EXAMTOPICS

-Expert Verified, Online, **Free**.



CERTIFICATION TEST

-CertificationTest.net - Cheap & Quality Resources With Best Support

Question #1 *Topic 1*

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

Suggested Answer: *A*
Reference: https://azure.microsoft.com/en-us/pricing/details/expressroute/

Community vote distribution
A (69%) D (25%)

kbakdev Most Recent 1 month, 2 weeks ago
Selected Answer: A
All in same region, so no need for additional expense.
upvoted 1 times

shaji111 7 months, 4 weeks ago
Selected Answer: A
all in same region no need of additional expensive to select other SKUs , local will meet the purpose
upvoted 1 times

3f92a3c 8 months ago
Selected Answer: A
Answer is A
upvoted 1 times

Margesh 10 months, 2 weeks ago
Selected Answer: A
i would like to use expressRoute local becasue all devcie are in local.
upvoted 2 times

JMAN78 1 year, 3 months ago
Selected Answer: D
Wouldn't it be standard since you're required to use an unlimited data plan. I say the answer is express route standard.
upvoted 1 times

nabeel79 1 year, 6 months ago
Selected Answer: B
o minimize costs while meeting the requirements
upvoted 2 times

Shoukathalimpm 1 year, 7 months ago
Selected Answer: A
To minimize costs while meeting the requirements, you should create an ExpressRoute Local circuit. This option is cost-effective because it allows you to connect to Azure resources within the same peering location (Washington DC) without incurring additional charges for data transfer across regions. It also supports the Unlimited data plan and the required bandwidth of up to 1 Gbps.
upvoted 1 times

a250fb0 1 year, 9 months ago

Selected Answer: A

ExpressRoute Local circuits are designed for scenarios where your on-premises datacenter and Azure region are in close proximity, which is the case here with both being in Washington DC.

upvoted 1 times

HoangNam2711 2 years, 4 months ago

Selected Answer: A

A is correct because Washing is in EastUS geopolitical

upvoted 1 times

ESAJRR 3 years, 1 month ago

Selected Answer: A

Correct.

upvoted 1 times

saurabhjsshukla 3 years, 1 month 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 3 years, 3 months 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 2 times

TJ001 3 years, 4 months ago

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

upvoted 1 times

IHensch 3 years, 5 months 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

IHensch 3 years, 5 months ago

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.I agree with your answer since you're required to use an unlimited data plan. I say the answer is express route standard."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

nostromer89 3 years, 5 months ago

Correct one is A

upvoted 1 times

JMAN78 1 year, 3 months ago

I agree with your answer since you're required to use an unlimited data plan. I say the answer is express route standard.

upvoted 1 times

EdwardY 3 years, 3 months 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 3 years, 8 months ago

ExpressRoute local, standard, global offer unlimited data plans.

ExpressRoute local: access azure region locally

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

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

upvoted 4 times

n0t4u2c 3 years, 8 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 3 years, 8 months ago

Selected Answer: A

so as in my previous message, A

upvoted 1 times

Question #2 *Topic 1*

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

Suggested Answer: *B*
Reference: https://docs.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about

Community vote distribution
B (100%)

kbakdev Most Recent 1 month, 2 weeks ago

Selected Answer: B

RADIUS server, because it validates user credentials against on-prem AD.

upvoted 1 times

Margesh 10 months, 2 weeks ago

Selected Answer: B

For an Azure Point-to-Site (P2S) VPN using OpenVPN, when users must authenticate against an on-premises Active Directory, Azure requires RADIUS-based authentication.

Azure VPN Gateway integrates with RADIUS (typically NPS on Windows Server).

The RADIUS server validates user credentials against on-prem Active Directory.

This is the supported method for AD-based authentication with OpenVPN P2S.

upvoted 1 times

nabeel79 1 year, 6 months ago

Selected Answer: B

The correct answer is B. a RADIUS server as I now

upvoted 2 times

Shoukathalimpm 1 year, 7 months ago

Selected Answer: B

To support VPN authentication for an Azure Point-to-Site (P2S) VPN using OpenVPN and an on-premises Active Directory domain, you should deploy a RADIUS server. The RADIUS server acts as an intermediary to authenticate users against the on-premises Active Directory.

upvoted 1 times

gsat2326 2 years, 1 month ago

Answer B

-The RADIUS server verifies the identity of the user or device attempting to connect to the VPN by checking the credentials (username, password, certificates, or tokens) provided by the VPN client.

-The credentials are compared against a database of valid users, which can be stored locally on the RADIUS server or accessed via external identity systems like Active Directory or LDAP.

