows ICMP traffic.

An application security group named ASG1 is associated to the network interface of VM1.

Azure Network Infrastructure Diagram



Azure Private DNS Zones

The Azure subscription contains the Azure private DNS zones shown in the following table.

Name	Location
zone1.contoso.com	Central US
zone2.contoso.com	West US

Zone1.contoso.com has the virtual network links shown in the following table.

Name	Virtual Network	Auto registration
Link1	Vnet2	No
Link2	Vnet3	Yes

Other Azure Resources

-

The Azure subscription contains additional resources as shown in the following table.

Name	Type	Location
DB1	Azure SQL Database	West US
storage1	Azure Storage account	West US
Registry1	Azure Container Registry	Central US
KeyVault1	Azure Key Vault	Central US

Requirements

-

Virtual Network Requirements

-

Contoso has the following virtual network requirements:

- Create a virtual network named Vnet6 in West US that will contain the following resources and configurations:
 - o Two container groups that connect to Vnet6
 - o Three virtual machines that connect to Vnet6
 - o Allow VPN connections to be established to Vnet6
 - o Allow the resources in Vnet6 to access KeyVault1, DB1, and Vnet1 over the Microsoft backbone network.
- The virtual machines in Vnet4 and Vnet5 must be able to communicate over the Microsoft backbone network.
- A virtual machine named VM-Analyze will be deployed to Subnet1. VM-Analyze must inspect the outbound network traffic from Subnet2 to the internet.

Network Security Requirements

-

Contoso has the following network security requirements:

- Configure Azure Active Directory (Azure AD) authentication for Point-to-Site (P2S) VPN users.
- Enable NSG flow logs for NSG3 and NSG4.
- Create an NSG named NSG10 that will be associated to Vnet1/Subnet1 and will have the custom inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
500	3389	TCP	10.1.0.0/16	Any	Deny
1000	Any	ICMP	10.10.0.0/16	VirtualNetwork	Deny

- Create an NSG named NSG11 that will be associated to Vnet1/Subnet2 and will have the custom outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
200	3389	TCP	10.1.0.0/16	VirtualNetwork	Deny

You need to meet the network security requirements for the NSG flow logs.

Which type of resource do you need, and how many instances should you create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Resource type:

- An Azure Monitor workbook
- An Azure Monitor data collection rule
- A Log Analytics workspace
- An NSG
- A storage account

Minimum number of instances:

- 0
- 1
- 2
- 3
- 4

店铺: IT认证考试服务

店铺: IT认证考试服务

Answer Area

Resource type:

- An Azure Monitor workbook
- An Azure Monitor data collection rule
- A Log Analytics workspace
- An NSG
- A storage account**


Correct Answer:

Minimum number of instances:

- 0
- 1**
- 2
- 3
- 4

 **Murad01** 1 month, 3 weeks ago

Given answer is true
upvoted 1 times

 **bp_a_user** 3 months, 1 week ago

True: Storage Accounts allow NSG Flow Log retention
upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT

You have the Azure firewall shown in the following exhibit.

The screenshot displays the configuration for an Azure Firewall named 'Firewall1'. The 'Essentials' section includes the resource group 'RG1', location 'North Europe', subscription 'Visual Studio Premium with MSDN', subscription ID '169d1bb-ba4c-471c-b513-092eb7063265', virtual network 'Vnet1', firewall policy 'FirewallPolicy1', and provisioning state 'Succeeded'. The 'Properties' section shows the firewall SKU as 'Standard', subnet as 'AzureFirewallSubnet', public IP as 'Firewall1-IP1', private IP as '10.100.253.4', management subnet as '-', management public IP as '-', and private IP ranges as 'Managed by Firewall Policy'.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

On Firewall1, forced tunneling **[answer choice]**.

- is enabled already
- cannot be enabled
- is disabled but can be enabled

On Firewall1, management by Azure Firewall Management **[answer choice]**.

- is enabled already
- cannot be enabled
- is disabled but can be enabled

Answer Area

On Firewall1, forced tunneling [answer choice].

Correct Answer:

is enabled already
cannot be enabled
is disabled but can be enabled

On Firewall1, management by Azure Firewall Management [answer choice].

is enabled already
cannot be enabled
is disabled but can be enabled

GBAU 3 months ago

FW has No Management Subnet or Management public IP assigned/defined/created.

-Forced Tunneling requires Management Subnet & Management public IP and it can only be created when the FW is created, so "cannot be enabled".

-Azure Firewall Management is clearly disabled (as the Management SN & IP are not there), but you can add this later so "is disabled but can be enabled".

upvoted 1 times

Lazylinux 3 months, 2 weeks ago

First given ans is incorrect, if forced Tunnelling is NOT enabled and FW already deployed then you cannot enable it, you WILL have to delete existing FW and deploy new one with forced tunnelling enabled

Second ans is correct

upvoted 3 times

Discussions22 3 months, 1 week ago

Hi, thanks you for explanation, still what about second answer, why it is correct?

upvoted 1 times

ironbornson 4 months, 1 week ago

"To support this configuration, you must create Azure Firewall with Forced Tunnel configuration enabled. This is a mandatory requirement to avoid service disruption. If this is a pre-existing firewall, you must recreate the firewall in Forced Tunnel mode to support this configuration."

<https://learn.microsoft.com/en-us/azure/firewall/forced-tunneling>

Repeated question, it's wrong

upvoted 3 times

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT

You have an Azure subscription that contains 10 virtual machines. The virtual machines are assigned private IP addresses. The subscription contains the resources shown in the following table.

Name	Type	Description
FWPolicy1	Azure Firewall Premium policy	None
Firewall1	Azure firewall	Firewall1 is linked to FWPolicy1. All internet traffic is routed through Firewall1.
VNet1	Virtual network	The virtual machines are connected to VNet1.

You need to configure FWPolicy1 to meet the following requirements:

- Allow incoming connections to the virtual machines from the internet on port 4567.
- Block outbound connections from the virtual machines to an FQDN of *.fabrikam.com.

What should you configure in FWPolicy1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

To allow inbound connections:

- A DNAT rule
- A network rule
- An application rule
- SNAT private IP ranges

To block outbound connections:

- A DNAT rule
- A network rule
- An application rule
- SNAT private IP ranges
- The DNS settings

Answer Area

To allow inbound connections:

- A DNAT rule**
- A network rule
- An application rule
- SNAT private IP ranges

Correct Answer:

To block outbound connections:

- A DNAT rule
- A network rule
- An application rule**
- SNAT private IP ranges
- The DNS settings

VeryOldITGuy 1 week, 4 days ago

Shouldn't it be a DNAT since you need to nat the outside IP to the inside IP ?
upvoted 1 times

VeryOldITGuy 2 days, 2 hours ago

That is what I figure too.. otherwise the port would not know to which VM it needs to go. That is what my network firewall background tells me at least

upvoted 1 times

🗨️ 👤 **SJHCI** 1 month ago

You just need a network rule, no Dnat required.

1 - A network Rule "You can use a network rule when you want to filter traffic based on IP addresses, any ports, and any protocols."

2 - An application Rule "ou can use an application rule when you want to filter traffic based on fully qualified domain names (FQDNs), URLs, and HTTP/HTTPS protocols."

Link: <https://learn.microsoft.com/en-us/azure/firewall/policy-rule-sets#rule-types>

upvoted 1 times

🗨️ 👤 **Bobip** 1 month, 2 weeks ago

I think for the first we may just need a "network rule". It's because it needs to allow a specific port, It is not about port mapping that we need a DNAT rule.

upvoted 2 times

🗨️ 👤 **ServerBrain** 1 month, 1 week ago

Correct

upvoted 1 times

🗨️ 👤 **jorgesoma** 2 months, 3 weeks ago

Answer is correct

upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

DRAG DROP

-

You have an Azure subscription that contains an Azure VPN gateway named GW1. GW1 provides Point-to-Site (P2S) VPN connectivity.

Users connect to GW1 from a Windows 11 device by using an SSTP connection.

You need to ensure that the P2S VPN connections support Azure AD authentication.

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.

NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

Actions

Download the Azure VPN Client profile configuration package and distribute the package to the users.

For the point-to-site configuration of GW1, set Authentication type to **Azure Active Directory** and set Tunnel type to **IKEv2 and SSTP (SSL)**.

Register the Microsoft.HybridNetwork resource provider.

For the point-to-site configuration of GW1, set Authentication type to **Azure Active Directory** and set Tunnel type to **OpenVPN (SSL)**.

Grant the Azure VPN application admin consent to the Azure AD tenant.

Answer Area

Answer Area

Grant the Azure VPN application admin consent to the Azure AD tenant.

Correct Answer:

For the point-to-site configuration of GW1, set Authentication type to **Azure Active Directory** and set Tunnel type to **IKEv2 and SSTP (SSL)**.

Download the Azure VPN Client profile configuration package and distribute the package to the users.

 **JackeD** Highly Voted 2 months, 2 weeks ago

this is wrong, openvpn is the right answer.

upvoted 5 times

 **msheraq** Highly Voted 2 months, 2 weeks ago

to AUthenticate using Azure AD , we have to use OpenVPN in the second action.

upvoted 5 times

 **Murad01** Most Recent 1 month, 3 weeks ago

Second selection is wrong, it should be OpenVPN (SSL)

upvoted 3 times

店铺: IT认证考试服务

店铺: IT认证考试服务

DRAG DROP

-

You have an Azure subscription that contains an Azure Firewall Premium policy named FWP1.

To FWP1, you plan to add the rule collections shown in the following table.

Name	Type
RC1	Network
RC2	Application
RC3	DNAT

Which priority should you assign to each rule collection? To answer, drag the appropriate priority values to the correct rule collections. Each value 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.

NOTE: Each correct selection is worth one point.

Priorities

100

200

300

Answer Area

RC1:

RC2:

RC3:

Answer Area

RC1: 200

Correct Answer:

RC2: 300

RC3: 100

 **shimapapa** 1 week, 2 days ago

correct

<https://learn.microsoft.com/en-us/azure/firewall/policy-rule-sets#rule-collection-groups>

upvoted 1 times

 **Adeolu007** 1 week, 5 days ago

correct, DNAT, Network and then Application rules

upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 Azure subscription that contains an Azure Front Door Premium profile named AFD1 and an Azure Web Application Firewall (WAF) policy named WAF1. AFD1 is associated with WAF1.

You need to configure a rate limit for incoming requests to AFD1.

Solution: You configure a managed rule for WAF1.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 Azure subscription that contains an Azure Front Door Premium profile named AFD1 and an Azure Web Application Firewall (WAF) policy named WAF1. AFD1 is associated with WAF1.

You need to configure a rate limit for incoming requests to AFD1.

Solution: You modify the policy settings of WAF1.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 Azure subscription that contains an Azure Front Door Premium profile named AFD1 and an Azure Web Application Firewall (WAF) policy named WAF1. AFD1 is associated with WAF1.

You need to configure a rate limit for incoming requests to AFD1.

Solution: You configure a custom rule for WAF1.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 Azure subscription that contains an Azure Front Door Premium profile named AFD1 and an Azure Web Application Firewall (WAF) policy named WAF1. AFD1 is associated with WAF1.

You need to configure a rate limit for incoming requests to AFD1.

Solution: You add a rule to the rule set of AFD1.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

HOTSPOT

You have an Azure subscription that contains an Azure Firewall policy named FWPolicy1.

You need to configure FWPolicy1 to meet the following requirements:

- Allow traffic based on the FQDN of the destination.
- Allow TCP traffic based on the source.

Which types of rules should you use for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Allow traffic based on the FQDN of the destination:

- Application only
- Network only
- Network or DNAT only
- Application or DNAT only
- Network or application only
- Network, application, or DNAT

Allow TCP traffic based on the source:

- Application only
- Network only
- Network or DNAT only
- Application or DNAT only
- Network or application only
- Network, application, or DNAT

Answer Area

Allow traffic based on the FQDN of the destination:

- Application only
- Network only
- Network or DNAT only
- Application or DNAT only
- Network or application only
- Network, application, or DNAT

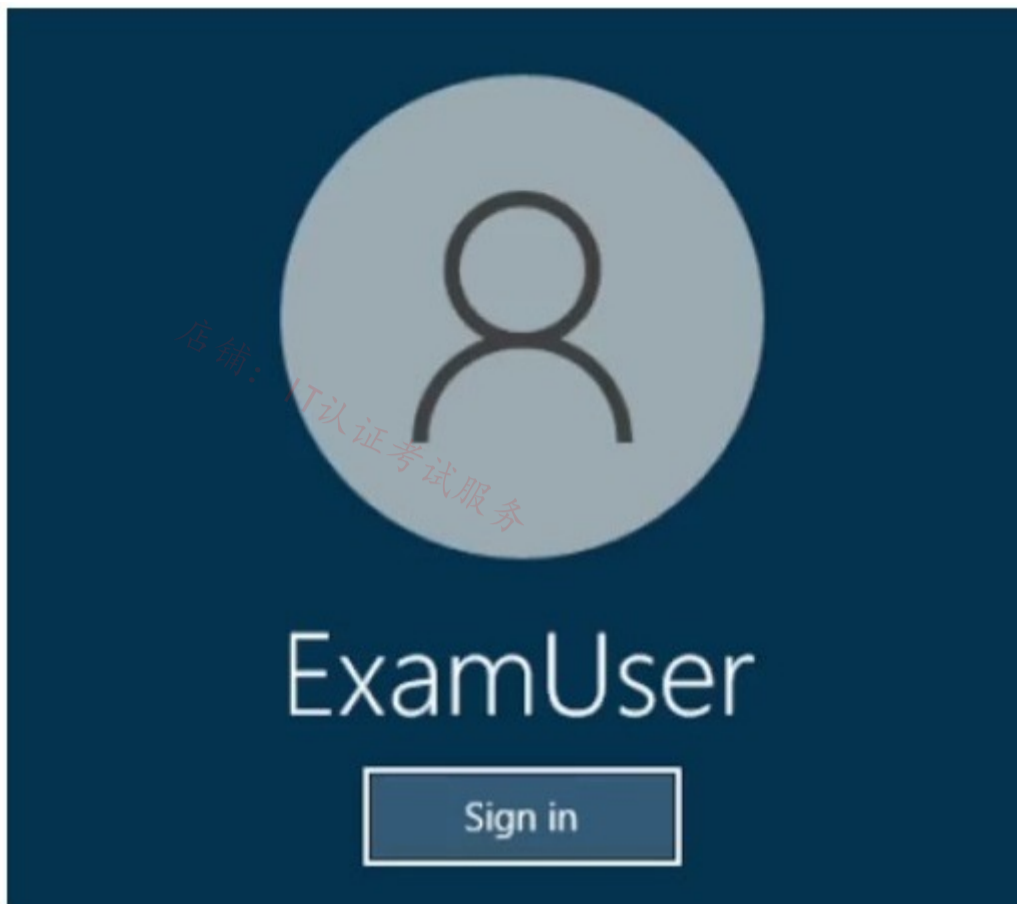
Correct Answer:

Allow TCP traffic based on the source:

- Application only
- Network only
- Network or DNAT only
- Application or DNAT only
- Network or application only
- Network, application, or DNAT

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You need to block all outbound internet traffic for HTTP and HTTPS that originates from subnet1-1. All other traffic must be allowed.

To complete this task, sign in to the Azure portal.

Correct Answer:

Use firewall to restrict outbound traffic using Azure portal
Azure Firewall can restrict outbound HTTP and HTTPS traffic.

Configure the firewall with network rules

Step 1: Navigate to Network rule collection > + Add network rule collection.

Step 2: On the Add network rule collection screen, provide the following information:
Top Section

Name: SomeRule
Priority: 200
Action: Block

Service section
Name: Rule_1
Protocols: HTTP, HTTPS
Source addresses: subnet1-1
Destination addresses: *
Destination ports: *

Add network rule collection

* Name: NRC01 ✓
* Priority: 200 ✓
* Action: Allow ✓

Rules

IP Addresses

NAME	PROTOCOL	SOURCE ADDRESSES	DESTINATION ADDRESSES	DESTINATION PORTS
Rule01 ✓	Any	* ✓	* ✓	123 ✓
	<input type="checkbox"/> TCP <input type="checkbox"/> UDP <input type="checkbox"/> ICMP <input checked="" type="checkbox"/> Any	*, 192.168.10.1, 192.168.10.0/24,...	*, 192.168.10.1, 192.168.10.0/24,...	8080, 8080-8090, *

Service Tags

NAME	SOURCE ADDRESSES	SERVICE TAGS	DESTINATION PORTS
	*, 192.168.10.1, 192.168.10.0/24,...	0 selected	8080, 8080-8090, *

Add

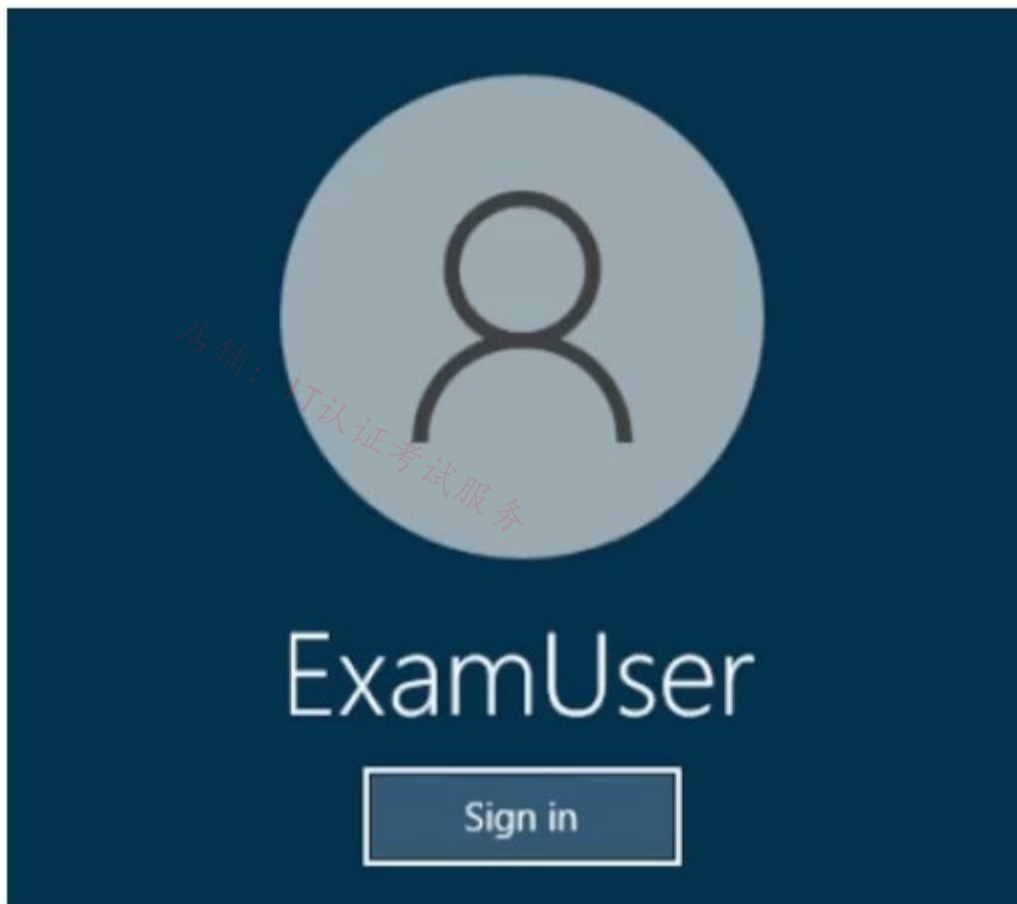
Step 3: Select Add.

Reference:

- <https://learn.microsoft.com/en-us/azure/hdinsight/hdinsight-restrict-outbound-traffic>
- <https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/plan-for-inbound-and-outbound-internet-connectivity>

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You need to restrict access to the storage35433841 storage account to ensure that only subnet1-2 can access the account.

To complete this task, sign in to the Azure portal.

Correct Answer:

Restrict network access to a subnet

By default, storage accounts accept network connections from clients in any network, including the internet. You can restrict network access from the internet, and all other subnets in all virtual networks (except the subnet-private subnet in the vnet-1 virtual network.)

To restrict network access to a subnet:

Step 1: In the search box at the top of the portal, enter Storage account. Select Storage accounts in the search results.

Step 2: Select the storage account storage35433841.

Step 2: Select your storage account storage32433841

Step 3: In Security + networking, select Networking.

Step 4: In the Firewalls and virtual networks tab, select Enabled from selected virtual networks and IP addresses in Public network access.

Step 5: In Virtual networks, select + Add existing virtual network.

Step 6: In Add networks, enter or select the following information:

Setting - Value

Subscription: Select your subscription.

Virtual networks: Select the available virtual network

Subnets: Select subnet1-2.

Home > Storage accounts > storage8675

storage8675 | Networking ☆ ...

Storage account

Search

Firewalls and virtual networks Private endpoint connections

Save Discard Refresh

Firewall settings restricting access to storage services will remain in effect for up to a minute after saving updated settings allowing access.

Public network access

Enabled from all networks

Enabled from selected virtual networks and IP addresses

Disabled

Configure network security for your storage accounts. [Learn more](#)

Virtual networks

+ Add existing virtual network + Add new virtual network

Virtual Network	Subnet	Address range
No network selected.		

Add

Step 7: Select Add.

Step 8: Select Save to save the virtual network configurations.

Home > Storage accounts > storage8675

storage8675 | Networking ☆ ...

Storage account

Search

Firewalls and virtual networks Private endpoint connections Custom domain

Save Discard Refresh

Firewall settings restricting access to storage services will remain in effect for up to a minute after saving updated settings allowing access.

Public network access

Enabled from all networks

Enabled from selected virtual networks and IP addresses

Disabled

Configure network security for your storage accounts. [Learn more](#)

Virtual networks

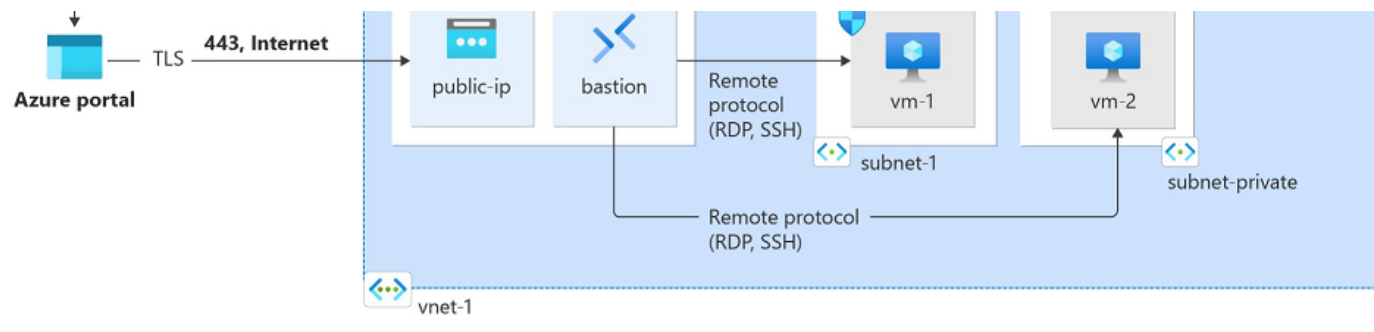
+ Add existing virtual network + Add new virtual network

Virtual Network	Subnet	Address range	Endpoint Status	Resource Group	Subscription
> vnet-1	1			test-rg	C&L content develo... ***

Note: Restrict network access to PaaS resources with virtual network service endpoints using the Azure portal

Note: Virtual network service endpoints enable you to limit network access to some Azure service resources to a virtual network subnet. You can also remove internet access to the resources. Service endpoints provide direct connection from your virtual network to supported Azure services, allowing you to use your virtual network's private address space to access the Azure services. Traffic destined to Azure resources through service endpoints always stays on the Microsoft Azure backbone network.





Reference:

<https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-restrict-network-access-to-resources>

店铺: IT认证考试服务

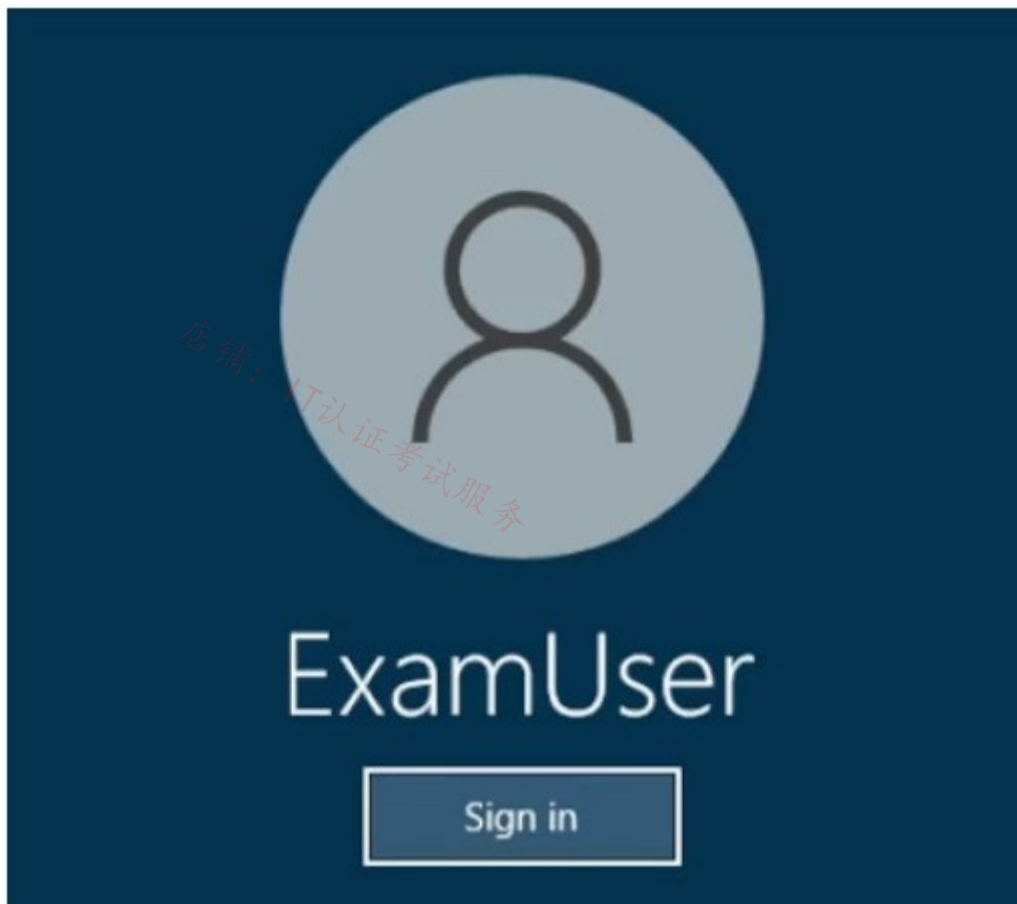
店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You need to ensure that subnet3-2 can only access resources on subnet3-1.

To complete this task, sign in to the Azure portal.

Correct Answer:

Azure network rules

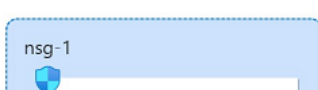
You can use a network security group to filter inbound and outbound network traffic to and from Azure resources in an Azure virtual network.

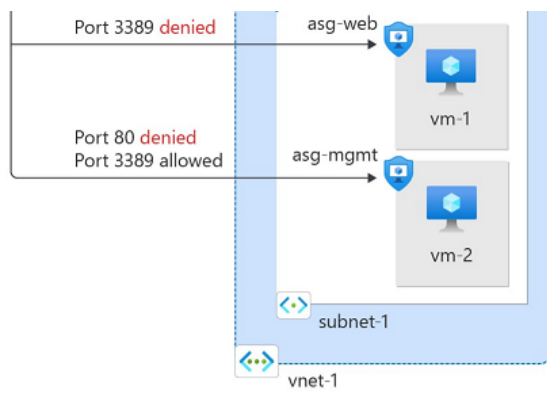
Network security groups contain security rules that filter network traffic by IP address, port, and protocol. When a network security group is associated with a subnet, security rules are applied to resources deployed in that subnet.



User

Port 80 allowed





Stage 1: Create a network security group

A network security group (NSG) secures network traffic in your virtual network.

Step 1: In the search box at the top of the portal, enter Network security group. Select Network security groups in the search results.

Step 2: Select + Create.

Step 3: On the Basics tab of Create network security group, enter or select something like this information

Project details

Subscription: Select your subscription.

Resource group: Select test-rg.

Instance details

Name: Enter nsg-1.

Location: Select East US 2.

Step 4: Select Review + create.

Step 5: Select Create.

Stage 2

Associate network security group to subnet

In this section, you associate the network security group with the subnet of the virtual network you created earlier.

Step 1: In the search box at the top of the portal, enter Network security group. Select Network security groups in the search results.

Step 2: Select nsg-1.

Step 3: Select Subnets from the Settings section of nsg-1.

Step 4: In the Subnets page, select + Associate:

Home > Network security groups > nsg-1

nsg-1 | Subnets ☆ ☆ ...

Search

+ Associate

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Inbound security rules
- Outbound security rules
- Network interfaces
- Subnets**
- Properties
- Locks

Search subnets

Name	↑↓	Address range	↑↓	Virtual network	↑↓
No results.					

Step 5: Under Associate subnet, select vnet-1 (test-rg) for Virtual network.

Step 6: Select subnet3-2 for Subnet, and then select OK.

Stage 3:

Create security rules

Step 1: Select Outbound security rules from the Settings section of nsg-1.

Step 2: In Outbound security rules page, select + Add.

Step 3: Create a security rule that allows any ports, any protocol, to subnet3-1.

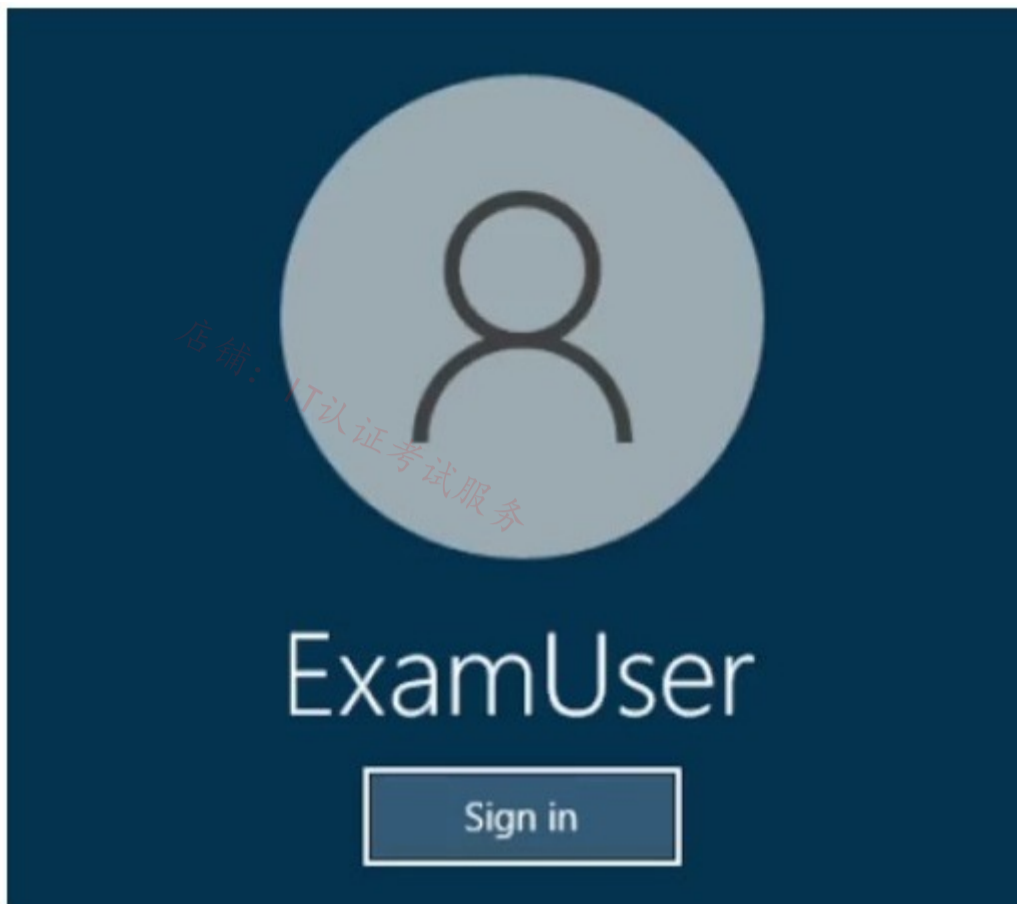
Step 4: Select Add.

Reference:

<https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic>

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You are planning security for Azure Front Door.

You need to create a rule that can be applied to Front Door hosts. The rule must prevent hosts in Japan from making more than 50 requests per minute. You do NOT need to associate the rule to a Front Door instance to complete this task.

To complete this task, sign in to the Azure portal.

Correct Answer:

Configure a Web Application Firewall rate-limit rule

The Azure Web Application Firewall rate-limit rule for Azure Front Door controls the number of requests allowed from a particular source IP address to the application during a rate-limit duration.

Stage 1: Create a policy
First, create a basic WAF policy

Step 1: On the upper left side of the portal, select Create a resource. Search for WAF, select Web Application Firewall, then select Create.

Step 2: On Create a WAF policy page, Basics tab, enter

Step 3: Select Review + create, then select Create.

Home > WAF policies > Create a WAF policy

Create a WAF policy

Basics Policy settings Managed rules Custom rules Association Tags Review + create

Malicious attacks such as SQL Injection, Cross Site Scripting (XSS), and other OWASP top 10 threats could cause service outage or data loss, and pose a big threat to web application owners. Web Application Firewall (WAF) protects your web applications from common web attacks, keeps your service available and helps you meet compliance requirements.
[Learn more about WAF policy for Front Door](#)
[Learn more about WAF policy for Application Gateway](#)

Project details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Policy for * ⓘ Regional WAF (Application Gateway) ▼

Subscription * ⓘ ANTman ▼

Resource group * (New) myPolicy ▼
[Create new](#)

Instance details

Policy name * ⓘ Policy1 ✓

Location * ⓘ (US) West US 2 ▼

Policy state ⓘ Enabled Disabled

Stage 2: Create a rate-limit rule

Step 1: Select Custom rules > Add custom rule.

MyWafPolicy | Custom rules ☆ ...
Front Door WAF policy

Search (Cmd+/) << Save Discard Refresh

Overview
Activity log
Access control (IAM)
Tags

Settings

Policy settings
Managed rules
Custom rules
Associations
Properties

Configure a policy with custom-authored rules. Once to the request. Once such a match is processed, rule: a rule denotes a higher priority. [Learn more](#)

+ Add custom rule

Priority	Name	Rule type
No custom rules to display.		

Step 2: Enter the information required to create a rate-limit rule:

Custom rule name: Enter the name of the custom rule, such as rateLimitRule.

Rule type: Select Rate limit.

Priority: Enter the priority of the rule, such as 1.

Rate limit duration: Select 1 minute.

Rate limit threshold (requests): Enter 50

Step 3: In Conditions, enter the information required to specify a match condition to identify requests. For Match type, select Geo location, for Value select JP (for Japan).

Match type: Geo Location.

Operation: Select is.

Match values: JP

Note: To create a geo-filtering custom rule in the Azure portal, select Geo location as the Match Type, and then select the country/region or countries/regions you want to allow/block from your application.

Add custom rule



A custom rule is made up of one or more conditions followed by an action. All custom rules for a WAF policy are match rules. [Learn more about custom rules](#)

Custom rule name *

Status Enabled Disabled

Rule type Match Rate limit

Priority *

Rate limit duration

Rate limit threshold (requests)

Conditions

If

Match type

Match variable *

Operation is is not

Operator *

Transformation

Match values

+ Add new condition

Then

Step 4: For Action, select Block.

Rate-limit rules only support Log and Block actions. Allow isn't supported.

Step 5: Select Add.

Step 6: Select Save.

Reference:

<https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/create-waf-policy-ag>

<https://learn.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-rate-limit-configure>

<https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/geomatch-custom-rules>

店铺: IT认证考试服务

店铺: IT认证考试服务

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You have an Azure subscription that contains an Azure Virtual WAN named VWAN1. VWAN1 contains a hub named Hub1.

Hub1 has a security status of Unsecured.

You need to ensure that the security status of Hub1 is marked as Secured.

Solution: You implement an Azure Front Door profile.

Does this meet the requirement?

- A. Yes
- B. No

Correct Answer: B

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You have an Azure subscription that contains an Azure Virtual WAN named VWAN1. VWAN1 contains a hub named Hub1.

Hub1 has a security status of Unsecured.

You need to ensure that the security status of Hub1 is marked as Secured.

Solution: You implement Azure Firewall.

Does this meet the requirement?

- A. Yes
- B. No

Correct Answer: A

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You have an Azure subscription that contains an Azure Virtual WAN named VWAN1. VWAN1 contains a hub named Hub1.

Hub1 has a security status of Unsecured.

You need to ensure that the security status of Hub1 is marked as Secured.

Solution: You implement Azure NAT Gateway.

Does this meet the requirement?

A. Yes

B. No

Correct Answer: B

Topic 5 - Question Set 5

店铺: IT认证考试服务

店铺: IT认证考试服务

You have the Azure resources shown in the following table.

Name	Type	Location	Description
storage1	Storage account	East US	Read-access geo-redundant storage (RA-GRS)
Vnet1	Virtual network	East US	Contains one subnet

You configure storage1 to provide access to the subnet in Vnet1 by using a service endpoint.

You need to ensure that you can use the service endpoint to connect to the read-only endpoint of storage1 in the paired Azure region.

What should you do first?

- A. Fail over storage1 to the paired Azure region.
- B. Configure the firewall settings for storage1.
- C. Create a virtual network in the paired Azure region.
- D. Create another service endpoint.

Correct Answer: B

The Azure storage firewall provides access control for the public endpoint of your storage account. You can also use the firewall to block all access through the public endpoint when using private endpoints.

Note: By default, service endpoints work between virtual networks and service instances in the same Azure region. When using service endpoints with Azure

Storage, service endpoints also work between virtual networks and service instances in a paired region.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security>

Community vote distribution

C (81%)

Other

 **sapien45** Highly Voted 1 year, 3 months ago

Selected Answer: C

When planning for disaster recovery during a regional outage, you should create the VNets in the paired region in advance. Enable service endpoints for Azure Storage, with network rules granting access from these alternative virtual networks. Then apply these rules to your geo-redundant storage accounts.

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

upvoted 17 times

 **Ditka** 6 months, 1 week ago

"Local and cross-region service endpoints can't coexist on the same subnet. To replace existing service endpoints with cross-region ones, delete the existing Microsoft.Storage endpoints and re-create them as cross-region endpoints (Microsoft.Storage.Global)."

upvoted 2 times

 **TJ001** 1 year ago

Answer C. Agreed

upvoted 1 times

 **Murad01** Most Recent 1 month, 3 weeks ago

Appeared on Exam November -2023

upvoted 1 times

 **Zika69** 7 months, 2 weeks ago

Selected Answer: B

An answer is needed to the question "ensure that you can use the service endpoint to connect to the read-only endpoint of storage1 in the paired Azure region" - and only possible answer is B

Answer C is for the question - "What you should do to create a RA-GRS instance"

upvoted 1 times

 **jarz** 8 months, 4 weeks ago

F#cking M\$ are sneaky mofos! You really got to RTFQ with these bastards!

It's asking what's the first thing you need to do. It's difficult to know exactly what's been done, and what needs to be done. Assuming nothing has been done, then configuring the vnets on the recovery site makes sense.

upvoted 3 times

🗨️ **Apptech** 10 months ago

Documentation says: "When planning for disaster recovery during a regional outage, you should create the VNets in the paired region in advance." But in our case the service endpoint for the Azure Storage already is in place. So this question is pretty unclear. If the Vnet also already is in place (we do not know for sure) then Firewall should be the next step.

upvoted 1 times

🗨️ **Neostar** 10 months, 2 weeks ago

Selected Answer: A

"Service endpoints allow continuity during a regional failover and access to read-only geo-redundant storage (RA-GRS) instances. Network rules that grant access from a virtual network to a storage account also grant access to any RA-GRS instance."

<https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal#available-virtual-network-regions>

upvoted 3 times

🗨️ **Bbb78** 12 months ago

Selected Answer: B

who is to say that the paired Azure region does not have a VNet yet ...maybe it just needs that firewall rule on the storage?

upvoted 1 times

🗨️ **GBAU** 3 months ago

In these exams you can't assume anything else exists unless it is 100% required for something that is stated to exist.

upvoted 1 times

🗨️ **alkorkin** 1 year ago

When planning for disaster recovery during a regional outage, you should create the VNets in the paired region in advance.

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

upvoted 1 times

🗨️ **varvare** 1 year, 1 month ago

This is the excerpt from the link above Service endpoints allow continuity during a regional failover and access to read-only geo-redundant storage (RA-GRS) instances. Network rules that grant access from a virtual network to a storage account also grant access to any RA-GRS instance.

When planning for disaster recovery during a regional outage, you should create the VNets in the paired region in advance. Enable service endpoints for Azure Storage, with network rules granting access from these alternative virtual networks. Then apply these rules to your geo-redundant storage accounts.

if you read past the section that makes B the answer, you see the pre-requisite that makes C the answer

upvoted 2 times

🗨️ **GohanF2** 1 year, 2 months ago

Answer is C.

By enabling Service Endpoint for access to our Azure resource, we are limiting the access to the "storage account" only to private IP address. So, we won't longer need the usage of a public IP address or NATting settings like in a firewall. So, the option of the firewall is no longer suitable in this case.

The first option about fail-over will work only if the primary "service point" fails, or for having active-active environment; but that will require too much effort.Plus, both "Subnet" and " Service endpoint" are located in the same region, it would be useful the "fail-over option if they are located in separated regions".

The other option about adding an additional "service endpoint" doesn't make sense due that the question says that we will need to grant access via the "Service endpoint" that was created.

upvoted 2 times

🗨️ **Ajdifasudfo** 1 year, 1 month ago

this is wrong. Service endpoints go via the public ip. That's there very difference compared to private endpoint

upvoted 4 times

🗨️ **Prutser2** 1 year, 3 months ago

Selected Answer: C

By default, service endpoints work between virtual networks and service instances in the same Azure region. When using service endpoints with Azure Storage, service endpoints also work between virtual networks and service instances in a paired region. If you want to use a service endpoint to grant access to virtual networks in other regions, you must register the AllowGlobalTagsForStorage feature in the subscription of the virtual network. This capability is currently in public preview.

Service endpoints allow continuity during a regional failover and access to read-only geo-redundant storage (RA-GRS) instances. Network rules that grant access from a virtual network to a storage account also grant access to any RA-GRS instance.

When planning for disaster recovery during a regional outage, you should create the VNets in the paired region in advance. Enable service endpoints for Azure Storage, with network rules granting access from these alternative virtual networks. Then apply these rules to your geo-redundant storage accounts.

upvoted 3 times

🗨️ **DevOpsJunior** 1 year, 4 months ago

B is correct, its clearly mentioned in the documentation.

upvoted 2 times

🗨️ **sapien45** 1 year, 3 months ago

And which documentation is it, junior?

upvoted 4 times

🗨️ 👤 **Akodo_Shado** 1 year ago

Answer is obviously B as DevOpsJunior pointed out.

<https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal#available-virtual-network-regions>
"When using service endpoints with Azure Storage, service endpoints also work between virtual networks and service instances in a paired region."

Lab tested.

upvoted 3 times

🗨️ 👤 **Ditka** 6 months, 1 week ago

Yes they do, but not at the same time. You cannot have a single subnet with both a local region service endpoint and a cross-region service endpoint (tested). The documentation states to set up a vnet in the paired local region with a local SE for DR purposes:

"Local and cross-region service endpoints can't coexist on the same subnet. To replace existing service endpoints with cross-region ones, delete the existing Microsoft.Storage endpoints and re-create them as cross-region endpoints (Microsoft.Storage.Global)."

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

upvoted 1 times

🗨️ 👤 **BlackZeros** 1 year, 4 months ago

Selected Answer: C

C is perhaps the right answer, you create a VNET on the paired region from where you will access the storage1

upvoted 1 times

🗨️ 👤 **sapien45** 1 year, 3 months ago

and PERHAPS instead of conjecturing, you should look for official Azure literature to document your arguments, This is whole point.

upvoted 2 times

🗨️ 👤 **Ditka** 6 months, 1 week ago

Here is the literature:

You cannot have a single subnet with both a local region service endpoint and a cross-region service endpoint (tested). The documentation states to set up a vnet in the paired local region with a local SE for DR purposes:

"Local and cross-region service endpoints can't coexist on the same subnet. To replace existing service endpoints with cross-region ones, delete the existing Microsoft.Storage endpoints and re-create them as cross-region endpoints (Microsoft.Storage.Global)."

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

upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT -

You have the Azure App Service app shown in the App Service exhibit.

as12
App Service

>> Browse Start Swap Restart Delete Get publish profile Reset publish profile ...

Warning: Your app is stopped. App Service plan charges still apply.

Essentials JSON View

Resource group (change) RG1	URL https://as12.azurewebsites.net
Status Stopped	Health Check Configured
Location North Europe	App Service Plan ASP1 (P1v2:1)
Subscription (change) Subscription1	FTP/deployment user set No FTP/deployment user set
Subscription ID 846f6nnt-nt8e-794i-k478-649ws1576487	FTP hostname ftp://waws-prod-db3-167.azurewebsites.windows.net/site/wwwroot
	FTPS hostname ftps://waws-prod-db3-167.azurewebsites.windows.net/site/wwwroot

Tags (change)
Click here to add tags

The VNet Integration settings for as12 are configured as shown in the Vnet Integration exhibit.

VNet Integration
as12

Disconnect Refresh

VNet Configuration

Securely access resources available in or through your Azure VNet. [Learn more](#)

VNet Details

VNet NAME	Vnet1
LOCATION	North Europe

VNet Address Space

Start Address	End Address
10.100.0.0	10.100.255.255

Subnet Details

Subnet NAME	Subnet1
-------------	---------

Subnet Address Space

Start Address	End Address
10.100.2.0	10.100.2.255

The Private Endpoint connections settings for as12 are configured as shown in the Private Endpoint connections exhibit.

Private Endpoint connections

+ Add Refresh | ✓ Approve ✗ Reject 🗑 Remove



Private Endpoint connections

Private access to services hosted on the Azure platform, keeping your data on the Microsoft network [Learn more](#)

Filter by name or description All connection states

Connection name ↑↓ Connection state ↑↓ Private endpoint ↑↓ Description

No results.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Subnet2 can contain only App Service apps in the ASP1 App Service plan	<input type="radio"/>	<input type="radio"/>
As12 will use an IP address from Subnet2 for network communications	<input type="radio"/>	<input type="radio"/>
Computers in Vnet1 will connect to a private IP address when they connect to as12	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
Subnet2 can contain only App Service apps in the ASP1 App Service plan	<input checked="" type="radio"/>	<input type="radio"/>
As12 will use an IP address from Subnet2 for network communications	<input checked="" type="radio"/>	<input type="radio"/>
Computers in Vnet1 will connect to a private IP address when they connect to as12	<input type="radio"/>	<input checked="" type="radio"/>

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/web-sites-integrate-with-vnet>

Geo13AZ Highly Voted 2 years ago

1. Yes: Virtual Network Integration supports only one virtual interface per worker. One virtual interface per worker means one regional virtual network integration per App Service plan. All the apps in the same App Service plan can use the same virtual network integration. <https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration> under section "How regional virtual network integration works".
2. Yes: "When regional virtual network integration is enabled, your app makes outbound calls through your virtual network. The outbound addresses that are listed in the app properties portal are the addresses still used by your app.". <https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration> under section "How regional virtual network integration works".
3. No: "you can't use virtual network integration to provide inbound access to your app.", if you need Inbound access to the App you will need to setup a Service Endpoint or Private Endpoint. <https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration> under "Regional virtual network integration".

upvoted 38 times

GohanF2 1 year, 2 months ago

Great Answer.
upvoted 2 times

GohanF2 1 year, 2 months ago

Well explained
upvoted 1 times

Pradh 1 year, 3 months ago

for 2nd question if you are saying this "The outbound addresses that are listed in the app properties portal are the addresses still used by your app" , then why is the answer yes ? it should be NO right ?
upvoted 2 times

🗳️ **Bharat** Highly Voted 2 years, 3 months ago

Clearly Subnet2 in the question statements has to be Subnet1?
upvoted 30 times

🗳️ **RandomUser** 2 years, 3 months ago

It is already fixed in the exam as of today. It shows Subnet2 in the picture, so it matches the question now.
upvoted 7 times

🗳️ **laige** 2 years, 3 months ago

agreed, otherwise it going to be 3 no.
upvoted 14 times

🗳️ **CiscoTerminator** Most Recent 5 months, 1 week ago

But lets be fair, question has Subnet 1 and you are busy endorsing answers from a question you created. As it stands, answer is NNY
upvoted 4 times

🗳️ **samir111** 1 week ago

100% lol
upvoted 1 times

🗳️ **samir111** 1 week ago

Btw last one should be N, as well as there is no endpoint Link, so traffic wont go using Private.... So it shall be NNN
upvoted 1 times

🗳️ **mrgreat** 10 months, 2 weeks ago

YYN.
Same question: <https://www.examttopics.com/exams/microsoft/az-700/view/11/>
upvoted 2 times

🗳️ **TJ001** 1 year ago

YYN - just ignore subnet name error as highlighted by others already :)
upvoted 3 times

🗳️ **jellybiscuit** 1 year, 3 months ago

As written/pictured it's NNN
If the vnet integration is really with subnet2, the it's YYN
upvoted 3 times

🗳️ **sapien45** 1 year, 3 months ago

If we replace Subnet1 by Subnet2 in the screenshot :
YYN
*"Subnet1" is dedicated to vnet integration
* as12 will use IP address from "subnet1" for outbound
*If you need Inbound access to the App you will need to setup a Service Endpoint or Private Endpoint.
upvoted 4 times

🗳️ **nakul115** 1 year, 4 months ago

it should be NNN
The App service status is "stopped"
upvoted 3 times

🗳️ **Skankhunt** 12 months ago

Lol where's the downvote button
upvoted 2 times

🗳️ **Cristoicach91** 1 year, 4 months ago

There is no private endpoint configured. NNN
upvoted 3 times

🗳️ **unclegrandfather** 1 year, 7 months ago

Appeared on exam Jun/28/22. Exam shows Subnet2 in the pictures.
upvoted 4 times

🗳️ **Fearless90** 1 year, 7 months ago

Subnet1 can contain only App Service apps in the ASP1 App Service plan > Yes
"Subnet1" is dedicated to vnet integration
Virtual Network Integration supports only one virtual interface per worker. One virtual interface per worker means one regional virtual network integration per App Service plan. All the apps in the same App Service plan can use the same virtual network integration.

<https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration#how-regional-virtual-network-integration-works>
The feature supports only one virtual interface per worker. One virtual interface per worker means one regional virtual network integration per App Service plan. All the apps in the same App Service plan can only use the same virtual network integration to a specific subnet. If you need an

app to connect to another virtual network or another subnet in the same virtual network, you need to create another App Service plan. The virtual interface used isn't a resource that customers have direct access to.

upvoted 1 times

  **Fearless90** 1 year, 7 months ago

as12 will use an IP address from Subnet1 for network communications > Yes
as12 will use IP address from "subnet1" for outbound

<https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration#how-regional-virtual-network-integration-works>
When regional virtual network integration is enabled, your app makes outbound calls through your virtual network. The outbound addresses that are listed in the app properties portal are the addresses still used by your app. However, if your outbound call is to a virtual machine or private endpoint in the integration virtual network or peered virtual network, the outbound address will be an address from the integration subnet. The private IP assigned to an instance is exposed via the environment variable, WEBSITE_PRIVATE_IP.

upvoted 2 times

  **Fearless90** 1 year, 7 months ago

Computers in Vnet1 will connect to a private IP address when they connect to as12 > No
"You can't use virtual network integration to provide inbound access to your app.", if you need Inbound access to the App you will need to setup a Service Endpoint or Private Endpoint.
The exhibit for private endpoints is empty.

<https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration#regional-virtual-network-integration>
When you use regional virtual network integration, you can use the following Azure networking features:
Network security groups (NSGs): You can block outbound traffic with an NSG that's placed on your integration subnet. The inbound rules don't apply because you can't use virtual network integration to provide inbound access to your app.

upvoted 1 times

  **kogunribido** 1 year, 7 months ago

Appeared on exam 6/27/2022
upvoted 1 times

  **Kimimoto** 1 year, 11 months ago

Appeared in exam on 11/Feb/2022
upvoted 1 times

  **sleekdunga** 1 year, 11 months ago

1.Yes
2.Yes. When regional virtual network integration is enabled, your app makes outbound calls through your virtual network. The outbound addresses that are listed in the app properties portal are the addresses still used by your app.
3.No. Virtual network integration doesn't enable your apps to be accessed privately

upvoted 4 times

  **sleekdunga** 1 year, 11 months ago

2. However, if your outbound call is to a virtual machine or private endpoint in the integration virtual network or peered virtual network, the outbound address will be an address from the integration subnet.

upvoted 1 times

  **Contactfornitish** 2 years ago

Appeared in exam on 17/01/2022
upvoted 1 times

  **Pravda** 2 years ago

Variant on exam 1/6/2022
upvoted 2 times

  **whatzapp95** 2 years, 1 month ago



Yes: "Subnet2" is dedicated to vnet integration
Yes: As12 will use ip address from "subnet 2" for outbound
Yes: Computer will use private endpoint for inbound to communicate to as12

upvoted 4 times

  **[Removed]** 2 years, 1 month ago

why is 3 Yes? It should be No. The exhibit for private endpoints is empty.

upvoted 12 times

  **Prutser2** 1 year, 3 months ago

box3: there is no private endpoint, exhibit has empty pr. endpoint, just saying, YYN

upvoted 2 times

DRAG DROP -

You have an Azure virtual network named Vnet1 that connects to an on-premises network.

You have an Azure Storage account named storageaccount1 that contains blob storage.

You need to configure a private endpoint for the blob storage. The solution must meet the following requirements:

- ☞ Ensure that all on-premises users can access storageaccount1 through the private endpoint.
- ☞ Prevent access to storageaccount1 from being interrupted.

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.

Select and Place:

Actions

- Install the DNS server role and configure the forwarding of blob.core.windows.net to 168.63.129.16
- Configure on-premises DNS servers to forward blob.core.windows.net to the virtual machine
- Configure a private endpoint on storageaccount1 and disable public access to the account
- Configure on-premises DNS server to forward blob.core.windows.net to 168.63.129.16
- Deploy a virtual machine to a subnet in Vnet1

Answer Area



Correct Answer:

Actions

-
-
-
- Configure on-premises DNS server to forward blob.core.windows.net to 168.63.129.16
-

Answer Area

- Configure a private endpoint on storageaccount1 and disable public access to the account
- Deploy a virtual machine to a subnet in Vnet1
- Install the DNS server role and configure the forwarding of blob.core.windows.net to 168.63.129.16
- Configure on-premises DNS servers to forward blob.core.windows.net to the virtual machine



168.63.129.16 is the IP address of Azure DNS which hosts Azure Private DNS zones. It is only accessible from within a VNet which is why we need to forward on-prem DNS requests to the VM running DNS in the VNet. The VM will then forward the request to Azure DNS for the IP of the storage account private endpoint.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-private-endpoints>

kerberos999 Highly Voted 2 years, 2 months ago

The order is wrong. If you need to avoid service interruption "Deny Public Access and Private Endpoint" should be configured at last
upvoted 48 times

_Cris 4 months, 1 week ago

I thought exactly the same, it wasn't that bad.
upvoted 2 times

waqas 2 years, 1 month ago

So plz guide what should be the right sequence and answer then????
upvoted 6 times

Chricrown 1 year, 4 months ago

Deploy VM --> Install DNS Server role --> Configure On-prem to fwd blob.core.windows.net --> disable public access.
upvoted 29 times

Pravda Highly Voted 2 years ago

Think through the steps and this is an easy question to answer.

+ 5 Deploy VM This VM is for DNS.

+ 1 Install DNS Role and create DNS forward entry DNS server in Azure has blob.core mapped to IP address 168.63.129.16

+ 2 ON-prem DNS to VM The on-prem DNS server lookup requests for blob need to be forwarded to the DNS server in Azure with the blob.core to IP address mapping.

+ 3 Private-endpoint creation and disable public access – With DNS settings complete users can connect to blob, without interruption. Public access can be disabled.

Not sure why 4 could not be used in place of creating VM and installing DNS role. I suspect it has something to do with interruption of service. But since we aren't told how they are accessing the blob now who knows.

upvoted 45 times

  **ian2387** 1 year, 9 months ago

I agree with this

upvoted 2 times

  **GBAU** Most Recent 3 months ago

If you set up the PEP and deny public access first, you interrupt access to the storage for onsite users (who are using Public Access).

You need to set up the DNS solution first, which will initially still give the Public IP resolution so maintain access.

Then you add the PEP and remove public Access. DNS will cut over to the PEP IP and users will continue to access it that way.

Of course, with DNS caching of the storages Public IP access, users will still get some interruptions to access...

To actually do this without interruption, you would need to create a static record in DNS for the storage accounts PEP first, then add the forwarder, wait for the TTL for the Public DNS records on the clients to expire, then remove the static entry. to let the forwarder take control.

upvoted 1 times

  **Zeppoonstream** 9 months, 2 weeks ago

From where do i get the info what the ip is ?!

upvoted 2 times

  **GohanF2** 1 year, 2 months ago

Answers are as following:

1. Deploy a virtual machine to a subnet in Vnet1
2. Install DNS server role and configure the forwarding of blob.core.windows.net to 168.63.129.16
3. Configure on-premises DNS servers to forward blob.core.windows.net to the virtual machine (This is assuming that there is an IPsec connection from your on-premises to your Azure Virtual Environment).
4. Configure a private endpoint on storageaccount1 and disable public access to the account. (This is option is done on last due that a storage account can only have one type of access mode at a time, if we set this option by first, we will be interrupting the access publicly and the question says that we need to avoid service interruption.)

The option of: Configure on-premises DNS server to forward blob.core.windows.net to 168.63.129.16 is wrong due that the ip address: 168.63.129.16 exists only in Azure Environment and our On-premises network won't know any route of how to get to that network.

upvoted 11 times

  **jellybiscuit** 1 year, 3 months ago

This is what I was doing, without really thinking about the disruption. After seeing the comments and thinking back on my answer, I think the key is to simply pause between enabling the private endpoint and disabling public access to allow DNS to propagate after you add the PE.

- deploy vm
- install dns
- on-prem dns forwards to vm
- configure private endpoint on storage account - [insert pause here] then disable public access



upvoted 4 times

  **sapien45** 1 year, 3 months ago

Very similar setup described here :

<https://learn.microsoft.com/en-us/azure/private-link/private-endpoint-dns#on-premises-workloads-using-a-dns-forwarder>

upvoted 2 times

  **Jamesat** 1 year, 5 months ago

To avoid service disruption you would have to do the Private Endpoint last.

Otherwise you've lost access until you have finished building the VMs and installing DNS etc.

upvoted 1 times

  **zerocool114** 1 year, 6 months ago

on exam today

upvoted 1 times

  **unclegrandfather** 1 year, 7 months ago

Appeared on exam Jun/28/22

upvoted 1 times

  **Fearless90** 1 year, 7 months ago

5. Deploy a virtual machine to a subnet in Vnet1

5. Deploy VM. This VM is for DNS.

1. Install the DNS server role and configure the forwarding of blob.core.windows.net to 168.63.129.16
 1. Install DNS Role and create DNS forward entry. DNS server in Azure has blob.core.windows.net mapped to IP address 168.63.129.16
 2. Configure on-premises DNS servers to forward blob.core.windows.net to the virtual machine
 2. ON-prem DNS to VM The on prem DNS server lookup requests for blob need to be forwarded to the DNS server in Azure with the blob.core.windows.net to IP address mapping.
 3. Configure a private endpoint on storageaccount1 and disable public access to the account
 3. Private-endpoint creation and disable public access
- With DNS settings complete users can connect to blob, without interruption. Public access can be disabled. Avoid service interruption "Deny Public Access and Private Endpoint" should be configured at last
- upvoted 1 times

🗄️ 👤 **kogunribido** 1 year, 7 months ago
Appeared on exam 6/27/2022
upvoted 1 times

🗄️ 👤 **kogunribido** 1 year, 7 months ago
Appeared on exam 6/27/2022
upvoted 1 times

🗄️ 👤 **Pravda** 2 years ago
Variant on exam 1/6/2022
upvoted 3 times

🗄️ 👤 **AidenYoukhana** 2 years ago
Correct Order:
5
1
2
3
upvoted 13 times

🗄️ 👤 **vivert** 2 years, 1 month ago
VM>DNSRole
+FwdtoAzureDNA+
ON-premDNStoFwdtoAzureVM
+Private-endpoint creation
upvoted 5 times

🗄️ 👤 **Pravda** 2 years, 1 month ago
What is the correct answer?
upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

You have an Azure virtual network named Vnet1 that has one subnet. Vnet1 is in the West Europe region. You deploy an Azure App Service app named App1 to the West Europe region. You need to provide App1 with access to the resources in Vnet1. The solution must minimize costs. What should you do first?

- A. Create a private link.
- B. Create a new subnet.
- C. Create a NAT gateway.
- D. Create a gateway subnet and deploy a virtual network gateway.

Correct Answer: D

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/web-sites-integrate-with-vnet>

Community vote distribution

B (94%)

6%

 **christianpageqc** Highly Voted 2 years, 3 months ago

I think answer should be B. Create a new subnet, since both Vnet and App Service are in the same region.
<https://docs.microsoft.com/en-us/azure/app-service/web-sites-integrate-with-vnet#enable-vnet-integration>
 Regional VNet Integration = "If the VNet is in the same region, either create a new subnet or select an empty pre-existing subnet"
 upvoted 83 times

 **Bharat** 2 years, 3 months ago

You are correct. Thanks for the reference link.
 upvoted 5 times

 **dpinlaguna** Highly Voted 2 years, 3 months ago

I think it should be B since resources are in the same region (Regional VNet Integration), new subnet does not incur cost. The VPN Gateway solution incurs a cost (Gateway-required VNet Integration...When you connect directly to VNet in other regions or to a classic virtual network in the same region, you need an Azure Virtual Network gateway provisioned in the target VNet.)
 upvoted 8 times

 **RandomUser** 2 years, 3 months ago

But don't forget VNet integration is only available from Premium onwards. That might also be quite an increase in cost.
 upvoted 2 times

 **RandomUser** 2 years, 3 months ago

My bad, VNet integration is already available in smaller SKUs as well. I fucked up this question in the exam so I thought I'd better fix my comment here.
 upvoted 19 times


 **breakpoint0815** Most Recent 10 months ago

Selected Answer: B

Answer D suggests creating a gateway subnet and deploying a virtual network gateway, which is used for connecting virtual networks across different regions or connecting to on-premises networks. While it would provide access to resources in Vnet1, it would incur additional costs and is not necessary for connecting an App Service app to a virtual network in the same region. Therefore, creating a new subnet (answer B) is the correct and more cost-effective solution in this scenario.
 upvoted 1 times

 **samir111** 11 months, 2 weeks ago

B should be the answer
 upvoted 1 times

 **ragav21** 1 year, 3 months ago

Selected Answer: B

B should be the right answer
 upvoted 1 times

 **sapien45** 1 year, 3 months ago

Selected Answer: B

Virtual network integration gives your app access to resources in your virtual network, but it doesn't grant inbound private access to your app from the virtual network. Private site access refers to making an app accessible only from a private network, such as from within an Azure virtual network. Virtual network integration is used only to make outbound calls from your app into your virtual network.
 Regional virtual network integration: When you connect to virtual networks in the same region, you must have a dedicated subnet in the virtual

network you're integrating with.
The virtual network integration feature:

Requires a supported Basic or Standard, Premium, Premium v2, Premium v3, or Elastic Premium App Service pricing tier.
upvoted 3 times

🗨️ **wetraining123** 1 year, 5 months ago

it should be B.
Create a subnet and Integrate it with the App1
upvoted 1 times

🗨️ **Pradh** 1 year, 3 months ago

existing subnet already seems empty. why need new subnet ?
upvoted 1 times

🗨️ **Jamesat** 1 year, 5 months ago

Selected Answer: B

B is correct as the resources are in the same region.

Why would you even think about a VPN gateway? Odd answer. Exam Topics should review this one!
upvoted 1 times

🗨️ **Goseu** 1 year, 6 months ago

Selected Answer: B

Answer is B
upvoted 2 times

🗨️ **rac_sp** 1 year, 6 months ago

Selected Answer: B

create a new subnet because both resources are in the same region, no need to a gateway that is only required when resources are in different regions.
upvoted 5 times

🗨️ **Pradh** 1 year, 3 months ago

existing subnet already seems empty. why need new subnet ?
upvoted 1 times

🗨️ **rac_sp** 1 year, 6 months ago

Selected Answer: B

In the same region there is no need of a Virtual Network Gateway
upvoted 3 times

🗨️ **zerocool114** 1 year, 6 months ago

on exam today, answer B
upvoted 1 times

🗨️ **unclegrandfather** 1 year, 7 months ago

Appeared on exam Jun/28/22
upvoted 2 times

🗨️ **kinder2** 1 year, 7 months ago

Selected Answer: B

"B"
Regional virtual network integration supports connecting to a virtual network in the same region and doesn't require a gateway.
<https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration#regional-virtual-network-integration>
upvoted 2 times

🗨️ **Pradh** 1 year, 3 months ago

existing subnet already seems empty. why need new subnet ?
upvoted 1 times

🗨️ **borekbp** 1 year, 10 months ago

but there is info in question that you have already one subnet, can we use it for gateway or vnet-integration? why create new one?
upvoted 1 times

🗨️ **Payday123** 1 year, 7 months ago

Because we need to provide access to resources in this one subnet. If this subnet is integrated with App Service we will not be able to create any other resources
upvoted 1 times

🗨️ **rockethack** 1 year, 11 months ago

This question was on the exam on 18th Feb 2022.
upvoted 1 times

🗨️ **nitinkumarmca** 1 year, 11 months ago

Selected Answer: B

Subnet as it doesn't incur additional cost. VPN Gateway is required for cross region integration or Classic VNET in same region.
upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com. The subscription contains the following resources:

- ☞ An Azure App Service app named App1
- ☞ An Azure DNS zone named contoso.com
- ☞ An Azure private DNS zone named private.contoso.com
- ☞ A virtual network named Vnet1

You create a private endpoint for App1. The record for the endpoint is registered automatically in Azure DNS.

You need to provide a developer with the name that is registered in Azure DNS for the private endpoint.

What should you provide?

- A. app1.contoso.onmicrosoft.com
- B. app1.private.contoso.com
- C. app1.privatelink.azurewebsites.net
- D. app1.contoso.com

Correct Answer: C

Community vote distribution

C (83%)

B (17%)

 **Sahildange** Highly Voted 2 years, 3 months ago

When you use Private Endpoint for Web App, the requested URL must match the name of your Web App. By default mywebappname.azurewebsites.net.

By default, without Private Endpoint, the public name of your web app is a canonical name to the cluster. For example, the name resolution will be:

DNS
Name Type Value
mywebapp.azurewebsites.net CNAME clustername.azurewebsites.windows.net
clustername.azurewebsites.windows.net CNAME cloudservicename.cloudapp.net
cloudservicename.cloudapp.net A 40.122.110.154

When you deploy a Private Endpoint, we update the DNS entry to point to the canonical name mywebapp.privatelink.azurewebsites.net. For example, the name resolution will be:

DNS
Name Type Value Remark
mywebapp.azurewebsites.net CNAME mywebapp.privatelink.azurewebsites.net
mywebapp.privatelink.azurewebsites.net CNAME clustername.azurewebsites.windows.net
clustername.azurewebsites.windows.net CNAME cloudservicename.cloudapp.net
cloudservicename.cloudapp.net A 40.122.110.154 <https://docs.microsoft.com/en-us/azure/app-service/networking/private-endpoint> Hence answer is C

upvoted 16 times

 **GohanF2** 1 year, 2 months ago

Well explained
upvoted 2 times

 **ExamTopics2_EIS** Most Recent 2 months, 3 weeks ago

Wow, if this is true that means the App name would have to be globally unique.
upvoted 1 times

 **AzureLearner01** 10 months, 2 weeks ago

For me the provided answer is correct. I've done a few tests in the lab and we only need to provide the dns record that is registered automatically in DNS to the developer. this is app1.privatelink.azurewebsite.net. My first opinion was app1.azurewebsites.net (which is not existing) that would be translated to app1.privatelink.azurewebsite.net. By default the app is not registered in the "custom" private DNS Zone private.contoso.com. It is auto registered only in privatelink.azurewebsites.net. I'm not 100% sure but i don't think there is no way to not register it in the privatelink.azurewebsites.net and instead register it in private.contoso.com by default.

upvoted 1 times

 **samir111** 11 months, 2 weeks ago

Selected Answer: C

C is correct
upvoted 1 times

 **DeepMoon** 1 year ago

Be mindful of group think; making you see this the wrong way and voting for the wrong answer. @zenithcsa1 pointed to the correct answer. Use the same connection string to connect to your App Configuration store using private endpoints as you would use for a public endpoint. Don't connect to the store using its privatelink subdomain URL.

<https://learn.microsoft.com/en-us/azure/azure-app-configuration/concept-private-endpoint#connecting-to-private-endpoints>
upvoted 1 times

🗨️ **Skankhunt** 12 months ago

The link you provided is specifically for Azure App Configuration.

Rather use the below article:

<https://learn.microsoft.com/en-us/azure/app-service/networking/private-endpoint>

upvoted 1 times

🗨️ **TJ001** 1 year ago

yes it does not connect with private end point URL.. however there is no better option in the available list. I dont agree with option B unless there is custom domain created for the App Service it does not make sense.. This question should have been phrased better.

upvoted 1 times

🗨️ **mingorad** 1 year, 4 months ago

C is correct

Expl : <https://learn.microsoft.com/en-us/azure/app-service/networking/private-endpoint>

"When you deploy a Private Endpoint, we update the DNS entry to point to the canonical name mywebapp.privatelink.azurewebsites.net."

"

upvoted 1 times

🗨️ **zenithcsa1** 1 year, 4 months ago

Selected Answer: B

Not sure what's the purpose of giving name to developers. Just be aware that you can NOT connect to the App Service through xxx.privatelink.azurewebsite.net. Azure DNS uses the name, not us.

<https://docs.microsoft.com/en-us/azure/azure-app-configuration/concept-private-endpoint#connecting-to-private-endpoints>

upvoted 1 times

🗨️ **phoenix14** 1 year, 1 month ago

Key to this question here is you need to provide hostname registered in Azure DNS and not your private zone. Hence answer is C.

upvoted 1 times

🗨️ **pinchocr** 1 year, 7 months ago

Selected Answer: C

Correct

upvoted 1 times

🗨️ **rockethack** 1 year, 11 months ago

This question was on the exam on 18th Feb 2022.

upvoted 1 times

🗨️ **Kimimoto** 1 year, 11 months ago

Appeared in exam on 11/Feb/2022

upvoted 1 times

🗨️ **kjfdzkkbsm** 1 year, 11 months ago

Selected Answer: C

From the docs: When you deploy a Private Endpoint, we update the DNS entry to point to the canonical name mywebapp.privatelink.azurewebsites.net.

<https://docs.microsoft.com/en-us/azure/app-service/networking/private-endpoint#dns>

upvoted 3 times

🗨️ **Contactforitish** 2 years ago

Appeared in exam on 17/01/2022 and I ended up putting A instead :(

upvoted 1 times

🗨️ **Pravda** 2 years ago

Much more complicated variant on the exam 1/6/2022

upvoted 3 times

🗨️ **AidenYoukhana** 2 years ago

Answer: app1.privatelink.azurewebsites.net

upvoted 3 times

🗨️ **dpinlaguna** 2 years, 3 months ago

<https://docs.microsoft.com/en-us/learn/modules/introduction-azure-private-link/3-how-azure-private-link-works>:

Clients that connect to a Private Link resource don't need to use the Private Endpoint's assigned IP address in the connection string. Instead, if you configure the Private Endpoint to integrate with your private DNS zone, then Azure automatically assigns a FQDN to the endpoint. For example, if the Private Link resource is an Azure Storage table, the FQDN will be something like mystorageaccount1234.table.core.windows.net.

upvoted 3 times

🗨️ 👤 **Bharat** 2 years, 3 months ago

Correct answer is A not C, i.e., app1.contoso.onmicrosoft.com
upvoted 1 times

🗨️ 👤 **christianpageqc** 2 years, 3 months ago

VNet DNS auto-registration won't create any DNS for private link according to this article : <https://docs.microsoft.com/en-us/azure/dns/private-dns-autoregistration#restrictions>

"Auto registration works only for virtual machines"

As for private link auto DNS, it seems bound to public Microsoft domains.. I think we would need to deploy DNS forwarder and CNAME to resolve something other than A.

upvoted 4 times

🗨️ 👤 **Bharat** 2 years, 3 months ago

So what should be the answer then?

upvoted 1 times

🗨️ 👤 **Bharat** 2 years, 3 months ago

Given answer is correct and I was wrong. @christianpageqc, thanks for the thoughtful answer. Here is an article that helped me clarify the answer: <https://blog.baeke.info/2021/06/22/azure-app-services-with-private-link/>

upvoted 2 times

🗨️ 👤 **Prutser2** 1 year, 3 months ago

great link, well explained!

upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

You have Azure App Service apps in the West US Azure region as shown in the following table.

Name	App Service Plan	Number of instances
App1	ASP1	3
App2	ASP1	3
App3	ASP2	2
App4	ASP3	1

You need to ensure that all the apps can access the resources in a virtual network named VNet1 without forwarding traffic through the internet.

How many integration subnets should you create?

- A. 0
- B. 1
- C. 3
- D. 4
- E. 6

Correct Answer: C

One integration subnet is required per App Service Plan regardless of how many apps are running in the App Service Plan.

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration>

Community vote distribution

C (100%)

 **pinchocr** Highly Voted 1 year, 7 months ago

Selected Answer: C

one per App Service Plan: The feature supports only one virtual interface per worker. One virtual interface per worker means one regional virtual network integration per App Service plan. All the apps in the same App Service plan can only use the same virtual network integration to a specific subnet. If you need an app to connect to another virtual network or another subnet in the same virtual network, you need to create another App Service plan. The virtual interface used isn't a resource that customers have direct access to.

<https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration#how-regional-virtual-network-integration-works>

upvoted 9 times

 **Murad01** Most Recent 1 month, 3 weeks ago

Appeared on Exam November - 2023

upvoted 2 times

 **Opala79** 2 months, 3 weeks ago


I select option D-4, because although app1 and app2 use the same app service plan, I have to create the integration in each webapp

upvoted 1 times

 **TJ001** 1 year ago

one per App Service Plan make sense..multiple apps with in the same plan can use the same subnet provided it has enough IP space....I will go with C


upvoted 3 times

 **jkklm** 1 year, 9 months ago

all azure app service apps in the same region, so we use regional virtual network integration.


All the apps in the same App Service plan can only use the same virtual network integration to a specific subnet. If you need an app to connect to another virtual network or another subnet in the same virtual network, you need to create another App Service plan

upvoted 1 times

 **jkklm** 1 year, 9 months ago

therefore 3 subnets = C

upvoted 3 times

 **FabioS** 1 year, 9 months ago

Subnet requirements

Virtual network integration depends on a dedicated subnet. When you create a subnet, the Azure subnet loses five IPs from the start. One address is used from the integration subnet for each plan instance. If you scale your app to four instances, then four addresses are used. Answer = D
upvoted 1 times

🗨️ 👤 **pinpin06** 1 year, 9 months ago

there is 3 plan instances ASP1, ASP2, ASP3, I would say this is response C
upvoted 3 times

🗨️ 👤 **sapien45** 1 year, 3 months ago

That is some weird logic here. If you need an app to connect to another virtual network or another subnet in the same virtual network, you need to create another App Service plan
 $1+1+1=3$
upvoted 1 times

店铺: IT认证考试服务

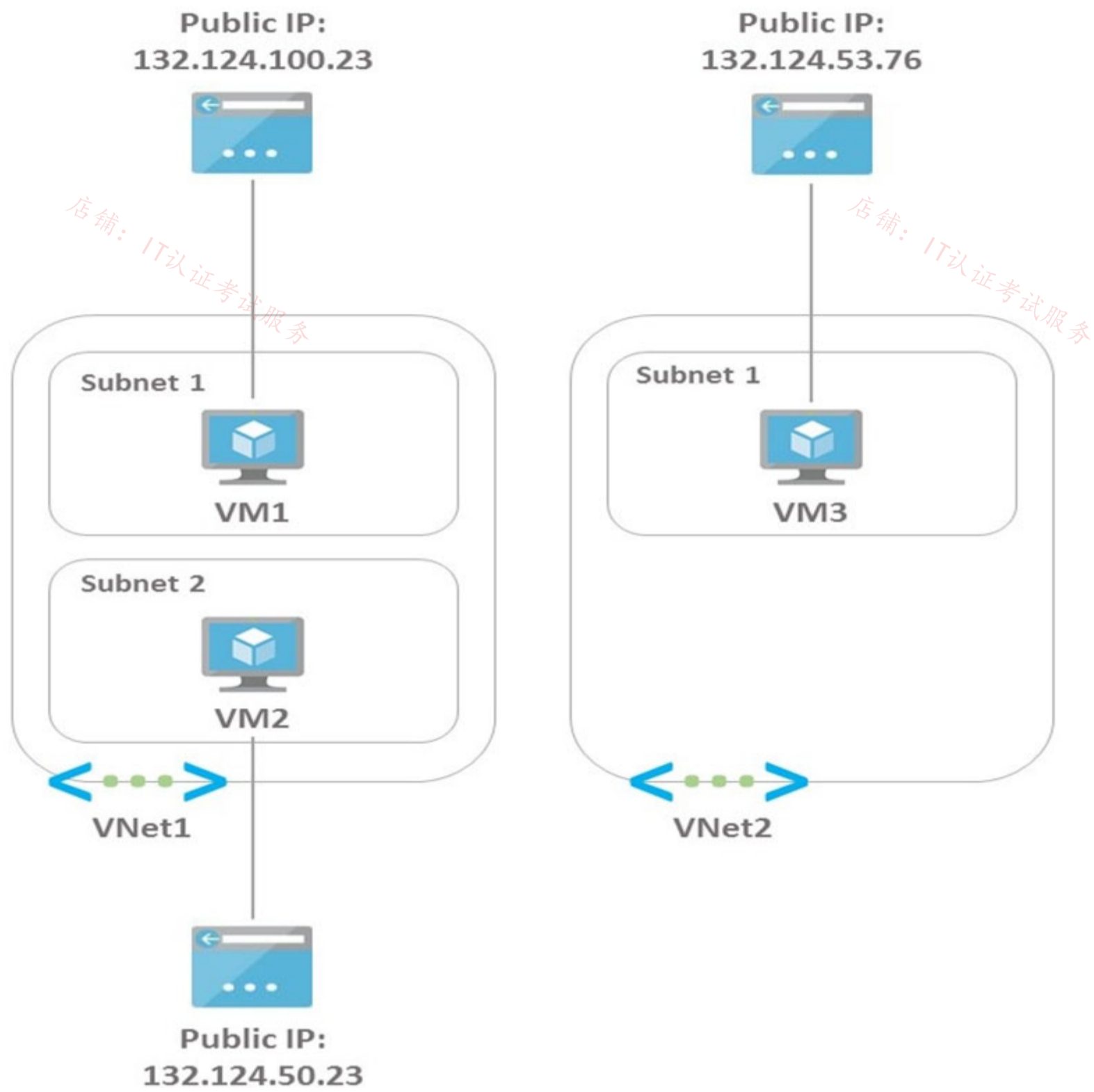
店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT -

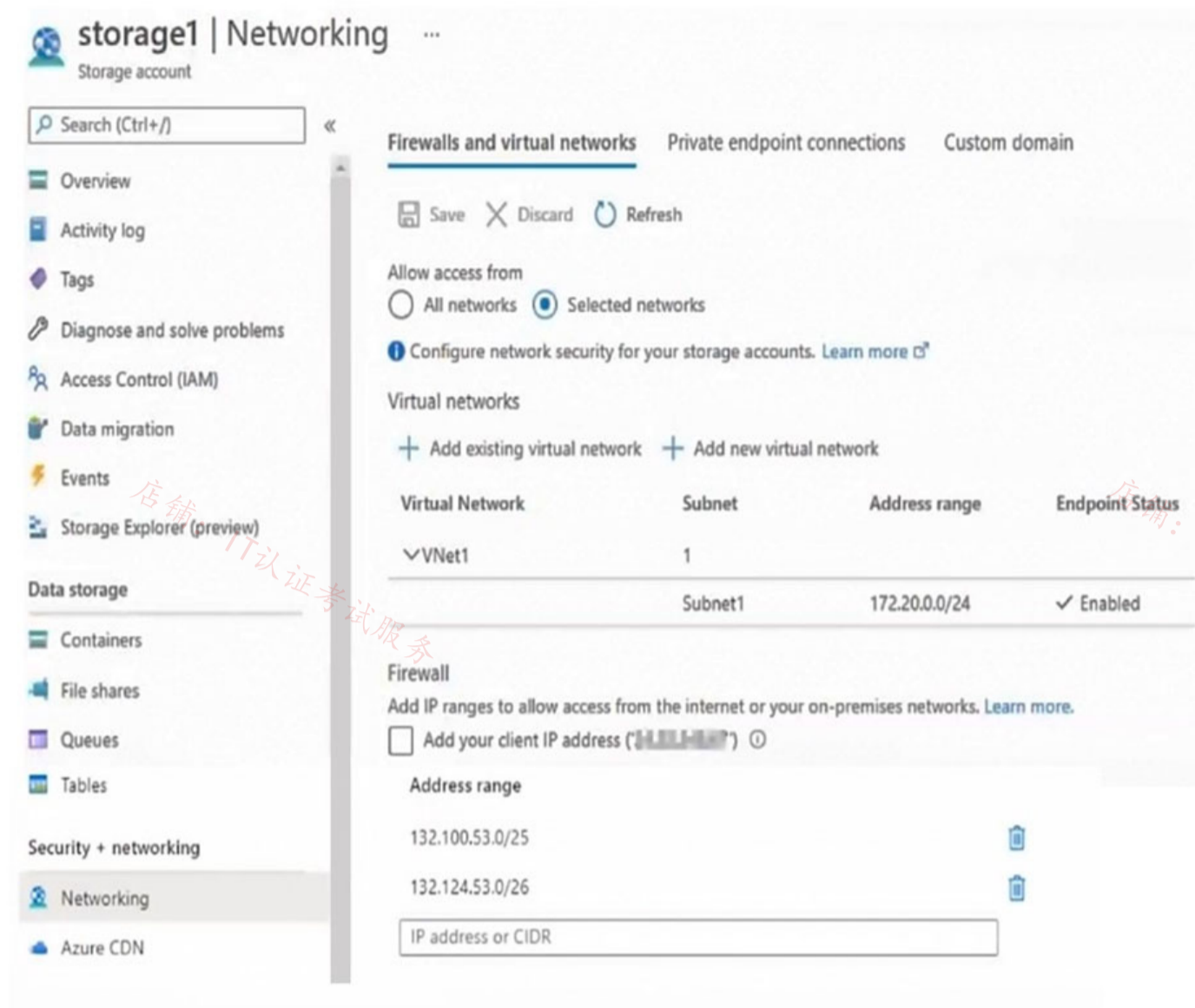
You have the Azure environment shown in the Azure Environment exhibit.



The settings for each subnet are shown in the following table.

Subnet	Service endpoint
Vnet1/Subnet1	Storage
Vnet1/Subnet2	Storage
Vnet2/Subnet1	None

The Firewalls and virtual networks settings for storage1 are configured as shown in the Storage1 exhibit.



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
VM1 can access storage1.	<input type="radio"/>	<input type="radio"/>
VM2 can access storage1 by using a service endpoint.	<input type="radio"/>	<input type="radio"/>
VM3 can access storage1 by using the public IP address.	<input type="radio"/>	<input type="radio"/>

店铺: IT认证考试服务

店铺: IT认证考试服务

Correct Answer:

Answer Area

Statements	Yes	No
VM1 can access storage1.	<input checked="" type="radio"/>	<input type="radio"/>
VM2 can access storage1 by using a service endpoint.	<input type="radio"/>	<input checked="" type="radio"/>
VM3 can access storage1 by using the public IP address.	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: Yes -

The firewall allows VNet1\Subnet1 through the service endpoint.

Box 2: No -

The firewall does not allow VNet1\Subnet2 through the service endpoint.

Box 3: No -

The firewall allows 132.124.53.0/26 which means it allows all IP addresses between 132.124.53.0 and 132.124.53.63. The public IP of VM3 is 132.124.53.76 which is outside the allowed range.

 **Jamesat** Highly Voted 1 year, 5 months ago

Correct tested in my lab.

Yes, No, No

For question 2 Subnet2 has a service endpoint but is not present in the Firewall settings so would be denied.

upvoted 22 times

 **Goofer** 1 year ago

IP network rules can't be used in the following cases:


To restrict access to clients in same Azure region as the storage account.

IP network rules have no effect on requests originating from the same Azure region as the storage account. Use Virtual network rules to allow same-region requests.

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

Yes, Yes, No

upvoted 2 times

 **flurgen248** 10 months, 1 week ago

I think it's Yes, No, No.

IP network rules have no effect on requests originating from the same Azure region as the storage account. Use Virtual network rules to allow same-region requests.

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

The service endpoint routes traffic from the VNet through an optimal path to the Azure Storage service. Administrators can then configure network rules for the storage account that allow requests to be received from specific subnets in a VNet.

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

If you look at the storage1 networking image, there are separate sections for IP addresses and virtual networks. The section with IP addresses is the "IP Network rules" section, but since it's also using the "Virtual Network" section then you can only access storage1 using service endpoints that are explicitly listed.

upvoted 2 times

 **JulienYork** Highly Voted 1 year, 8 months ago

Box 1: Yes -

The firewall allows VNet1\Subnet1 through the service endpoint.