-If the credentials are valid, the RADIUS server approves the connection request.

upvoted 2 times

Edward1 2 years, 1 month 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

IHensch Highly Voted 2 years, 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 11 times

trashbox 3 years, 1 month 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

nostromer89 3 years, 11 months ago

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

upvoted 1 times

jilguens 4 years, 2 months ago

Selected Answer: B

radius server

upvoted 2 times

1particle 4 years, 3 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

jj22222 4 years, 7 months ago

Selected Answer: B

B. a RADIUS server

upvoted 1 times

d0bermannn 4 years, 9 months ago

Selected Answer: B

B. a RADIUS server is correct

upvoted 1 times

AidenYoukhana 4 years, 10 months ago

A RADIUS Server.

upvoted 1 times

walkwolf3 Highly Voted 5 years 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 22 times

leslie79 5 years ago

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

upvoted 1 times

chreaxa 5 years ago

Correct

upvoted 2 times

AKYK 5 years, 1 month ago

Correct answer!

upvoted 2 times

Question #3 *Topic 1*

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

Suggested Answer: *A, D*
Reference: https://docs.microsoft.com/en-us/azure/vpn-gateway/bgp-howto

Community vote distribution
AD (100%)

kbakdev Most Recent 1 month, 2 weeks ago

Selected Answer: AD

Always Local Network Gateway and Virtual Network Gateway for a S2S VPN connection.
upvoted 1 times

Edward1 2 years, 1 month 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 3 times

1particle 2 years, 1 month 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

lHensch Highly Voted 2 years, 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 9 times

1particle 4 years, 3 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

milan92stankovic 4 years, 7 months ago

Selected Answer: AD

Correct answer A & D.

upvoted 2 times

d0bermannn 4 years, 9 months ago

Selected Answer: AD

A&D is correct as virt NGW & local NGW are prereq for s2s vpn

upvoted 1 times

chreaxa 5 years ago

Correct

upvoted 4 times

crawfish Highly Voted 5 years 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 22 times

AmalMOQ 5 years, 1 month ago

correct !

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.

upvoted 3 times

AKYK 5 years, 1 month ago

Given answers are correct!

upvoted 3 times

Question #4 *Topic 1*

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

Suggested Answer: *A*
Reference: https://docs.microsoft.com/en-us/azure/vpn-gateway/troubleshoot-vpn-with-azure-diagnostics

Community vote distribution
A (100%)

kbakdev Most Recent 1 month, 2 weeks ago

Selected Answer: A

IKEDianosticLog = Internet Key Exchange (IKE) protocol is crucial for establishing the IPsec tunnel.

upvoted 1 times

Shoukathalimpm 1 year, 7 months ago

Selected Answer: A

To troubleshoot the issue with the IPsec tunnel for your Site-to-Site VPN connection, you should review the IKEDiagnosticLog. This log provides detailed information about the Internet Key Exchange (IKE) protocol, which is crucial for establishing the IPsec tunnel. It can help identify configuration errors or connectivity issues.

upvoted 2 times

1particle 3 years, 3 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 3 years, 3 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 3 years, 7 months ago

Selected Answer: A

A.

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

upvoted 1 times

AidenYoukhana 3 years, 10 months ago

Selected Answer: A

IKEDiagnosticLog

upvoted 4 times

chreaxa 4 years ago

Correct

upvoted 1 times

crawfish Highly Voted 4 years 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 55 times

RandomUser 4 years, 1 month 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 4 years, 1 month 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

Question #5 *Topic 1*

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

Suggested Answer: *B, G*
Reference: https://docs.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal

Community vote distribution
BG (100%)

kbakdev Most Recent 1 month, 2 weeks ago

Selected Answer: BG

Always Virtual Network Gateway + Local Virtual Network Gateway = S2S

upvoted 1 times

omgMerrick Highly Voted 2 years, 1 month 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 11 times

1particle 2 years, 1 month 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 3 times

trashbox 3 years, 1 month ago

Selected Answer: BG

The answers are correct.

upvoted 1 times

ESAJRR 3 years, 7 months ago

Selected Answer: BG

It's corrects.