This is wrong in the answer

Box 2: YES

It is already accessing with service endpoint no need to access via firewall

Box 3: No -

The firewall allows 132.124.53.0/26 which means it allows all IP addresses between 132.124.53.0 and 132.124.53.63. The public IP of VM3 is 132.124.53.76 which is outside the allowed range.

upvoted 12 times

  **jellybiscuit** 1 year, 3 months ago

I would agree with you if we were discussing private endpoints, as they bypass public access and firewall rules. Service Endpoints do not. VM2 can pass through subnet 1 to get to the endpoint, but its source address is still subnet 2 which has not been granted access on the storage account.

If a storage account has a Private Endpoint and no rules you can connect to it.

If a storage account has a Service Endpoint and no rules you cannot connect to it.

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

"You can enable a Service endpoint for Azure Storage within the VNet. The service endpoint routes traffic from the VNet through an optimal path to the Azure Storage service. The identities of the subnet and the virtual network are also transmitted with each request. Administrators can then configure network rules for the storage account that allow requests to be received from specific subnets in a VNet. Clients granted access via these network rules must continue to meet the authorization requirements of the storage account to access the data."

upvoted 12 times

  **sapien45** 1 year, 3 months ago

YYN, I concur

upvoted 3 times

  **sapien45** 1 year, 3 months ago



I stand corrected by jellybiscuit YNN

upvoted 6 times

  **Ajdlfasudfo** 1 year, 1 month ago

you better go do AZ-900. seems to be more fitting your skill level

upvoted 1 times

  **Takloy** 1 year, 1 month ago

the fact that you're using dumps to review is also not something to be proud of. everybody here is an AZ900 skill level.

upvoted 6 times

  **Lazylinux** Most Recent 1 month, 1 week ago

For sure YNN as per below from MS Doco

Virtual network service endpoints are public and accessible via the internet. The Azure Storage firewall provides the ability to control access to your storage account over such public endpoints. When you enable public network access to your storage account, all incoming requests for data are blocked by default. Only applications that request data from allowed sources that you configure in your storage account firewall settings will be able to access your data. Sources can include the source IP address or virtual network subnet of a client, or an Azure service or resource instance through which clients or services access your data. Requests that are blocked include those from other Azure services, from the Azure portal, and from logging and metrics services, unless you explicitly allow access in your firewall configuration.

continued next ==>

upvoted 1 times

  **Lazylinux** 1 month, 1 week ago

A private endpoint uses a private IP address from your virtual network to access a storage account over the Microsoft backbone network. With a private endpoint, traffic between your virtual network and the storage account are secured over a private link. Storage firewall rules only apply to the public endpoints of a storage account, not private endpoints. The process of approving the creation of a private endpoint grants implicit access to traffic from the subnet that hosts the private endpoint

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

Also during my testing i noticed the following, if i ADD vNET and chose subnet, the process will automatically create Service-Endpoint and hence having SEP doesnt mean you automatically granted access unless you are in the allow list of the FW otherwise Private Endpoint is ONLY way to bypass the FW

upvoted 1 times

  **Murad01** 1 month, 3 weeks ago

Appeared on Exam November- 2023

upvoted 1 times

  **azure_dori** 5 months, 1 week ago

Can somebody address the elephant in the room? VM1's IP address is 132.124.100.23. It doesn't belong to 132.100.53.0/25. Moreover, it doesn't belong to 132.124.53.0/26 either. How? Or rather WHY it has access to storage1?

upvoted 2 times

  **mabalon** 5 months ago

The subnet1 is allowed, check the config of the Storage networking

upvoted 2 times

  **TJ001** 1 year ago

Agree with Yes No No

upvoted 5 times

🗨️ **chatlisi** 1 year ago

According this, it should be Y, Y, N

"With service endpoints, the source IP addresses of the virtual machines in the subnet for service traffic switches from using public IPv4 addresses to using private IPv4 addresses. Existing Azure service firewall rules using Azure public IP addresses will stop working with this switch."

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

upvoted 1 times

🗨️ **_fvt** 9 months, 3 weeks ago

Yes you are well explaining why the public allowed IP range will not allow the connection from VM2 and why the private IP addresses from VNet1/Subnet2 should be allowed instead (only VNet1/subnet1 is allowed if you look on the storage account configuration)

So, Y,N,N.

upvoted 1 times

🗨️ **unclegrandfather** 1 year, 7 months ago

A version of this appeared on the exam Jun/28/22. Make sure you understand the concepts here

upvoted 2 times

🗨️ **pinchocr** 1 year, 7 months ago

You cannot filter public IPs when the vnet and the storage accounts are in the same regions. The answer is correct YES-NO-NO

upvoted 5 times

🗨️ **Jun_AZ500** 1 year, 7 months ago

Correct me if I'm wrong on Q2, the answer still No according to this

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

IP network rules can't be used in the following cases:

To restrict access to clients in same Azure region as the storage account.

IP network rules have no effect on requests originating from the same Azure region as the storage account. Use Virtual network rules to allow same-region requests.

upvoted 1 times

🗨️ **jpetix** 1 year, 8 months ago

But the Firewall in question is on the Service endpoint, and it only allows Vnet1, Subnet1.

upvoted 1 times

🗨️ **wsrudmen** 1 year, 8 months ago

It's YES-YES-NO

But I'm disagree with you Julien for Box2.

VM2 is in Subnet2 that is not linked to the storage account like Subnet1.

So VM2 can only access through Internet using its public IP. And in The Firewall table VM2 is allowed.

NB: Please correct me if I'm wrong

upvoted 2 times

🗨️ **Payday123** 1 year, 7 months ago

Question is if it access using service endpoint not public IP

upvoted 3 times

店铺: IT认证考试服务

店铺: IT认证考试服务

DRAG DROP -

You have two Azure subscriptions named Subscription1 and Subscription2. Subscription1 contains a virtual network named Vnet1. Vnet1 contains an application server. Subscription2 contains a virtual network named Vnet2.

You need to provide the virtual machines in Vnet2 with access to the application server in Vnet1 by using a private endpoint.

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.

Select and Place:

Actions

In Subscription 1, accept the private endpoint connection request.

In Subscription 1, create a private link service and attach the service to the frontend IP configuration of the load balancer.

Enable virtual network peering between Vnet1 and Vnet2.

Deploy an Azure Standard Load Balancer in front of the application server.

In Subscription 2, create a private endpoint by using the private link service.

Answer Area



Correct Answer:

Actions

Enable virtual network peering between Vnet1 and Vnet2.

Answer Area

Deploy an Azure Standard Load Balancer in front of the application server.

In Subscription 1, create a private link service and attach the service to the frontend IP configuration of the load balancer.

In Subscription 2, create a private endpoint by using the private link service.

In Subscription 1, accept the private endpoint connection request.



Step 1: Deploy an Azure Load Balancer in front of the application server

Configure your application to run behind a standard load balancer in your virtual network.

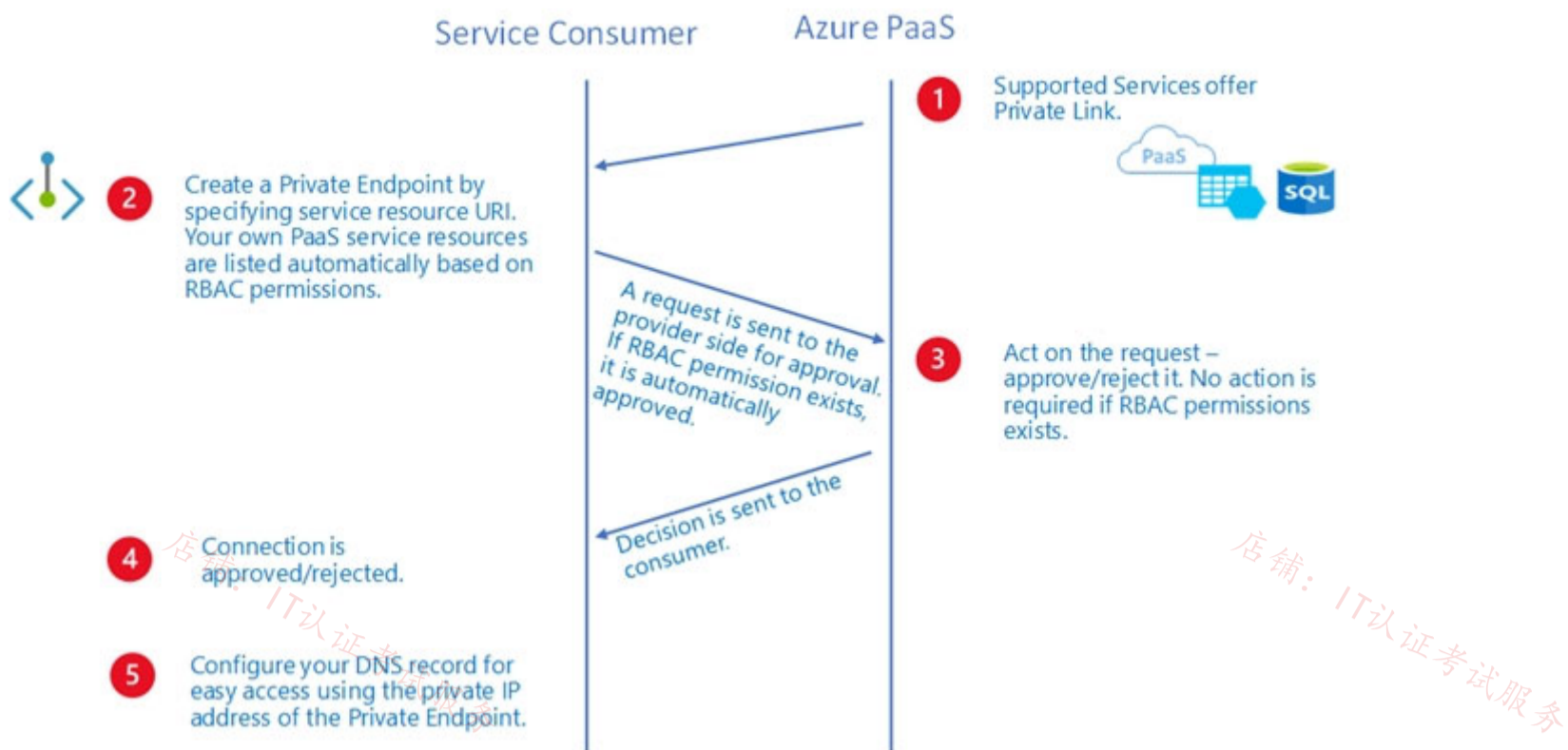
Step 2: In Subscription 1, create a private link service and attach the service to the frontend IP configuration of the load balancer.

Create a Private Link Service referencing the load balancer above.

Step 3: In Subscription 2, create a private endpoint by using the private link service.

Private Link service can be accessed from approved private endpoints in any public region. The private endpoint can be reached from the

same virtual network, regionally peered VNets, globally peered VNets and on premises using private VPN or ExpressRoute connections.



Step 4: In Subscription1, accept the private endpoint connection request.

Network connections can be initiated only by clients that are connecting to the private endpoint.

Not:

Incorrect: Enable virtual network peering between Vnet1 and Vnet2.

Reference:

<https://docs.microsoft.com/en-us/azure/private-link/private-link-service-overview> <https://docs.microsoft.com/en-us/azure/private-link/private-endpoint-overview>

jellybiscuit (Highly Voted) 1 year, 3 months ago

I spent the entire time wondering why I'm creating a load balancer. Finally realized it's an "application server" and not an "app service"

Answer is correct.
upvoted 12 times

TJ001 (Most Recent) 1 year ago

Answer is correct
Please not peering is not required .. the whole point of Private Link is to provide connectivity without peering..
upvoted 1 times

alexGv 1 year, 1 month ago

I seeing something a little confused, maybe the question itself is "wrong" because how is possible to use a LoadBalancer that I assume as "Internal" to publish a Private Endpoint "attaching the service private IP of the Private Endpoint as frontend IP of the Load Balancer" and not "as the Backend pool of it".
Then why we need a NLB if the Private Endpoint itself is capable to "hear" connections through his own private IP address"
Can somebody else try to explain me...Thanks!
upvoted 1 times

alexGv 1 year, 1 month ago

Sorry, reviewed,
<https://learn.microsoft.com/en-us/azure/private-link/private-link-service-overview#workflow>
upvoted 1 times

GohanF2 1 year, 2 months ago

Answer is correct.
upvoted 1 times

ragav21 1 year, 3 months ago

Why is peering not sufficient ?
upvoted 2 times

tfkfk 8 months ago

we use private link service to avoid ips overlap
upvoted 1 times

Leib 1 year, 3 months ago

it is but, you need to use private endpoint.
upvoted 4 times

Cristoicach91 1 year, 4 months ago

correct

upvoted 4 times

店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com. The subscription contains the following resources:

- ☞ A virtual network named Vnet1
- ☞ An App Service plan named ASP1
- ☞ An Azure App Service named webapp1

An Azure private DNS zone named private.contoso.com

- ☞ Virtual machines on Vnet1 that cannot communicate outside the virtual network

You need to ensure that the virtual machines on Vnet1 can access webapp1 by using a URL of <https://www.private.contoso.com>.

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

NOTE: Each correct selection is worth one point.

- A. Create a CNAME record that maps www.private.contoso.com to webapp1.contoso.onmicrosoft.com.
- B. Create a CNAME record that maps www.private.contoso.com to webapp1.private.contoso.com.
- C. Create a service endpoint for webapp1.
- D. Register an enterprise application in Azure AD for webapp1.
- E. Create a private endpoint for webapp1.
- F. Create a CNAME record that maps www.private.contoso.com to webapp1.privatelink.azurewebsites.net.

Correct Answer: EF

E: You can use private DNS zones to override the DNS resolution for a private endpoint. A private DNS zone can be linked to your virtual network to resolve specific domains.

When you use Private Endpoint for Web App, the requested URL must match the name of your Web App. When you deploy a Private Endpoint, we update the

DNS entry to point to the canonical name mywebapp.privatelink.azurewebsites.net. For example, the name resolution will be (Name, Type, Value): mywebapp.azurewebsites.net CNAME mywebapp.privatelink.azurewebsites.net

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/networking/private-endpoint>

Community vote distribution

EF (100%)

🗳️ 👤 **Lazylinux** 3 months, 1 week ago

Selected Answer: EF

EF are correct as per answer - outbound from App Services to vNET requires vNET integration where as inbound i.e. from vNET to App services requires private endpoint

upvoted 1 times

🗳️ 👤 **TJ001** 1 year ago

EF, only assumption custom domain is added for App Service already

upvoted 3 times

🗳️ 👤 **Prutser2** 1 year, 3 months ago

Selected Answer: EF

correct

upvoted 2 times

🗳️ 👤 **jellybiscuit** 1 year, 3 months ago

Selected Answer: EF

correct

upvoted 1 times

🗳️ 👤 **StephenKDS** 1 year, 4 months ago

Selected Answer: EF

correct - makes sense

upvoted 1 times

You have an Azure Front Door instance named FD1 that is protected by using Azure Web Application Firewall (WAF).

FD1 uses a frontend host named app1.contoso.com to provide access to Azure web apps hosted in the East US Azure region and the West US Azure region.

You need to configure FD1 to block requests to app1.contoso.com from all countries other than the United States.

What should you include in the WAF policy?

- A. a custom rule that uses a match rule
- B. a frontend host association
- C. a custom rule that uses a rate limit rule
- D. a managed rule set

Correct Answer: A

Community vote distribution

A (100%)

 **StephenKDS** Highly Voted 1 year, 4 months ago

*hast = host

upvoted 11 times

 **sapien45** Highly Voted 1 year, 3 months ago

Selected Answer: A

Custom rules allow you to create tailored rules to suit the exact needs of your applications and security policies. Now, you can restrict access to your web applications by country/region. As with all custom rules, this logic can be compounded with other rules to suit the needs of your application.

To create a geo-filtering custom rule in the Azure portal, simply select Geo location as the Match Type, and then select the country/region or countries/regions you want to allow/block from your application.

upvoted 6 times

 **omgMerrick** Most Recent 11 months, 1 week ago

Selected Answer: A

Answer is correct.

A. a custom rule that uses a match rule

Source:

<https://learn.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-geo-filtering>

upvoted 1 times

You are planning the IP addressing for the subnets in Azure virtual networks.

Which type of resource requires IP addresses in the subnets?

- A. Azure DDoS Protection for virtual networks
- B. private endpoints
- C. Azure Virtual Network NAT
- D. service endpoint policies

Correct Answer: B

Community vote distribution

B (100%)

 **Lazylinux** 3 months, 1 week ago

Selected Answer: B

B is Honey

upvoted 2 times

 **omgMerrick** 11 months, 2 weeks ago

Selected Answer: B

B. private endpoints

Private endpoints require IP addresses in the subnets. Other resources such as Azure DDoS Protection for virtual networks, Azure Virtual Network NAT, and service endpoint policies do not require IP addresses in the subnets.

upvoted 3 times

 **lambdaCarre** 1 year ago

Private endpoint is the correct answer. Indeed each private endpoint is associated with a network interface card which has a private IP

upvoted 3 times

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

Name	Type	Description
VNet1	Virtual network	Contains two subnets named Subnet1 and Subnet2
VM1	Virtual machine	Connected to Subnet1
azsql1	Azure SQL Database logical server	Has a private endpoint on Subnet2

You need to ensure that the apps hosted on VM1 can resolve the IP address of the private endpoint for azsql1.database.windows.net.

What should you create first?

- A. a public DNS zone named database.windows.net
- B. a private DNS zone named database.windows.net
- C. a public DNS zone named privatelink.database.windows.net
- D. a private DNS zone named privatelink.database.windows.net

Correct Answer: D

Community vote distribution

D (100%)

 **omgMerrick** Highly Voted 11 months, 2 weeks ago

Selected Answer: D

Answer is correct.

D. a private DNS zone named privatelink.database.windows.net

The private link resource type is a SQL database, therefore the recommended private DNS zone name is privatelink.database.windows.net.

Source:

<https://learn.microsoft.com/en-us/azure/private-link/private-endpoint-dns#azure-services-dns-zone-configuration>

upvoted 5 times

 **mabalon** Most Recent 5 months ago

As the documentarion says "To configure properly, you need the following resources:"

- 1.- Client virtual network
- 2.- Private DNS zone privatelink.database.windows.net with type A record
- 3.- Private endpoint information (FQDN record name and private IP address)

Reference: <https://learn.microsoft.com/en-us/azure/private-link/private-endpoint-dns#virtual-network-workloads-without-custom-dns-server>

upvoted 1 times

 **JennyHuang36** 11 months, 1 week ago

In exam Feb, 2023

upvoted 3 times

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

Name	Type	Description
VNet1	Virtual network	Contains a subnet named Subnet1
storage1	Storage account	None
VM1	Virtual machine	Linked to Subnet1
VM2	Virtual machine	Linked to Subnet1

You need to ensure that VM1 and VM2 can connect only to storage1. The solution must meet the following requirements:

- Prevent VM1 and VM2 from accessing any other storage accounts
- Ensure that storage1 is accessible from the internet.

What should you use?

- A. a network security group (NSG)
- B. a service endpoint policy
- C. a private link
- D. a private endpoint

Correct Answer: B

Community vote distribution

B (77%) A (15%) 8%

 **omgMerrick** Highly Voted 11 months, 2 weeks ago

Selected Answer: B

Answer appears to be correct.

B. a service endpoint policy

Virtual Network (VNet) service endpoint policies allow you to filter egress virtual network traffic to Azure Storage accounts over service endpoint, and allow data exfiltration to only specific Azure Storage accounts. Endpoint policies provide granular access control for virtual network traffic to Azure Storage when connecting over service endpoint.

Source:

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoint-policies-overview>

upvoted 8 times

 **roshingrg** Highly Voted 8 months ago

B. a service endpoint policy

A service endpoint policy can be used to control the access to Azure Storage accounts from virtual networks. By creating a service endpoint policy, you can specify which storage accounts are allowed to be accessed from the virtual network, while blocking access to other storage accounts.

In this case, you can create a service endpoint policy that allows access to storage1 and associate it with the virtual network containing VM1 and VM2. This will ensure that VM1 and VM2 can only connect to storage1 and will be prevented from accessing any other storage accounts.

Additionally, to ensure that storage1 is accessible from the internet, you can configure the storage account's networking settings to allow public access. This can be done by enabling the appropriate settings such as allowing public access to blobs or enabling a public endpoint.

Using a network security group (NSG) would not provide the required granular control over specific storage accounts. A private link or private endpoint would enable private access to the storage account but would not allow access from the internet, which is a requirement in this scenario. Therefore, the best option is to use a service endpoint policy.

upvoted 6 times

 **am156** Most Recent 2 weeks ago

Selected Answer: D

I believe the answer is D - Private Endpoint.

Options A (network security group), B (service endpoint policy), and C (private link) are also Azure networking features, but they may not provide the same level of isolation and control over the specific access requirements described in the scenario. Private endpoint is specifically designed to enable private connectivity to Azure services over a private IP address.

By using private endpoints for storage1, you can ensure that VM1 and VM2 can connect to storage1 using the private endpoint while preventing them from accessing other storage accounts.

upvoted 1 times

🗨️ 👤 **Lazylinux** 3 months, 1 week ago

Selected Answer: B

B is Honey

For sure B as if NSG is used can only be used with AZ service tags and that will include all storage accounts and cannot differentiate and hence either allow to all storage account or deny all

Where as SE policy you can use a resource in SCOPE of SINGLE account in this case 1 storage account or in RG or subscription based then you associate a subnet to the resource in this case the subnet 1 where VMs reside

upvoted 2 times

🗨️ 👤 **tomtom2022** 8 months, 4 weeks ago

Selected Answer: A

The answer is A.

NSG only can filter whether the VMs can access the storage accounts via the service tag, but can't filter which storage account can be accessed.

upvoted 1 times

🗨️ 👤 **MrBlueSky** 9 months, 2 weeks ago

Selected Answer: A

I believe the answer is A. NSG

Storage accounts are accessible from the internet by default so all we need to worry about is restricting the VMs access to all other storage accounts. This is only doable with an NSG from the options listed.

upvoted 1 times

🗨️ 👤 **TheBigMan** 7 months, 2 weeks ago

With NSG/service tags you can only limit the region. Like sql.EastUs .

Only viable in my opinion B

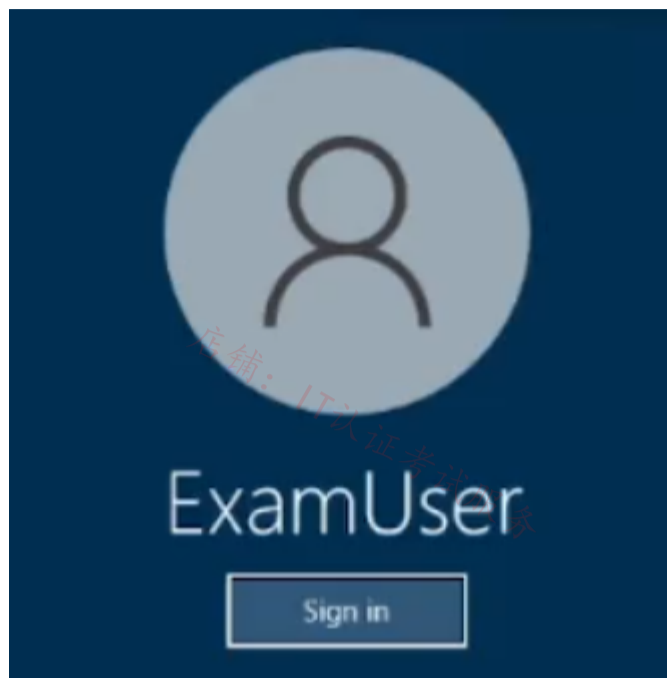
upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You need to ensure that connections to the storage12345678 storage account can be made by using an IP address in the 10.1.1.0/24 range and the name storage12345678.privatelink.blob.core.windows.net.

To complete this task, sign in to the Azure portal.

Correct Answer:

Use private endpoints for Azure Storage

You can use private endpoints for your Azure Storage accounts to allow clients on a virtual network (VNet) to securely access data over a Private Link. The private endpoint uses a separate IP address from the VNet address space for each storage account service.

Plan:

Stage 1: Create a virtual network and subnet

Stage 2: Create a private endpoint

Stage 1: Create a virtual network and subnet

Step 1: Sign in to the Azure portal.

Step 2: In the search box at the top of the portal, enter Virtual network. In the search results, select Virtual networks.

Step 3: Select + Create in Virtual networks.

Step 4: In the Basics tab of Create virtual network, enter or select the following information.

Subscription - Select your subscription.

Resource group - Select Create new.

Enter SomeName in Name and select OK.

Instance details

Name - Enter myVNet for example

Region - Select West Europe.

Step 5: Select Next: IP Addresses or the IP Addresses tab.

Step 6: Select the IP Addresses tab or select Next: IP Addresses at the bottom of the page.

Step 7: In the IP Addresses tab, enter the following information:

* IPv4 address space - Enter 10.1.0.0/16

Step 8: Select Add subnet. In Edit subnet, enter the following information:

Subnet name - Enter mySubnet

Subnet address range - Enter 10.1.1.0/24 (as specified in the question)

Step 9: For the subnet: Select the Review + create tab or select the Review + create button.

Step 10: For the Virtual network: Select the Review + create tab or select the Review + create button.

Stage 2: Create a private endpoint

Step 1: In the search box at the top of the portal, enter Private endpoint. Select Private endpoints.

Step 2: Select + Create in Private endpoints.

Step 3: In the Basics tab of Create a private endpoint, enter or select the following information.

* Storage subresource - storage12345678.privatelink.blob.core.windows.net

* Private DNS integration.

Integrate with private DNS zone - Leave the default Yes.

* Private DNS Zone

Leave the default (New) privatelink.blob.core.windows.net.

Step 4: Select Next: Resource.

Step 5: In the Resource pane, leave the defaults.

Step 6: Select Next: Virtual Network.

Step 7: In Virtual Network, enter or select the following information.

Virtual network - Select the virtual network you created in stage 1.

Subnet - Select the subnet you created in stage 1.

Step 8: Select Next: DNS.

Step 9: Leave the defaults in DNS. Select Next: Tags, then Next: Review + create.

Step 10: Select Create.

Reference:

<https://learn.microsoft.com/en-us/azure/storage/common/storage-private-endpoints>

<https://learn.microsoft.com/en-us/azure/private-link/create-private-endpoint-portal>

Currently there are no comments in this discussion, be the first to comment!

店铺：IT认证考试服务

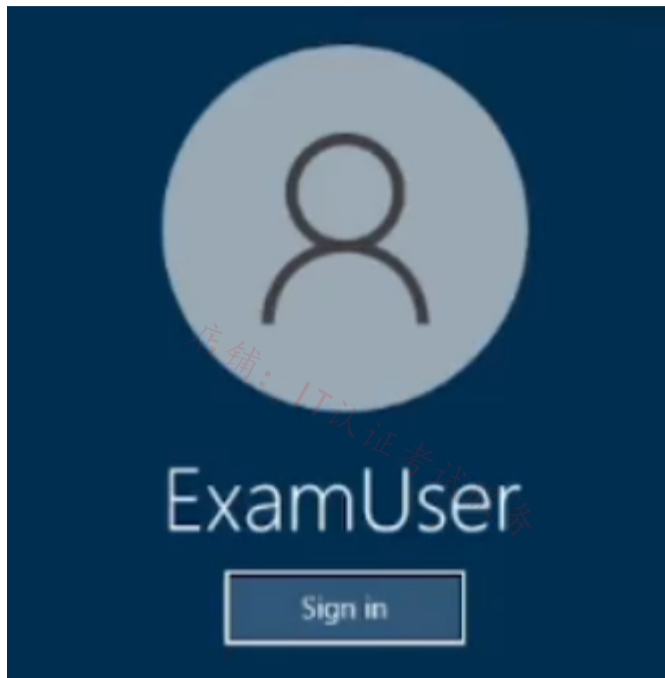
店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You need to ensure that requests for www.relecloud.com from any of your Azure virtual networks resolve to frontdoor1.azurefd.net.

To complete this task, sign in to the Azure portal.

Correct Answer:

Stage 1: Create an Azure private DNS zone using the Azure portal.

Step 1: On the portal search bar, type private dns zones in the search text box and press Enter.

Step 2: Select Private DNS zone.

Step 3: Select Create private dns zone.

On the Create Private DNS zone page, type or select appropriate values:

Resource group: Select Create new, enter something X, and select OK. The resource group name must be unique within the Azure subscription.

Name: Type private.relecloud.com.

Resource group location:

Step 4: Select Review + Create.

Step 5: Select Create.

Stage 2: Create a CNAME DNS record

Step 6: Open the X resource group you created earlier and select the private.relecloud.com private zone. You can enter private.relecloud.com the Filter by name box to find it more easily.

Step 7: At the top of the DNS zone page, select + Record set.

Step 8: On the Add record set page, type or select the following values:

Name: Type www.

Type: CNAME

Record set properties: frontdoor1.azurefd.net

Step 9: Select Save at the top of the page to save your settings. Then close the page.

Reference:

<https://learn.microsoft.com/en-us/azure/dns/private-dns-getstarted-portal>

<https://learn.microsoft.com/en-us/azure/dns/dns-operations-recordsets-portal>

 **tzatziki** Highly Voted 11 months, 3 weeks ago

Excuse my, perhaps, silly question but why private.relecloud.com and not simply relecloud.com as concerns the naming of the private dns zone? would typing www.private.relecloud.com or www.relecloud.com would resolve the same way or smt???


upvoted 5 times

 **ExamTopics2_EIS** 2 months, 3 weeks ago

From my research it should be relecloud.com and not private.relecloud.com.
<https://learn.microsoft.com/en-us/azure/dns/private-dns-getstarted-portal>

otherwise, it's www.private.relecloud.com

upvoted 1 times

 **hal01** 9 months, 1 week ago

it's a way to differentiate between the publicly accessible domain and the privately accessible domain. This naming convention may help prevent confusion and ensure that requests for private resources are directed to the correct DNS zone.

upvoted 1 times

 **mabew316** Most Recent 1 month, 1 week ago

itexamslab.com

Given answer is correct


upvoted 2 times

 **WELCOMEEEBRO** 1 month, 1 week ago

itexamslab.com

Only Azure networks

upvoted 2 times

 **Bobip** 1 month, 1 week ago

The steps for the answer looks ok except we need to create a private DNS zone as: relecloud.com not private.relecloud.com. If we name the DNS zone as private.relecloud.com then creating the CNAME for www makes a record as www.private.relecloud.com which is

different with the requirement of the question that says www.relecloud.com.

upvoted 1 times

🗨️ **Lazylinux** 1 month, 1 week ago

Given answer is correct =>

1- Private DNS zone (NO public DNS zone as vNETS will not be able to use it as NOT linked) if No private DNS than Azure default DNS is used and will not meet the object as you ca NOT edit the zone i.e. you cannot make CNAME record!!

2- Create CNAME Hostname = www.relecloud.com and value = frontdoor1.azurefd.net

Further confirmed here

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-name-resolution-for-vms-and-role-instances?tabs=redhat>

Check the table in the link

upvoted 1 times

🗨️ **mabalon** 4 months, 4 weeks ago

i think that we have two options:

- Create private dns zone for relecloud.com, record www. CNAME to frontdoor and make the link between the zone and the VNET.

- On the public dns zone relecloud.com create the register www. CNAME to frontdoor.

The Lab requirement is from ANY VNET, not only from the VNET, so if we create a public dns record any VNET will be able re resolve the dns record

upvoted 2 times

🗨️ **JohnnyChimpo** 7 months, 3 weeks ago

For anyone saying you have to use a public DNS - you are wrong. You need to create a virtual network links to the vnets in order for them to resolve the CNAME of www.relecloud.com to frontdoor1.azurefd.net - you cannot create vnet links to public DNS zones, only private DNS

upvoted 2 times

🗨️ **Rododendron2** 1 month, 1 week ago

That's the point, we don't need to create links

upvoted 1 times

🗨️ **hal01** 9 months, 1 week ago

To ensure that requests for www.relecloud.com from any of your Azure virtual networks resolve to frontdoor1.azurefd.net, you can follow these steps:

Go to the Azure portal and navigate to the Relecloud DNS zone.

Create a new CNAME record by clicking on the "+ Record set" button.

In the "Name" field, enter "www".

In the "Type" field, select "CNAME".

In the "Alias" field, enter "frontdoor1.azurefd.net".

Save the record set by clicking the "Save" button.

This will create a CNAME record that maps the hostname "www.relecloud.com" to "frontdoor1.azurefd.net". Once this DNS change propagates to your virtual networks, requests to www.relecloud.com will resolve to frontdoor1.azurefd.net.

Note that you may need to update any firewall rules or network security groups to allow traffic to flow to frontdoor1.azurefd.net.

upvoted 4 times

🗨️ **Cabelen** 10 months ago

You forgot to add the virtual networks links to the subnet that will use that private DNS zone.

upvoted 2 times

🗨️ **breakpoint0815** 10 months ago

Only Azure networks are needed to resolve the address. Therefore -> private DNS zone

upvoted 2 times

🗨️ **Aziza_Adam** 11 months, 1 week ago

It should be a public DNS not private

upvoted 2 times

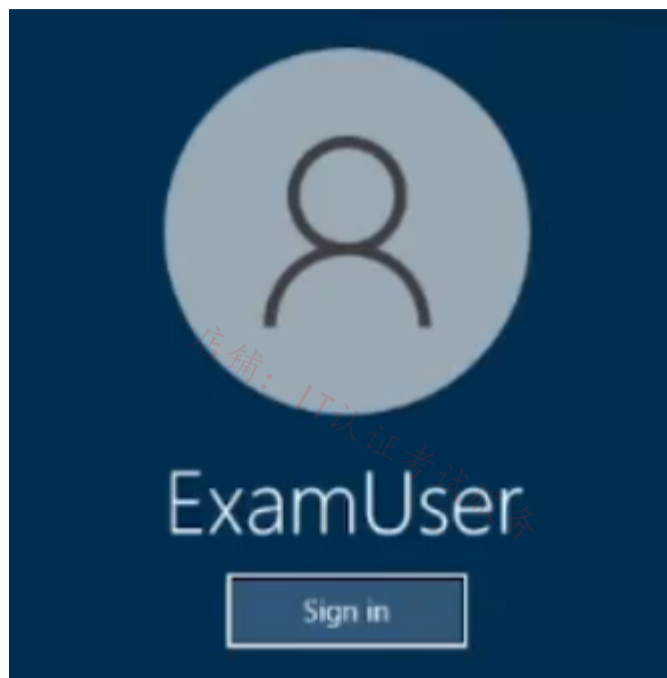
🗨️ **cypkir** 11 months, 1 week ago

You Have to use An Azure DNS zone and not a An Azure private DNS zone

upvoted 2 times

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You need to ensure that the storage12345678 storage account will only accept connections from the hosts on VNET1.

To complete this task, sign in to the Azure portal.

Correct Answer:

Azure storage account accepts connections from Virtual network.

Use private endpoints for Azure Storage

You can use private endpoints for your Azure Storage accounts to allow clients on a virtual network (VNet) to securely access data over a Private Link. The private endpoint uses a separate IP address from the VNet address space for each storage account service. Network traffic between the clients on the VNet and the storage account traverses over the VNet and a private link on the Microsoft backbone network, eliminating exposure from the public internet.

Link the private endpoint to the existing storage account

Step 1: In the search box at the top of the portal, enter Storage account. Select Storage accounts in the search results.

Step 2: Select or Search&find storage account storage12345678

Step 3: Select the Networking tab or select Next: Advanced then Next: Networking.

Step 4: In the Networking tab, under Network connectivity select Disable public access and use private access.

Step 5: In Private endpoint, select + Add private endpoint.

Step 6: In the Basics tab of Create a private endpoint, enter or select basic information for the endpoint.

Step 7: Select Next: Resource.

Step 8: In the Resource pane, enter or select basic information for the resource.

Step 9: Select Next: Virtual Network.

Step 10: In Virtual Network, enter or select:

* Virtual network: VNET1.

Step 11: Select Next: DNS.

Step 12: Leave the defaults in DNS. Select Next: Tags, then Next: Review + create.

Step 13: Select Create.

Back in the setting of settings of the Storage Account.

Step 14: Save.

Reference:

<https://learn.microsoft.com/en-us/azure/private-link/tutorial-private-endpoint-storage-portal>

<https://learn.microsoft.com/en-us/azure/private-link/create-private-endpoint-portal>

 **Bbb78** Highly Voted 11 months, 3 weeks ago

This seems incorrect - the question only asks to accept connections only from VNET1 hosts!

This can be done with the Storage Network/Firewall settings.

upvoted 19 times

 **wooyourdaddy** 10 months, 2 weeks ago

Agree, this one seems easier to do with Service Endpoints rather than Private Endpoints. Change Public network access on the storage account to 'Enabled from selected virtual networks and IP addresses'. Under Virtual Networks, choose VNET1 and its subnets.

On the subnets in VNET1, edit and add the Microsoft.Storage service under Service Endpoints.

upvoted 5 times

 **Ws1234** 9 months ago

You'd have to add every new subnet of VNET1 to the 'selected virtual networks' manually. When using a private endpoint, all subnets in the VNET automatically have access. Both will work, Private endpoint seems like the better option to me.

upvoted 4 times

 **Lazylinux** Most Recent 3 months, 1 week ago

My take on it

Service End point – YES can achieve the Goal required however there is ONE major PROBLEM and that is you will still have to go to the storage account and from the networking is to DSIABLE the public access!! And hence doing double work and Also you SEP can only be created from vNET but question is referencing the storage

Storage Account – Networking

Choosing Enabled from selected virtual networks and IP addresses, this will work however it requires more work in managing the firewall but also there is another issue and that is in order allow vNET – once selected, you also have to have Service Endpoint on EACH subnet you chose and if no SP configured on subnet prior you get the below message forcing SP creation by default!!

upvoted 2 times

  **Lazylinux** 3 months, 1 week ago

continuing

The following networks don't have service endpoints enabled for 'Microsoft.Storage'. Enabling access will take up to 15 minutes to complete. After starting this operation, it is safe to leave and return later if you do not wish to wait.

Private end point guarantees what is required and choosing at same time BLOCK public access will achieve the result and requires least effort in all 3 solutions

NOTE: Enabling storage account FIREWALL will by default block all public access unless explicitly allowed

Important point: All 3 solutions i.e. Service Endpoint, Enable from selected Networks and Private Endpoint all you have to chose SUBNETS and they DO NOT include the whole vnet so if vnet has 5 subnets than you chose them independently hence question is bit misleading by saying vNET without emphasizing on subnet wording

upvoted 2 times

  **Lazylinux** 3 months, 1 week ago

Continuing

So I would chose Private END POINT

Please read the below link

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

upvoted 2 times

  **Aziza_Adam** 11 months, 1 week ago

Private endpoint is correct as it ensures that there is no connection except to the linked vnet

upvoted 4 times

  **barte** 11 months ago

you also have to remember to disable public access for storage

upvoted 3 times

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT

You have two Azure subscriptions named Subscription1 and Subscription2.

There are no connections between the virtual networks in the two subscriptions.

You configure a private link service as shown in the privatelinkservice1 exhibit. (Click the privatelinkservice1 tab.)

The screenshot shows the configuration for a Private Link Service named 'privatelinkservice1'. The configuration details are as follows:

Resource group (move)	: rg1	Alias	: privatelinkservice1.955063e0-3b92-468a-a054-22c729f62297.eastus2.azure.privatelinkservice
Status	: Succeeded	NAT subnet	: vnet2/subnet1
Location	: East US 2	NAT IPs	: 10.3.0.7
Subscription (move)	: subscription1	Load balancer	: lb1
Subscription ID	: c40e35e3-7605-4f12-ba4c-90d200425073	Visibility	: All
Tags (edit)	: Click here to add tags		

You create a load balancer name in Subscription1 and configure the backend pool shown in the lb1 exhibit. (Click the lb1 tab.)

The screenshot shows the configuration for a Load Balancer named 'lb1'. The configuration details are as follows:

Resource group (move)	: rg1	Backend pool	: backendpool1 (1 virtual machine)
Location	: East US 2	Load balancing rule	: rule1 (Tcp/80)
Subscription (move)	: subscription1	Health probe	: probe1 (Http/80)
Subscription ID	: c40e35e3-7605-4f12-ba4c-90d200425073	NAT rules	: 0 inbound
SKU	: Standard	Tier	: Regional
Tags (edit)	: Click here to add tags		
Private IP address	: 10.3.0.6		

You create a private endpoint in Subscription2 as shown in the privateendpoint4 exhibit. (Click the privateendpoint4 tab.)

The screenshot shows the Private Link Center interface with a table of private endpoints. The table contains the following data:

Name	Private IP	Resource	Subnet	Connection State
privateendpoint4	10.5.0.7	privatelinkservice1.955063e0-3b92-468a-a054-22c729f62297.eastus2.azure.privatelinkservice	vnet5/subnet1	Pending

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area	Statements	Yes	No
	The resources that will be accessed by using privatelinkservice1 must be added to backendpool1 on LB1.	<input type="radio"/>	<input type="radio"/>
	Users in Subscription2 can connect to the resources published by privatelinkservice1 by using IP address 10.3.0.7.	<input type="radio"/>	<input type="radio"/>
	The private endpoint must be approved by an administrator in Subscription1.	<input type="radio"/>	<input type="radio"/>

Answer Area	Statements	Yes	No
Correct Answer:	The resources that will be accessed by using privatelinkservice1 must be added to backendpool1 on LB1.	<input checked="" type="radio"/>	<input type="radio"/>
	Users in Subscription2 can connect to the resources published by privatelinkservice1 by using IP address 10.3.0.7.	<input type="radio"/>	<input checked="" type="radio"/>
	The private endpoint must be approved by an administrator in Subscription1.	<input checked="" type="radio"/>	<input type="radio"/>

_fvt Highly Voted 9 months, 3 weeks ago

Y,N,Y, seems good.

<https://learn.microsoft.com/en-us/azure/private-link/create-private-link-service-portal>

<https://learn.microsoft.com/en-us/azure/private-link/private-link-overview>

upvoted 9 times

hasim_uddin 6 months ago

Last one is "NO"

Approval method for private endpoint: Typically, a network administrator creates a private endpoint. Depending on your Azure role-based access control (RBAC) permissions, a private endpoint that you create is either automatically approved to send traffic to the API Management instance, or requires the resource owner to manually approve the connection.

upvoted 2 times

Lazylinux 1 month, 1 week ago

No sure what are you talking about and why someone voted thumbs up!!

You DO NOT see to see the obvious - in private endpoint in Subscription2 you can see the CONNECTION STATE is PENDING meaning needs approval from administrator!!!

Also RBAC has NOTHING to do with Servicelink and PE

Therefore answer is YES

upvoted 4 times

hogegehoge Most Recent 2 months, 1 week ago

The answer of Q2 is Yes.Because the IP is changed by NAT rule.

upvoted 2 times

GBAU 3 months ago

q3) Y

Notice the Connection Status for the Private Endpoint in Sub2 is "Pending"

<https://learn.microsoft.com/en-us/azure/private-link/private-link-service-overview>

"The private endpoint connection will be created in a Pending state on the Private Link service object. The service provider is responsible for acting on the connection request."