upvoted 3 times

TJ001 3 years, 10 months ago

BG is correct

upvoted 1 times

HasanHHH 4 years, 1 month ago

Selected Answer: BG

Main Component of S2S VPN

local network gateway & virtual network gateway

upvoted 3 times

BlackZeros 4 years, 1 month ago

Selected Answer: BG

similar to another question with less options

upvoted 3 times

milan92stankovic 4 years, 5 months ago

Selected Answer: BG

Correct Answer

upvoted 3 times

Whatsamattr81 4 years, 5 months ago

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

upvoted 2 times

Question #6 *Topic 1*

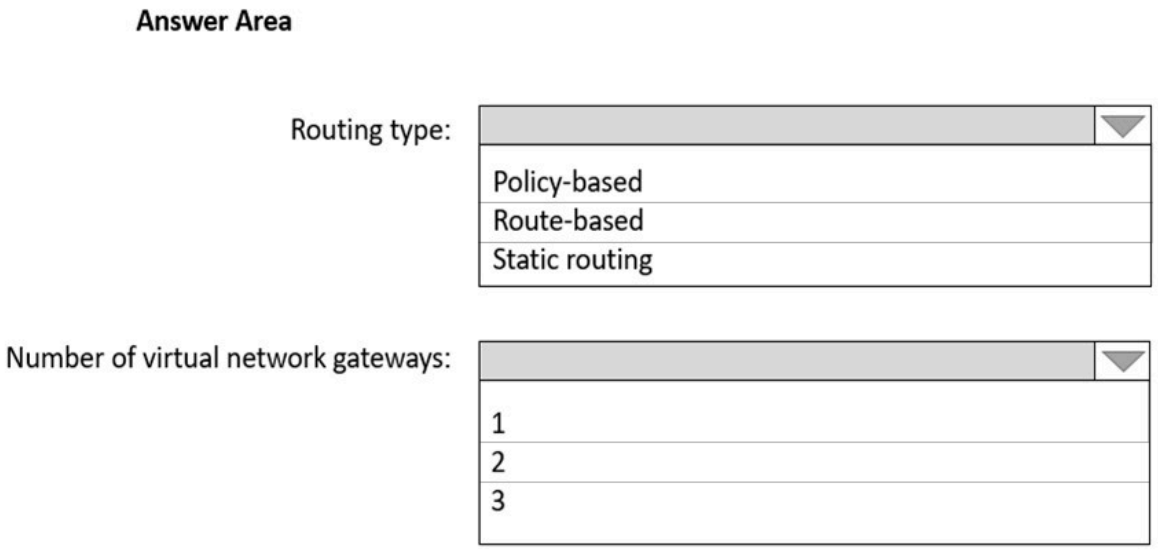
HOTSPOT -

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.

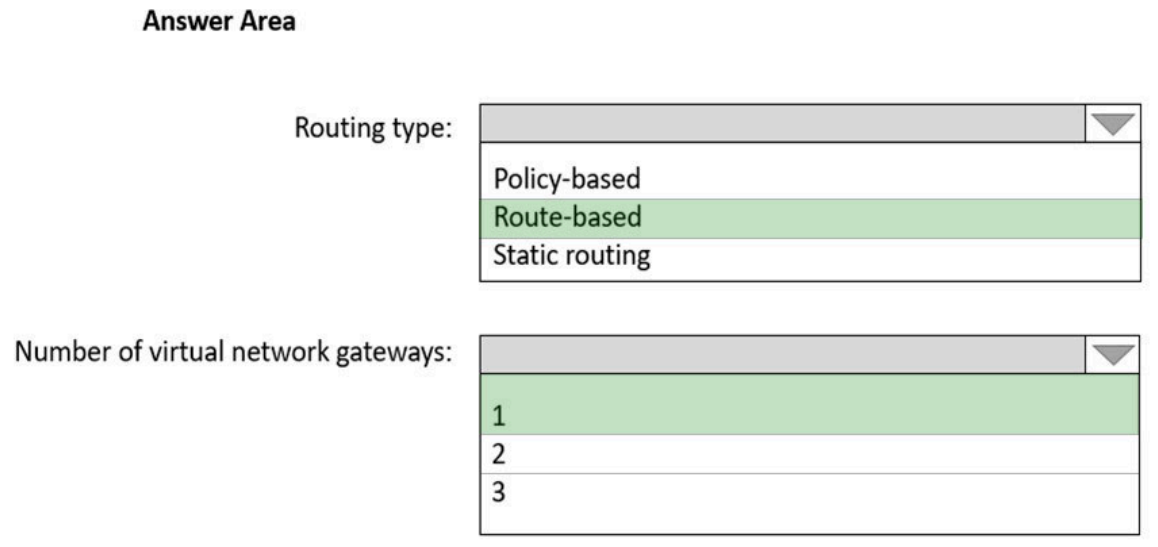
What should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Suggested Answer:



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

nawere Highly Voted 4 years, 6 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-failoverYou are 100 Percent! correct, in a Virtual Network (VNET) you can have two Gateways. - One VPN Gateway - One Express Route Gatewayin 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 103 times

nawere Highly Voted 4 years, 6 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 103 times

Libaax01 3 years, 8 months ago

You are 100 Percent! correct, in a Virtual Network (VNET) you can have two Gateways. - One VPN Gateway - One Express Route Gatewayin 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 3 times

Libaax01 3 years, 8 months ago

You are 100 Percent! correct, in a Virtual Network (VNET) you can have two Gateways. - One VPN Gateway - One Express Route Gateway

upvoted 3 times

Libaax01 3 years, 8 months 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 2 times

a250fb0 Most Recent 1 year, 9 months ago

Routing Type: Use Route-based routing. Route-based VPNs are required for dynamic routing with BGP, which is essential for supporting failover between ExpressRoute and Site-to-Site VPN. Number of Virtual Network Gateways: You need to configure two virtual network gateways: One ExpressRoute gateway for the primary connection. One VPN gateway for the Site-to-Site VPN failover

upvoted 1 times

DPK11 1 year, 9 months ago

- route based - one virtual network gateways You should configure coexistence of ExpressRoute and Site-to-Site VPN https://learn.microsoft.com/en-us/azure/expressroute/how-to-configure-coexisting-gateway-portal