In this case you are also the Service Provider and will need to go back into Sub1 and authorise the connection you initiated from Sub2.

upvoted 1 times

mabalon 5 months ago

My two cents

The last question depends of the interpretation of "There are no connections between the virtual networks in the two subscriptions.",

- if "there arent no connections" means for networks and administrations -> We need the approval

if "there arent no connections" is only for peering and the admistrator is the same on both subscriptions -> The approval will be approved automatically

upvoted 1 times



Tasli6 6 months, 4 weeks ago



Yes, privatelinkservice1 is a frontend of the load balancer so the resourced need to be added to the backendpool1.

No, its a privateendpoint and can only be accessed using the url.

No, "Typically, a network administrator creates a private endpoint. Depending on your Azure role-based access control (RBAC) permissions, a private endpoint that you create is either automatically approved to send traffic to the API Management instance, or requires the resource owner to manually approve the connection." <https://learn.microsoft.com/en-us/azure/api-management/private-endpoint>

upvoted 2 times

  **occupatissimo** 8 months, 3 weeks ago
NNY, backendpool already have a VM in
upvoted 1 times

  **Apptech** 8 months, 2 weeks ago
we do not know if VM hosts the resources that should be access. For that reason we can state: Yes, generally speaking, we must add resources to the load balancer
upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

You have an Azure subscription that contains an Azure Front Door named FD1.

You plan to deploy an app named App1 by using Azure App Service. Users will access App1 by using FD1.

You need to provide FD1 with access to App1. The solution must meet the following requirements:

- Ensure that users can only access App1 by using FD1.
- Ensure that users cannot access App1 directly from the internet.

What should you create for App1?

- A. an access restriction
- B. a private endpoint
- C. a subnet delegation
- D. a service endpoint

Correct Answer: B

Community vote distribution


A (86%)

14%

 **Rododendron2** 1 month, 1 week ago

Selected Answer: B

<https://learn.microsoft.com/en-us/azure/frontdoor/standard-premium/how-to-enable-private-link-web-app>
upvoted 1 times

 **Lazylinux** 3 months, 1 week ago

A is correct and you should also configure this setting/option X-Azure-FDID header
upvoted 1 times

 **Billabongs** 6 months ago

Selected Answer: A

Access Restriction
Create a Rule pointing to Azure Front Door
<https://techcommunity.microsoft.com/t5/azure-architecture-blog/permit-access-only-from-azure-front-door-to-azure-app-service-as/bap/2000173>
upvoted 2 times

 **Ditka** 6 months, 1 week ago

If you must use FD, then you must use Access Restrictions:

<https://learn.microsoft.com/en-us/azure/app-service/networking-features#use-cases-and-features>
upvoted 3 times

 **nrv1020** 7 months, 1 week ago

Selected Answer: A

Not clear how creating a private endpoint limits connections from the Internet.
upvoted 1 times

 **Rododendron2** 1 month, 1 week ago

<https://learn.microsoft.com/en-us/azure/frontdoor/standard-premium/how-to-enable-private-link-web-app>
upvoted 1 times

 **Ben_88** 7 months, 2 weeks ago



Selected Answer: A

if you follow this procedure
<https://techcommunity.microsoft.com/t5/azure-architecture-blog/permit-access-only-from-azure-front-door-to-azure-app-service-as/bap/2000173>
upvoted 3 times

 **Apptech** 8 months, 2 weeks ago

In my opinion it should be a private endpoint. See here: <https://learn.microsoft.com/en-us/azure/frontdoor/standard-premium/how-to-enable-private-link-web-app#approve-azure-front-door-premium-private-endpoint-connection-from-app-service>

upvoted 2 times

  **khksoma** 8 months, 3 weeks ago

It should be A

<https://techcommunity.microsoft.com/t5/azure-architecture-blog/permit-access-only-from-azure-front-door-to-azure-app-service-as/bap/2000173>

upvoted 2 times

  **Apptech** 8 months, 2 weeks ago

If you follow your own link under headline access restrictions you also can find a link that states that a private endpoint is needed:

<https://learn.microsoft.com/de-de/azure/app-service/networking-features#access-restrictions>

upvoted 2 times

  **occupatissimo** 8 months, 3 weeks ago

A, access comes from internet

<https://learn.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions?tabs=azurecli>

upvoted 4 times

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT

-

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

Name	Type	Description
appservice1	Azure App Service	Hosts an app named App1
contoso.com	Azure DNS zone	Resolves name requests from the internet
FD1	Azure Front Door	Standard profile with App1 configured as the origin
KeyVault1	Azure Key Vault	Key vault with Permission model set to Vault access policy
KeyVault2	Azure Key Vault	Key vault with Permission model set to Azure role-based access control

You purchase a certificate for app1.contoso.com from a public certification authority (CA) and install the certificate on appservice1.

You need to ensure that App1 can be accessed by using a URL of https://app1.contoso.com. The solution must ensure that all the traffic for App1 is routed via FD1.

Which type of DNS record should you create, and where should you store the certificate? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

DNS record type:

- A
- CNAME
- SRV
- TXT

Store the certificate in:

- FD1
- KeyVault1
- KeyVault2

Answer Area

DNS record type:

- A
- CNAME
- SRV
- TXT**

Correct Answer:

Store the certificate in:

- FD1
- KeyVault1
- KeyVault2**

 **jonav94** Highly Voted 8 months, 3 weeks ago

I disagree with proposed answers, they must be:

DNS: CNAME (When you added a custom domain to your Front Door's frontend hosts, you created a CNAME record in the DNS table of your domain registrar to map it to your Front Door's default .azurefd.net hostname)

Store certificate in: KeyVault1 (Your key vault must be configured to use the Key Vault access policy permission model.)

There you have a link with all explained <https://learn.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain-https>.

upvoted 19 times

 **crypto700** Highly Voted 8 months, 3 weeks ago

The Right answers are:

1-CNAME

2- Key Vault 1

<https://learn.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain-https>

Key Vault access policy permission model.

upvoted 13 times

 **Murad01** Most Recent 1 month, 3 weeks ago

Appeared on Exam November - 2023

upvoted 2 times

 **Murad01** 1 month, 3 weeks ago

Appeared on Exam November-2023

upvoted 1 times

 **Lazylinux** 3 months, 1 week ago

Confusing to say least

At first based on the fact that KV Access Policy is legacy now and MS is recommending migration from it and implementation of RBAC, this is true for almost everything in Azure with exception App Services, no support yet for RBAC as per MS comment and the link below, I was going to chose KV with RBAC but based on the above the correct answer is KV with Access Policy model

<https://learn.microsoft.com/en-us/azure/app-service/configure-ssl-app-service-certificate?tabs=portal>

as of 28 July 2023 of the above article "App Service certificates support only Key Vault access policies, not the RBAC model."

continued ...

upvoted 1 times

 **Lazylinux** 3 months, 1 week ago

here more

As for the Custom domain with Azure FD, well quite NOT clear if the domain had been validated? If NOT than TXT record needs be created first than once domain validated CNAME is created to associate the custom domain to Azure FD endpoint

Now Assumption, because we already have Azure public DNS zone named contoso.com and app1 is going to be subdomain hence the domain is already validated and the next step is CNAME

See this video goes through whole process

<https://www.youtube.com/watch?v=mVNB59VK-DQ>

upvoted 1 times

 **raffykian** 5 months, 1 week ago

cname and keyvault 1 - on exam 8-23

upvoted 5 times

店铺: IT认证考试服务

店铺: IT认证考试服务

You have an Azure subscription that contains four virtual machines. The virtual machines host an app named App1.

You deploy an Azure Standard Load Balancer named LB1 to load balance incoming HTTPS requests to App1.

You need to reduce how long it takes for LB1 to stop sending App1 traffic to failed servers. The solution must minimize administrative effort.

What should you modify?

- A. the Backend pools settings
- B. the Diagnostic settings
- C. the Load-balancing rules
- D. the Health probes settings

Correct Answer: D

Community vote distribution

D (100%)

 **Apptech** Highly Voted 8 months, 2 weeks ago

True, in the health probe settings you can configure the interval of health probe. The amount of time (in seconds) between consecutive health check attempts to the virtual machines

<https://learn.microsoft.com/en-us/azure/load-balancer/manage-probes-how-to>

upvoted 5 times

 **Lazylinux** Most Recent 3 months, 1 week ago

D is correct Interval settings at health probes config

upvoted 1 times

 **Billabongs** 6 months ago

Selected Answer: D

Healthy Probe - Interval Settings

upvoted 2 times

You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains the following subnets:

- AzureFirewallSubnet
- GatewaySubnet
- Subnet1
- Subnet2
- Subnet3

Subnet2 has a delegation to the Microsoft.Web/serverfarms service.

The subscription contains the resources shown in the following table.

Name	Type	Connected to
AZVNGW1	Azure VPN Gateway	GatewaySubnet
AZFW1	Azure Firewall Premium	AzureFirewallSubnet
VMSS1	Virtual machine scale set	Subnet1

You need to implement an Azure application gateway named AG1 that will be integrated with an Azure Web Application Firewall (WAF). AG1 will be used to publish VMSS1.

To which subnet should you connect AG1?

- A. GatewaySubnet
- B. AzureFirewallSubnet
- C. Subnet2
- D. Subnet1
- E. Subnet3

Correct Answer: E

Community vote distribution

E (100%)

khksoma Highly Voted 8 months, 3 weeks ago

An application gateway is a dedicated deployment in your virtual network. Within your virtual network, a dedicated subnet is required for the application gateway. You can have multiple instances of a given application gateway deployment in a subnet. You can also deploy other application gateways in the subnet. But you can't deploy any other resource in the application gateway subnet.

Subnet 3

upvoted 6 times

crypto700 Most Recent 8 months, 3 weeks ago

what about Subnet2?

upvoted 1 times

JackCoole95 8 months, 3 weeks ago

Because Subnet2 is delegated to Microsoft.Web/serverfarms and therefore is not eligible deploy an AppGW in to.

upvoted 4 times

jonav94 8 months, 3 weeks ago

Selected Answer: E

It's ok, it cannot use the others subnets because they've already have another services deployed on them.

upvoted 4 times

You have an Azure virtual network named VNet1 that contains the subnets shown in the following table.

Name	Is a gateway subnet	Description
Subnet1	No	Has connected virtual machines
Subnet2	No	Has no connected resources
GatewaySubnet	Yes	None

You need to deploy an Azure application gateway named AppGW1 to VNet1.

To where can you deploy AppGW1?

- A. GatewaySubnet only
- B. Subnet2 only
- C. Subnet1 or Subnet2 only
- D. Subnet2 or GatewaySubnet only
- E. Subnet1, Subnet2, and GatewaySubnet

Correct Answer: B

Community vote distribution

B (100%)

 **Lazylinux** 3 months, 1 week ago

Selected Answer: B

is B is Honey

App GWY subnet can only have App GWY and nothing also due to dynamic deployment of App GWY instance if required - V1 require /26 subnet but v1 no longer valid, V2 App GWY requires /24 subnet.

You may ask yourself how would App GWY deployment NOT pickup certain subnets even though they are /24, this is because of the NAMING - if name of GatewaySubnet exist it will not choose it as Valid subnet more here

Application Gateway (Standard or WAF) SKU can support up to 32 instances (32 instance IP addresses + 1 private frontend IP configuration + 5 Azure reserved) – so a minimum subnet size of /26 is recommended

Application Gateway (Standard_v2 or WAF_v2 SKU) can support up to 125 instances (125 instance IP addresses + 1 private frontend IP configuration + 5 Azure reserved). A minimum subnet size of /24 is recommended.

upvoted 1 times

 **tfkfk** 8 months ago


Selected Answer: B

provided answer is correct !

a dedicated subnet is required for the application gateway.You can have multiple instances of a given application gateway deployment in a subnet. You can also deploy other application gateways in the subnet. But you can't deploy any other resource in the application gateway subnet. You can't mix v1 and v2 Azure Application Gateway SKUs on the same subnet.

<https://learn.microsoft.com/en-us/azure/application-gateway/configuration-infrastructure>

upvoted 4 times

 **jonav94** 8 months, 3 weeks ago

Selected Answer: B

Subnet2 is the only one that doesn't have any resources and it is not a gateway subnet.

upvoted 3 times

HOTSPOT

-

You have an Azure subscription that contains multiple virtual machine scale sets and multiple Azure load balancers. The load balancers balance traffic across the scale sets.

You plan to deploy Azure Front Door to load balance traffic across the load balancers.

You need to identify which Front Door SKU to configure, and what to use to route the traffic to the load balancers. The solution must minimize costs.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

SKU:

- Classic
- Premium
- Standard

Use:

- Azure Private Link
- Azure Route Server
- A service endpoint

Answer Area**Correct Answer:**

SKU:

- Classic
- Premium**
- Standard

Use:


- Azure Private Link**
- Azure Route Server
- A service endpoint

 **Murad01** 1 month, 3 weeks ago

I do agree with Premium SKU for the first selection, But why it is private link instead of Route server, does anyone has reference
upvoted 1 times

 **Apptech** 8 months, 2 weeks ago

Premium SKU is the only tier which includes private link. <https://learn.microsoft.com/en-us/azure/frontdoor/standard-premium/tier-comparison>
upvoted 3 times

 **khksoma** 8 months, 3 weeks ago

Not sure if the question is framed right. Found this in the FAQ.

Azure Front Door Standard, Premium and (classic) tier requires a public IP or publicly resolvable DNS name to route traffic to backend resources. Azure resources such as Application Gateways or Azure Load Balancers can enable routing to resources within a virtual network. If you're using a Front Door Premium tier, you can enable Private Link to connect to origins behind an internal load balancer over a private endpoint.

upvoted 4 times

You have an Azure subscription that contains the following resources:

- A virtual network named Vnet1
- Two subnets named subnet1 and AzureFirewallSubnet
- A public Azure Firewall named FW1
- A route table named RT1 that is associated to Subnet1
- A rule routing of 0.0.0.0/0 to FW1 in RT1

After deploying 10 servers that run Windows Server to Subnet1, you discover that none of the virtual machines were activated.

You need to ensure that the virtual machines can be activated.

What should you do?


- A. Deploy a NAT gateway.
- B. Deploy an Azure Standard Load Balancer that has an outbound NAT rule.
- C. On FW1, create an outbound network rule that allows traffic to the Azure Key Management Service (KMS).
- D. To Subnet1, associate a network security group (NSG) that allows outbound access to port 1688.

Correct Answer: C

Community vote distribution

C (100%)

 **Annie1210** Highly Voted 8 months, 3 weeks ago
Repeated
upvoted 6 times

 **Lazylinux** Most Recent 3 months, 1 week ago
Selected Answer: C
Given answer is correct
upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

DRAG DROP

-

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

Name	Type	Description
App1	Azure App Service app	Accessed by using a URL of https://app1.contoso.com/
FD1	Azure Front Door Premium profile	Configured as an endpoint for App1
contoso.com	Azure DNS zone	Contains a DNS CNAME record for App1 that resolves to an FQDN of app1.azurewebsites.net

You discover that users connect directly to App1.

You need to meet the following requirements:

- Administrators must only access App1 by using a private endpoint.
- All user connections to App1 must be routed through FD1.
- The downtime of connections to App1 must be minimized.

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.

Actions

- In the settings of App1, approve a pending private endpoint connection.
- For fd1.contoso.com, create a DNS A record that resolves to the IP address of the private endpoint.
- Change the DNS record of app1.contoso.com to resolve to the FQDN of FD1.
- In the settings of App1, create a private endpoint.
- In the settings of FD1, configure the origin group to enable the Azure Private Link service.
- For app1.contoso.com, create a DNS A record that resolves to the IP address of the private endpoint.

Answer Area



Correct Answer:

- Answer Area**
- In the settings of FD1, configure the origin group to enable the Azure Private Link service.
 - In the settings of App1, approve a pending private endpoint connection.
 - In the settings of App1, create a private endpoint.

emsaho 4 months, 2 weeks ago

It is correct, from <https://learn.microsoft.com/en-us/azure/frontdoor/private-link>
upvoted 1 times

fred99 4 months, 2 weeks ago

No it is not. Review your link it says: When you enable Private Link to your origin in Azure Front Door Premium, Front Door creates a private endpoint on your behalf.

My take:

Change DNS record of app1
configure the origin group
approve the private endpoint connection
upvoted 4 times

ironbornson 4 months, 1 week ago

You have to minimize impact on users, so wouldn't it be?
1-configure the origin group
2-approve the private endpoint connection
3-Change DNS record of app1
upvoted 16 times

Your on-premises network contains a DNS server named Server1.

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

Name	Type	Description
VNet1	Virtual network	None
VM1	Virtual machine	Connected to VNet1 Connected to storage1 by using a private endpoint
storage1	Storage account	None

The on-premises network is connected to VNet1 by using a Site-to-Site (S2S) VPN.

You need to ensure that Server1 can resolve the DNS name of storage1. The solution must minimize costs and administrative effort.

What should you use?

- A. Azure DNS Private Resolver
- B. an Azure public DNS zone
- C. an Azure Private DNS zone
- D. an Azure virtual machine that hosts a DNS service

Correct Answer: A

Community vote distribution

A (100%)

 **c2e9cb4** 3 weeks ago

Selected Answer: A

correctm new az managed dns feature
upvoted 1 times

 **Acaer** 4 months, 2 weeks ago

Selected Answer: A

A. Azure DNS Private Resolver
Azure DNS Private Resolver is a new service that enables you to query Azure DNS private zones from an on-premises environment and vice versa without deploying VM based DNS servers.
<https://learn.microsoft.com/en-us/azure/dns/dns-private-resolver-overview>
upvoted 4 times

You have an Azure Private Link service named PL1 that uses an Azure load balancer named LB1.

You need to ensure that PL1 can support a higher volume of outbound traffic.

What should you do?

- A. Increase the number of frontend IP configurations for LB1.
- B. Increase the number of NAT IP addresses assigned to PL1.
- C. Deploy an Azure Application Gateway v2 instance to the source NAT subnet.
- D. Redeploy LB1 with a different SKU.

Correct Answer: B

 **Acaer** 4 months, 2 weeks ago

B. Increase the number of NAT IP addresses assigned to PL1.

Since the question ask for outbound traffic:

Each NAT IP provides 64k TCP connections (64k ports) per VM behind the Standard Load Balancer. In order to scale and add more connections, you can either add new NAT IPs or add more VMs behind the Standard Load Balancer. Doing so will scale the port availability and allow for more connections. Connections will be distributed across NAT IPs and VMs behind the Standard Load Balancer.

<https://learn.microsoft.com/en-us/azure/private-link/private-link-faq#what-is-the-nat--network-address-translation--ip-configuration-used-in-private-link-service--how-can-i-scale-in-terms-of-available-ports-and-connections-->

upvoted 2 times

 **ironbornson** 4 months, 2 weeks ago

Oh yeah baby, so correct: <https://learn.microsoft.com/en-us/azure/private-link/private-link-service-overview>

Private Link service can have more than one NAT IP configurations linked to it. Choosing more than one NAT IP configurations can help service providers to scale. Today, service providers can assign up to eight NAT IP addresses per Private Link service. With each NAT IP address, you can assign more ports for your TCP connections and thus scale out.

upvoted 1 times

You have an on-premises network named Site1.

You have an Azure subscription that contains a virtual network named VNet1 and a storage account named storage1.

Site1 and VNet1 are connected by using a Site-to-Site (S2S) VPN.

You need to ensure that the servers in Site1 can connect to storage1 by using the S2S VPN. The solution must minimize administrative effort.

What should you create on VNet1?

- A. an Azure application gateway
- B. an Azure Private Link service
- C. a service endpoint
- D. a private endpoint

Correct Answer: D

Community vote distribution

D (100%)

 **SJHCI** 1 week ago

Selected Answer: D

D is correct

upvoted 1 times

 **Murad01** 1 month, 3 weeks ago

Given Answer is Correct D

upvoted 1 times

 **jorgesoma** 2 months, 3 weeks ago

Correct.

upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

HOTSPOT

-

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

Name	Type	Location	Description
VNet1	Virtual network	East US	Contains a subnet named Subnet1
storage1	Storage account	East US	Uses read-access geo-redundant storage (RA-GRS) redundancy
sql1	Azure SQL server	East US	Hosts a database named SQLDB1

You need to restrict access to storage1 and sql1 by using service endpoints. The solution must meet the following requirements:

- Allow access from Subnet1 to SQLDB1.
- Implement service endpoint policies to restrict access to supported resources.
- Allow access from Subnet1 to storage1 and the read-only replica of storage1 in the paired Azure region.

What is the minimum number of service endpoints and service endpoint policies you should create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Service endpoint:

1

2

3

Service endpoint policies:

1

2

3

Answer Area

Correct Answer:

Service endpoint:

1

2

3

Service endpoint policies:

1

2

3

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a financial company that has a main datacenter in Boston and 20 branch offices across the United States. Users have Android, iOS, and Windows 10 devices.

Existing Environment -

Hybrid Environment -

The on-premises network contains an Active Directory forest named litwareinc.com that syncs to an Azure Active Directory (Azure AD) tenant named litwareinc.com by using Azure AD Connect.

All offices connect to a virtual network named Vnet1 by using a Site-to-Site VPN connection.

Azure Environment -

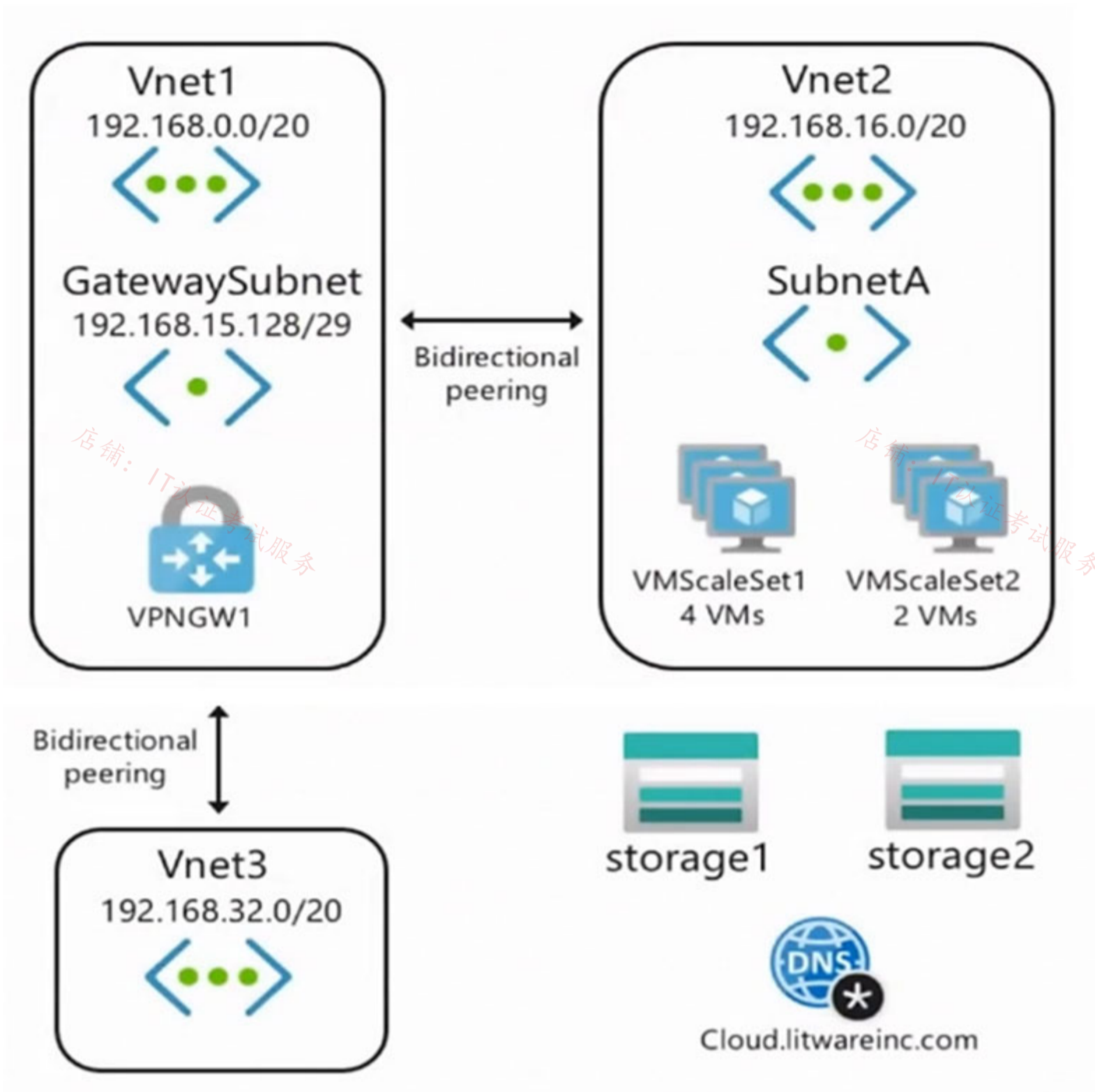
Litware has an Azure subscription named Sub1 that is linked to the litwareinc.com Azure AD tenant. Sub1 contains resources in the East US Azure region as shown in the following table.

Name	Type	Description
Vnet1	Virtual network	Uses an IP address space of 192.168.0.0/20
GatewaySubnet	Virtual network subnet	Located in Vnet1 and uses an IP address space of 192.168.15.128/29
VPNGW1	VPN gateway	Deployed to Vnet1
Vnet2	Virtual network	Uses an IP address space of 192.168.16.0/20
SubnetA	Virtual network subnet	Located in Vnet2 and uses an IP address space of 192.168.16.0/24
Vnet3	Virtual network	Uses an IP address space of 192.168.32.0/20
cloud.litwareinc.com	Private DNS zone	None
VMScaleSet1	Virtual machine scale set	Contains four virtual machines deployed to SubnetA
VMScaleSet2	Virtual machine scale set	Contains two virtual machines deployed to SubnetA
storage1	Storage account	Has the public endpoint blocked
storage2	Storage account	Has the public endpoint blocked

A diagram of the resource in the East US Azure region is shown in the Azure Network Diagram exhibit.

There is bidirectional peering between Vnet1 and Vnet2. There is bidirectional peering between Vnet1 and Vnet3. Currently, Vnet2 and Vnet3 cannot communicate directly.

Azure Network Diagram -



Requirements -

Business Requirements -

Litware wants to minimize costs whenever possible, as long as all other requirements are met.

Virtual Networking Requirements -

Litware identifies the following virtual networking requirements:

Direct the default route of 0.0.0.0/0 on Vnet2 and Vnet3 to the Boston datacenter over an ExpressRoute circuit.

Ensure that the records in the cloud.litwareinc.com can be resolved from the on-premises locations.

Automatically register the DNS names of Azure virtual machines to the cloud.litwareinc.com zone.

Minimize the size of the subnets allocated to platform-managed services.

Allow traffic from VMScaleSet1 to VMScaleSet2 on the TCP port 443 only.

Hybrid Networking Requirements -

Litware identifies the following hybrid networking requirements:

Users must be able to connect to Vnet1 by using a Point-to-Site (P2S) VPN when working remotely. Connections must be authenticated by Azure AD.

Latency of the traffic between the Boston datacenter and all the virtual networks must be minimized.

The Boston datacenter must connect to the Azure virtual networks by using an ExpressRoute FastPath connection.

Traffic between Vnet2 and Vnet3 must be routed through Vnet1.

PaaS Networking Requirements -

Litware identifies the following networking requirements for platform as a service (PaaS):

The storage1 account must be accessible from all on-premises locations without exposing the public endpoint of storage1.

The storage2 account must be accessible from Vnet2 and Vnet3 without exposing the public endpoint of storage2.

Question

HOTSPOT -

You need to recommend a configuration for the ExpressRoute connection from the Boston datacenter. The solution must meet the hybrid networking requirements and business requirements.

What should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Set the ExpressRoute gateway type to:

▼
High Performance (ERGW2AZ)
Standard Performance (ERGW1AZ)
Ultra Performance (ERGW3AZ)

To minimize latency of traffic to Vnet2:

▼
Create a dedicated ExpressRoute circuit for Vnet2
Connect Vnet2 directly to the ExpressRoute circuit
Configure gateway transit for the peering between Vnet1 and Vnet2

Correct Answer:

Answer Area

Set the ExpressRoute gateway type to:

▼
High Performance (ERGW2AZ)
Standard Performance (ERGW1AZ)
Ultra Performance (ERGW3AZ)

To minimize latency of traffic to Vnet2:

▼
Create a dedicated ExpressRoute circuit for Vnet2
Connect Vnet2 directly to the ExpressRoute circuit
Configure gateway transit for the peering between Vnet1 and Vnet2

JennyHuang36 Highly Voted 11 months, 1 week ago

In exam Feb, 2023
upvoted 8 times

alfonzo47 Highly Voted 1 year ago

Correct answers are:

- Ultra performance: <https://learn.microsoft.com/en-us/azure/expressroute/about-fastpath#gateways>
 - Gateway transit for peering: <https://learn.microsoft.com/en-us/azure/expressroute/about-fastpath#virtual-network-vnet-peering>
- upvoted 6 times

Billabongs Most Recent 6 months ago

Virtual network (VNet) Peering

FastPath will send traffic directly to any VM deployed in a virtual network peered to the one connected to ExpressRoute, bypassing the ExpressRoute virtual network gateway. This feature is available for both IPv4 and IPv6 connectivity.

upvoted 2 times

GohanF2 1 year, 2 months ago

This is a tricky question on regard of the second option. It's true that FastPath now can send traffic directly to the VM including the peered networks. But , this is talking about if we have only in place express route Direct. For the other options express route, it's not available yet and still it on public review. The case study says that they want to minimize costs..so having an express route direct circuit is not the best idea. However, by adding express route Ultra performance gateway , we can say that we can afford express route direct ... cheapest solution would be to add the vm2 traffic directly through the express route circuit... But , once again it's tricky... I will take the Risk and select the option of enabling gateway transit .

upvoted 4 times

GohanF2 1 year, 2 months ago

Here is the updated link of fastpath new availability just in case u guys don't have it : <https://learn.microsoft.com/en-us/azure/expressroute/about-fastpath>

upvoted 3 times

Prutser2 1 year, 3 months ago

<https://learn.microsoft.com/en-us/azure/expressroute/about-fastpath>

so in box 2: peering with transit gateway, leveraging off the fastpath feature in vnet1

upvoted 2 times

🗨️ **sapien45** 1 year, 3 months ago

FastPath now supports virtual network peering . FastPath will send traffic directly to any VM deployed in a spoke virtual network peered to the virtual network where the ExpressRoute virtual network gateway is deployed.

<https://azure.microsoft.com/en-ca/updates/general-availability-expressroute-fastpath-support-for-virtual-network-vnet-peering-and-user-defined-routes-udrs-2/>

upvoted 2 times

🗨️ **A_A_AB** 1 year, 4 months ago

First answer is correct as FastPath only works with Ultra Performance SKU.

The second answer must be the dedicated ER:

If you have other virtual networks peered with the one that is connected to ExpressRoute, the network traffic from your on-premises network to the other virtual networks (i.e., the so-called "Spoke" VNets) will continue to be sent to the virtual network gateway. The workaround is to connect all the virtual networks to the ExpressRoute circuit directly.

upvoted 1 times

🗨️ **wwwww** 1 year, 4 months ago

FastPath doesn't work for peered VNets, thus Vnet2 needs a direct connection to the ExpressRoute as well. The data can still flow through Vnet1: Vnet 2 > ExpressRoute > Vnet 1 -> ExpressRoute > ...

upvoted 2 times

🗨️ **[Removed]** 1 year, 4 months ago

I agree:

VNet Peering: If you have other virtual networks peered with the one that is connected to ExpressRoute, the network traffic from your on-premises network to the other virtual networks (i.e., the so-called "Spoke" VNets) will continue to be sent to the virtual network gateway. The workaround is to connect all the virtual networks to the ExpressRoute circuit directly.

upvoted 1 times

🗨️ **tkcltoh** 1 year, 4 months ago

but there is a condition that Traffic between Vnet2 and Vnet3 must be routed through Vnet1.

i think the gateway transit in vnet1 is correct.

upvoted 1 times

🗨️ **ChinkSantana** 1 year ago

Traffic between VNET2 and 3 and not traffic between VNET2 and On-Prem

upvoted 1 times

🗨️ **Cristoicach91** 1 year, 4 months ago

correct

upvoted 1 times

🗨️ **Cristoicach91** 1 year, 4 months ago

Correcting myself here. Should be Ultra for the first box and the second box since it mentions FastPath it needs to have Vnet2 directly connected to ExpressRoute.

upvoted 7 times

Topic 7 - Testlet 10

店铺: IT认证考试服务

店铺: IT认证考试服务

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a financial company that has a main datacenter in Boston and 20 branch offices across the United States. Users have Android, iOS, and Windows 10 devices.

Existing Environment -

Hybrid Environment -

The on-premises network contains an Active Directory forest named litwareinc.com that syncs to an Azure Active Directory (Azure AD) tenant named litwareinc.com by using Azure AD Connect.

All offices connect to a virtual network named Vnet1 by using a Site-to-Site VPN connection.

Azure Environment -

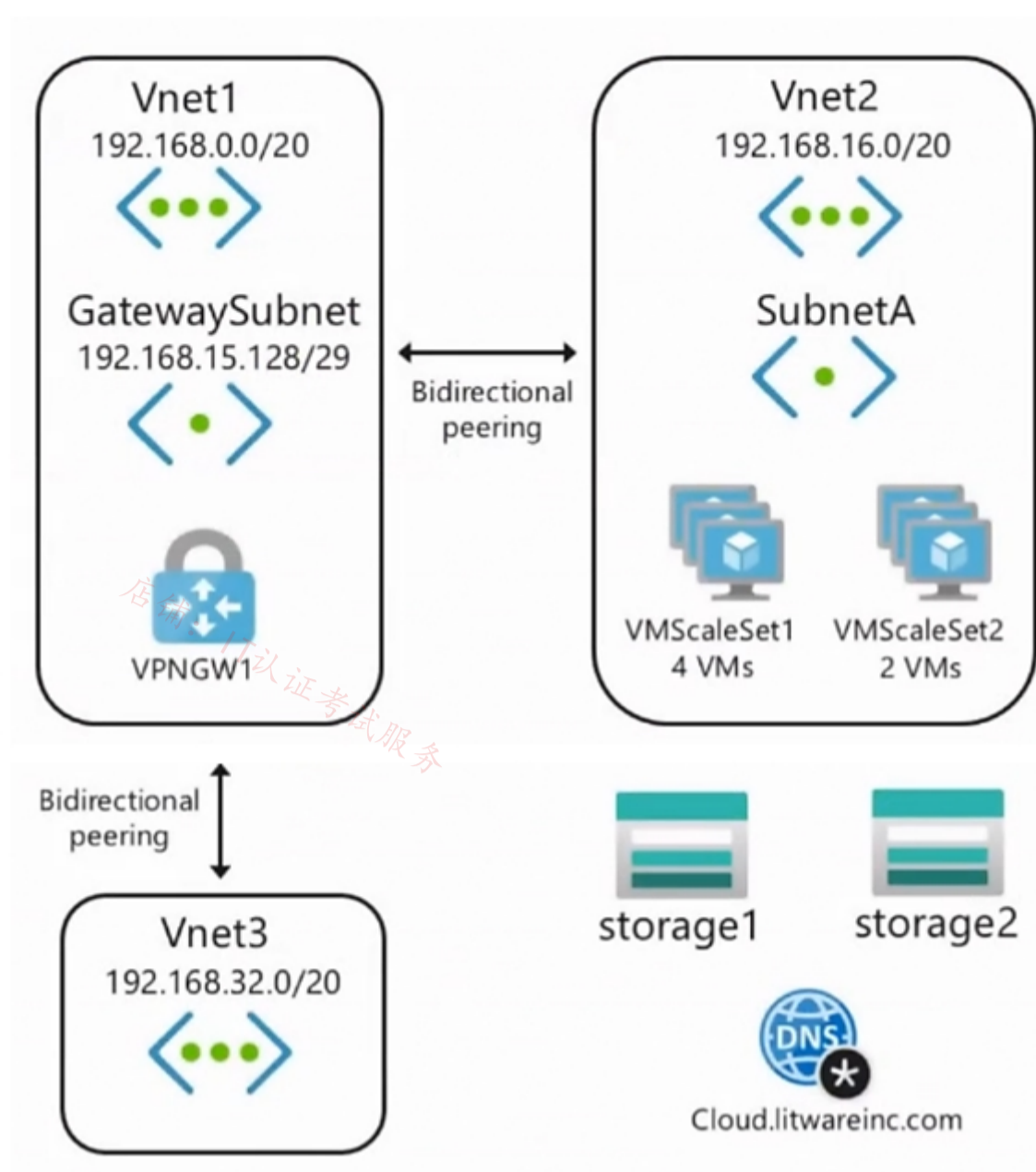
Litware has an Azure subscription named Sub1 that is linked to the litwareinc.com Azure AD tenant. Sub1 contains resources in the East US Azure region as shown in the following table.

Name	Type	Description
Vnet1	Virtual network	Uses an IP address space of 192.168.0.0/20
GatewaySubnet	Virtual network subnet	Located in Vnet1 and uses an IP address space of 192.168.15.128/29
VPNGW1	VPN gateway	Deployed to Vnet1
Vnet2	Virtual network	Uses an IP address space of 192.168.16.0/20
SubnetA	Virtual network subnet	Located in Vnet2 and uses an IP address space of 192.168.16.0/24
Vnet3	Virtual network	Uses an IP address space of 192.168.32.0/20
cloud.litwareinc.com	Private DNS zone	None
VMScaleSet1	Virtual machine scale set	Contains four virtual machines deployed to SubnetA
VMScaleSet2	Virtual machine scale set	Contains two virtual machines deployed to SubnetA
storage1	Storage account	Has the public endpoint blocked
storage2	Storage account	Has the public endpoint blocked

A diagram of the resource in the East US Azure region is shown in the Azure Network Diagram exhibit.

There is bidirectional peering between Vnet1 and Vnet2. There is bidirectional peering between Vnet1 and Vnet3. Currently, Vnet2 and Vnet3 cannot communicate directly.

Azure Network Diagram -



Requirements -

Business Requirements -

Litware wants to minimize costs whenever possible, as long as all other requirements are met.

Virtual Networking Requirements -

Litware identifies the following virtual networking requirements:

Direct the default route of 0.0.0.0/0 on Vnet2 and Vnet3 to the Boston datacenter over an ExpressRoute circuit.

Ensure that the records in the cloud.litwareinc.com can be resolved from the on-premises locations.

Automatically register the DNS names of Azure virtual machines to the cloud.litwareinc.com zone.

Minimize the size of the subnets allocated to platform-managed services.

Allow traffic from VMScaleSet1 to VMScaleSet2 on the TCP port 443 only.

Hybrid Networking Requirements -

Litware identifies the following hybrid networking requirements:

Users must be able to connect to Vnet1 by using a Point-to-Site (P2S) VPN when working remotely. Connections must be authenticated by Azure AD.

Latency of the traffic between the Boston datacenter and all the virtual networks must be minimized.

The Boston datacenter must connect to the Azure virtual networks by using an ExpressRoute FastPath connection.

Traffic between Vnet2 and Vnet3 must be routed through Vnet1.

PaaS Networking Requirements -

Litware identifies the following networking requirements for platform as a service (PaaS):

The storage1 account must be accessible from all on-premises locations without exposing the public endpoint of storage1.

The storage2 account must be accessible from Vnet2 and Vnet3 without exposing the public endpoint of storage2.

Question

You need to provide access to storage1. The solution must meet the PaaS networking requirements and the business requirements.

What should you include in the solution?

- A. a private endpoint
- B. Azure Traffic Manager

- C. Azure Front Door
- D. a service endpoint

Correct Answer: D

Community vote distribution

A (100%)

 **Cristoicach91** Highly Voted 1 year, 4 months ago

Selected Answer: A

The storage1 account must be accessible from all on-premises locations without exposing the public endpoint of storage1.
upvoted 21 times

 **tkcltoh** Highly Voted 1 year, 4 months ago

Selected Answer: A

service endpoint limitation
Endpoints are enabled on subnets configured in Azure virtual networks. Endpoints can't be used for traffic from your premises to Azure services
upvoted 10 times

 **daemon101** 6 months, 2 weeks ago

However, you can still allow certain public IP addresses to access storage account even though it's enabled with service endpoint.

Storage Account -> Networking -> Public Access -> Firewall Rules
upvoted 1 times

 **JohnnyChimpo** 9 months ago

NICE! Thanks for this
upvoted 1 times

 **sapien45** 1 year, 3 months ago

Good catch Sir
upvoted 4 times

 **JennyHuang36** Most Recent 11 months, 1 week ago

In exam Feb, 2023
upvoted 2 times

 **jtdw** 10 months, 1 week ago

What was your answer in the exam, A or D? I see a lot of people is in favor of A.
upvoted 2 times

 **TJ001** 1 year ago

private endpoint for on-premise access ..
Correct Answer A
upvoted 1 times


 **chatlisi** 1 year ago

Selected Answer: A

Service Endpoints Limitations:
"Endpoints can't be used for traffic from your premises to Azure services."
<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview#limitations>
upvoted 1 times

 **GohanF2** 1 year, 2 months ago

It's A.
Service endpoints are used when we want to call data from our Apps in Azure to our on premise services .
upvoted 3 times

 **ragav21** 1 year, 3 months ago

Selected Answer: A

Matches the requirement for private endpoint
upvoted 1 times

 **jellybiscuit** 1 year, 3 months ago

Selected Answer: A

Private endpoint fulfills all the requirements and is the current "microsoft way".
upvoted 2 times

 **khanwoo** 1 year, 4 months ago

<https://jeffbrown.tech/azure-private-service-endpoint/>
Answer should be A


upvoted 1 times

 **zenithcsa1** 1 year, 4 months ago

Selected Answer: A

private endpoint, 100%

upvoted 3 times

 **erima21** 1 year, 4 months ago

Correct!

- Service endpoints does not remove public endpoint.
- Private endpoints remove public access.

upvoted 7 times

 **Azuriste** 1 year, 5 months ago

i think is correct

upvoted 3 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a financial company that has a main datacenter in Boston and 20 branch offices across the United States. Users have Android, iOS, and Windows 10 devices.

Existing Environment -

Hybrid Environment -

The on-premises network contains an Active Directory forest named litwareinc.com that syncs to an Azure Active Directory (Azure AD) tenant named litwareinc.com by using Azure AD Connect.

All offices connect to a virtual network named Vnet1 by using a Site-to-Site VPN connection.