upvoted 2 times

Jamesat 2 years, 1 month ago

The answer is Route Based and 2 Virtual Network Gateways. Both the Expressroute and VPN need distinct gateways identified by their SKU. You cannot have Expressroute on a VpnGw SKU. It must be on a dedicated ExpressRoute SKU gateway. Both VPN Gateways will exist inside the same subnet but the connection are via 2 separate gateways. This doc clearly shows the step of create 2 gateways. https://docs.microsoft.com/en-us/azure/expressroute/expressroute-howto-coexist-resource-manager Step 10: $gw = New-AzVirtualNetworkGateway -Name "ERGateway" -ResourceGroupName $resgrp.ResourceGroupName -Location $location -IpConfigurations $gwConfig -GatewayType "ExpressRoute" -GatewaySku Standard

upvoted 4 times

Gambito11 2 years, 1 month ago

The correct answer for me is routed based and 2. Create the site-to-site VPN gateway and local network gateway ---- https://learn.microsoft.com/en-us/azure/expressroute/how-to-configure-coexisting-gateway-portal

upvoted 1 times

Jamezz 3 years, 4 months ago

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

upvoted 1 times

henryhung 3 years, 7 months 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 4 times

NoeHdzMll 3 years, 10 months 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 3 years, 10 months 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

varundhiman 3 years, 11 months 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

Pradh 4 years, 1 month ago

ROUTE BASED 2 VNG This is the right answer .

upvoted 3 times

HasanHHH 4 years, 1 month 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

Sai_cebu 4 years, 1 month ago

Possible, when you add connection on the Vnet GW connection type options are : Vnet-to-Vnet, Site-to-site and ExpressRoute. I'll go with 1 Vnet Gateway

upvoted 1 times

BlackZeros 4 years, 1 month ago

two gateways = 1 gateway should be onprem (for site to site) and 2nd one is combined in Azure for S2S and ER.

upvoted 1 times

AdityaGupta 4 years, 2 months ago

Route Based and 2 VNet Gateway, as gateway type is different for ER and S2S connections.

upvoted 1 times

GetulioJr 4 years, 2 months ago

Route Based 2

upvoted 2 times

DerekKey 4 years, 2 months ago

Route-base and 2 VNet gateways. People referring to https://docs.microsoft.com/en-us/azure/expressroute/expressroute-howto-coexist-resource-manager should read it carefully because it says exactly that you need 2 gateways. "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), ... you have to first delete the virtual network gateway and increase the gateway subnet size."

upvoted 1 times

Question #7 *Topic 1*

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.

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?

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

A. 1

B. 2

C. 3

D. 4

E. 5

Suggested Answer: *A*
Reference: https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction

Community vote distribution
A (91%) B (9%)

AdityaGupta Highly Voted 4 years, 1 month 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.it's in the same metro, so local is fine
upvoted 8 times

Ajdlfasudfo0 3 years, 11 months ago
it's in the same metro, so local is fine
upvoted 3 times

stormtraining Highly Voted 2 years, 1 month ago
people saying A-1 is correct have 0 knowledge of how Networking Infrastructure works. You need 2: Since all resources in the subscriptions are in either the West US or the West US 2 regions, and you plan to connect all the subscriptions to the on-premises network, you only need one circuit per region. Therefore, a total of two ExpressRoute circuits are required, one for West US and one for West US 2.Since all resources in the subscriptions are in either the West US or the West US 2 regions - if all resources exist in 1 region, Local SKU and 1 circuit is enough. The question does not even mention a SKU, it just asks about the number of circuits.
upvoted 6 times

stormtraining 2 years, 1 month ago
people saying A-1 is correct have 0 knowledge of how Networking Infrastructure works. You need 2: Since all resources in the subscriptions are in either the West US or the West US 2 regions, and you plan to connect all the subscriptions to the on-premises network, you only need one circuit per region. Therefore, a total of two ExpressRoute circuits are required, one for West US and one for West US 2.
upvoted 6 times

xRiot007 1 year, 7 months ago

Since all resources in the subscriptions are in either the West US or the West US 2 regions - if all resources exist in 1 region, Local SKU and 1 circuit is enough. The question does not even mention a SKU, it just asks about the number of circuits.

upvoted 2 times

shaji111 Most Recent 7 months, 4 weeks ago

The question is not specifically asking which SKUs, the default is standard SKU, which can connect multiple region in the same geographical area , so answer A is most appropriate in this context.

upvoted 2 times

IngeTahiti 1 year, 10 months ago

Correct answer.

upvoted 1 times

thekhijir 1 year, 11 months ago

A One ER Required.

upvoted 1 times

sapien45 2 years, 1 month ago

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

khanda 2 years, 1 month ago

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 4 times

TheBlob 2 years, 4 months ago

Answer A is correct. As already mentioned by others you can connect 10 Virtual Networks to a single ExpressRoute Circuit (Standard SKU or higher required). What is important to understand is that those Virtual Networks (e.g., Virtual Network Gateways) must be in the same geographical region. Well, 'West US' and 'West US 2' are in the same geographical region.