Azure Environment -

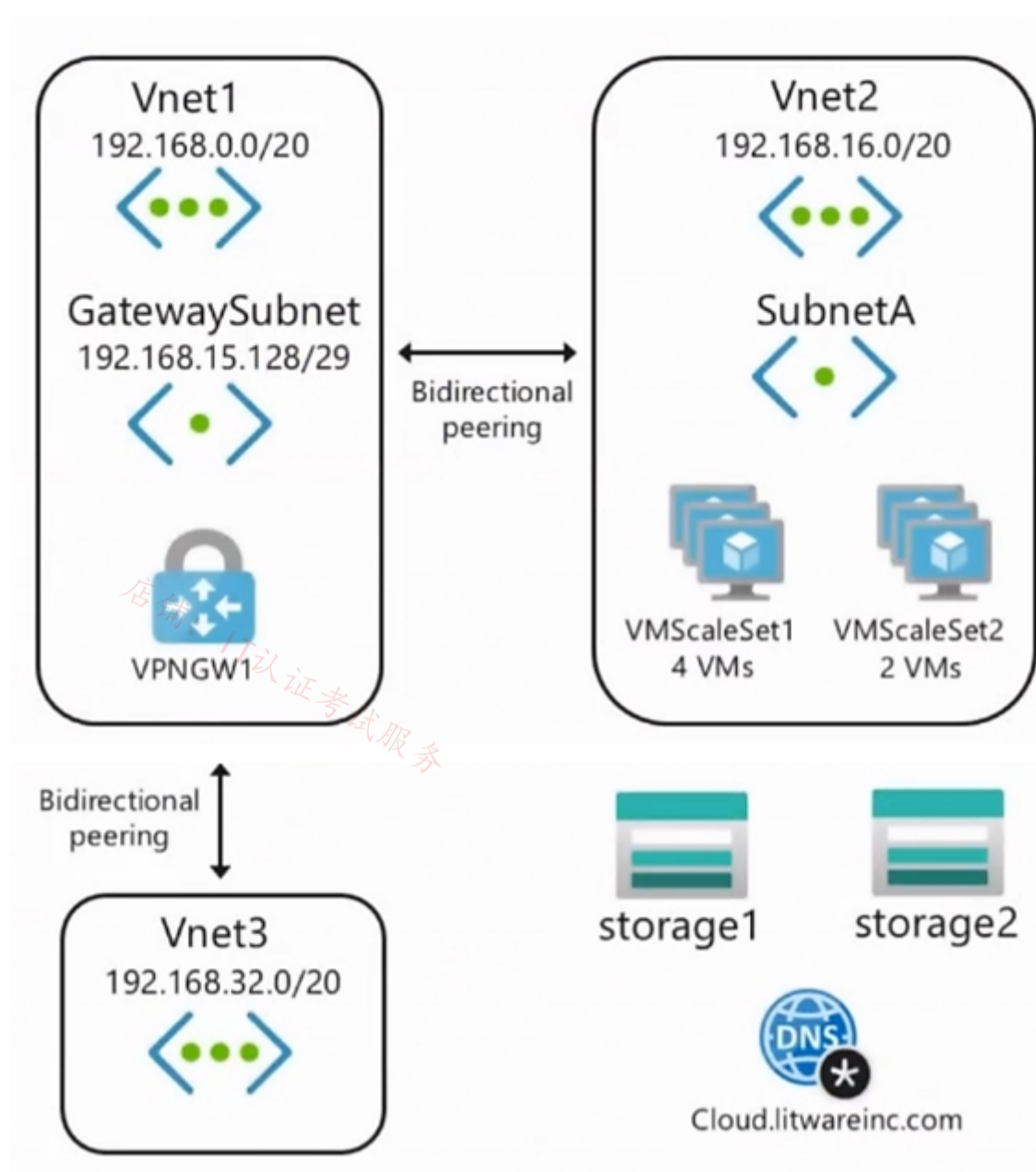
Litware has an Azure subscription named Sub1 that is linked to the litwareinc.com Azure AD tenant. Sub1 contains resources in the East US Azure region as shown in the following table.

Name	Type	Description
Vnet1	Virtual network	Uses an IP address space of 192.168.0.0/20
GatewaySubnet	Virtual network subnet	Located in Vnet1 and uses an IP address space of 192.168.15.128/29
VPNGW1	VPN gateway	Deployed to Vnet1
Vnet2	Virtual network	Uses an IP address space of 192.168.16.0/20
SubnetA	Virtual network subnet	Located in Vnet2 and uses an IP address space of 192.168.16.0/24
Vnet3	Virtual network	Uses an IP address space of 192.168.32.0/20
cloud.litwareinc.com	Private DNS zone	None
VMScaleSet1	Virtual machine scale set	Contains four virtual machines deployed to SubnetA
VMScaleSet2	Virtual machine scale set	Contains two virtual machines deployed to SubnetA
storage1	Storage account	Has the public endpoint blocked
storage2	Storage account	Has the public endpoint blocked

A diagram of the resource in the East US Azure region is shown in the Azure Network Diagram exhibit.

There is bidirectional peering between Vnet1 and Vnet2. There is bidirectional peering between Vnet1 and Vnet3. Currently, Vnet2 and Vnet3 cannot communicate directly.

Azure Network Diagram -



Requirements -

Business Requirements -

Litware wants to minimize costs whenever possible, as long as all other requirements are met.

Virtual Networking Requirements -

Litware identifies the following virtual networking requirements:

Direct the default route of 0.0.0.0/0 on Vnet2 and Vnet3 to the Boston datacenter over an ExpressRoute circuit.

Ensure that the records in the cloud.litwareinc.com can be resolved from the on-premises locations.

Automatically register the DNS names of Azure virtual machines to the cloud.litwareinc.com zone.

Minimize the size of the subnets allocated to platform-managed services.

Allow traffic from VMScaleSet1 to VMScaleSet2 on the TCP port 443 only.

Hybrid Networking Requirements -

Litware identifies the following hybrid networking requirements:

Users must be able to connect to Vnet1 by using a Point-to-Site (P2S) VPN when working remotely. Connections must be authenticated by Azure AD.

Latency of the traffic between the Boston datacenter and all the virtual networks must be minimized.

The Boston datacenter must connect to the Azure virtual networks by using an ExpressRoute FastPath connection.

Traffic between Vnet2 and Vnet3 must be routed through Vnet1.

PaaS Networking Requirements -

Litware identifies the following networking requirements for platform as a service (PaaS):

The storage1 account must be accessible from all on-premises locations without exposing the public endpoint of storage1.

The storage2 account must be accessible from Vnet2 and Vnet3 without exposing the public endpoint of storage2.

Question

You need to provide access to storage2. The solution must meet the PaaS networking requirements and the business requirements.

Which connectivity method should you use?

- A. a private endpoint
- B. Azure Firewall

- C. Azure Front Door
- D. a service endpoint

Correct Answer: D

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview>

Community vote distribution

A (62%)

D (38%)

  **wrudmen** Highly Voted 1 year, 8 months ago

Selected Answer: A

Azure Service Endpoint provides secure and direct connectivity to Azure PaaS services over an optimized route over the Azure backbone network. Traffic still left your VNet and hit the public endpoint of PaaS service. ==> Then it can't meet the goal because of the public IP

Azure Private Link (or Private Endpoint) allows you to access Azure PaaS services over Private IP address within the VNet. It's then OK

A is the answer
upvoted 26 times

  **siddique12345** 2 months, 1 week ago

According to this link, service point is the answer:

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview#key-benefits>

Service endpoints enable securing of Azure service resources to your virtual network by extending VNet identity to the service. Once you enable service endpoints in your virtual network, you can add a virtual network rule to secure the Azure service resources to your virtual network. The rule addition provides improved security by fully removing public internet access to resources and allowing traffic only from your virtual network.

upvoted 1 times

  **erima21** 1 year, 4 months ago

Correct!

- Service endpoints does not remove public endpoint.
- Private endpoints remove public access.

upvoted 8 times

  **jeffangel28** 1 year, 5 months ago

Perfectly explained!

upvoted 1 times

  **Payday123** Highly Voted 1 year, 7 months ago

Selected Answer: D

"Virtual Network (VNet) service endpoint provides secure and direct connectivity to Azure services over an optimized route over the Azure backbone network. Endpoints allow you to secure your critical Azure service resources to only your virtual networks. Service Endpoints enables private IP addresses in the VNet to reach the endpoint of an Azure service without needing a public IP address on the VNet."

And it is cheaper

upvoted 12 times

  **c2e9cb4** Most Recent 2 weeks ago

Selected Answer: D

i validate reponse D for low cost and fitting requiremnet

upvoted 1 times

  **Rododendron2** 1 month, 1 week ago

Selected Answer: D

D - requirements met & better cost. As well, there shall not be access from on premises - additional work to filter

upvoted 1 times

  **GBAU** 3 months ago

This question is likely EOL given:

<https://learn.microsoft.com/en-us/azure/expressroute/about-fastpath>

Virtual network (VNet) Peering

FastPath sends traffic directly to any VM deployed in a virtual network peered to the one connected to ExpressRoute, bypassing the ExpressRoute virtual network gateway. This feature is available for both IPv4 and IPv6 connectivity.

So with FastPath to Vnet1, it sends traffic directly to Vnet2 and Vnet3 as well (both being peered). I take this to mean no new connections for the circuit needed, and no need for a gateway transit in the peering.

upvoted 1 times

  **GBAU** 3 months ago

How did this end up in this one, it was meant for the other version of the question, doh!

upvoted 1 times

derp12352 5 months, 1 week ago

It doesn't matter if a service endpoint uses the public IP. You can still use it without EXPOSING it (the requirement listed). You would just have public access disabled.

upvoted 3 times

JennyHuang36 11 months, 1 week ago

In exam Feb, 2023

upvoted 4 times

energie 11 months, 2 weeks ago

Selected Answer: A

"Virtual Network (VNet) Service Endpoint provides secure and direct connectivity to (native)Azure services"(NOT the private services provisioned by you).

Private Endpoint brings the private services provisioned by you(like Azure Storage, Azure SQL Database etc.) to the VNet.

upvoted 1 times

staffo 11 months, 3 weeks ago

Both answers are technically correct (As the public ip is already blocked) except when it comes to costs. Service Endpoints are free and private endpoints include additional costs. So to minimise costs use Service Endpoints.

upvoted 5 times

TJ001 1 year ago

Service end point still connect to public IP of the storage account ...The question should have been better phrased to have proper use case for service endpoint..I

upvoted 2 times

chatlisi 1 year ago

Selected Answer: D

Storage 1 can be accessed from on prem via Private Endpoint only (Service Endpoint does not support on prem access)

Storage 2 should be via Service Endpoint since the communication is within Azure only.

upvoted 6 times

jellybiscuit 1 year, 3 months ago

Selected Answer: A

A - private endpoint

- a service endpoint does not remove the public endpoint. The storage account could be accessed both through the service endpoint and publicly.

I have a hard time imagining that service endpoint is the correct answer to any question that would appear on the test today.

upvoted 1 times

[Removed] 1 year, 4 months ago

Selected Answer: D

D is correct

upvoted 1 times

promto 1 year, 4 months ago

Selected Answer: A

private ip - no public access

upvoted 2 times

zenithcsa1 1 year, 4 months ago

Selected Answer: D

private / service endpoint both meet the goal, providing private connectivity from specific vNet. However, private endpoint needs more conditions such as firewall that blocking traffic from on-premises to the private endpoint or NSG for vNet1. More conditions also include more money.

Moreover, public IP address of xxx.blob.core.windows.net is always visible through nslookup even though you disabled public access in Storage-Firewall setting, adding private endpoint or private DNS zone to vNet, etc.

upvoted 1 times

zenithcsa1 1 year, 2 months ago

Ignore my answer, just confused what 'exposing the public endpoint' really means. The answer is A - private endpoint.

upvoted 1 times

examtaker20398 1 year, 6 months ago

Selected Answer: A

Service Endpoints expose a Public IP address still

upvoted 2 times

unclegrandfather 1 year, 7 months ago

Appeared on exam Jun/28/22. There were two separate questions, one about storage1 and one about storage2. Understand the concepts behind both.

upvoted 3 times

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a financial company that has a main datacenter in Boston and 20 branch offices across the United States. Users have Android, iOS, and Windows 10 devices.

Existing Environment -

Hybrid Environment -

The on-premises network contains an Active Directory forest named litwareinc.com that syncs to an Azure Active Directory (Azure AD) tenant named litwareinc.com by using Azure AD Connect.

All offices connect to a virtual network named Vnet1 by using a Site-to-Site VPN connection.

Azure Environment -

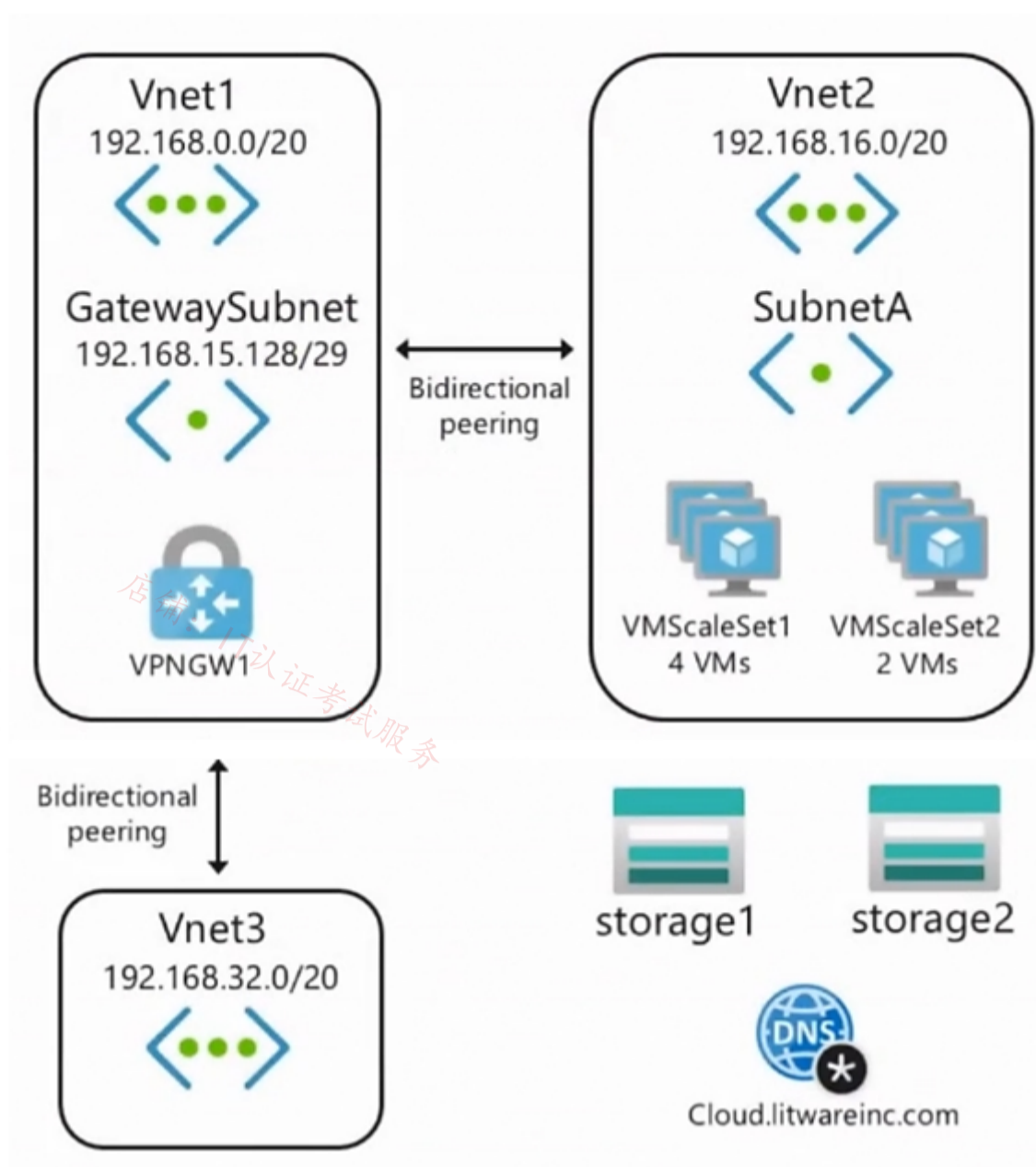
Litware has an Azure subscription named Sub1 that is linked to the litwareinc.com Azure AD tenant. Sub1 contains resources in the East US Azure region as shown in the following table.

Name	Type	Description
Vnet1	Virtual network	Uses an IP address space of 192.168.0.0/20
GatewaySubnet	Virtual network subnet	Located in Vnet1 and uses an IP address space of 192.168.15.128/29
VPNGW1	VPN gateway	Deployed to Vnet1
Vnet2	Virtual network	Uses an IP address space of 192.168.16.0/20
SubnetA	Virtual network subnet	Located in Vnet2 and uses an IP address space of 192.168.16.0/24
Vnet3	Virtual network	Uses an IP address space of 192.168.32.0/20
cloud.litwareinc.com	Private DNS zone	None
VMScaleSet1	Virtual machine scale set	Contains four virtual machines deployed to SubnetA
VMScaleSet2	Virtual machine scale set	Contains two virtual machines deployed to SubnetA
storage1	Storage account	Has the public endpoint blocked
storage2	Storage account	Has the public endpoint blocked

A diagram of the resource in the East US Azure region is shown in the Azure Network Diagram exhibit.

There is bidirectional peering between Vnet1 and Vnet2. There is bidirectional peering between Vnet1 and Vnet3. Currently, Vnet2 and Vnet3 cannot communicate directly.

Azure Network Diagram -



Requirements -

Business Requirements -

Litware wants to minimize costs whenever possible, as long as all other requirements are met.

Virtual Networking Requirements -

Litware identifies the following virtual networking requirements:

Direct the default route of 0.0.0.0/0 on Vnet2 and Vnet3 to the Boston datacenter over an ExpressRoute circuit.

Ensure that the records in the cloud.litwareinc.com can be resolved from the on-premises locations.

Automatically register the DNS names of Azure virtual machines to the cloud.litwareinc.com zone.

Minimize the size of the subnets allocated to platform-managed services.

Allow traffic from VMScaleSet1 to VMScaleSet2 on the TCP port 443 only.

Hybrid Networking Requirements -

Litware identifies the following hybrid networking requirements:

Users must be able to connect to Vnet1 by using a Point-to-Site (P2S) VPN when working remotely. Connections must be authenticated by Azure AD.

Latency of the traffic between the Boston datacenter and all the virtual networks must be minimized.

The Boston datacenter must connect to the Azure virtual networks by using an ExpressRoute FastPath connection.

Traffic between Vnet2 and Vnet3 must be routed through Vnet1.

PaaS Networking Requirements -

Litware identifies the following networking requirements for platform as a service (PaaS):

The storage1 account must be accessible from all on-premises locations without exposing the public endpoint of storage1.

The storage2 account must be accessible from Vnet2 and Vnet3 without exposing the public endpoint of storage2.

Question

HOTSPOT -

You need to implement name resolution for the cloud.litwareinc.com. The solution must meet the networking requirements.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To implement automatic DNS name registration in cloud.litwareinc.com:

	▼
Create virtual network links	
Configure conditional forwarding	
Create an SOA record in cloud.litwareinc.com	

To implement name resolution of the cloud.litwareinc.com DNS records from the on-premises locations:

	▼
Enable the Azure Firewall DNS proxy	
Create SRV records in cloud.litwareinc.com	
Deploy an Azure virtual machine configured as a DNS server to Vnet1	

Correct Answer:

Answer Area

To implement automatic DNS name registration in cloud.litwareinc.com:

	▼
Create virtual network links	
Configure conditional forwarding	
Create an SOA record in cloud.litwareinc.com	


To implement name resolution of the cloud.litwareinc.com DNS records from the on-premises locations:

	▼
Enable the Azure Firewall DNS proxy	
Create SRV records in cloud.litwareinc.com	
Deploy an Azure virtual machine configured as a DNS server to Vnet1	

Reference:

<https://docs.microsoft.com/en-us/azure/dns/private-dns-autoregistration> <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-name-resolution-for-vms-and-role-instances>


 **GhostMan135710** Highly Voted 1 year, 5 months ago
Congratulations making it to the end!
upvoted 33 times

 **jellybiscuit** Highly Voted 1 year, 3 months ago
- Typically, the test answer to this type of scenario is to build a DNS server. That does work.
- DNS proxy would also work.


If you already had a firewall, I'd go with the proxy option.
You don't though, and VMs are cheaper than firewalls.

I'm sticking with:
- virtual network link
- build a DNS server (and the implied forwarder steps that follow)

DNS Proxy
<https://azure.microsoft.com/en-us/blog/new-enhanced-dns-features-in-azure-firewall-now-generally-available/>
upvoted 8 times

 **mammoot** 11 months, 1 week ago
And this has all changed since Private DNS Resolver was introduced.. which isn't even in the exam
<https://learn.microsoft.com/en-us/azure/dns/dns-private-resolver-overview>
upvoted 4 times

 **JennyHuang36** Most Recent 11 months, 1 week ago
In exam Feb, 2023
upvoted 3 times

 **GohanF2** 1 year, 2 months ago

We cannot use DNS proxy due that there is not a firewall in place in the case, so yeah I will stick with the answer of adding a VM and add the DNS role to that server.

upvoted 3 times

🗨️ 👤 **sapien45** 1 year, 3 months ago

Firewall as a DNS Proxy would have been a great option, if there was a Firewall deployed ...
Second best option, is to deploy a dedicated VM acting as a DNS forwarded, as proposed

upvoted 1 times

🗨️ 👤 **jeffangel28** 1 year, 5 months ago

Create virtual network links -> Right

Deploy azure virtual machine.... -> False because one simplest way to do is using firewall dns proxy (<https://azure.microsoft.com/en-us/blog/new-enhanced-dns-features-in-azure-firewall-now-generally-available/>)

upvoted 2 times

🗨️ 👤 **JNishant** 1 year, 5 months ago

case study as no mention about use of Firewall.

upvoted 8 times

🗨️ 👤 **unclegrandfather** 1 year, 7 months ago

Appeared on exam Jun/28/22

upvoted 4 times

🗨️ 👤 **WickedMJ** 1 year, 5 months ago

Can you please be more helpful and tell us the answer instead?

upvoted 4 times

🗨️ 👤 **Aunehwet79** 1 year, 1 month ago

Personally, I do find it helpful to know if it turns up in the exam. Don't expect answers to be given. Use these to test your knowledge

upvoted 4 times

Topic 8 - Testlet 2

店铺: IT认证考试服务

店铺: IT认证考试服务

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in San Francisco and a branch office in Dallas.

Contoso recently purchased an Azure subscription and is performing its first pilot project in Azure.

Existing Environment -

Azure Network Infrastructure -

Contoso has an Azure Active Directory (Azure AD) tenant named contoso.com.

The Azure subscription contains the virtual networks shown in the following table.

Name	Resource group	IP address space	Location	Peered with
Vnet1	RG1	10.1.0.0/16	West US	Vnet2, Vnet3
Vnet2	RG1	172.16.0.0/16	Central US	Vnet1, Vnet3, Vnet4
Vnet3	RG2	192.168.0.0/16	Central US	Vnet1, Vnet2
Vnet4	RG2	10.10.0.0/16	West US	Vnet2
Vnet5	RG3	10.20.0.0/16	East US	None

Vnet1 contains a virtual network gateway named GW1.

Azure Virtual Machines -

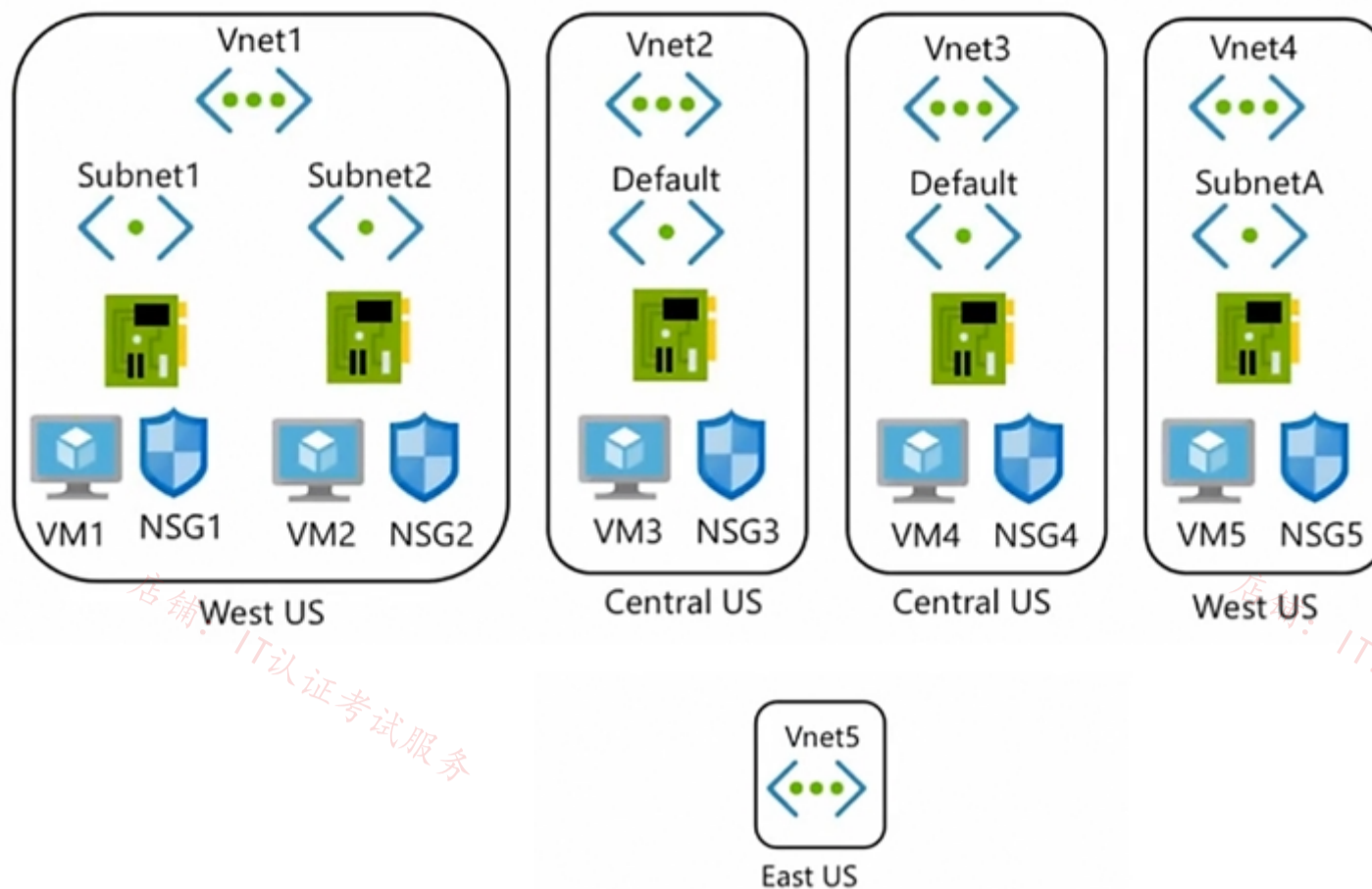
The Azure subscription contains virtual machines that run Windows Server 2019 as shown in the following table.

Name	Location	Connected to	Network security group (NSG)
VM1	West US	Vnet1/Subnet1	NSG1
VM2	West US	Vnet1/Subnet2	NSG2
VM3	Central US	Vnet2/Default	NSG3
VM4	Central US	Vnet3/Default	NSG4
VM5	West US	Vnet4/SubnetA	NSG5

The NSGs are associated to the network interfaces on the virtual machines. Each NSG has one custom security rule that allows RDP connections from the internet. The firewall on each virtual machine allows ICMP traffic.

An application security group named ASG1 is associated to the network interface of VM1.

Azure Network Infrastructure Diagram



Azure Private DNS Zones -

The Azure subscription contains the Azure private DNS zones shown in the following table.

Name	Location
zone1.contoso.com	Central US
zone2.contoso.com	West US

Zone1.contoso.com has the virtual network links shown in the following table.

Name	Virtual Network	Auto registration
Link1	Vnet2	No
Link2	Vnet3	Yes

Other Azure Resources -

The Azure subscription contains additional resources as shown in the following table.

Name	Type	Location
DB1	Azure SQL Database	West US
storage1	Azure Storage account	West US
Registry1	Azure Container Registry	Central US
KeyVault1	Azure Key Vault	Central US

Requirements -

Virtual Network Requirements -

Contoso has the following virtual network requirements:

Create a virtual network named Vnet6 in West US that will contain the following resources and configurations:

- Two container groups that connect to Vnet6
- Three virtual machines that connect to Vnet6
- Allow VPN connections to be established to Vnet6
- Allow the resources in Vnet6 to access KeyVault1, DB1, and Vnet1 over the Microsoft backbone network.

The virtual machines in Vnet4 and Vnet5 must be able to communicate over the Microsoft backbone network.

A virtual machine named VM-Analyze will be deployed to Subnet1. VM-Analyze must inspect the outbound network traffic from Subnet2 to the internet.

Network Security Requirements -

Contoso has the following network security requirements:

Configure Azure Active Directory (Azure AD) authentication for Point-to-Site (P2S) VPN users.

Enable NSG flow logs for NSG3 and NSG4.

Create an NSG named NSG10 that will be associated to Vnet1/Subnet1 and will have the custom inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
500	3389	TCP	10.1.0.0/16	Any	Deny
1000	Any	ICMP	10.10.0.0/16	VirtualNetwork	Deny

Create an NSG named NSG11 that will be associated to Vnet1/Subnet2 and will have the custom outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
200	3389	TCP	10.1.0.0/16	VirtualNetwork	Deny

Question

You need to configure GW1 to meet the network security requirements for the P2S VPN users.

Which Tunnel type should you select in the Point-to-site configuration settings of GW1?

- A. IKEv2 and OpenVPN (SSL)
- B. IKEv2
- C. IKEv2 and SSTP (SSL)
- D. OpenVPN (SSL)
- E. SSTP (SSL)

Correct Answer: D

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/openvpn-azure-ad-tenant>

Community vote distribution

D (100%)

 **wsrudmen** Highly Voted 1 year, 8 months ago

Azure AD authentication is supported for OpenVPN® protocol connections only and requires the Azure VPN Client.

And also SSTP and IKEv2 don't support all client devices:

SSTP limited to Windows

IKEv2 limited to Mac devices

upvoted 25 times

 **KeenOnTech** 3 months, 3 weeks ago

OpenVPN is correct.

As a side note though, IKEv2 is available on all three platforms and not just MacOS: <https://learn.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about#what-are-the-client-configuration-requirements>

upvoted 1 times

 **derrp** Highly Voted 1 year, 6 months ago

mnemonic device:

If you try to read this very long case study during the exam, you're going to run out of time and open up a can of worms.

open.

openVPN.

upvoted 16 times

 **Prutser2** Most Recent 1 year, 3 months ago

Selected Answer: D

openVPN, has been asked many times before

upvoted 1 times

 **jellybiscuit** 1 year, 3 months ago

Selected Answer: D

P2S + AD authentication = OpenVPN

Recurring question in multiple tests.

<https://learn.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about#authenticate-using-native-azure-active-directory-authentication>

upvoted 1 times

店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a financial company that has a main datacenter in Boston and 20 branch offices across the United States. Users have Android, iOS, and Windows 10 devices.

Existing Environment -

Hybrid Environment -

The on-premises network contains an Active Directory forest named litwareinc.com that syncs to an Azure Active Directory (Azure AD) tenant named litwareinc.com by using Azure AD Connect.

All offices connect to a virtual network named Vnet1 by using a Site-to-Site VPN connection.

Azure Environment -

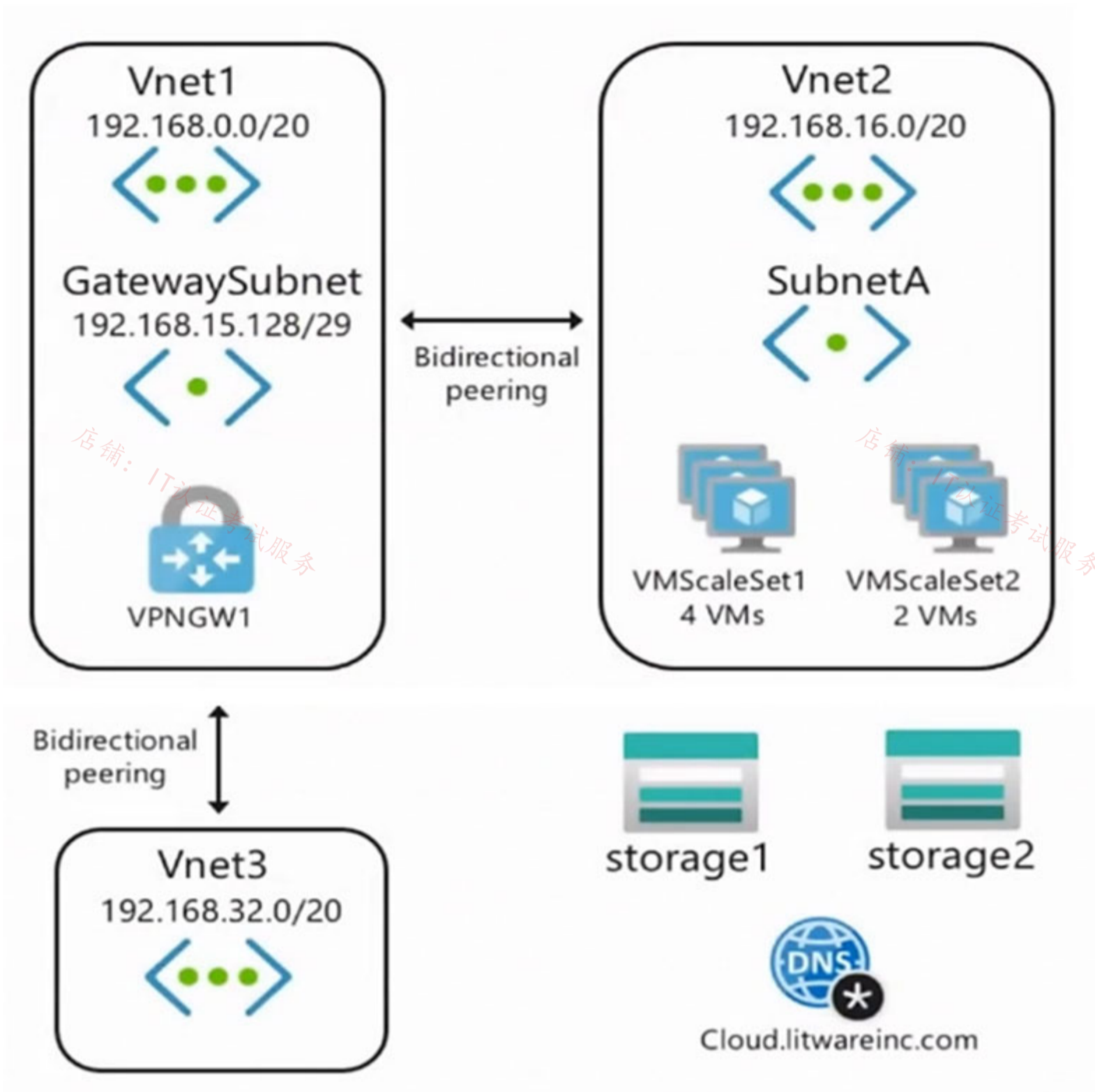
Litware has an Azure subscription named Sub1 that is linked to the litwareinc.com Azure AD tenant. Sub1 contains resources in the East US Azure region as shown in the following table.

Name	Type	Description
Vnet1	Virtual network	Uses an IP address space of 192.168.0.0/20
GatewaySubnet	Virtual network subnet	Located in Vnet1 and uses an IP address space of 192.168.15.128/29
VPNGW1	VPN gateway	Deployed to Vnet1
Vnet2	Virtual network	Uses an IP address space of 192.168.16.0/20
SubnetA	Virtual network subnet	Located in Vnet2 and uses an IP address space of 192.168.16.0/24
Vnet3	Virtual network	Uses an IP address space of 192.168.32.0/20
cloud.litwareinc.com	Private DNS zone	None
VMScaleSet1	Virtual machine scale set	Contains four virtual machines deployed to SubnetA
VMScaleSet2	Virtual machine scale set	Contains two virtual machines deployed to SubnetA
storage1	Storage account	Has the public endpoint blocked
storage2	Storage account	Has the public endpoint blocked

A diagram of the resource in the East US Azure region is shown in the Azure Network Diagram exhibit.

There is bidirectional peering between Vnet1 and Vnet2. There is bidirectional peering between Vnet1 and Vnet3. Currently, Vnet2 and Vnet3 cannot communicate directly.

Azure Network Diagram -



Requirements -

Business Requirements -

Litware wants to minimize costs whenever possible, as long as all other requirements are met.

Virtual Networking Requirements -

Litware identifies the following virtual networking requirements:

Direct the default route of 0.0.0.0/0 on Vnet2 and Vnet3 to the Boston datacenter over an ExpressRoute circuit.

Ensure that the records in the cloud.litwareinc.com can be resolved from the on-premises locations.

Automatically register the DNS names of Azure virtual machines to the cloud.litwareinc.com zone.

Minimize the size of the subnets allocated to platform-managed services.

Allow traffic from VMScaleSet1 to VMScaleSet2 on the TCP port 443 only.

Hybrid Networking Requirements -

Litware identifies the following hybrid networking requirements:

Users must be able to connect to Vnet1 by using a Point-to-Site (P2S) VPN when working remotely. Connections must be authenticated by Azure AD.

Latency of the traffic between the Boston datacenter and all the virtual networks must be minimized.

The Boston datacenter must connect to the Azure virtual networks by using an ExpressRoute FastPath connection.

Traffic between Vnet2 and Vnet3 must be routed through Vnet1.

PaaS Networking Requirements -

Litware identifies the following networking requirements for platform as a service (PaaS):

The storage1 account must be accessible from all on-premises locations without exposing the public endpoint of storage1.

The storage2 account must be accessible from Vnet2 and Vnet3 without exposing the public endpoint of storage2.

Question

DRAG DROP -

You need to prepare Vnet1 for the deployment of an ExpressRoute gateway. The solution must meet the hybrid connectivity requirements and the business requirements.

Which three actions should you perform in sequence for Vnet1? To answer, move the appropriate actions from the list of actions to the answer.

Select and Place:

Actions	Answer Area
Delete VPN GW1.	
Create a VPN gateway by using the Basic SKU.	
Set the subnet mask of Gateway Subnet to /27.	
Assign a user-defined route to Gateway Subnet.	
Create a VPN gateway by using the VPN GW1 SKU.	

Correct Answer:

Actions	Answer Area
	Delete VPN GW1.
	Create a VPN gateway by using the Basic SKU.
	Set the subnet mask of Gateway Subnet to /27.
Assign a user-defined route to Gateway Subnet.	
Create a VPN gateway by using the VPN GW1 SKU.	

Step 1: Delete the VPN GW1.

The existing VPN GW1 GatewaySubnet is too small with /29.

Users must be able to connect to Vnet1 by using a Point-to-Site (P2S) VPN when working remotely. Connections must be authenticated by Azure AD.

Litware wants to minimize costs whenever possible, as long as all other requirements are met.

Name	Type	Description
Vnet1	Virtual network	Uses an IP address space of 192.168.0.0/20
GatewaySubnet	Virtual network subnet	Located in Vnet1 and uses an IP address space of 192.168.15.128/29
VPNGW1	VPN gateway	Deployed to Vnet1

Step 2: Create a VPN gateway by using Basic SKU.

Basic SKU is good enough.

Note -

The Basic gateway SKU does not support IKEv2 or RADIUS authentication. If you plan on having Mac clients connect to your virtual network, do not use the Basic SKU.

Step 3: Set the subnet mask of Gateway Subnet to /27.

When you create the gateway subnet, you specify the number of IP addresses that the subnet contains. The number of IP addresses needed depends on the VPN gateway configuration that you want to create. Some configurations require more IP addresses than others. We [Microsoft] recommend that you create a gateway subnet that uses a /27 or /28.

It's best to specify /27 or larger (/26,/25 etc.). This allows enough IP addresses for future changes, such as adding an ExpressRoute

gateway.

Reference:

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

 **zenithcsa1** Highly Voted 1 year, 4 months ago

1. Delete VPN GW1.
2. Set the subnet mask of Gateway Subnet to /27.
3. Create a VPN gateway by using the VPN GW1 SKU.

Basic VPN Gateway does not support P2S.

If the gateway subnet is /29, you've to first delete the virtual network gateway and increase the gateway subnet size.

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways>

<https://docs.microsoft.com/en-us/azure/expressroute/how-to-configure-coexisting-gateway-portal>

upvoted 21 times

 **[Removed]** 1 year, 4 months ago

I agree, but basic VPN gateway does support P2S (SSTP Connections) but not P2S IKEv2/OpenVPN Connections. And openVPN is needed for AzureAD.

So basic can't be used here

upvoted 3 times

 **Alessandro365** Highly Voted 1 year, 4 months ago

1. Delete VPN GW1.
2. Set the subnet mask of Gateway Subnet to /27.
3. Create a VPN gateway by using the VPN GW1 SKU.

<https://learn.microsoft.com/en-us/azure/expressroute/how-to-configure-coexisting-gateway-portal>

"To configure coexisting connections for an already existing VNet:

- 1- Delete the existing ExpressRoute or Site-to-site VPN gateway.
- 2 - Delete and recreate the GatewaySubnet to have prefix of /27 or shorter.
- 3- Configure a VNet with a Site-to-Site connection and then Configure the ExpressRoute gateway.
- 4 - Once the ExpressRoute gateway is deployed, you can link the virtual network to the ExpressRoute circuit."

upvoted 10 times

 **Prutser2** 1 year, 3 months ago

also to reaffirm VPN gateway type:

ExpressRoute-VPN Gateway coexist configurations are not supported on the Basic SKU.

as per <https://learn.microsoft.com/en-us/azure/expressroute/how-to-configure-coexisting-gateway-portal> s. so concur

upvoted 1 times

 **Apptech** Most Recent 10 months ago

About the Gateway Subnet:

"When you're planning your gateway subnet size, refer to the documentation for the configuration that you're planning to create. For example, the ExpressRoute/VPN Gateway coexist configuration requires a larger gateway subnet than most other configurations. Further more, you may want to make sure your gateway subnet contains enough IP addresses to accommodate possible future configurations. While you can create a gateway subnet as small as /29, we recommend that you create a gateway subnet of /27 or larger (/27, /26 etc.). If you plan on connecting 16 ExpressRoute circuits to your gateway, you must create a gateway subnet of /26 or larger. If you're creating a dual stack gateway subnet, we recommend that you also use an IPv6 range of /64 or larger. This set up will accommodate most configurations."

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-about-virtual-network-gateways#gwsub>

upvoted 1 times

 **sellamibassem** 10 months, 3 weeks ago

Sorry. VPN GW basic sku should not work as we have Azure AD authentication

upvoted 1 times

 **sellamibassem** 10 months, 3 weeks ago

VPN GW Basic sku is enough as we have only 10 devices.

upvoted 1 times

 **JennyHuang36** 11 months, 1 week ago

In exam Feb 2023

upvoted 1 times

 **magikmarcus** 12 months ago

Also as they need to auth on the VPN PS2 with Azure AD. It needs to be OpenVPN

OpenVPN is not supported on basic SKU

<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways#gwsku>

upvoted 1 times

 **jellybiscuit** 1 year, 3 months ago

Once you realize you need to resize the subnet, the first two should be obvious.

- 1) delete gw
- 2) set subnet mask
- 3) I personally went with the "what's there is probably fine" assumption, but as others have pointed out, Basic would not work.

Sometimes you get lucky.

upvoted 4 times

  **smosmo** 1 year, 4 months ago

Following this documentation Basic Gateway is not enough for P2S Connection, but there is no other option to choose. Any comments/ideas? Should we create based on the VPN GW 1 SKU instead?

upvoted 1 times



  **tdienst** 1 year, 4 months ago

1. Delete GW1
2. Create VPN GW with GW1 SKU
3. Edit subnet mask to /27

ExpressRoute-VPN Gateway coexist configurations are not supported on the Basic SKU.
<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways>

although i feel that 2-3 are interchangeable.

upvoted 5 times

  **Cristoicach91** 1 year, 4 months ago

You need to prepare Vnet1 for the deployment of an ExpressRoute gateway.

You need to have a standard SKU VPN gate for express route p2s and s2s.

upvoted 4 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺: IT认证考试服务

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a financial company that has a main datacenter in Boston and 20 branch offices across the United States. Users have Android, iOS, and Windows 10 devices.

Existing Environment -

Hybrid Environment -

The on-premises network contains an Active Directory forest named litwareinc.com that syncs to an Azure Active Directory (Azure AD) tenant named litwareinc.com by using Azure AD Connect.

All offices connect to a virtual network named Vnet1 by using a Site-to-Site VPN connection.

Azure Environment -

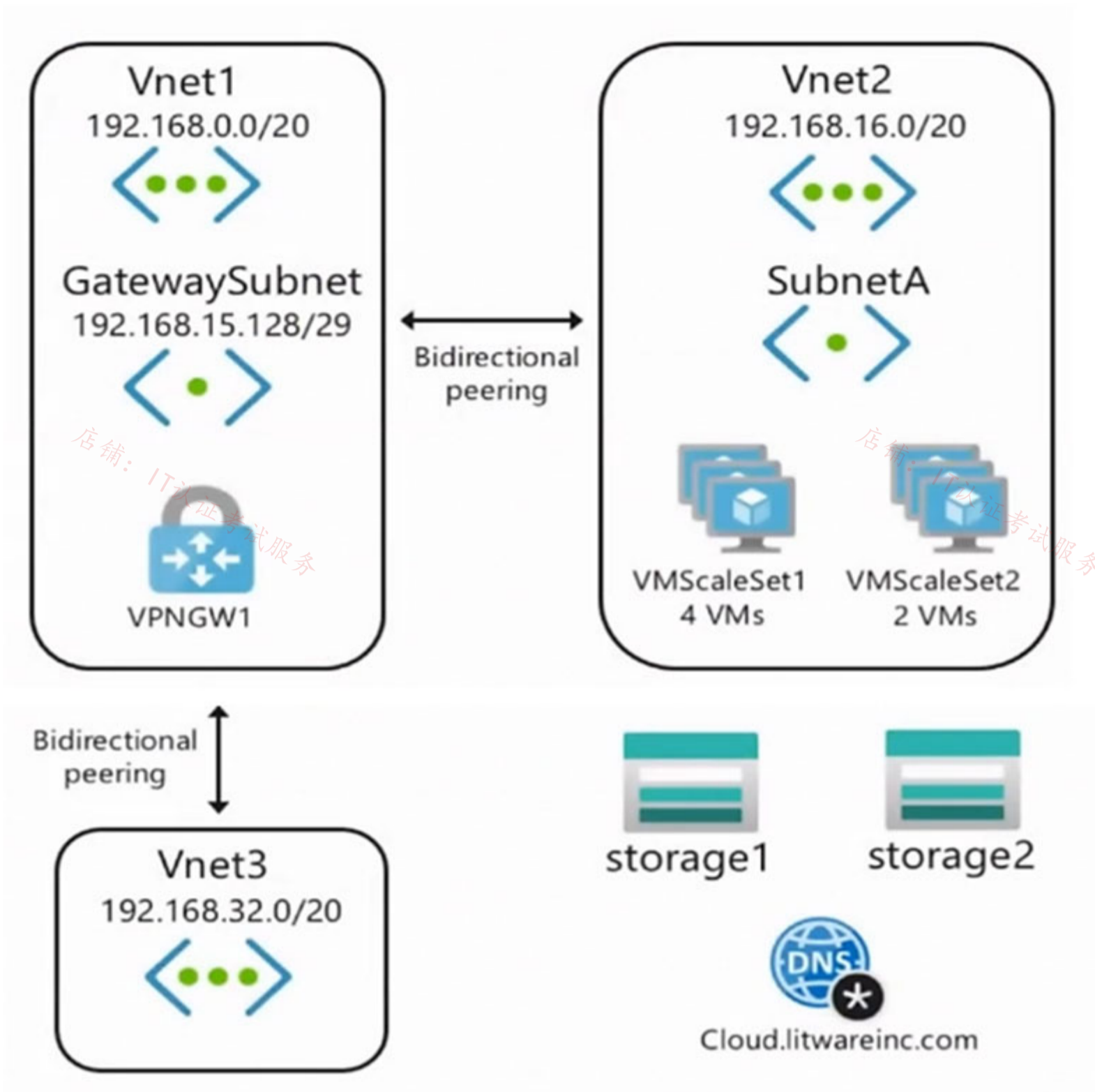
Litware has an Azure subscription named Sub1 that is linked to the litwareinc.com Azure AD tenant. Sub1 contains resources in the East US Azure region as shown in the following table.

Name	Type	Description
Vnet1	Virtual network	Uses an IP address space of 192.168.0.0/20
GatewaySubnet	Virtual network subnet	Located in Vnet1 and uses an IP address space of 192.168.15.128/29
VPNGW1	VPN gateway	Deployed to Vnet1
Vnet2	Virtual network	Uses an IP address space of 192.168.16.0/20
SubnetA	Virtual network subnet	Located in Vnet2 and uses an IP address space of 192.168.16.0/24
Vnet3	Virtual network	Uses an IP address space of 192.168.32.0/20
cloud.litwareinc.com	Private DNS zone	None
VMScaleSet1	Virtual machine scale set	Contains four virtual machines deployed to SubnetA
VMScaleSet2	Virtual machine scale set	Contains two virtual machines deployed to SubnetA
storage1	Storage account	Has the public endpoint blocked
storage2	Storage account	Has the public endpoint blocked

A diagram of the resource in the East US Azure region is shown in the Azure Network Diagram exhibit.

There is bidirectional peering between Vnet1 and Vnet2. There is bidirectional peering between Vnet1 and Vnet3. Currently, Vnet2 and Vnet3 cannot communicate directly.

Azure Network Diagram -



Requirements -

Business Requirements -

Litware wants to minimize costs whenever possible, as long as all other requirements are met.

Virtual Networking Requirements -

Litware identifies the following virtual networking requirements:

Direct the default route of 0.0.0.0/0 on Vnet2 and Vnet3 to the Boston datacenter over an ExpressRoute circuit.

Ensure that the records in the cloud.litwareinc.com can be resolved from the on-premises locations.

Automatically register the DNS names of Azure virtual machines to the cloud.litwareinc.com zone.

Minimize the size of the subnets allocated to platform-managed services.

Allow traffic from VMScaleSet1 to VMScaleSet2 on the TCP port 443 only.

Hybrid Networking Requirements -

Litware identifies the following hybrid networking requirements:

Users must be able to connect to Vnet1 by using a Point-to-Site (P2S) VPN when working remotely. Connections must be authenticated by Azure AD.

Latency of the traffic between the Boston datacenter and all the virtual networks must be minimized.

The Boston datacenter must connect to the Azure virtual networks by using an ExpressRoute FastPath connection.

Traffic between Vnet2 and Vnet3 must be routed through Vnet1.

PaaS Networking Requirements -

Litware identifies the following networking requirements for platform as a service (PaaS):

The storage1 account must be accessible from all on-premises locations without exposing the public endpoint of storage1.

The storage2 account must be accessible from Vnet2 and Vnet3 without exposing the public endpoint of storage2.

Question

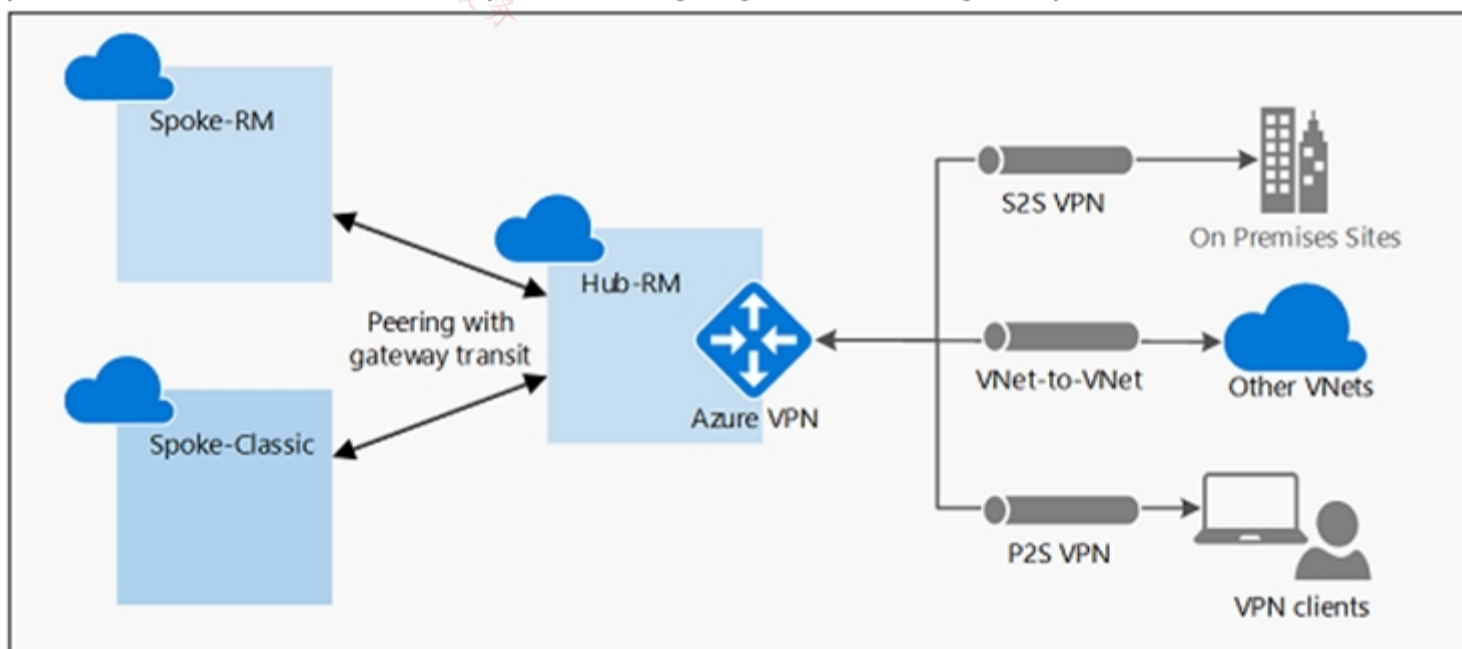
You need to connect Vnet2 and Vnet3. The solution must meet the virtual networking requirements and the business requirements. Which two actions should you include in the solution? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. On the peering from Vnet1, select Allow gateway transit.
- B. On the peerings from Vnet2 and Vnet3, select Use remote gateways.
- C. On the peerings from Vnet2 and Vnet3, select Allow gateway transit.
- D. On the peering from Vnet1, select Use remote gateways.
- E. On the peering from Vnet1, select Allow forwarded traffic.

Correct Answer: AB

Virtual network peering seamlessly connects two Azure virtual networks, merging the two virtual networks into one for connectivity purposes. Gateway transit is a peering property that lets one virtual network use the VPN gateway in the peered virtual network for cross-premises or VNet-to-VNet connectivity. The following diagram shows how gateway transit works with virtual network peering.



In the diagram, gateway transit allows the peered virtual networks to use the Azure VPN gateway in Hub-RM. Connectivity available on the VPN gateway, including S2S, P2S, and VNet-to-VNet connections,

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-peering-gateway-transit>

Community vote distribution

AB (60%)

BE (30%)

10%

mabalon 5 months ago

Looks like that question could be old.

<https://azure.microsoft.com/fr-fr/blog/create-a-transit-vnet-using-vnet-peering/>

In that blog we can see the option "allow gateway transit" on hub-to-spoke peering.

upvoted 1 times

mabalon 5 months ago

Selected Answer: AB

AB

To use virtual network peerings, in the virtual network Peering setup:

- Configure the peering connection in the hub to Allow gateway transit.
- Configure the peering connection in each spoke to Use the remote virtual network's gateway.
- Configure all peering connections to Allow forwarded traffic.

<https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke?tabs=cli#spoke-connections-to-remote-networks-through-a-hub-gateway>

upvoted 1 times

Billabongs 6 months ago


- If you consider that all the steps are being performed on the portal, there is no "Allow Gateway Transit" to be "Selected" as described in the article below:

<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-peering-gateway-transit#to-add-a-peering-and-enable-transit>

- If you consider all the steps are being performed in PowerShell, using "Add-AzVirtualNetworkPeering" command, so, you have the attribute "AllowGatewayTransit" to be "Set" not "Selected", since its a boolean option.

<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-peering-gateway-transit#ps-same>

upvoted 1 times

 **Zika69** 7 months, 2 weeks ago

Selected Answer: BE


You cannot select Gateway transit on peering on vnet1 - only allow traffic forwarded from remote virtual network

upvoted 3 times

 **nrw1020** 7 months, 1 week ago

Agree with Zika69

upvoted 1 times

 **JennyHuang36** 11 months, 1 week ago

In exam Feb, 2023

upvoted 3 times

 **TJ001** 1 year ago

AB correct however from peering perspective .. There is no mention of FW/RouteServer/NVA in the Vnet 1...so assume the VNET2 and VNET3 will learn the route from the GW

upvoted 1 times

 **alkorkin** 1 year ago

There's no option "gateway transit." in the peering configuration.

There's only "traffic forwarded from remote virtual network"

upvoted 2 times

 **alkorkin** 1 year ago

We can use "AllowGatewayTransit" in PowerShell command for peering configuration

upvoted 3 times

 **vivikar** 1 year ago

The sentence should be modified without creating confusion


upvoted 1 times

 **Prutser2** 1 year, 3 months ago

Selected Answer: AB

vnets 2 and 3 need to peer with vnet1.

upvoted 3 times

 **Alessandro365** 1 year, 3 months ago

Selected Answer: AB

A and B are the correct answer

upvoted 2 times

 **sapien45** 1 year, 3 months ago

Selected Answer: DE

There is no such thing as gateway transit option in VPC peering

gateway transit is the feature

upvoted 1 times

 **MariusKas** 1 year, 3 months ago

VPC is in GCP cloud

upvoted 2 times

 **abdx** 10 months, 2 weeks ago

AWS as well

upvoted 1 times

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a financial company that has a main datacenter in Boston and 20 branch offices across the United States. Users have Android, iOS, and Windows 10 devices.

Existing Environment -

Hybrid Environment -

The on-premises network contains an Active Directory forest named litwareinc.com that syncs to an Azure Active Directory (Azure AD) tenant named litwareinc.com by using Azure AD Connect.

All offices connect to a virtual network named Vnet1 by using a Site-to-Site VPN connection.

Azure Environment -

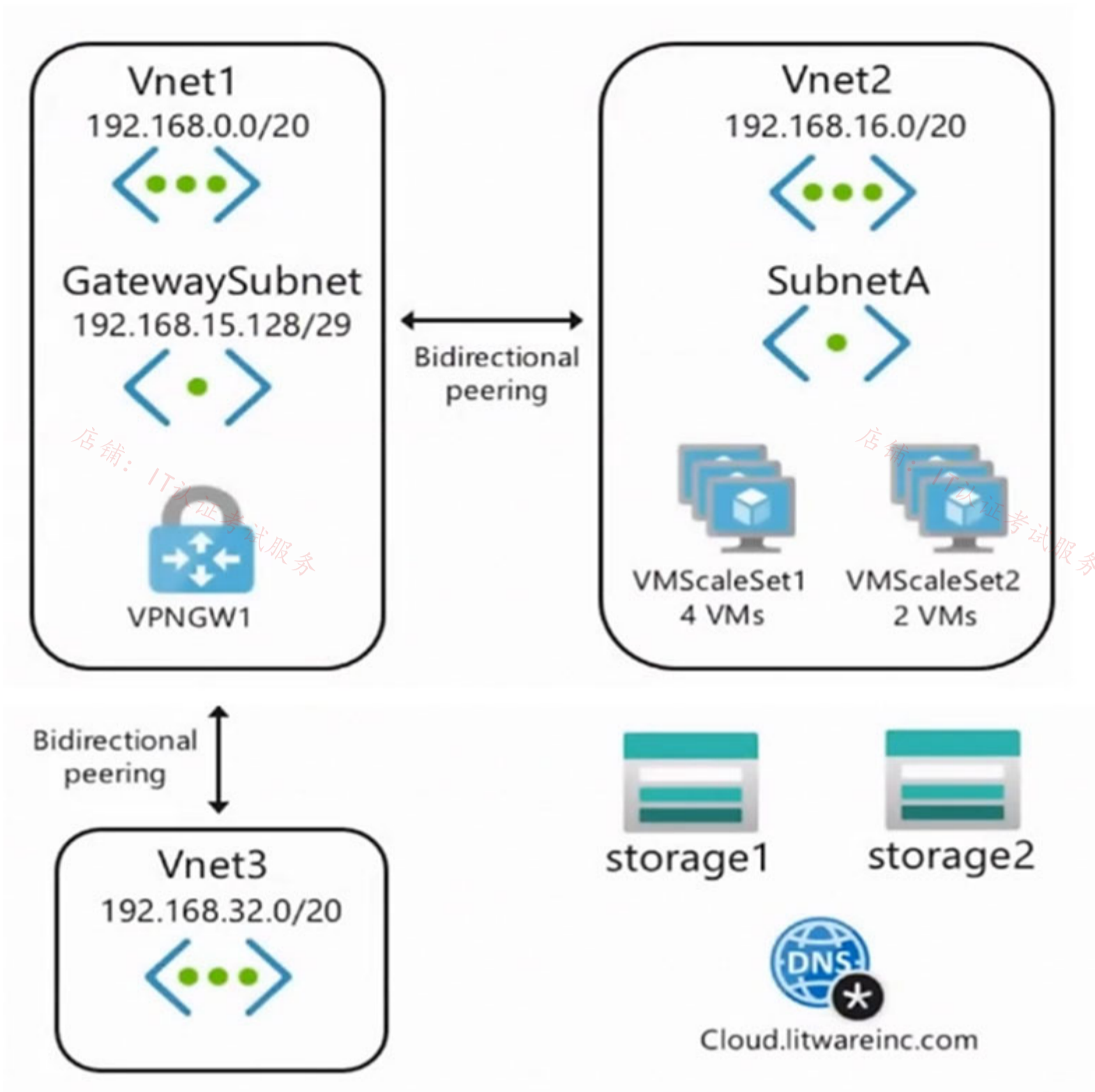
Litware has an Azure subscription named Sub1 that is linked to the litwareinc.com Azure AD tenant. Sub1 contains resources in the East US Azure region as shown in the following table.

Name	Type	Description
Vnet1	Virtual network	Uses an IP address space of 192.168.0.0/20
GatewaySubnet	Virtual network subnet	Located in Vnet1 and uses an IP address space of 192.168.15.128/29
VPNGW1	VPN gateway	Deployed to Vnet1
Vnet2	Virtual network	Uses an IP address space of 192.168.16.0/20
SubnetA	Virtual network subnet	Located in Vnet2 and uses an IP address space of 192.168.16.0/24
Vnet3	Virtual network	Uses an IP address space of 192.168.32.0/20
cloud.litwareinc.com	Private DNS zone	None
VMScaleSet1	Virtual machine scale set	Contains four virtual machines deployed to SubnetA
VMScaleSet2	Virtual machine scale set	Contains two virtual machines deployed to SubnetA
storage1	Storage account	Has the public endpoint blocked
storage2	Storage account	Has the public endpoint blocked

A diagram of the resource in the East US Azure region is shown in the Azure Network Diagram exhibit.

There is bidirectional peering between Vnet1 and Vnet2. There is bidirectional peering between Vnet1 and Vnet3. Currently, Vnet2 and Vnet3 cannot communicate directly.

Azure Network Diagram -



Requirements -

Business Requirements -

Litware wants to minimize costs whenever possible, as long as all other requirements are met.

Virtual Networking Requirements -

Litware identifies the following virtual networking requirements:

Direct the default route of 0.0.0.0/0 on Vnet2 and Vnet3 to the Boston datacenter over an ExpressRoute circuit.

Ensure that the records in the cloud.litwareinc.com can be resolved from the on-premises locations.

Automatically register the DNS names of Azure virtual machines to the cloud.litwareinc.com zone.

Minimize the size of the subnets allocated to platform-managed services.

Allow traffic from VMScaleSet1 to VMScaleSet2 on the TCP port 443 only.

Hybrid Networking Requirements -

Litware identifies the following hybrid networking requirements:

Users must be able to connect to Vnet1 by using a Point-to-Site (P2S) VPN when working remotely. Connections must be authenticated by Azure AD.

Latency of the traffic between the Boston datacenter and all the virtual networks must be minimized.

The Boston datacenter must connect to the Azure virtual networks by using an ExpressRoute FastPath connection.

Traffic between Vnet2 and Vnet3 must be routed through Vnet1.

PaaS Networking Requirements -

Litware identifies the following networking requirements for platform as a service (PaaS):

The storage1 account must be accessible from all on-premises locations without exposing the public endpoint of storage1.

The storage2 account must be accessible from Vnet2 and Vnet3 without exposing the public endpoint of storage2.

Question

HOTSPOT -

You need to implement a P2S VPN for the users in the branch office. The solution must meet the hybrid networking requirements.

What should you do? To answer, select the appropriate options in the answer area.

Hot Area:

Answer Area

On the VPN gateway in Vnet1, set the P2S VPN tunnel type to:

	▼
IKEv2	
OpenVPN (SSL)	
SSTP (SSL)	

In the litwareinc.com tenant:

	▼
Create a device object	
Create a managed identity	
Grant consent to an Azure AD application	

Correct Answer:

Answer Area

On the VPN gateway in Vnet1, set the P2S VPN tunnel type to:

	▼
IKEv2	
OpenVPN (SSL)	
SSTP (SSL)	

In the litwareinc.com tenant:

	▼
Create a device object	
Create a managed identity	
Grant consent to an Azure AD application	

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/openvpn-azure-ad-tenant>

wsrudmen Highly Voted 1 year, 8 months ago

Correct

OpenVPN because there's many device type (Users have Android, iOS, and Windows 10 devices). It's the only one configuration suitable for this.

To enable Azure AD authentication on the VPN Gateway, as Global admin you have to give consent to Azure VPN (listed as an Enterprise application)

upvoted 19 times

Prutser2 Highly Voted 1 year, 3 months ago

the way i do these exhibit questions, that usually contain a multitude of information (some of which is useless), is to go straight to the question. sometime the question does not require you to read all the exhibit info, but if it doesn, then based on the question you can filter out the relevant exhibit info, this will save you time!

upvoted 12 times

wwwmmm 2 months, 3 weeks ago

I think this even applies to the other questions as well, it's normally phrased as "you need to configure ...", then you will know what's relevant.

upvoted 1 times

JennyHuang36 Most Recent 11 months, 1 week ago

In exam Feb, 2023

upvoted 3 times

Prutser2 1 year, 3 months ago

correct

upvoted 1 times

hogs 1 year, 5 months ago

Appeared on exam Aug2022

upvoted 1 times

derrrp 1 year, 6 months ago

From the Microsoft Support Documentation:

"Sign in to the Azure portal as a user that is assigned the Global administrator role. Next, grant admin consent for your organization. This allows the Azure VPN application to sign in and read user profiles."

<https://docs.microsoft.com/en-us/azure/vpn-gateway/openvpn-azure-ad-tenant>
upvoted 1 times

 **unclegrandfather** 1 year, 7 months ago

Appeared on exam Jun/28/22
upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

Topic 10 - Testlet 4

店铺: IT认证考试服务

店铺: IT认证考试服务

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in San Francisco and a branch office in Dallas. Contoso recently purchased an Azure subscription and is performing its first pilot project in Azure.

Existing Environment -

Azure Network Infrastructure -

Contoso has an Azure Active Directory (Azure AD) tenant named contoso.com. The Azure subscription contains the virtual networks shown in the following table.

Name	Resource group	IP address space	Location	Peered with
Vnet1	RG1	10.1.0.0/16	West US	Vnet2, Vnet3
Vnet2	RG1	172.16.0.0/16	Central US	Vnet1, Vnet3, Vnet4
Vnet3	RG2	192.168.0.0/16	Central US	Vnet1, Vnet2
Vnet4	RG2	10.10.0.0/16	West US	Vnet2
Vnet5	RG3	10.20.0.0/16	East US	None

Vnet1 contains a virtual network gateway named GW1.

Azure Virtual Machines -

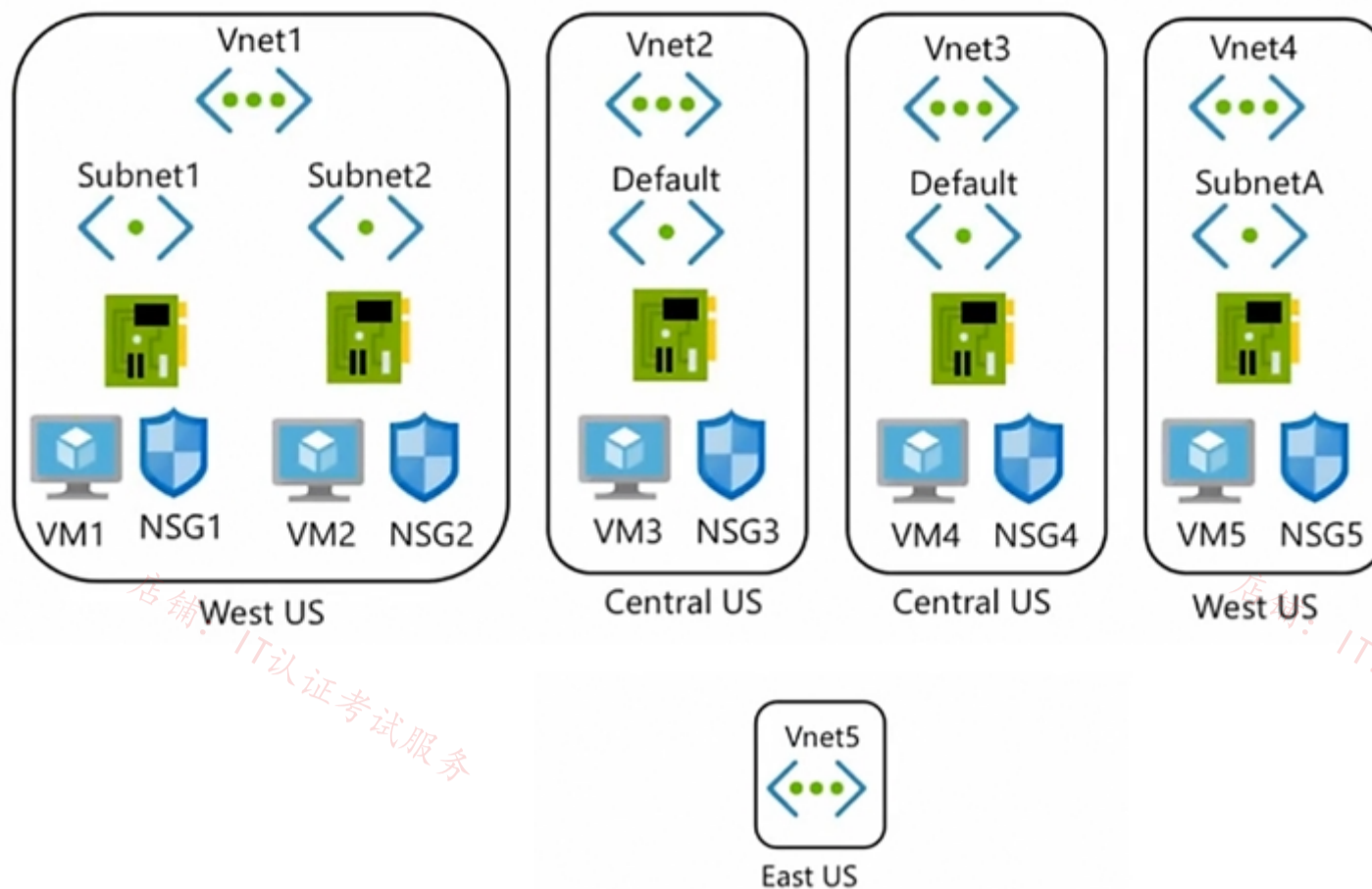
The Azure subscription contains virtual machines that run Windows Server 2019 as shown in the following table.

Name	Location	Connected to	Network security group (NSG)
VM1	West US	Vnet1/Subnet1	NSG1
VM2	West US	Vnet1/Subnet2	NSG2
VM3	Central US	Vnet2/Default	NSG3
VM4	Central US	Vnet3/Default	NSG4
VM5	West US	Vnet4/SubnetA	NSG5

The NSGs are associated to the network interfaces on the virtual machines. Each NSG has one custom security rule that allows RDP connections from the internet. The firewall on each virtual machine allows ICMP traffic.

An application security group named ASG1 is associated to the network interface of VM1.

Azure Network Infrastructure Diagram



Azure Private DNS Zones -

The Azure subscription contains the Azure private DNS zones shown in the following table.

Name	Location
zone1.contoso.com	Central US
zone2.contoso.com	West US

Zone1.contoso.com has the virtual network links shown in the following table.

Name	Virtual Network	Auto registration
Link1	Vnet2	No
Link2	Vnet3	Yes

Other Azure Resources -

The Azure subscription contains additional resources as shown in the following table.

Name	Type	Location
DB1	Azure SQL Database	West US
storage1	Azure Storage account	West US
Registry1	Azure Container Registry	Central US
KeyVault1	Azure Key Vault	Central US

Requirements -

Virtual Network Requirements -

Contoso has the following virtual network requirements:

Create a virtual network named Vnet6 in West US that will contain the following resources and configurations:

- Two container groups that connect to Vnet6
- Three virtual machines that connect to Vnet6
- Allow VPN connections to be established to Vnet6
- Allow the resources in Vnet6 to access KeyVault1, DB1, and Vnet1 over the Microsoft backbone network.

The virtual machines in Vnet4 and Vnet5 must be able to communicate over the Microsoft backbone network.

A virtual machine named VM-Analyze will be deployed to Subnet1. VM-Analyze must inspect the outbound network traffic from Subnet2 to the internet.

Network Security Requirements -

Contoso has the following network security requirements:

Configure Azure Active Directory (Azure AD) authentication for Point-to-Site (P2S) VPN users.

Enable NSG flow logs for NSG3 and NSG4.

Create an NSG named NSG10 that will be associated to Vnet1/Subnet1 and will have the custom inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
500	3389	TCP	10.1.0.0/16	Any	Deny
1000	Any	ICMP	10.10.0.0/16	VirtualNetwork	Deny

Create an NSG named NSG11 that will be associated to Vnet1/Subnet2 and will have the custom outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
200	3389	TCP	10.1.0.0/16	VirtualNetwork	Deny

Question

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Currently, VM5 can resolve names in zone2.contoso.com.	<input type="radio"/>	<input type="radio"/>
VM4 has an automatic registration in zone1.contoso.com.	<input type="radio"/>	<input type="radio"/>
You can link zone2.contoso.com to Vnet3 and enable auto registration.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
Currently, VM5 can resolve names in zone2.contoso.com.	<input type="radio"/>	<input checked="" type="radio"/>
VM4 has an automatic registration in zone1.contoso.com.	<input checked="" type="radio"/>	<input type="radio"/>
You can link zone2.contoso.com to Vnet3 and enable auto registration.	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: No -

Zone2.contoso.com is not linked to any virtual networks. Therefore, no VMs are able to resolve names in the zone.

Box 2: Yes -

VM4 is in VNet3. Zone1.contoso.com has a link to VNet3 and auto-registration is enabled on the link.

Box3: No -

VNet3 is linked to zone1.contoso.com and auto-registration is enabled on the link. A virtual network can only have one registration zone.

You can link zone2.contoso.com to VNet3 but you won't be able to enable auto-registration on the link.

 **derrp** Highly Voted 1 year, 6 months ago

No:

Zone 2 is not linked to any VNETs therefor no VMs can resolve names in Zone 2.

Yes:

VM4 is in VNET3 which has autoregistration enabled with a Link to Zone 1

No:

VNETs can only be linked to one Zone. VNET3 is already linked to Zone 1.

All answers can be interpreted by analysis of the above information without any surprises.

upvoted 25 times

 **Dimetrodon** 1 year, 3 months ago

To clarify point 3, yes you are right about a VNET can be linked to only 1 zone. However this is if the zone is set to auto-registration. i.e. Registration virtual network

If the vnet is linked to a private DNS zone and has auto registration turned off i.e. A Resolution virtual network, then the vnet can have multiple virtual network links from that vnet, however only one of those links can be a Registration virtual network. i.e. - set for auto registration.

upvoted 3 times

 **Madball** 11 months, 3 weeks ago

You can have two private DNS zones linked to the same vnet, however only 1 private DNS zone can have auto-registration enabled, this is why the final question is no.

upvoted 6 times

 **Prutser2** 1 year, 3 months ago

zone 2 is not explicitly "not linked", so therefore assuming it is not linked at all.

they way these questions are written up popen for suggestions/assumptions, is just mind baffling

upvoted 2 times

 **wsrudmen** Highly Voted 1 year, 8 months ago

CORRECT

upvoted 5 times

 **TJ001** Most Recent 1 year ago

Correct No Yes No

upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in San Francisco and a branch office in Dallas.

Contoso recently purchased an Azure subscription and is performing its first pilot project in Azure.

Existing Environment -

Azure Network Infrastructure -

Contoso has an Azure Active Directory (Azure AD) tenant named contoso.com.

The Azure subscription contains the virtual networks shown in the following table.

Name	Resource group	IP address space	Location	Peered with
Vnet1	RG1	10.1.0.0/16	West US	Vnet2, Vnet3
Vnet2	RG1	172.16.0.0/16	Central US	Vnet1, Vnet3, Vnet4
Vnet3	RG2	192.168.0.0/16	Central US	Vnet1, Vnet2
Vnet4	RG2	10.10.0.0/16	West US	Vnet2
Vnet5	RG3	10.20.0.0/16	East US	None

Vnet1 contains a virtual network gateway named GW1.

Azure Virtual Machines -

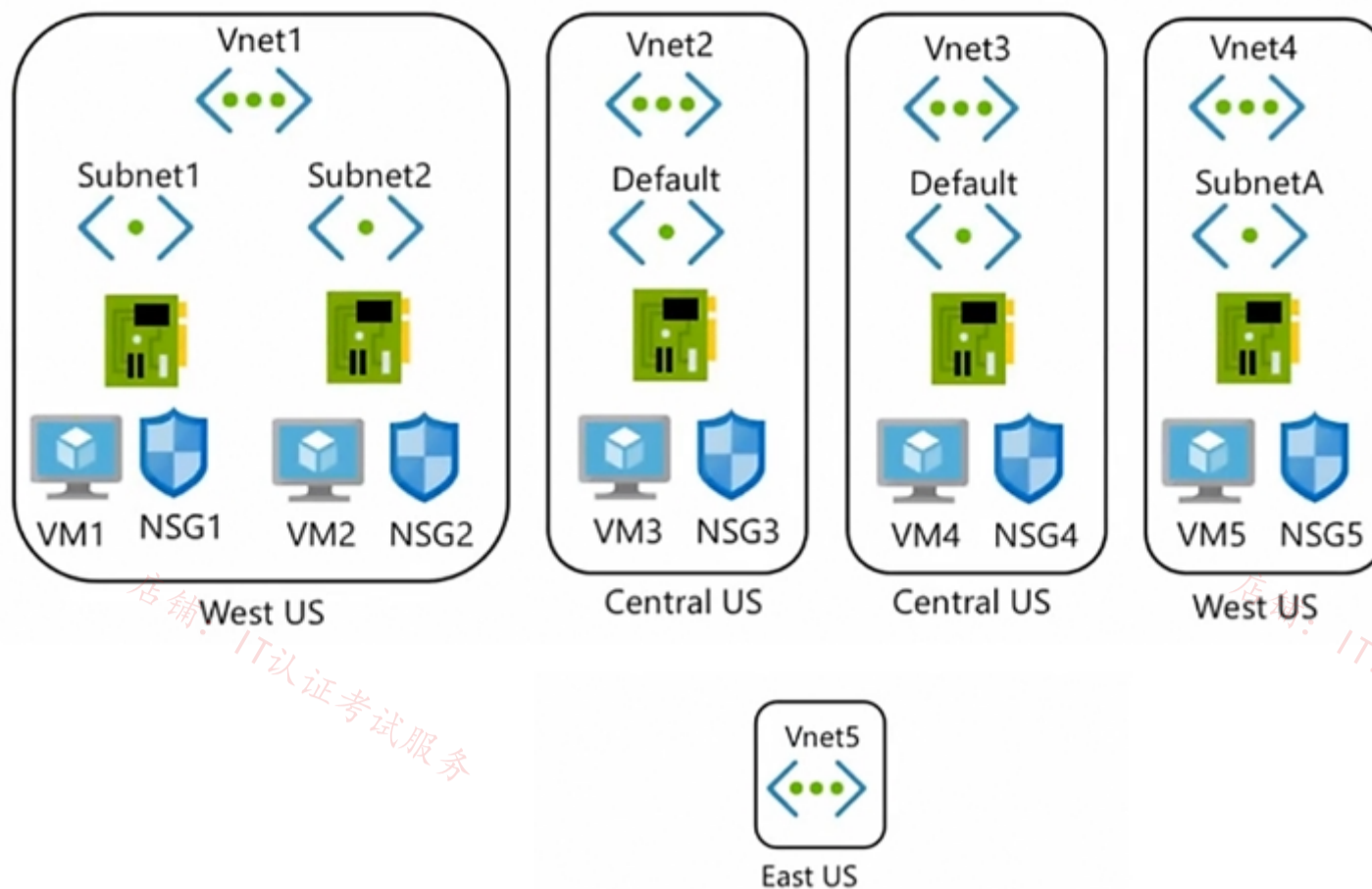
The Azure subscription contains virtual machines that run Windows Server 2019 as shown in the following table.

Name	Location	Connected to	Network security group (NSG)
VM1	West US	Vnet1/Subnet1	NSG1
VM2	West US	Vnet1/Subnet2	NSG2
VM3	Central US	Vnet2/Default	NSG3
VM4	Central US	Vnet3/Default	NSG4
VM5	West US	Vnet4/SubnetA	NSG5

The NSGs are associated to the network interfaces on the virtual machines. Each NSG has one custom security rule that allows RDP connections from the internet. The firewall on each virtual machine allows ICMP traffic.

An application security group named ASG1 is associated to the network interface of VM1.

Azure Network Infrastructure Diagram



Azure Private DNS Zones -

The Azure subscription contains the Azure private DNS zones shown in the following table.

Name	Location
zone1.contoso.com	Central US
zone2.contoso.com	West US

Zone1.contoso.com has the virtual network links shown in the following table.

Name	Virtual Network	Auto registration
Link1	Vnet2	No
Link2	Vnet3	Yes

Other Azure Resources -

The Azure subscription contains additional resources as shown in the following table.

Name	Type	Location
DB1	Azure SQL Database	West US
storage1	Azure Storage account	West US
Registry1	Azure Container Registry	Central US
KeyVault1	Azure Key Vault	Central US

Requirements -

Virtual Network Requirements -

Contoso has the following virtual network requirements:

Create a virtual network named Vnet6 in West US that will contain the following resources and configurations:

- Two container groups that connect to Vnet6
- Three virtual machines that connect to Vnet6
- Allow VPN connections to be established to Vnet6
- Allow the resources in Vnet6 to access KeyVault1, DB1, and Vnet1 over the Microsoft backbone network.

The virtual machines in Vnet4 and Vnet5 must be able to communicate over the Microsoft backbone network.

A virtual machine named VM-Analyze will be deployed to Subnet1. VM-Analyze must inspect the outbound network traffic from Subnet2 to the internet.

Network Security Requirements -

Contoso has the following network security requirements:

Configure Azure Active Directory (Azure AD) authentication for Point-to-Site (P2S) VPN users.

Enable NSG flow logs for NSG3 and NSG4.

Create an NSG named NSG10 that will be associated to Vnet1/Subnet1 and will have the custom inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
500	3389	TCP	10.1.0.0/16	Any	Deny
1000	Any	ICMP	10.10.0.0/16	VirtualNetwork	Deny

Create an NSG named NSG11 that will be associated to Vnet1/Subnet2 and will have the custom outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
200	3389	TCP	10.1.0.0/16	VirtualNetwork	Deny

Question

HOTSPOT -

Which virtual machines can VM1 and VM4 ping successfully? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

VM1:

	▼
VM2 only	
VM2 and VM4 only	
VM2, VM3, and VM4 only	
VM2, VM3, VM4, and VM5	

VM4:

	▼
VM3 only	
VM1 and VM3 only	
VM1, VM2, and VM3 only	
VM1, VM2, VM3, and VM5	

Answer Area

VM1:

	▼
VM2 only	
VM2 and VM4 only	
VM2, VM3, and VM4 only	
VM2, VM3, VM4, and VM5	

Correct Answer:

VM4:

	▼
VM3 only	
VM1 and VM3 only	
VM1, VM2, and VM3 only	
VM1, VM2, VM3, and VM5	

Box 1: VM2, VM3 and VM4.

VM1 is in VNet1/Subnet1. VNet1 is peered with VNet2 and VNet3.

There are no NSGs blocking outbound ICMP from VNet1. There are no NSGs blocking inbound ICMP to VNet1/Subnet2, VNet2 or VNet3.

Therefore, VM1 can ping VM2 in VNet1/Subnet2, VM3 in VNet2 and VM4 in VNet3.

Box 2:

VM4 is in VNet3. VNet3 is peered with VNet1 and VNet2. There are no NSGs blocking outbound ICMP from VNet3. There are no NSGs blocking inbound ICMP to VNet1/Subnet1, VNet1/Subnet2 or VNet2 from VNet3 (NSG10 blocks inbound ICMP from VNet4 but not from VNet3). Therefore, VM4 can ping VM1 in VNet1/Subnet1, VM2 in VNet1/Subnet2 and VM3 in VNet2.