upvoted 1 times

Ben_88 3 years, 5 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

ESAJRR 3 years, 6 months ago

Answer: A - 1

upvoted 1 times

mauchi 3 years, 8 months 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 3 years, 9 months ago

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

AdityaGupta 4 years, 2 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 4 years, 2 months ago

Answer: A - 1

upvoted 1 times

Jamesat 4 years, 3 months ago

ExpressRoute circuits can be shared between subscriptions. Correct answer is A

upvoted 4 times

iwikneerg 4 years, 3 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 4 years, 3 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-regionhttps://docs.microsoft.com/en-us/azure/expressroute/expressroute-locations#locations See North America geopolitical region

upvoted 2 times

iwikneerg 4 years, 3 months ago

https://docs.microsoft.com/en-us/azure/expressroute/expressroute-locations#locations See North America geopolitical region

upvoted 1 times

milan92stankovic 4 years, 6 months ago

Answer: A

upvoted 4 times

Question #8 *Topic 1*

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

Suggested Answer: *B*
Reference: https://docs.microsoft.com/en-us/azure/expressroute/expressroute-global-reach

Community vote distribution
B (100%)

kbakdev Most Recent 1 month, 2 weeks ago

Selected Answer: B

ER Global Reach links the two circuits together, so Amsterdam and New York can talk to each other over Microsoft's backbone network.

FastPath makes traffic from your office to Azure VMs faster by skipping the gateway. It doesn't connect offices to each other.

Direct lets you plug straight into MIcrosoft's network at very high speeds. It's about physical cable, not office-to-office.

Local is a cheaper plan for sending data to the one Azure region nearest you. It doesn't connect offices either.

Always when it's about office <-> office over ExpressRoute = Global Reach.

upvoted 1 times

IngeTahiti 1 year, 10 months ago

Selected Answer: B

ExpressRoute Global Reach is the correct answer.

upvoted 2 times

ESAJRR 2 years, 6 months ago

Selected Answer: B

Global Reach classic

upvoted 1 times

Mo22 Highly Voted 2 years, 9 months 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 8 times

Takloy 3 years ago

Selected Answer: B

ExpressRoute Global Reach is the right answer.

upvoted 1 times

HasanHHH 3 years, 1 month 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 3 years, 1 month 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 3 years, 2 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 3 years, 2 months ago

Selected Answer: B

ExpressRoute Global Reach

upvoted 1 times

azeem0077 3 years, 2 months ago

Selected Answer: B

ExpressRoute Global Reach is the correct answer

upvoted 2 times

derrrp 3 years, 3 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 3 years, 4 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 3 years, 5 months ago

Selected Answer: B

Correct answer - Global Reach!

upvoted 3 times

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)

Suggested Answer:

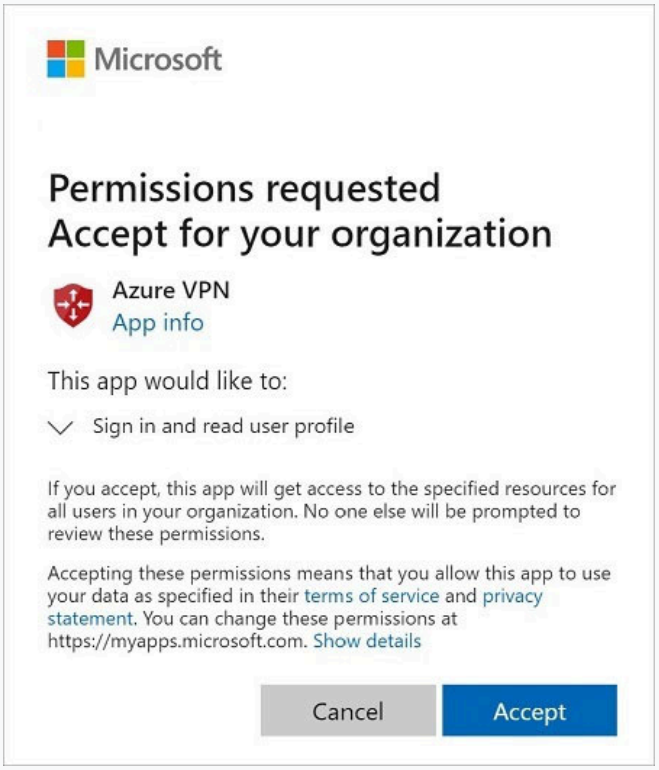
Answer Area:

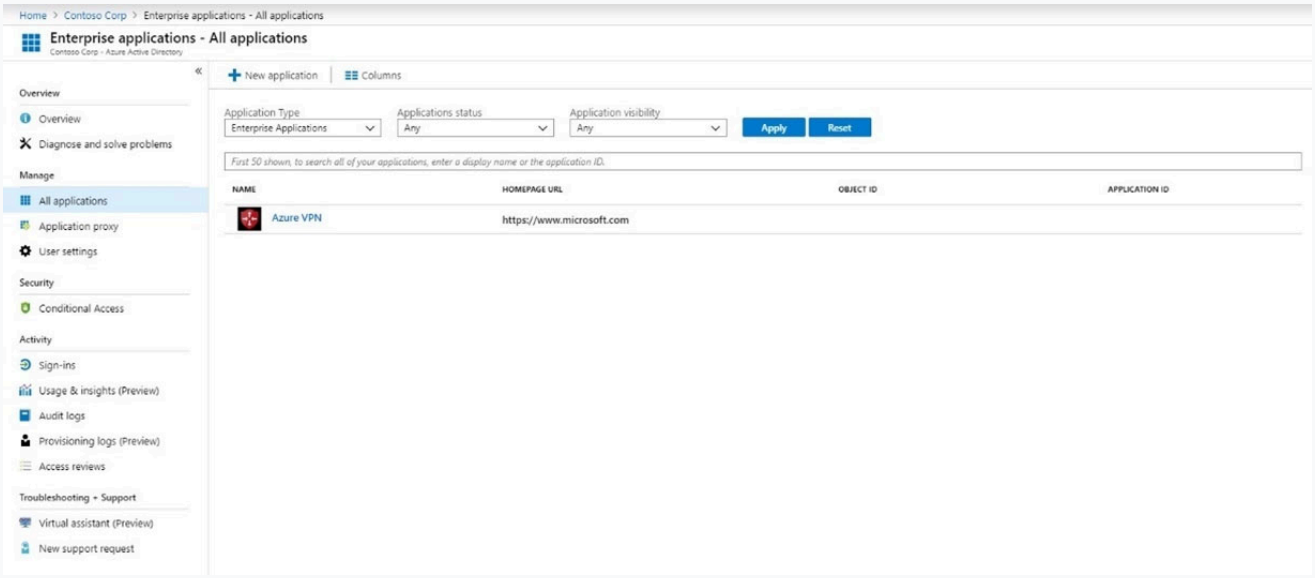
Azure AD configuration:

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

TJ001 Most Recent 2 years, 4 months ago

correct answers

upvoted 2 times

Takloy 2 years, 8 months ago

The answer is correct! Enterprise Application and OpenVPN (SSL).

upvoted 3 times

DerekKey 2 years, 8 months ago

Correct

upvoted 2 times

HOTSPOT -

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

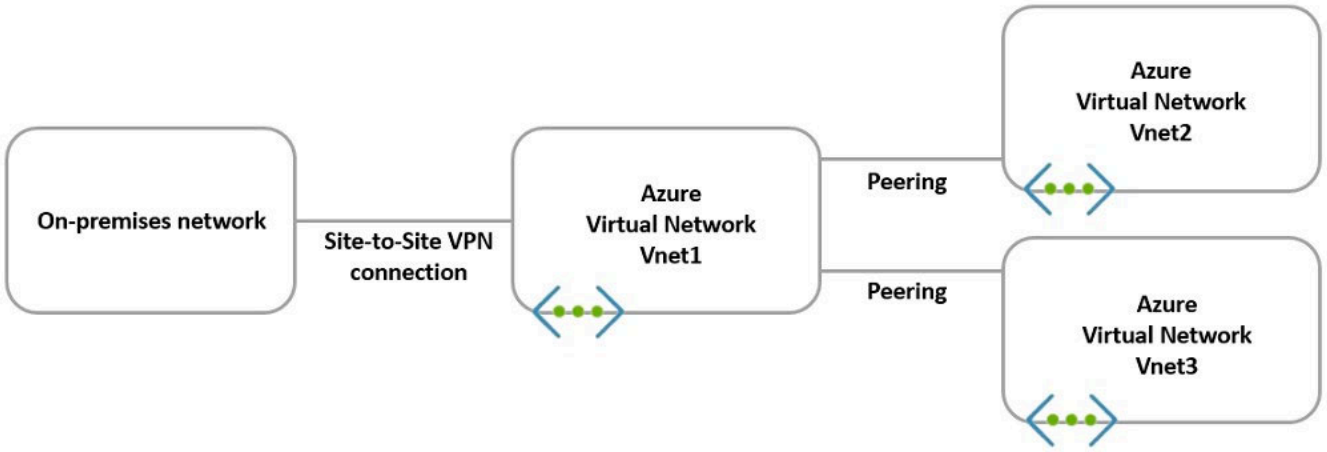
You have a peering connection between Vnet1 and Vnet2 as shown in the Peering-Vnet1-Vnet2 exhibit.