 **derrrp** Highly Voted 1 year, 6 months ago

Been cramming on this one all week. Reviewed this question so many times now, it's muscle memory: The sequence is 234 then 123

Write that sequence down several times on your keyboard and you'll never forget it:

234123 234123 234123


Hope this helps!

upvoted 15 times

 **Ayokun** 11 months ago

I think just excluding VM5 is simpler lol

upvoted 7 times

 **Aunehwet79** 1 year, 1 month ago

Thanks this does help

upvoted 1 times

 **Ajdlfasudfo** 1 year, 1 month ago

big IQ brain that tries to just remember it

upvoted 1 times

 **wooyourdaddy** 1 year, 5 months ago

Nice memory association tip ;-)

upvoted 1 times

 **vikrants31** Most Recent 1 month, 2 weeks ago

vnet1(VM1+VM2) --peering-->vnet2(VM3) --peering-->vnet4(VM5)

\ /

peering peering

\ /

vnet3(VM4)

> I think VM1 can ping: 2,3,4,5 (see above diagram)


> I think VM4 can ping VM2, VM3, VM5 but since there is no option for that so, the only available correct option is "VM3 only"

upvoted 1 times

 **ejml** 12 months ago

There is a peering between VN2 and VN5, why is not reachable VM4 from VM1 and VM4?

upvoted 1 times

 **MrBlueSky** 9 months, 2 weeks ago

There is not a peering between Vnet2 and Vnet5.

upvoted 3 times

 **dsmurray88** 1 year ago

Default NSG rule allows all ports inbound and outbound for the VirtualNetwork service tag. This encompasses any peered networks

The VM Firewalls allow ICMP

So any VMs in peered VNets can ping

The answer is 1234 (1 > 2,3,4) (4 > 1,2,3)

upvoted 2 times

 **TJ001** 1 year ago

correct answer

upvoted 1 times

 **TJ001** 1 year ago

It is not hard ...only two things to be checked ...

1) Is there a peering in place ?

2) Is there a NSG rule blocking ?

Do that is order and we are good with the answers

upvoted 1 times

 **DeepMoon** 1 year ago


Default Inbound or Outbound rule doesn't allow ICMP.

VM1 can only ping VM2. Default rule for inside vnet will allow it.

VM4 cannot ping anything. Default Outbound rule will block it.

<https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#default-security-rules>

upvoted 1 times

  **Aanandan** 1 year, 3 months ago

They ask from which VM's can ping VM1 and VM4 successfully... We can ping VM1 from VM2,VM3,VM4 and VM4 from VM1,VM2,VM3...
Because
NSG Inbound rule deny the RDP port from 10.1.x.x to any destination...
NSG Inbound rule deny the ICMP from 10.10.x.x to any destination
10.0.0.0/16 is Vnet4 address space..so VM5 only is available in this Vnet..


NSG outbound rule deny the RDP port from 10.1.x.x to any destination...
By default outbound rule for any to any virtual network is enabled..
Already peering is enabled between Vnet1,vnet2,vnet3... obviously ping will happen successfully...
Please correct me if anything wrong in my understanding

upvoted 1 times

  **GeorgeMilev91** 1 year ago

no mate, they are not asking this, please read the question again, they are asking from vm1 and vm4 which hosts you can ping i.e. vm1, vm4 -> vm2 and etc, not vice-versa..

upvoted 1 times

  **lobs_wort** 1 year, 6 months ago

Answer is correct, appeared in exam 22-July-2022.

upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in San Francisco and a branch office in Dallas. Contoso recently purchased an Azure subscription and is performing its first pilot project in Azure.

Existing Environment -

Azure Network Infrastructure -

Contoso has an Azure Active Directory (Azure AD) tenant named contoso.com. The Azure subscription contains the virtual networks shown in the following table.

Name	Resource group	IP address space	Location	Peered with
Vnet1	RG1	10.1.0.0/16	West US	Vnet2, Vnet3
Vnet2	RG1	172.16.0.0/16	Central US	Vnet1, Vnet3, Vnet4
Vnet3	RG2	192.168.0.0/16	Central US	Vnet1, Vnet2
Vnet4	RG2	10.10.0.0/16	West US	Vnet2
Vnet5	RG3	10.20.0.0/16	East US	None

Vnet1 contains a virtual network gateway named GW1.

Azure Virtual Machines -

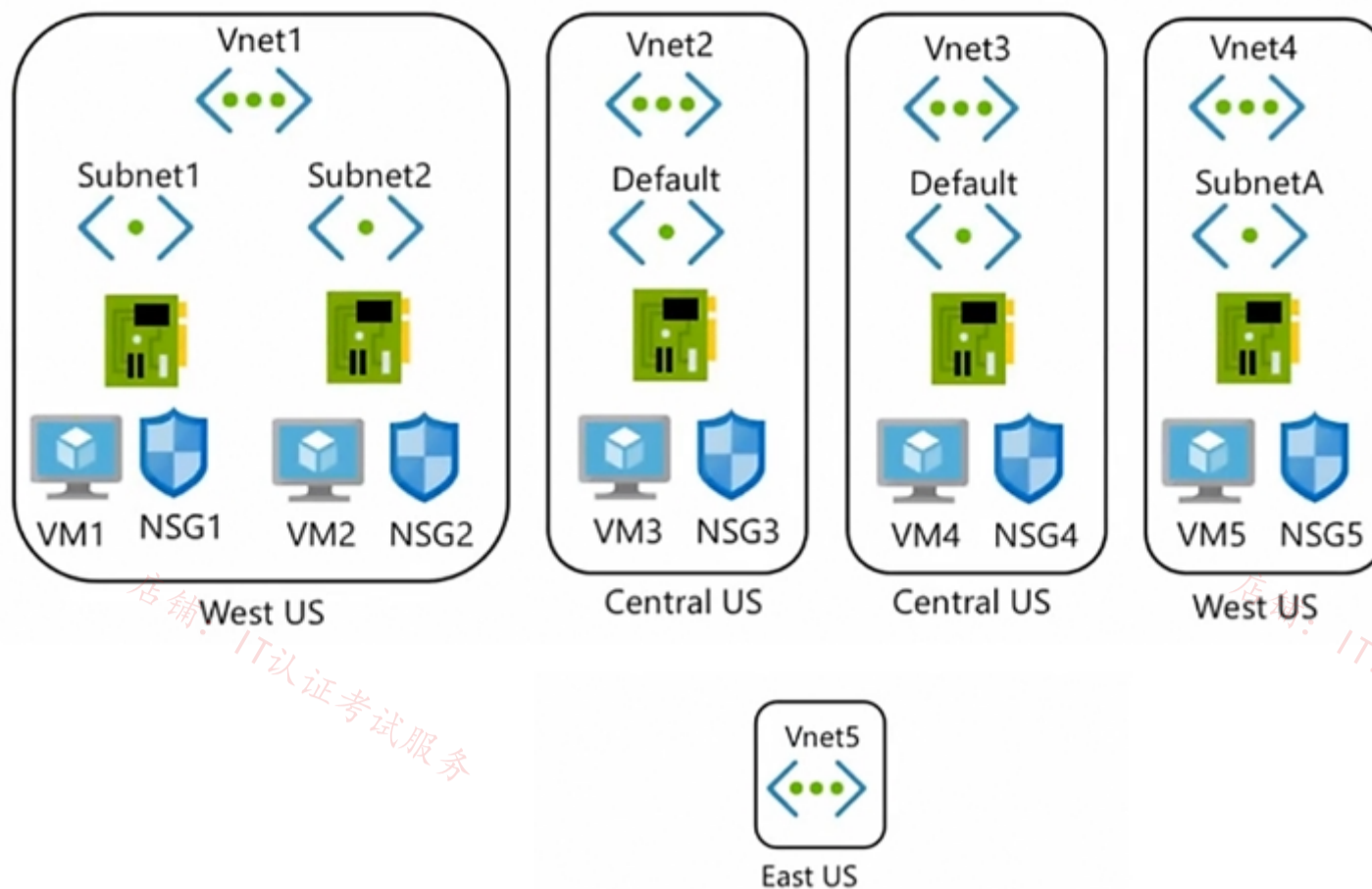
The Azure subscription contains virtual machines that run Windows Server 2019 as shown in the following table.

Name	Location	Connected to	Network security group (NSG)
VM1	West US	Vnet1/Subnet1	NSG1
VM2	West US	Vnet1/Subnet2	NSG2
VM3	Central US	Vnet2/Default	NSG3
VM4	Central US	Vnet3/Default	NSG4
VM5	West US	Vnet4/SubnetA	NSG5

The NSGs are associated to the network interfaces on the virtual machines. Each NSG has one custom security rule that allows RDP connections from the internet. The firewall on each virtual machine allows ICMP traffic.

An application security group named ASG1 is associated to the network interface of VM1.

Azure Network Infrastructure Diagram



Azure Private DNS Zones -

The Azure subscription contains the Azure private DNS zones shown in the following table.

Name	Location
zone1.contoso.com	Central US
zone2.contoso.com	West US

Zone1.contoso.com has the virtual network links shown in the following table.

Name	Virtual Network	Auto registration
Link1	Vnet2	No
Link2	Vnet3	Yes

Other Azure Resources -

The Azure subscription contains additional resources as shown in the following table.

Name	Type	Location
DB1	Azure SQL Database	West US
storage1	Azure Storage account	West US
Registry1	Azure Container Registry	Central US
KeyVault1	Azure Key Vault	Central US

Requirements -

Virtual Network Requirements -

Contoso has the following virtual network requirements:

Create a virtual network named Vnet6 in West US that will contain the following resources and configurations:

- Two container groups that connect to Vnet6
- Three virtual machines that connect to Vnet6
- Allow VPN connections to be established to Vnet6
- Allow the resources in Vnet6 to access KeyVault1, DB1, and Vnet1 over the Microsoft backbone network.

The virtual machines in Vnet4 and Vnet5 must be able to communicate over the Microsoft backbone network.

A virtual machine named VM-Analyze will be deployed to Subnet1. VM-Analyze must inspect the outbound network traffic from Subnet2 to the internet.

Network Security Requirements -

Contoso has the following network security requirements:

Configure Azure Active Directory (Azure AD) authentication for Point-to-Site (P2S) VPN users.

Enable NSG flow logs for NSG3 and NSG4.

Create an NSG named NSG10 that will be associated to Vnet1/Subnet1 and will have the custom inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
500	3389	TCP	10.1.0.0/16	Any	Deny
1000	Any	ICMP	10.10.0.0/16	VirtualNetwork	Deny

Create an NSG named NSG11 that will be associated to Vnet1/Subnet2 and will have the custom outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
200	3389	TCP	10.1.0.0/16	VirtualNetwork	Deny

Question

What should you implement to meet the virtual network requirements for the virtual machines that connect to Vnet4 and Vnet5?

- A. a private endpoint
- B. a routing table
- C. a service endpoint
- D. a private link service
- E. a virtual network peering

Correct Answer: E

There is no virtual network peering between VM4's VNet (VNet3) and VM5's VNet (VNet4). To enable the VMs to communicate over the Microsoft backbone network a VNet peering is required between VNet3 and VNet4.

Community vote distribution

E (100%)

Lazylinux 3 months ago

Selected Answer: E

E is correct however it should say GLOBAL virtual Network peering since both vNET 4 and 5 are in different regions
<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview>
 upvoted 1 times

lfteris_k 11 months ago

Selected Answer: E

Vnet Peering with no doubt
 upvoted 2 times

omgMerrick 11 months, 1 week ago

Selected Answer: E

Answer is correct: E. virtual network peering

Virtual network peering connects two Azure virtual networks. Once peered, the virtual networks appear as one for connectivity purposes. Traffic between virtual machines in the peered virtual networks is routed through the Microsoft backbone infrastructure, through private IP addresses only. No public internet is involved.

Source:

<https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/vnet-peering#virtual-network-connection-types>
 upvoted 1 times

Prutser2 1 year, 3 months ago

Selected Answer: E

correct
 upvoted 1 times

GhostMan135710 1 year, 5 months ago

Selected Answer: E

Correct

upvoted 2 times

Topic 11 - Testlet 5

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a financial company that has a main datacenter in Boston and 20 branch offices across the United States. Users have Android, iOS, and Windows 10 devices.

Existing Environment -

Hybrid Environment -

The on-premises network contains an Active Directory forest named litwareinc.com that syncs to an Azure Active Directory (Azure AD) tenant named litwareinc.com by using Azure AD Connect.

All offices connect to a virtual network named Vnet1 by using a Site-to-Site VPN connection.

Azure Environment -

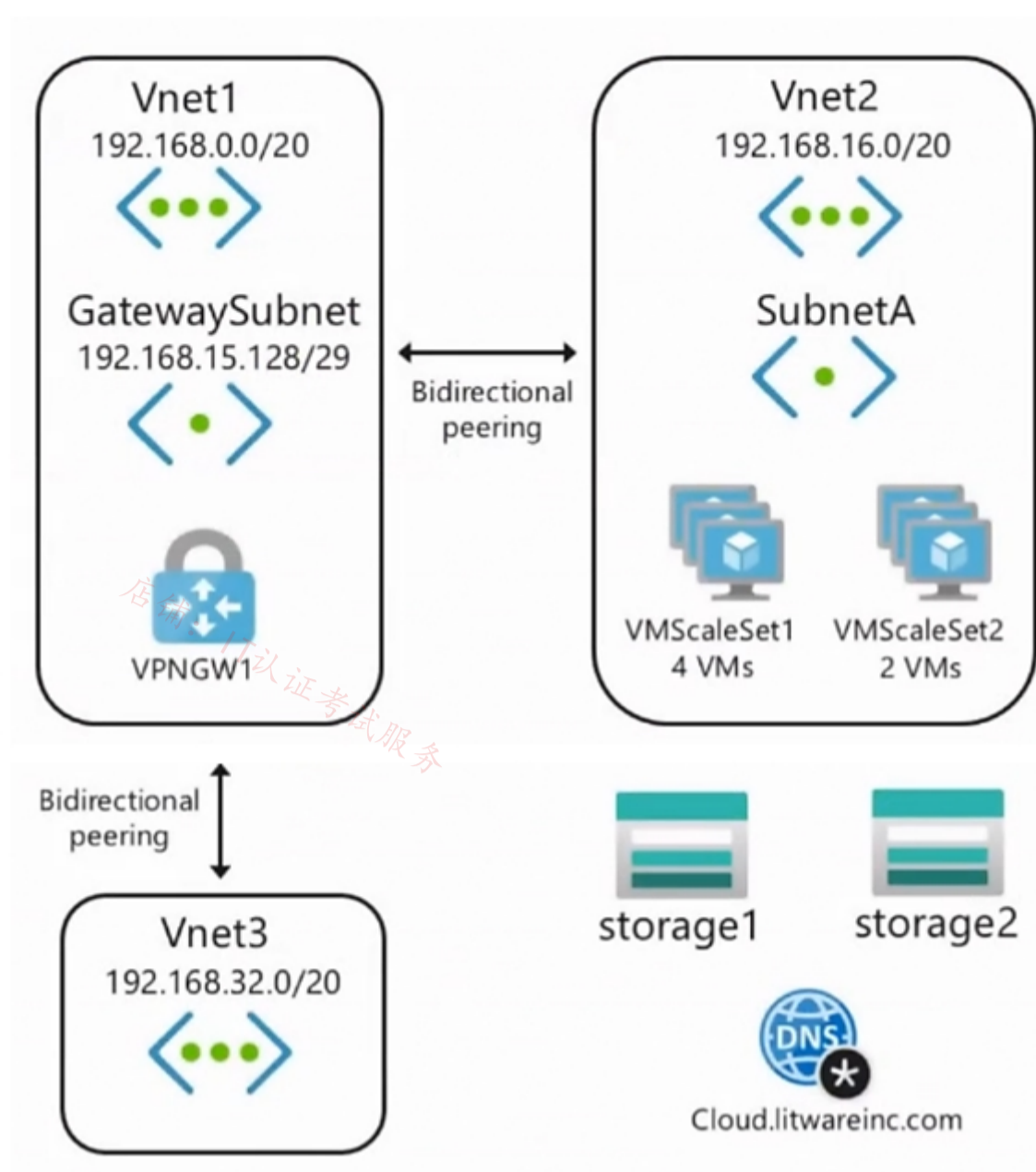
Litware has an Azure subscription named Sub1 that is linked to the litwareinc.com Azure AD tenant. Sub1 contains resources in the East US Azure region as shown in the following table.

Name	Type	Description
Vnet1	Virtual network	Uses an IP address space of 192.168.0.0/20
GatewaySubnet	Virtual network subnet	Located in Vnet1 and uses an IP address space of 192.168.15.128/29
VPNGW1	VPN gateway	Deployed to Vnet1
Vnet2	Virtual network	Uses an IP address space of 192.168.16.0/20
SubnetA	Virtual network subnet	Located in Vnet2 and uses an IP address space of 192.168.16.0/24
Vnet3	Virtual network	Uses an IP address space of 192.168.32.0/20
cloud.litwareinc.com	Private DNS zone	None
VMScaleSet1	Virtual machine scale set	Contains four virtual machines deployed to SubnetA
VMScaleSet2	Virtual machine scale set	Contains two virtual machines deployed to SubnetA
storage1	Storage account	Has the public endpoint blocked
storage2	Storage account	Has the public endpoint blocked

A diagram of the resource in the East US Azure region is shown in the Azure Network Diagram exhibit.

There is bidirectional peering between Vnet1 and Vnet2. There is bidirectional peering between Vnet1 and Vnet3. Currently, Vnet2 and Vnet3 cannot communicate directly.

Azure Network Diagram -



Requirements -

Business Requirements -

Litware wants to minimize costs whenever possible, as long as all other requirements are met.

Virtual Networking Requirements -

Litware identifies the following virtual networking requirements:

Direct the default route of 0.0.0.0/0 on Vnet2 and Vnet3 to the Boston datacenter over an ExpressRoute circuit.

Ensure that the records in the cloud.litwareinc.com can be resolved from the on-premises locations.

Automatically register the DNS names of Azure virtual machines to the cloud.litwareinc.com zone.

Minimize the size of the subnets allocated to platform-managed services.

Allow traffic from VMScaleSet1 to VMScaleSet2 on the TCP port 443 only.

Hybrid Networking Requirements -

Litware identifies the following hybrid networking requirements:

Users must be able to connect to Vnet1 by using a Point-to-Site (P2S) VPN when working remotely. Connections must be authenticated by Azure AD.

Latency of the traffic between the Boston datacenter and all the virtual networks must be minimized.

The Boston datacenter must connect to the Azure virtual networks by using an ExpressRoute FastPath connection.

Traffic between Vnet2 and Vnet3 must be routed through Vnet1.

PaaS Networking Requirements -

Litware identifies the following networking requirements for platform as a service (PaaS):

The storage1 account must be accessible from all on-premises locations without exposing the public endpoint of storage1.

The storage2 account must be accessible from Vnet2 and Vnet3 without exposing the public endpoint of storage2.

Question

You need to configure the default route on Vnet2 and Vnet3. The solution must meet the virtual networking requirements.

What should you use to configure the default route?

- A. route filters
- B. BGP route exchange

- C. a user-defined route assigned to GatewaySubnet in Vnet1
- D. a user-defined route assigned to GatewaySubnet in Vnet2 and Vnet3

Correct Answer: B

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview>

Community vote distribution

B (100%)

Fearless90 Highly Voted 1 year, 7 months ago

Selected Answer: B

B. BGP route exchange

Virtual Networking Requirements

Direct the default route of 0.0.0.0/0 on Vnet2 and Vnet3 to the Boston datacenter over an ExpressRoute circuit.

upvoted 11 times

Fearless90 1 year, 7 months ago

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview#border-gateway-protocol>

Border gateway protocol

An on-premises network gateway can exchange routes with an Azure virtual network gateway using the border gateway protocol (BGP). Using BGP with an Azure virtual network gateway is dependent on the type you selected when you created the gateway. If the type you selected were:

- ExpressRoute: You must use BGP to advertise on-premises routes to the Microsoft Edge router. You can't create user-defined routes to force traffic to the ExpressRoute virtual network gateway if you deploy a virtual network gateway deployed as type: ExpressRoute. You can use user-defined routes for forcing traffic from the Express Route to, for example, a Network Virtual Appliance.

upvoted 2 times

Fearless90 1 year, 7 months ago

Repeated question

<https://www.examtopycs.com/discussions/microsoft/view/74497-exam-az-700-topic-10-question-3-discussion/>

upvoted 2 times

Fearless90 1 year, 7 months ago

Repeated question

<https://www.examtopycs.com/discussions/microsoft/view/64711-exam-az-700-topic-9-question-2-discussion/>

upvoted 2 times

Fearless90 1 year, 7 months ago

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

Virtual network gateway: Specify when you want traffic destined for specific address prefixes routed to a virtual network gateway. The virtual network gateway must be created with type VPN. You can't specify a virtual network gateway created as type ExpressRoute in a user-defined route because with ExpressRoute, you must use BGP for custom routes. You can't specify Virtual Network Gateways if you have VPN and ExpressRoute coexisting connections either. You can define a route that directs traffic destined for the 0.0.0.0/0 address prefix to a route-based virtual network gateway. On your premises, you might have a device that inspects the traffic and determines whether to forward or drop the traffic. If you intend to create a user-defined route for the 0.0.0.0/0 address prefix, read 0.0.0.0/0 address prefix first. Instead of configuring a user-defined route for the 0.0.0.0/0 address prefix, you can advertise a route with the 0.0.0.0/0 prefix via BGP, if you've enabled BGP for a VPN virtual network gateway.

upvoted 2 times

Lazylinux Most Recent 3 months ago

Selected Answer: B

Is B Is Honey as per

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview>

upvoted 1 times

mrgreat 10 months ago

To configure the default route on Vnet2 and Vnet3, we can use BGP route exchange. This would allow us to advertise the default route of 0.0.0.0/0 from the Boston datacenter over an ExpressRoute circuit to Vnet2 and Vnet3. This meets the requirement to direct the default route of 0.0.0.0/0 on Vnet2 and Vnet3 to the Boston datacenter over an ExpressRoute circuit.

Option A, route filters, are used to allow or deny routes based on a set of defined rules. They are not used to configure the default route.

Option C, a user-defined route assigned to GatewaySubnet in Vnet1, would only affect traffic within Vnet1, and not traffic from Vnet2 and Vnet3 to the Boston datacenter.

Option D, a user-defined route assigned to GatewaySubnet in Vnet2 and Vnet3, would only affect traffic within Vnet2 and Vnet3, and not traffic from Vnet2 and Vnet3 to the Boston datacenter.

Therefore, the correct answer is B. BGP route exchange.

upvoted 4 times

JennyHuang36 11 months, 1 week ago

In exam Feb 2023

upvoted 2 times

 **mhmyz** 1 year ago

I think D is Ans.

If you enable BGP and 0.0.0.0/0 is propagated from on-premises,
Works like a request.

However, this question does not have information that confirms that it is propagated from on-premises.
No.

<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-forced-tunneling>

There is also a method of setting a forced tunnel with UDR without using BGP as follows,

There is a possibility that D is the correct answer

In that case, the next hop will be the gateway.

upvoted 2 times

 **cypher9** 1 year, 6 months ago

B is correct.

upvoted 1 times

 **Payday123** 1 year, 7 months ago

All answers are wrong :) BGP will not help to propagate default route? VNet2 and VNet3 don't know that they have to send default traffic (0.0.0.0/0) to Vnet1

upvoted 4 times

 **sapien45** 1 year, 3 months ago

You are wrong homie.

BGP enables multiple gateways to learn and propagate prefixes from different networks, whether they are directly or indirectly connected. This can enable transit routing with Azure VPN gateways between your on-premises sites or across multiple Azure Virtual Networks.

<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-bgp-overview#transitrouting>

upvoted 1 times

 **sapien45** 1 year, 3 months ago

<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-bgp-resource-manager-ps?toc=%2Fazure%2Fvirtual-network%2Ftoc.json#part-3---establish-a-vnet-to-vnet-connection-with-bgp>

VNet2 and VNet3 will exchange route informations though vnet to vnet connection via bgp with vnet1

upvoted 1 times

 **unclegrandfather** 1 year, 7 months ago

Appeared on exam Jun/28/22

upvoted 1 times

 **wsrudmen** 1 year, 8 months ago


Selected Answer: B

It's correct.

You can create custom routes by either creating user-defined routes, or by exchanging border gateway protocol (BGP) routes between your on-premises network gateway and an Azure virtual network gateway.

As it's mentioned "Direct the default route of 0.0.0.0/0 on Vnet2 and Vnet3 to the Boston datacenter over an ExpressRoute circuit." then UDR doesn't match, we need BGP protocol

upvoted 1 times

 **Kay04** 1 year, 9 months ago

is the answer B or C?

upvoted 1 times

 **RVR** 1 year, 8 months ago

the action on vnet 1 is c, but the question is what needs to be done on vnet2 &3, so i guess enabling bgp is required.

upvoted 1 times

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a financial company that has a main datacenter in Boston and 20 branch offices across the United States. Users have Android, iOS, and Windows 10 devices.

Existing Environment -

Hybrid Environment -

The on-premises network contains an Active Directory forest named litwareinc.com that syncs to an Azure Active Directory (Azure AD) tenant named litwareinc.com by using Azure AD Connect.

All offices connect to a virtual network named Vnet1 by using a Site-to-Site VPN connection.

Azure Environment -

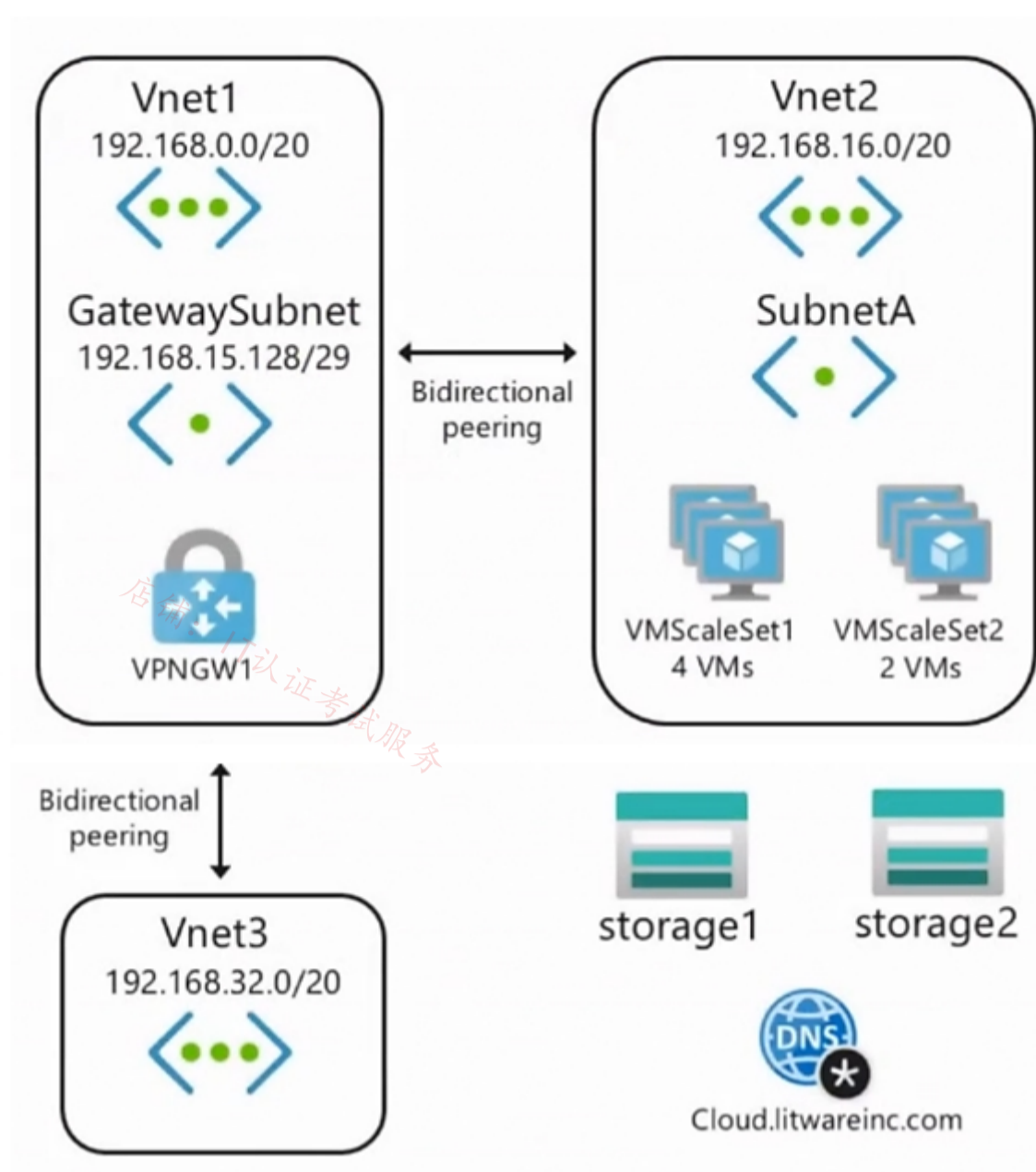
Litware has an Azure subscription named Sub1 that is linked to the litwareinc.com Azure AD tenant. Sub1 contains resources in the East US Azure region as shown in the following table.

Name	Type	Description
Vnet1	Virtual network	Uses an IP address space of 192.168.0.0/20
GatewaySubnet	Virtual network subnet	Located in Vnet1 and uses an IP address space of 192.168.15.128/29
VPNGW1	VPN gateway	Deployed to Vnet1
Vnet2	Virtual network	Uses an IP address space of 192.168.16.0/20
SubnetA	Virtual network subnet	Located in Vnet2 and uses an IP address space of 192.168.16.0/24
Vnet3	Virtual network	Uses an IP address space of 192.168.32.0/20
cloud.litwareinc.com	Private DNS zone	None
VMScaleSet1	Virtual machine scale set	Contains four virtual machines deployed to SubnetA
VMScaleSet2	Virtual machine scale set	Contains two virtual machines deployed to SubnetA
storage1	Storage account	Has the public endpoint blocked
storage2	Storage account	Has the public endpoint blocked

A diagram of the resource in the East US Azure region is shown in the Azure Network Diagram exhibit.

There is bidirectional peering between Vnet1 and Vnet2. There is bidirectional peering between Vnet1 and Vnet3. Currently, Vnet2 and Vnet3 cannot communicate directly.

Azure Network Diagram -



Requirements -

Business Requirements -

Litware wants to minimize costs whenever possible, as long as all other requirements are met.

Virtual Networking Requirements -

Litware identifies the following virtual networking requirements:

Direct the default route of 0.0.0.0/0 on Vnet2 and Vnet3 to the Boston datacenter over an ExpressRoute circuit.

Ensure that the records in the cloud.litwareinc.com can be resolved from the on-premises locations.

Automatically register the DNS names of Azure virtual machines to the cloud.litwareinc.com zone.

Minimize the size of the subnets allocated to platform-managed services.

Allow traffic from VMScaleSet1 to VMScaleSet2 on the TCP port 443 only.

Hybrid Networking Requirements -

Litware identifies the following hybrid networking requirements:

Users must be able to connect to Vnet1 by using a Point-to-Site (P2S) VPN when working remotely. Connections must be authenticated by Azure AD.

Latency of the traffic between the Boston datacenter and all the virtual networks must be minimized.

The Boston datacenter must connect to the Azure virtual networks by using an ExpressRoute FastPath connection.

Traffic between Vnet2 and Vnet3 must be routed through Vnet1.

PaaS Networking Requirements -

Litware identifies the following networking requirements for platform as a service (PaaS):

The storage1 account must be accessible from all on-premises locations without exposing the public endpoint of storage1.

The storage2 account must be accessible from Vnet2 and Vnet3 without exposing the public endpoint of storage2.

Question

DRAG DROP -

You need to implement outbound connectivity for VMScaleSet1. The solution must meet the virtual networking requirements and the business requirements.

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.

Select and Place:

Actions

Create a health probe

Create a public load balancer in the Standard SKU

Create a public load balancer in the Basic SKU

Create a backend pool that contains VMSScaleSet1

Create a NAT rule

Create an outbound rule

Answer Area



Correct Answer:

Actions

Create a health probe

Create a public load balancer in the Basic SKU

Create a NAT rule

Answer Area

Create a public load balancer in the Standard SKU

Create a backend pool that contains VMSScaleSet1

Create an outbound rule



Reference:

<https://docs.microsoft.com/en-us/azure/load-balancer/skus>

<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-outbound-connections#outboundrules>

Fearless90 Highly Voted 1 year, 7 months ago

Answer

Create a public load balancer in the Standard SKU

Create a backend pool that contains VMSScaleSet1

Create an outbound rule

upvoted 13 times

Fearless90 1 year, 7 months ago

Repeat

<https://www.examtopy.com/discussions/microsoft/view/68612-exam-az-700-topic-9-question-1-discussion/>

upvoted 1 times

Lazylinux Most Recent 3 months ago

Given answer is correct HTTPS health probe and Outbound Rules are ONLY supported on STD LB

upvoted 1 times

roshingrg 8 months ago

public Standard Load Balancer with an HTTPS configuration, along with a backend pool, health probe, and outbound rule, you can follow the steps outlined in the Microsoft Learn module you provided. However, I can provide you with a high-level overview of the steps involved:

Create a Standard Load Balancer:

Specify the load balancer's name, SKU (Standard), and public frontend IP configuration.

Configure the HTTPS protocol for the frontend IP configuration.

Set up the SSL certificate if required.

Create a Backend Pool:

Create a backend pool that includes the virtual machines in VMSScaleSet1.

Associate the backend pool with the frontend IP configuration of the load balancer.

Configure Health Probe:

Create a health probe with the required settings, such as the port (443) and probe interval.

Associate the health probe with the backend pool.

Create Outbound Rule:
Define an outbound rule for the load balancer.
Specify the backend pool and health probe to use for outbound traffic.
upvoted 2 times

🗨️ 👤 **Crazysaffer** 8 months, 1 week ago

As far as i know, if you don't create a health probe, then the LB is not going to work. I think it should be in this order
1 - Create a public load Standard balancer (HTTPS = Standard)
2 - Create a backend pool that contains VMScaleSet1
3 - Create a Health probe (port 443)
4 - Create a Outbound rule (needs a backend pool and a Health Probe)
upvoted 1 times

🗨️ 👤 **TJ001** 1 year ago

correct answer
upvoted 1 times

🗨️ 👤 **Goofer** 1 year ago

1 - Create a public load Standard balancer (HTTPS = Standard)
2 - Create a backend pool that contains VMScaleSet1
3 - Create a Health probe (port 443)
4 - Create a Outbound rule (needs a backend pool and a Health Probe)

<https://learn.microsoft.com/en-us/training/modules/load-balancing-non-https-traffic-azure/4-exercise-create-configure-azure-load-balancer>
upvoted 3 times

🗨️ 👤 **Goofer** 1 year ago

1 - Create a public Standard Load balancer (HTTPS = Standard)

<https://learn.microsoft.com/en-us/training/modules/load-balancing-non-https-traffic-azure/3-design-implement-azure-load-balancer-using-azure-portal>

upvoted 1 times

🗨️ 👤 **unclegrandfather** 1 year, 7 months ago

Appeared on exam Jun/28/22
upvoted 3 times

🗨️ 👤 **Fearless90** 1 year, 7 months ago

<https://docs.microsoft.com/en-us/azure/load-balancer/skus>
SKU comparison

Azure Load Balancer has 3 SKUs - Basic, Standard, and Gateway. Each SKU is catered towards a specific scenario and has differences in scale, features, and pricing.

To compare and understand the differences between Basic and Standard SKU, see the following table.

Outbound Rules

Standard Load Balancer - Declarative outbound NAT configuration

Basic Load Balancer - Not available

upvoted 3 times

🗨️ 👤 **Fearless90** 1 year, 7 months ago

<https://docs.microsoft.com/en-us/azure/load-balancer/quickstart-load-balancer-standard-public-portal>

Create load balancer

In this section, you'll create a zone redundant load balancer that load balances virtual machines. With zone-redundancy, one or more availability zones can fail and the data path survives as long as one zone in the region remains healthy.

During the creation of the load balancer, you'll configure:

Frontend IP address

Backend pool

Inbound load-balancing rules

Health probe

Note

In this example we'll create a NAT gateway to provide outbound Internet access. The outbound rules tab in the configuration is bypassed as it's optional isn't needed with the NAT gateway. For more information on Azure NAT gateway, see [What is Azure Virtual Network NAT?](#) For more information about outbound connections in Azure, see [Source Network Address Translation \(SNAT\) for outbound connections](#)

upvoted 2 times

🗨️ 👤 **Fearless90** 1 year, 7 months ago

<https://docs.microsoft.com/en-us/azure/load-balancer/quickstart-load-balancer-standard-public-portal>

Create the virtual network

In this section, you'll create a virtual network, subnet, and Azure Bastion host. The virtual network and subnet contains the load balancer and virtual machines. The bastion host is used to securely manage the virtual machines and install IIS to test the load balancer.

upvoted 1 times

🗨️ 👤 **Fearless90** 1 year, 7 months ago


<https://docs.microsoft.com/en-us/azure/load-balancer/quickstart-load-balancer-standard-public-portal>

Create virtual machines

In this section, you'll create two VMs (myVM1 and myVM2) in two different zones (Zone 1, and Zone 2).

These VMs are added to the backend pool of the load balancer that was created earlier.

upvoted 1 times

 **Fearless90** 1 year, 7 months ago

<https://docs.microsoft.com/en-us/azure/load-balancer/quickstart-load-balancer-standard-public-portal>

Note

Azure provides a default outbound access IP for VMs that either aren't assigned a public IP address or are in the back-end pool of an internal basic Azure load balancer. The default outbound access IP mechanism provides an outbound IP address that isn't configurable.

For more information, see Default outbound access in Azure.

The default outbound access IP is disabled when either a public IP address is assigned to the VM or the VM is placed in the back-end pool of a standard load balancer, with or without outbound rules. If an Azure Virtual Network network address translation (NAT) gateway resource is assigned to the subnet of the virtual machine, the default outbound access IP is disabled.

VMs that are created by virtual machine scale sets in flexible orchestration mode don't have default outbound access.

For more information about outbound connections in Azure, see Use source network address translation (SNAT) for outbound connections.
upvoted 1 times

 **wsrudmen** 1 year, 8 months ago

It's correct.

Outbound rules is not available for Basic Load Balancer then Standard SKU is required.

After it's a backend pool to link VMScaleSet and the LB. And it's an outbound rule as there's no address translation in this case.

upvoted 2 times

Topic 12 - Testlet 6

店铺: IT认证考试服务

店铺: IT认证考试服务

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in San Francisco and a branch office in Dallas. Contoso recently purchased an Azure subscription and is performing its first pilot project in Azure.

Existing Environment -

Azure Network Infrastructure -

Contoso has an Azure Active Directory (Azure AD) tenant named contoso.com. The Azure subscription contains the virtual networks shown in the following table.

Name	Resource group	IP address space	Location	Peered with
Vnet1	RG1	10.1.0.0/16	West US	Vnet2, Vnet3
Vnet2	RG1	172.16.0.0/16	Central US	Vnet1, Vnet3, Vnet4
Vnet3	RG2	192.168.0.0/16	Central US	Vnet1, Vnet2
Vnet4	RG2	10.10.0.0/16	West US	Vnet2
Vnet5	RG3	10.20.0.0/16	East US	None

Vnet1 contains a virtual network gateway named GW1.

Azure Virtual Machines -

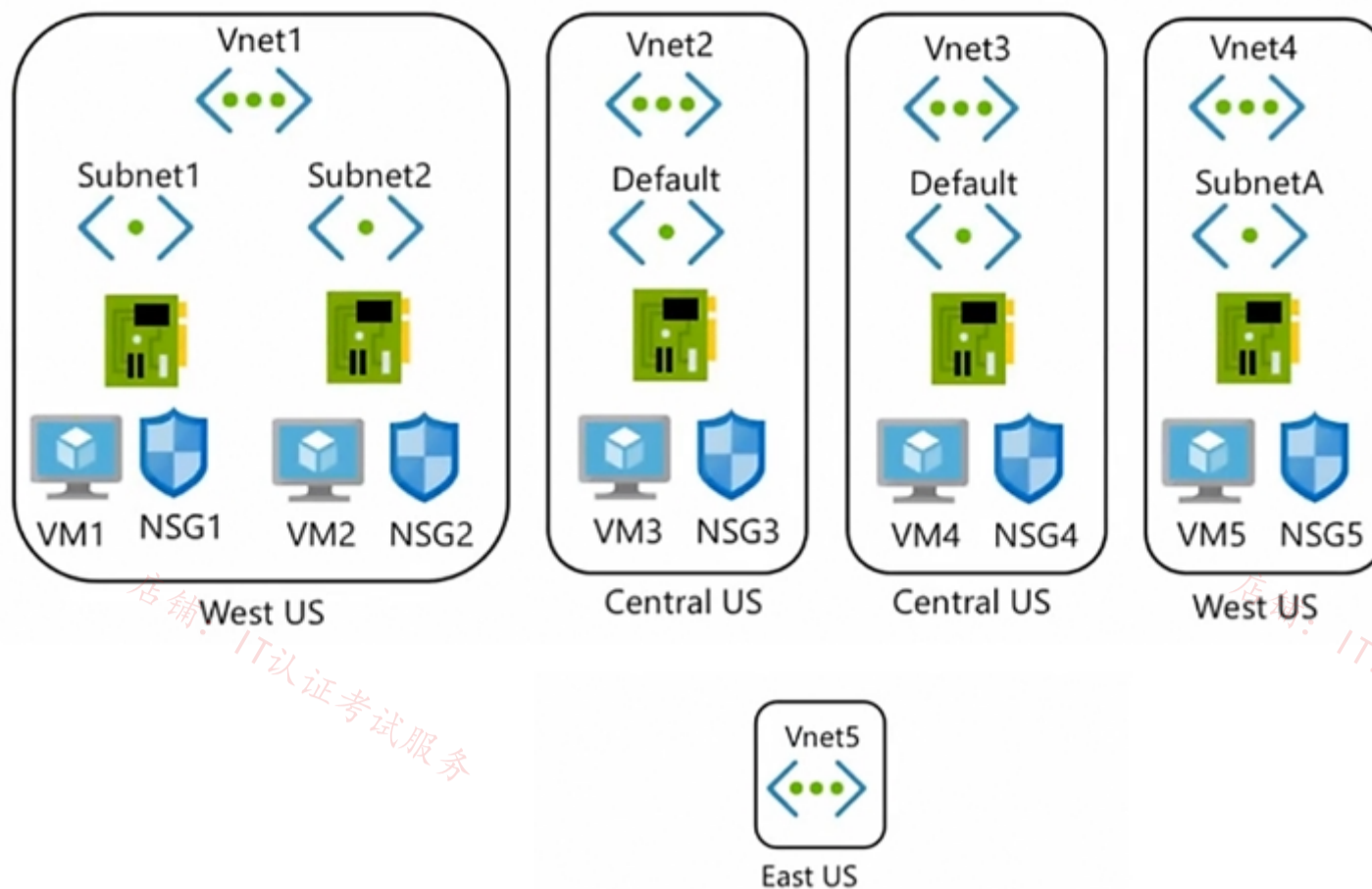
The Azure subscription contains virtual machines that run Windows Server 2019 as shown in the following table.

Name	Location	Connected to	Network security group (NSG)
VM1	West US	Vnet1/Subnet1	NSG1
VM2	West US	Vnet1/Subnet2	NSG2
VM3	Central US	Vnet2/Default	NSG3
VM4	Central US	Vnet3/Default	NSG4
VM5	West US	Vnet4/SubnetA	NSG5

The NSGs are associated to the network interfaces on the virtual machines. Each NSG has one custom security rule that allows RDP connections from the internet. The firewall on each virtual machine allows ICMP traffic.

An application security group named ASG1 is associated to the network interface of VM1.

Azure Network Infrastructure Diagram



Azure Private DNS Zones -

The Azure subscription contains the Azure private DNS zones shown in the following table.

Name	Location
zone1.contoso.com	Central US
zone2.contoso.com	West US

Zone1.contoso.com has the virtual network links shown in the following table.

Name	Virtual Network	Auto registration
Link1	Vnet2	No
Link2	Vnet3	Yes

Other Azure Resources -

The Azure subscription contains additional resources as shown in the following table.

Name	Type	Location
DB1	Azure SQL Database	West US
storage1	Azure Storage account	West US
Registry1	Azure Container Registry	Central US
KeyVault1	Azure Key Vault	Central US

Requirements -

Virtual Network Requirements -

Contoso has the following virtual network requirements:

Create a virtual network named Vnet6 in West US that will contain the following resources and configurations:

- Two container groups that connect to Vnet6
- Three virtual machines that connect to Vnet6
- Allow VPN connections to be established to Vnet6
- Allow the resources in Vnet6 to access KeyVault1, DB1, and Vnet1 over the Microsoft backbone network.

The virtual machines in Vnet4 and Vnet5 must be able to communicate over the Microsoft backbone network.

A virtual machine named VM-Analyze will be deployed to Subnet1. VM-Analyze must inspect the outbound network traffic from Subnet2 to the internet.

Network Security Requirements -

Contoso has the following network security requirements:

Configure Azure Active Directory (Azure AD) authentication for Point-to-Site (P2S) VPN users.

Enable NSG flow logs for NSG3 and NSG4.

Create an NSG named NSG10 that will be associated to Vnet1/Subnet1 and will have the custom inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
500	3389	TCP	10.1.0.0/16	Any	Deny
1000	Any	ICMP	10.10.0.0/16	VirtualNetwork	Deny

Create an NSG named NSG11 that will be associated to Vnet1/Subnet2 and will have the custom outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
200	3389	TCP	10.1.0.0/16	VirtualNetwork	Deny

Question

HOTSPOT -

You are implementing the virtual network requirements for VM-Analyze.

What should you include in a custom route that is linked to Subnet2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Address prefix:

▼
0.0.0.0/0
0.0.0.0/32
10.1.0.0/16
255.255.255.255/0
255.255.255.255/32

Next hop type:

▼
None
Internet
Virtual appliance
Virtual network
Virtual network gateway

店铺: IT认证考试服务

店铺: IT认证考试服务

Answer Area

Address prefix:

	▼
0.0.0.0/0	
0.0.0.0/32	
10.1.0.0/16	
255.255.255.255/0	
255.255.255.255/32	

Correct Answer:

Next hop type:

	▼
None	
Internet	
Virtual appliance	
Virtual network	
Virtual network gateway	

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview>

🗨️ **tng69** Highly Voted 1 year, 5 months ago

If I understand this correctly, we create a Route Table with a UDR that points 0.0.0.0/0 to a Virtual Appliance and assign it to Subnet2.

The IP of the virtual appliance (not asked for here) would then be VM-Analyze which then inspects the traffic. In my opinion then, the answers should be fine.

upvoted 19 times

🗨️ **jeffangel28** Highly Voted 1 year, 5 months ago

Given answer is correct!

upvoted 8 times

🗨️ **Lazylinux** Most Recent 3 months ago

Given Answer is correct

upvoted 1 times

🗨️ **TJ001** 1 year ago

classic use case for Hub NVA/Firewall

upvoted 1 times

Topic 13 - Testlet 7

upvoted 1 times

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in San Francisco and a branch office in Dallas.

Contoso recently purchased an Azure subscription and is performing its first pilot project in Azure.

Existing Environment -

Azure Network Infrastructure -

Contoso has an Azure Active Directory (Azure AD) tenant named contoso.com.

The Azure subscription contains the virtual networks shown in the following table.

Name	Resource group	IP address space	Location	Peered with
Vnet1	RG1	10.1.0.0/16	West US	Vnet2, Vnet3
Vnet2	RG1	172.16.0.0/16	Central US	Vnet1, Vnet3, Vnet4
Vnet3	RG2	192.168.0.0/16	Central US	Vnet1, Vnet2
Vnet4	RG2	10.10.0.0/16	West US	Vnet2
Vnet5	RG3	10.20.0.0/16	East US	None

Vnet1 contains a virtual network gateway named GW1.

Azure Virtual Machines -

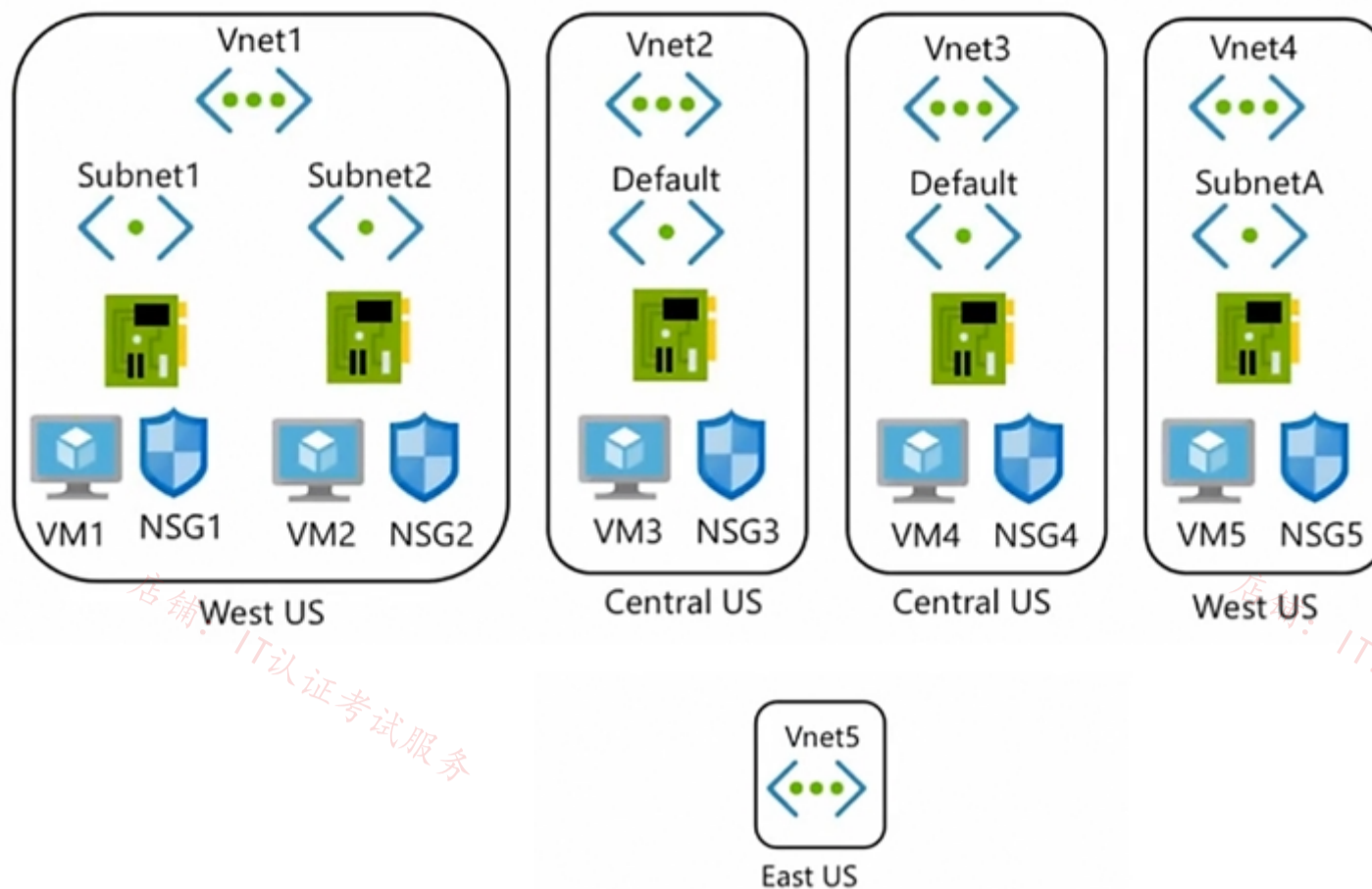
The Azure subscription contains virtual machines that run Windows Server 2019 as shown in the following table.

Name	Location	Connected to	Network security group (NSG)
VM1	West US	Vnet1/Subnet1	NSG1
VM2	West US	Vnet1/Subnet2	NSG2
VM3	Central US	Vnet2/Default	NSG3
VM4	Central US	Vnet3/Default	NSG4
VM5	West US	Vnet4/SubnetA	NSG5

The NSGs are associated to the network interfaces on the virtual machines. Each NSG has one custom security rule that allows RDP connections from the internet. The firewall on each virtual machine allows ICMP traffic.

An application security group named ASG1 is associated to the network interface of VM1.

Azure Network Infrastructure Diagram



Azure Private DNS Zones -

The Azure subscription contains the Azure private DNS zones shown in the following table.

Name	Location
zone1.contoso.com	Central US
zone2.contoso.com	West US

Zone1.contoso.com has the virtual network links shown in the following table.

Name	Virtual Network	Auto registration
Link1	Vnet2	No
Link2	Vnet3	Yes

Other Azure Resources -

The Azure subscription contains additional resources as shown in the following table.

Name	Type	Location
DB1	Azure SQL Database	West US
storage1	Azure Storage account	West US
Registry1	Azure Container Registry	Central US
KeyVault1	Azure Key Vault	Central US

Requirements -

Virtual Network Requirements -

Contoso has the following virtual network requirements:

Create a virtual network named Vnet6 in West US that will contain the following resources and configurations:

- Two container groups that connect to Vnet6
- Three virtual machines that connect to Vnet6
- Allow VPN connections to be established to Vnet6
- Allow the resources in Vnet6 to access KeyVault1, DB1, and Vnet1 over the Microsoft backbone network.

The virtual machines in Vnet4 and Vnet5 must be able to communicate over the Microsoft backbone network.

A virtual machine named VM-Analyze will be deployed to Subnet1. VM-Analyze must inspect the outbound network traffic from Subnet2 to the internet.

Network Security Requirements -

Contoso has the following network security requirements:

Configure Azure Active Directory (Azure AD) authentication for Point-to-Site (P2S) VPN users.

Enable NSG flow logs for NSG3 and NSG4.

Create an NSG named NSG10 that will be associated to Vnet1/Subnet1 and will have the custom inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
500	3389	TCP	10.1.0.0/16	Any	Deny
1000	Any	ICMP	10.10.0.0/16	VirtualNetwork	Deny

Create an NSG named NSG11 that will be associated to Vnet1/Subnet2 and will have the custom outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
200	3389	TCP	10.1.0.0/16	VirtualNetwork	Deny

Question

HOTSPOT -

You create NSG10 and NSG11 to meet the network security requirements.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
From VM1, you can establish a Remote Desktop session with VM2	<input type="radio"/>	<input type="radio"/>
From VM2, you can ping VM1	<input type="radio"/>	<input type="radio"/>
From VM2, you can establish a Remote Desktop session with VM1	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
From VM1, you can establish a Remote Desktop session with VM2	<input type="radio"/>	<input checked="" type="radio"/>
From VM2, you can ping VM1	<input checked="" type="radio"/>	<input type="radio"/>
From VM2, you can establish a Remote Desktop session with VM1	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: No -

NSG10 which is attached to VM1's subnet blocks RDP (port TCP 3389) to 'Any' which means the port is blocked to all destinations.

Box 2: Yes -

NSG10 blocks ICMP from VNet4 (source 10.10.0.0/16) but it is not blocked from VM2's subnet (VNet1/Subnet2).

Box 3: No -

NSG11 blocks RDP (port TCP 3389) destined for 'VirtualNetwork'. VirtualNetwork is a service tag and means the address space of the virtual network (VNet1) which in this case is 10.1.0.0/16. Therefore, RDP traffic from subnet2 to anywhere else in VNet1 is blocked.

pinpin06 Highly Voted 1 year, 9 months ago

I thin the response should be YES, YES, NO

1) VM1 can establish a RDP session to VM as the filtering is set to inbound even if the rule would have matched (it would have required outbound)

2) as stated already, this is for vnet4, so no problem, the traffic will be granted

3) the traffic will be dropped by NSG11 set as abound and from the subnet 10.1.0.0/16 to the vnet, so it matches and is dropped.

upvoted 46 times

pijp 5 months ago

Tested and you are right!

upvoted 2 times

 **asdasd123123iu** 5 months, 3 weeks ago

3 - outbound means from inside of subnet to outside so in my opinion NSG allows RDP connection. If rule would be associated with inbound direction then traffic should be blocked.

So, correct should be YYY

upvoted 2 times

 **Prutser2** 1 year, 3 months ago

agreed

upvoted 1 times

 **jeffangel28** 1 year, 5 months ago

You are right!

upvoted 5 times

 **Bon_** Highly Voted 1 year, 5 months ago

Yes, Yes, No is correct. Make sure you double-check each of the NSG rules, so it's clear!

1. From VM1 to inbound RDP VM2, there are no NSGs blocking this. There is only a custom inbound NSG for VM1, and a custom outbound NSG for VM2-- neither of which will block our connection

2. VM2 outbound NSG has no rules blocking ping (ICMP). Next review the inbound NSG for VM1. There is an priority rule 1000 -- inbound ICMP deny, but the source is pointing to VNET4 (tricky!)

3. Blocked. VM2 NSG has an outbound deny for 3389 RDP.

upvoted 15 times

 **jakubklapka** Most Recent 4 months ago

In exam Sep, 2023

upvoted 2 times

 **Apptech** 10 months ago

Some basics:

1. NSG on NIC always takes precedence over NSG on Subnet.

2. Default setting for NSG is DenyAllInbound. There is one rule for all NSG linked to NIC which says RDP from Internet is allowed, which indicates that default setting for Inbound is active.

What does ist mean? It means that VM1 cannot establish RDP to VM2 which NSG2 only allows RDP from Internet.

Q1: No

For outbound traffic default setting is Allow All. NSG10 (VNET1/Subnet2) denies ICMP only to Vnet4.

Q2: YES

NSG 11 on Vnet1/Subnet2 does not allow outbound for Virtual Network

Also Default for NSG of Vm3 (NIC) is DenyAllInbound.

Q3: NO

So, in my opinion NYN is correct.

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

upvoted 5 times

 **mabalon** 5 months ago

Carefull with the point 2. yesm you have the DenyAllinbound, but also have AllowVNetInBound with better priority. with the default rules All inbound traffic from the vnet is allowed.

upvoted 1 times

 **JennyHuang36** 11 months, 1 week ago

In exam Feb 2023

upvoted 2 times

 **TJ001** 1 year ago

yes yes no

upvoted 3 times

 **TJ001** 1 year ago

same vnet so route is present ...only check NSG rules....

upvoted 2 times

 **Mahakal_123** 1 year ago

Answer is correct, it will be NYN.

No - Traffic will be dropped by NSG10. Subnet NSG will take precedence over VM interface NSG.

Yes - ICMP is allowed.

No - Traffic will be be dropped by NSG11.

upvoted 1 times

 **wetraining123** 1 year, 1 month ago

check these two NSGS table

Create an NSG named NSG10 that will be associated to Vnet1/Subnet1 and will have the custom inbound security rules shown in the following table.

Create an NSG named NSG11 that will be associated to Vnet1/Subnet2 and will have the custom outbound security rules shown in the following table.

so the answer is NNN
upvoted 1 times

 **wetraining123** 1 year, 1 month ago

its NNN , AS THE custom nsg denies any communication from 10.1.0.0/16 which is the address space of vnet1 , and vm1 and vm2 uses that address space
upvoted 1 times


 **Gronow** 1 year, 2 months ago

What about the NSG's connected to the NIC's? There is only 1 rule (inbound), which is to allow RDP from Internet. Won't these block any VM/subnet RDP connections allowed via the subnet NSG?

'The NSGs are associated to the network interfaces on the virtual machines. Each NSG has one custom security rule that allows RDP connections from the internet'
upvoted 1 times

 **azeem0077** 1 year, 5 months ago


Yes, Yes, No
upvoted 1 times

 **kinder2** 1 year, 7 months ago


Y,Y,N.
upvoted 3 times

 **Whatsamattr81** 1 year, 8 months ago

NSG10 is an inbound rule attached to subnet 1... It doesn't prevent an outbound RDP to subnet 2. Its Yes, Yes, No
upvoted 6 times

 **Kay04** 1 year, 9 months ago

I believe yes yes no, no outbound filter on subnet 1.
upvoted 3 times

 **petermogaka91** 1 year, 9 months ago

I think YYN for the answers
upvoted 5 times

Topic 14 - Testlet 8

店铺: IT认证考试服务

店铺: IT认证考试服务

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a financial company that has a main datacenter in Boston and 20 branch offices across the United States. Users have Android, iOS, and Windows 10 devices.

Existing Environment -

Hybrid Environment -

The on-premises network contains an Active Directory forest named litwareinc.com that syncs to an Azure Active Directory (Azure AD) tenant named litwareinc.com by using Azure AD Connect.

All offices connect to a virtual network named Vnet1 by using a Site-to-Site VPN connection.

Azure Environment -

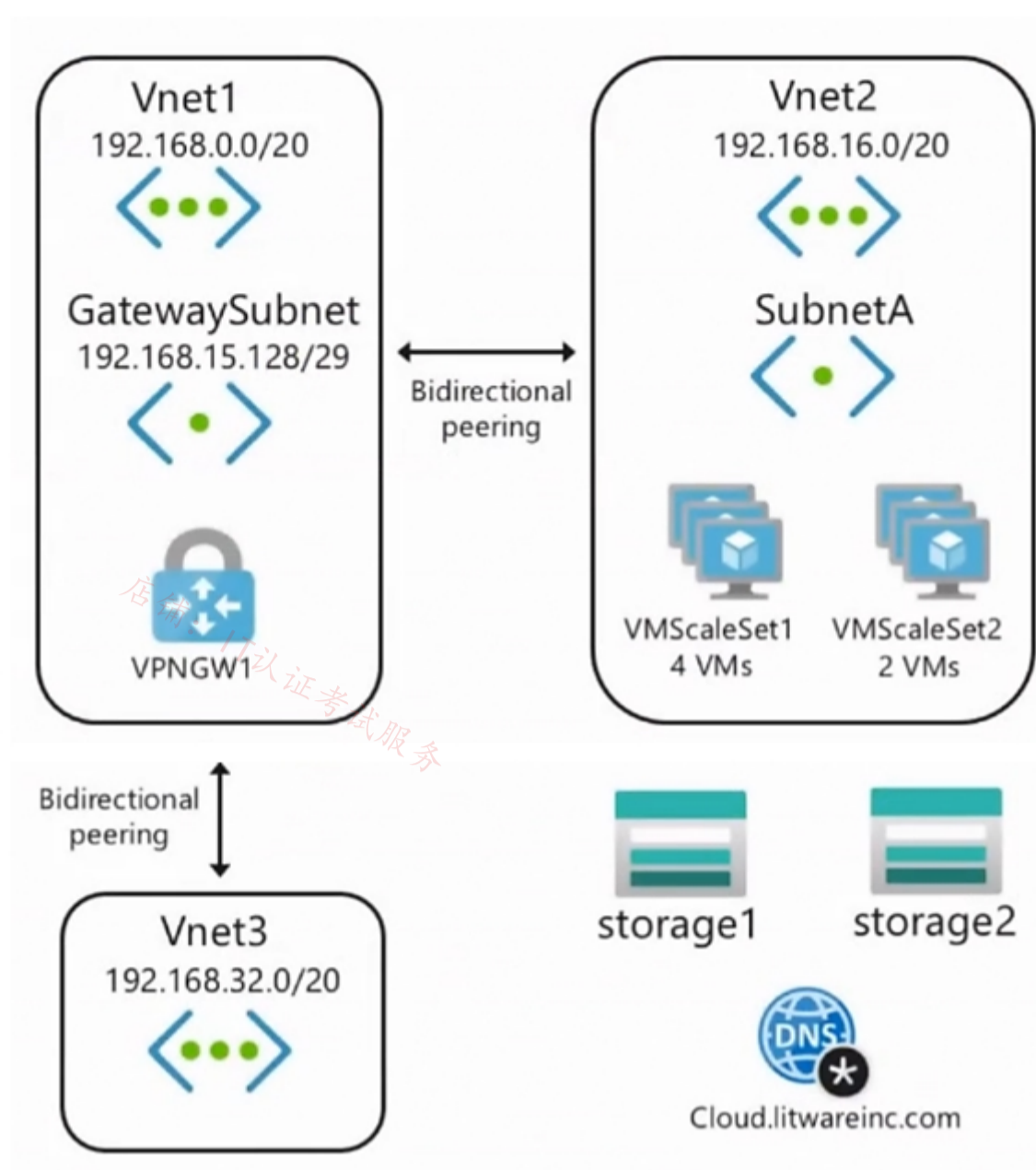
Litware has an Azure subscription named Sub1 that is linked to the litwareinc.com Azure AD tenant. Sub1 contains resources in the East US Azure region as shown in the following table.

Name	Type	Description
Vnet1	Virtual network	Uses an IP address space of 192.168.0.0/20
GatewaySubnet	Virtual network subnet	Located in Vnet1 and uses an IP address space of 192.168.15.128/29
VPNGW1	VPN gateway	Deployed to Vnet1
Vnet2	Virtual network	Uses an IP address space of 192.168.16.0/20
SubnetA	Virtual network subnet	Located in Vnet2 and uses an IP address space of 192.168.16.0/24
Vnet3	Virtual network	Uses an IP address space of 192.168.32.0/20
cloud.litwareinc.com	Private DNS zone	None
VMScaleSet1	Virtual machine scale set	Contains four virtual machines deployed to SubnetA
VMScaleSet2	Virtual machine scale set	Contains two virtual machines deployed to SubnetA
storage1	Storage account	Has the public endpoint blocked
storage2	Storage account	Has the public endpoint blocked

A diagram of the resource in the East US Azure region is shown in the Azure Network Diagram exhibit.

There is bidirectional peering between Vnet1 and Vnet2. There is bidirectional peering between Vnet1 and Vnet3. Currently, Vnet2 and Vnet3 cannot communicate directly.

Azure Network Diagram -



Requirements -

Business Requirements -

Litware wants to minimize costs whenever possible, as long as all other requirements are met.

Virtual Networking Requirements -

Litware identifies the following virtual networking requirements:

Direct the default route of 0.0.0.0/0 on Vnet2 and Vnet3 to the Boston datacenter over an ExpressRoute circuit.

Ensure that the records in the cloud.litwareinc.com can be resolved from the on-premises locations.

Automatically register the DNS names of Azure virtual machines to the cloud.litwareinc.com zone.

Minimize the size of the subnets allocated to platform-managed services.

Allow traffic from VMScaleSet1 to VMScaleSet2 on the TCP port 443 only.

Hybrid Networking Requirements -

Litware identifies the following hybrid networking requirements:

Users must be able to connect to Vnet1 by using a Point-to-Site (P2S) VPN when working remotely. Connections must be authenticated by Azure AD.

Latency of the traffic between the Boston datacenter and all the virtual networks must be minimized.

The Boston datacenter must connect to the Azure virtual networks by using an ExpressRoute FastPath connection.

Traffic between Vnet2 and Vnet3 must be routed through Vnet1.

PaaS Networking Requirements -

Litware identifies the following networking requirements for platform as a service (PaaS):

The storage1 account must be accessible from all on-premises locations without exposing the public endpoint of storage1.

The storage2 account must be accessible from Vnet2 and Vnet3 without exposing the public endpoint of storage2.

Question

HOTSPOT -

You need to restrict traffic from VMScaleSet1 to VMScaleSet2. The solution must meet the virtual networking requirements.

What is the minimum number of custom NSG rules and NSG assignments required? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Minimum number of custom NSG rules:

1
2
3
4
5

Minimum number of NSG assignments:

1
2
3
4
5

店铺: IT认证考试服务

店铺: IT认证考试服务

Answer Area

Minimum number of custom NSG rules:

1
2
3
4
5

Correct Answer:

Minimum number of NSG assignments:

1
2
3
4
5

Box 2: One NSG -

The minimum requirement is one NSG. You could attach the NSG to VMSScaleSet1 and restrict outbound traffic, or you could attach the NSG to VMSScaleSet2 and restrict inbound traffic. Either way you would need two custom NSG rules.

Box 1: Two custom rules -

With the NSG attached to VMSScaleSet2, you would need to create a custom rule blocking all traffic from VMSScaleSet1. Then you would need to create another custom rule with a higher priority than the first rule that allows traffic on port 443.

The default rules in the NSG will allow all other traffic to VMSScaleSet2.

 **derrp** Highly Voted 1 year, 6 months ago

2 Rules 1 Assignment
Reminds me of an old video I once saw on the internet...
upvoted 23 times

 **sapien45** 1 year, 3 months ago

I saw a variant of that movie : 3 rHoles 1 Assgnment
I just saw a few minutes though
upvoted 2 times

 **MariusKas** 1 year, 3 months ago

I tested your movie in lab - got all Yesses
upvoted 2 times

 **jeffangel28** 1 year, 5 months ago

Right, validated!
upvoted 1 times

店铺: IT认证考试服务

店铺: IT认证考试服务

🗄️ 👤 **Webesciaki** Most Recent 2 weeks, 4 days ago

why not 1:1 ?

1 - assignment to just VMSS2 as "Network Security Groups can be applied directly to a scale set, by adding a reference to the network interface configuration section of the scale set virtual machine properties."

1 rule - block TCP/443 with source of subnet1 and deny. REST VNET's cidrs would be allowed by default.

out of the scope of this question I guess but you could assign ASG to VMSS1 and use that as source in that single blocking rule assigned directly to VMSS2

upvoted 1 times

🗄️ 👤 **Webesciaki** 2 weeks, 3 days ago

my bad - I misread the requirements

1:2

1 assignment

2 rules: 1st allow tcp/443, 2nd block subnet1 as source

upvoted 1 times

🗄️ 👤 **mrgreat** 10 months ago

To restrict traffic from VMScaleSet1 to VMScaleSet2 on TCP port 443, we need to create a custom NSG rule to allow traffic on port 443 and apply it to both VMScaleSet1 and VMScaleSet2. We also need to create a custom NSG rule to deny all traffic and apply it to VMScaleSet1.

So the minimum number of custom NSG rules and NSG assignments required would be:

2 custom NSG rules: 1 to allow traffic on TCP port 443 and 1 to deny all traffic

2 NSG assignments: 1 for VMScaleSet1 and 1 for VMScaleSet2

Therefore, the answer is:

Minimum number of custom NSG rules = 2

Minimum number of NSG assignments = 2

Note: It's important to note that we could potentially use an existing NSG that is already assigned to the virtual machines and add the necessary rules to it. In that case, the minimum number of NSG assignments would be 1.

upvoted 3 times

🗄️ 👤 **MrBlueSky** 9 months, 2 weeks ago

You could just apply the NSG to the subnet that both VMSS are in.

Min number of rules = 2

Min number of assignments = 1

upvoted 5 times

🗄️ 👤 **BenH** 1 year, 8 months ago

Correct

upvoted 2 times

店铺: IT认证考试服务

店铺: IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

店铺：IT认证考试服务

Introductory Info

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in San Francisco and a branch office in Dallas. Contoso recently purchased an Azure subscription and is performing its first pilot project in Azure.

Existing Environment -

Azure Network Infrastructure -

Contoso has an Azure Active Directory (Azure AD) tenant named contoso.com. The Azure subscription contains the virtual networks shown in the following table.

Name	Resource group	IP address space	Location	Peered with
Vnet1	RG1	10.1.0.0/16	West US	Vnet2, Vnet3
Vnet2	RG1	172.16.0.0/16	Central US	Vnet1, Vnet3, Vnet4
Vnet3	RG2	192.168.0.0/16	Central US	Vnet1, Vnet2
Vnet4	RG2	10.10.0.0/16	West US	Vnet2
Vnet5	RG3	10.20.0.0/16	East US	None

Vnet1 contains a virtual network gateway named GW1.

Azure Virtual Machines -

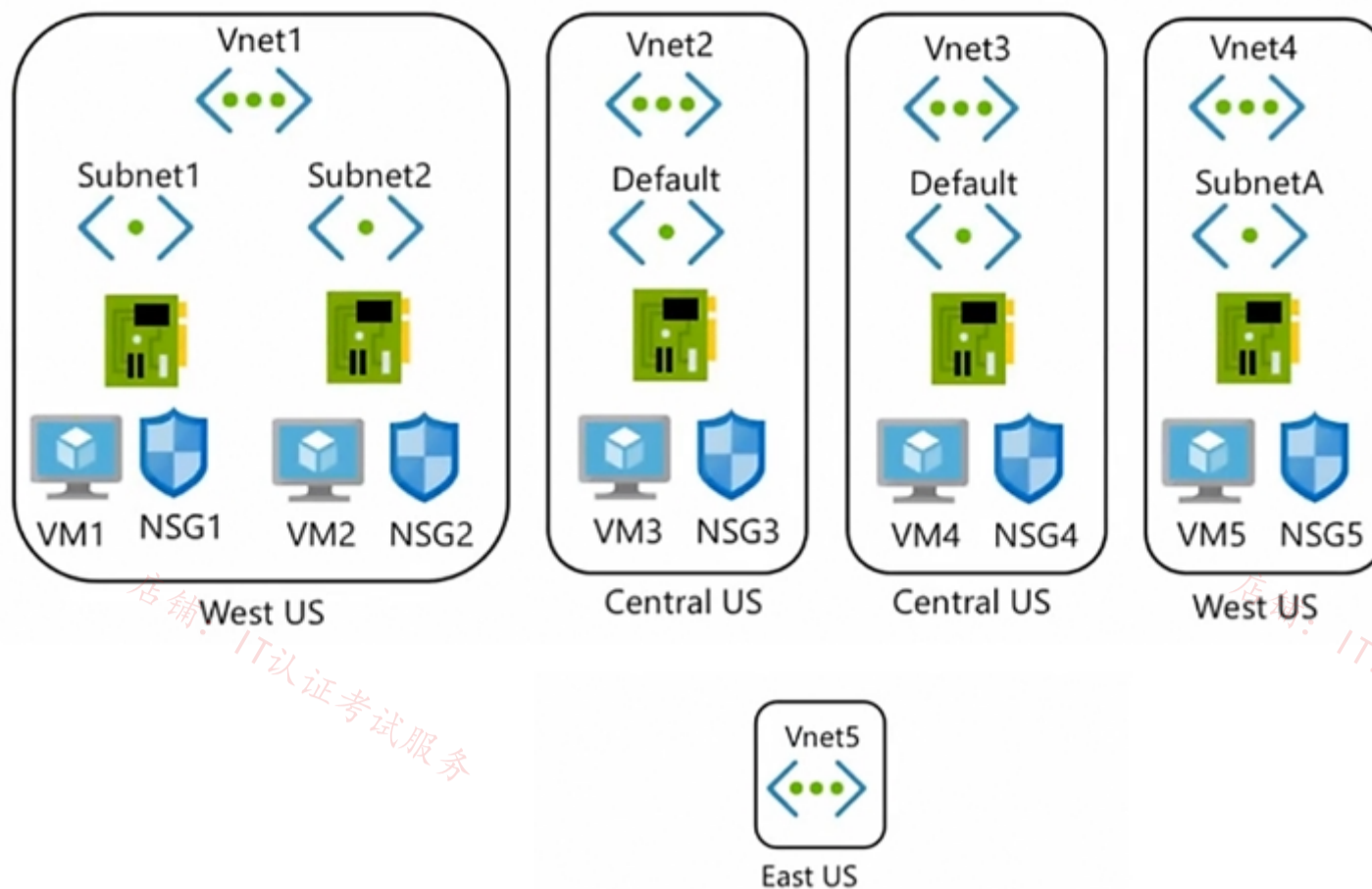
The Azure subscription contains virtual machines that run Windows Server 2019 as shown in the following table.

Name	Location	Connected to	Network security group (NSG)
VM1	West US	Vnet1/Subnet1	NSG1
VM2	West US	Vnet1/Subnet2	NSG2
VM3	Central US	Vnet2/Default	NSG3
VM4	Central US	Vnet3/Default	NSG4
VM5	West US	Vnet4/SubnetA	NSG5

The NSGs are associated to the network interfaces on the virtual machines. Each NSG has one custom security rule that allows RDP connections from the internet. The firewall on each virtual machine allows ICMP traffic.

An application security group named ASG1 is associated to the network interface of VM1.

Azure Network Infrastructure Diagram



Azure Private DNS Zones -

The Azure subscription contains the Azure private DNS zones shown in the following table.

Name	Location
zone1.contoso.com	Central US
zone2.contoso.com	West US

Zone1.contoso.com has the virtual network links shown in the following table.

Name	Virtual Network	Auto registration
Link1	Vnet2	No
Link2	Vnet3	Yes

Other Azure Resources -

The Azure subscription contains additional resources as shown in the following table.

Name	Type	Location
DB1	Azure SQL Database	West US
storage1	Azure Storage account	West US
Registry1	Azure Container Registry	Central US
KeyVault1	Azure Key Vault	Central US

Requirements -

Virtual Network Requirements -

Contoso has the following virtual network requirements:

Create a virtual network named Vnet6 in West US that will contain the following resources and configurations:

- Two container groups that connect to Vnet6
- Three virtual machines that connect to Vnet6
- Allow VPN connections to be established to Vnet6
- Allow the resources in Vnet6 to access KeyVault1, DB1, and Vnet1 over the Microsoft backbone network.

The virtual machines in Vnet4 and Vnet5 must be able to communicate over the Microsoft backbone network.

A virtual machine named VM-Analyze will be deployed to Subnet1. VM-Analyze must inspect the outbound network traffic from Subnet2 to the internet.

Network Security Requirements -

Contoso has the following network security requirements:

Configure Azure Active Directory (Azure AD) authentication for Point-to-Site (P2S) VPN users.

Enable NSG flow logs for NSG3 and NSG4.

Create an NSG named NSG10 that will be associated to Vnet1/Subnet1 and will have the custom inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
500	3389	TCP	10.1.0.0/16	Any	Deny
1000	Any	ICMP	10.10.0.0/16	VirtualNetwork	Deny

Create an NSG named NSG11 that will be associated to Vnet1/Subnet2 and will have the custom outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
200	3389	TCP	10.1.0.0/16	VirtualNetwork	Deny

Question

HOTSPOT -

In which NSGs can you use ASG1 and to which virtual machine network interfaces can you associate ASG1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

NSGs:

NSG1 only
NSG1 and NSG2 only
NSG1, NSG2, and NSG5 only
NSG1, NSG2, NSG4, and NSG5 only
NSG1, NSG2, NSG3, NSG4, and NSG5

Virtual machines:

VM2 only
VM2 and VM5 only
VM2, VM4, and VM5 only
VM2, VM3, VM4, and VM5

店铺: IT认证考试服务

店铺: IT认证考试服务

Correct Answer:

Answer Area

NSGs:

NSG1 only
NSG1 and NSG2 only
NSG1, NSG2, and NSG5 only
NSG1, NSG2, NSG4, and NSG5 only
NSG1, NSG2, NSG3, NSG4, and NSG5

Virtual machines:

VM2 only
VM2 and VM5 only
VM2, VM4, and VM5 only
VM2, VM3, VM4, and VM5

leo87las2 Highly Voted 1 year, 4 months ago

NSG1,NSG2 same vnet
VM2 only NIC in same Vnet
<https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups>
upvoted 28 times

GBAU 3 months ago
Yep, so

NSGs (only in the same region*, West US): NSG1, NSG2 & NSG5 only
*Tested in a lab:
-ASG in Australia SE
-NSG in Australia SE => New inbound rule, source ASG, ASG listed in the drop down box
-NSG in SE Asia => New inbound rule, source ASG, NO ASGs listed in the drop down box to select from

VM (only in the same vNet**): VM2 only
* already assigned to VM1 so limited to Vnet1
<https://learn.microsoft.com/en-us/azure/virtual-network/application-security-groups>
"All network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in."
upvoted 1 times

zenithcsa1 Highly Voted 1 year, 4 months ago

Tested
NSG1, NSG2, and NSG5 only : ASG and NSG must be in the same region
VM2 only : network interfaces attached to an ASG must be in the same vNet.
<https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups>
upvoted 18 times

tdienst 1 year, 4 months ago
NSG1 & NSG2
VM2 Only

NSG5 also is out of the question:
All network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in. For example, if the first network interface assigned to an application security group named AsgWeb is in the virtual network named VNet1, then all subsequent network interfaces assigned to ASGWeb must exist in VNet1. You cannot add network interfaces from different virtual networks to the same application security group.
ref: <https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups>
upvoted 14 times

zenithcsa1 1 year, 2 months ago

Please read the question again, and the next paragraph in the link. The question is about connection between ASG and NSG, not between ASG and NIC.
upvoted 1 times

wooyourdaddy 10 months, 3 weeks ago

I was initially only NSG1 & NSG2 only, but came across these 2 websites:

<https://medium.com/awesome-azure/azure-application-security-group-asg-1e5e2e5321c3>
<https://petri.com/understanding-application-security-groups-in-the-azure-portal/>

Which both state:

Source and Destination in the new rule blade allow you to select any application security group in the same region.

So while their may be not practical use case for using ASG1 in NSG5 in this case, the ASG can be selected by any NSGs in the same region.

The only caveat being:

If you specify an application security group as the source and destination in a security rule, the network interfaces in both application security groups must exist in the same virtual network.

So I would agree that NSG1, NSG2 and NSG5 can use ASG1. And only VM2 can be added to ASG1 due to the NICs needing to be in the same VNET.

upvoted 3 times

  **wooyourdaddy** 9 months, 4 weeks ago

I set up this lab scenario. When I go to NSG5 and create an inbound rule, I am able to change the destination to application security group and ASG1 is visible as an option to select. When I try in NSG3 and NSG4, the Destination application security groups drop down is greyed out and says 'No application security groups found'.

When I go to Network under Settings on VM5, the ASG1 application security group is visible as an option to choose. However, when I click save, the operation fails indicating that the ASG is already attached to another device in a separate subnet.

I was successfully able to add VM2 to the ASG, but ASG1 was not even visible to VM3 and VM4.

The questions seems to want to drive home the point that NSGs and ASGs need to be in the same region if you intend to use the ASG in an NSG rule, while VM NICs added to an ASG need to be in the same VNET.

upvoted 2 times

  **GiorgioLDN** 1 year, 3 months ago

Correct. ASG1 is applied on VM1. VM1's interface is the first network interface assigned to ASG1, thus all subsequent network interfaces assigned to ASG1 must exist in VNet1. NSG2 exists in VNet1.

upvoted 1 times

  **wooyourdaddy** 10 months, 2 weeks ago

I set up this lab scenario. When I go to NSG5 and create an inbound rule, I am able to change the destination to application security group and ASG1 is visible as an option to select. When I try in NSG3 and NSG4, the Destination application security groups drop down is greyed out and says 'No application security groups found'.

When I go to Network under Settings on VM5, the ASG1 application security group is visible as an option to choose. However, when I click save, the operation fails indicating that the ASG is already attached to another device in a separate subnet.

I was successfully able to add VM2 to the ASG, but ASG1 was not even visible to VM3 and VM4.

The questions seems to want to drive home the point that NSGs and ASGs need to be in the same region if you intend to use the ASG in an NSG rule, while VM NICs added to an ASG need to be in the same VNET.

upvoted 1 times

  **somenick** 10 months, 1 week ago

NSG1, NSG2, and NSG5 only. Also tested and it's true. You can use ASG from another VNET in the same region.

upvoted 2 times

  **jakubklapka** Most Recent 4 months ago

In exam Sep, 2023

upvoted 2 times

  **JohnnyChimpo** 8 months, 4 weeks ago

Congrats on making it to the last question. Godspeed and best of luck everyone :D

upvoted 10 times

  **_fvt** 9 months, 3 weeks ago

- All network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in. For example, if the first network interface assigned to an application security group named AsgWeb is in the virtual network named VNet1, then all subsequent network interfaces assigned to ASGWeb must exist in VNet1. You cannot add network interfaces from different virtual networks to the same application security group.

- If you specify an application security group as the source and destination in a security rule, the network interfaces in both application security groups must exist in the same virtual network. For example, if AsgLogic contained network interfaces from VNet1, and AsgDb contained network interfaces from VNet2, you could not assign AsgLogic as the source and AsgDb as the destination in a rule. All network interfaces for both the source and destination application security groups need to exist in the same virtual network.

So, you can apply the ASG to all NSG within the same region :

=> "NSG1, NSG2, and NSG5 only"

But, as VM1 NIC is already in the ASG, you cannot add another NIC from a different VNet:

=> "VM2 only"

upvoted 1 times

🗨️ **Madball** 11 months, 3 weeks ago

I believe the answers are:

NSGS = NSG1, NSG2 and NSG5 only.

My reasoning for this is that an ASG can be used in NSG rules for any NSG within the same region.

Virtual Machines = VM2 only

The ASG can only be attached to NICS within the same virtual network.

I have tested this in my lab.

upvoted 3 times

🗨️ **TJ001** 1 year ago

Box 1: NSG 1 and NSG 2

Box 2: VM2

upvoted 2 times

🗨️ **vivikar** 1 year ago

NSG 1 and NSG2: As per All network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in. For example, if the first network interface assigned to an application security group named AsgWeb is in the virtual network named VNet1, then all subsequent network interfaces assigned to ASGWeb must exist in VNet1. You cannot add network interfaces from different virtual networks to the same application security group.

upvoted 1 times

🗨️ **winy** 1 year, 2 months ago

Box 1: NSG 1 and NSG 2

Box 2: VM2 , VM1 only

This has been tested on the LAB.

All network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in. For example, if the first network interface assigned to an application security group named AsgWeb is in the virtual network named VNet1, then all subsequent network interfaces assigned to ASGWeb must exist in VNet1. You cannot add network interfaces from different virtual networks to the same application security group.

<https://learn.microsoft.com/en-us/azure/virtual-network/application-security-groups#allow-database-businesslogic>

upvoted 4 times

🗨️ **winy** 1 year, 2 months ago

Box 1: NSG 1 and NSG 2

Box 2: VM2

All network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in. For example, if the first network interface assigned to an application security group named AsgWeb is in the virtual network named VNet1, then all subsequent network interfaces assigned to ASGWeb must exist in VNet1. You cannot add network interfaces from different virtual networks to the same application security group.

<https://learn.microsoft.com/en-us/azure/virtual-network/application-security-groups#allow-database-businesslogic>

upvoted 2 times

🗨️ **Prutser2** 1 year, 3 months ago

box1: only vnets 1 and 4 are in westUS, so only NSGs in this region can re-use the existing ASG1

result: NSG1, NSG2 and NSG5

box2:

All network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in. For example, if the first network interface assigned to an application security group named AsgWeb is in the virtual network named VNet1, then all subsequent network interfaces assigned to ASGWeb must exist in VNet1. You cannot add network interfaces from different virtual networks to the same application security group.

source:<https://learn.microsoft.com/en-us/azure/virtual-network/application-security-groups>

result:Vm2 only (was already assigned to VM1, which is in vnet1)

upvoted 1 times

🗨️ **Pradh** 1 year, 3 months ago

These are correct answers !! Rest is your wish to opt for .

NSG1, NSG2, and NSG5 only

VM2 only

upvoted 2 times

🗨️ **Cristoicach91** 1 year, 4 months ago

Correct.

upvoted 2 times