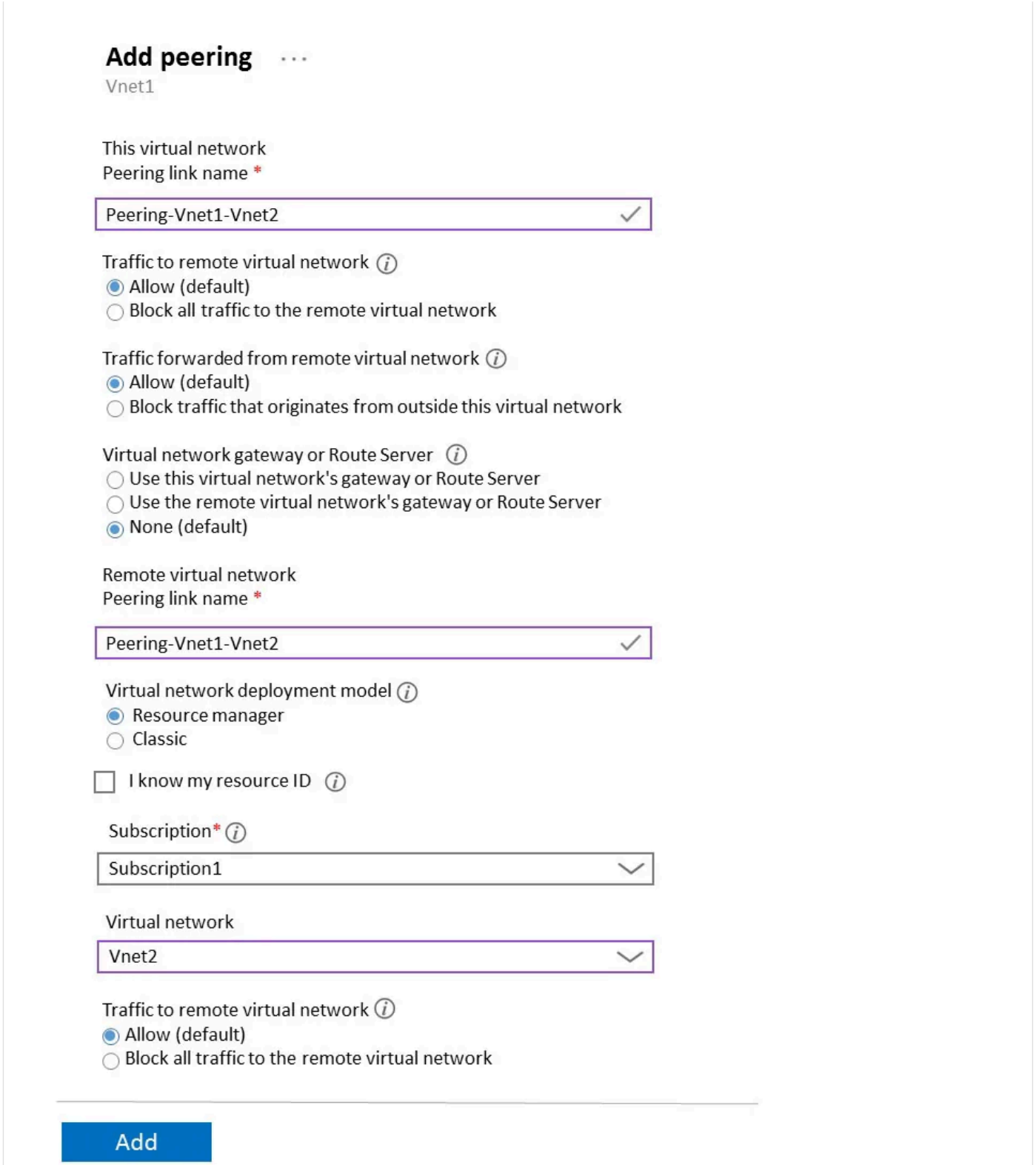
You have a peering connection between Vnet1 and Vnet3 as shown in the Peering-Vnet1-Vnet3 exhibit.

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:




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

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

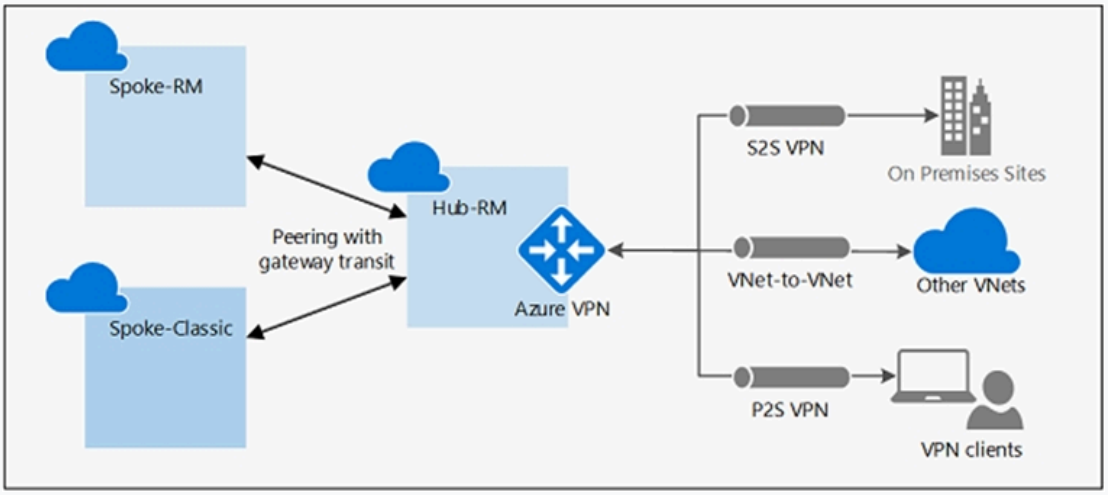
Answer Area:

Statements	Yes	No
The resources in Vnet2 can communicate with the resources in Vnet1.	○	○
The resources in Vnet2 can communicate with the resources in Vnet3.	○	○
The resources in Vnet2 can communicate with the resources in the on-premises network.	○	○

Suggested Answer:

Answer Area:

Statements	Yes	No
The resources in Vnet2 can communicate with the resources in Vnet1.	●	○
The resources in Vnet2 can communicate with the resources in Vnet3.	○	●
The resources in Vnet2 can communicate with the resources in the on-premises network.	○	●



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. 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 3 years, 9 months 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 23 times

Prutser2 Highly Voted 4 years, 1 month ago

correct, vnet1 cannot be a trnsit between vnets2 and 3, without using the gateway as transit

upvoted 6 times

Prutser2 4 years, 1 month ago

correct, vnet1 cannot be a trnsit between vnets2 and 3, without using the gateway as transitIncorrect. 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 6 times

vikrants31 2 years, 11 months 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 2 times

Takemi Most Recent 9 months ago

This question is outdated. Currently, the VNET peering configuration differs from the parameters in the question.

upvoted 2 times

Jastix 2 years, 8 months ago

YYN amt2022. Unfortunately your are incorrect. VNet peering is non-transitive by default. This default behaviour can be altered by selecting the appropriate option 'allow forwarded traffic from the peered vnet'. This would allow 'vnet-3' to receive forwarded traffic from 'vnet-1' (i.e. traffic that is sent from vnet2 is forwarded from vnet1 to vnet2. So the correct option in box 2 is YES. Therefore the answer to the question is YYN. Vnet1 does not allow gateway transit, so vnet3 cannot communicate with the on-prem network.

upvoted 2 times

Jastix 2 years, 8 months ago

YYN amt2022. Unfortunately your are incorrect. VNet peering is non-transitive by default. This default behaviour can be altered by selecting the appropriate option 'allow forwarded traffic from the peered vnet'. This would allow 'vnet-3' to receive forwarded traffic from 'vnet-1' (i.e. traffic that is sent from vnet2 is forwarded from vnet1 to vnet2. So the correct option in box 2 is YES. Therefore the answer to the question is YYN. Vnet1 does not allow gateway transit, so vnet3 cannot communicate with the on-prem network.This is not correct. If you actually bother to create a virtual network and check the description that is shown for this option. It reads: Enabling this option will allow the peered virtual network to receive traffic from virtual networks peered to 'test'. For example, if vnet-2 has an NVA that receives traffic from outside of vnet-2 that gets forwards to vnet-1, you can select this setting to allow that traffic to reach vnet-1 from vnet-2. While enabling this capability allows the forwarded traffic through the peering, it doesn't create any user-defined routes or network virtual appliances. User-defined routes and network virtual appliances are created separately. Meaning that only selecting this option won't enable the peering between VNET 2 & VNET 3

upvoted 2 times

morito 2 years, 4 months ago

This is not correct. If you actually bother to create a virtual network and check the description that is shown for this option. It reads: Enabling this option will allow the peered virtual network to receive traffic from virtual networks peered to 'test'. For example, if vnet-2 has an NVA that receives traffic from outside of vnet-2 that gets forwards to vnet-1, you can select this setting to allow that traffic to reach vnet-1 from vnet-2. While enabling this capability allows the forwarded traffic through the peering, it doesn't create any user-defined routes or network virtual appliances. User-defined routes and network virtual appliances are created separately. Meaning that only selecting this option won't enable the peering between VNET 2 & VNET 3

upvoted 2 times

bp_a_user 3 years, 1 month 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 3 years, 1 month 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.I am wrong, I think it that old screenshot, the option "remote gateway or route server" should be enabled

upvoted 1 times

bp_a_user 3 years, 1 month ago

I am wrong, I think it that old screenshot, the option "remote gateway or route server" should be enabled

upvoted 3 times

vDreams 3 years, 2 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 3 years, 8 months ago

Answer is correct. Y N N

upvoted 2 times

TJ001 3 years, 10 months ago

yes,no,no

upvoted 2 times

zukako 3 years, 10 months ago

correct vnet1 not use its gateway for vnet2

upvoted 1 times

DeepMoon 4 years, 1 month ago

Doesn't the 2nd Link name on both those peerings are wrong matter?

upvoted 1 times

GetulioJr 4 years, 2 months ago

Answer is correct, The option: Use the remote virtual network's gateway" is not enabled

upvoted 2 times

DerekKey 4 years, 2 months ago

Correct

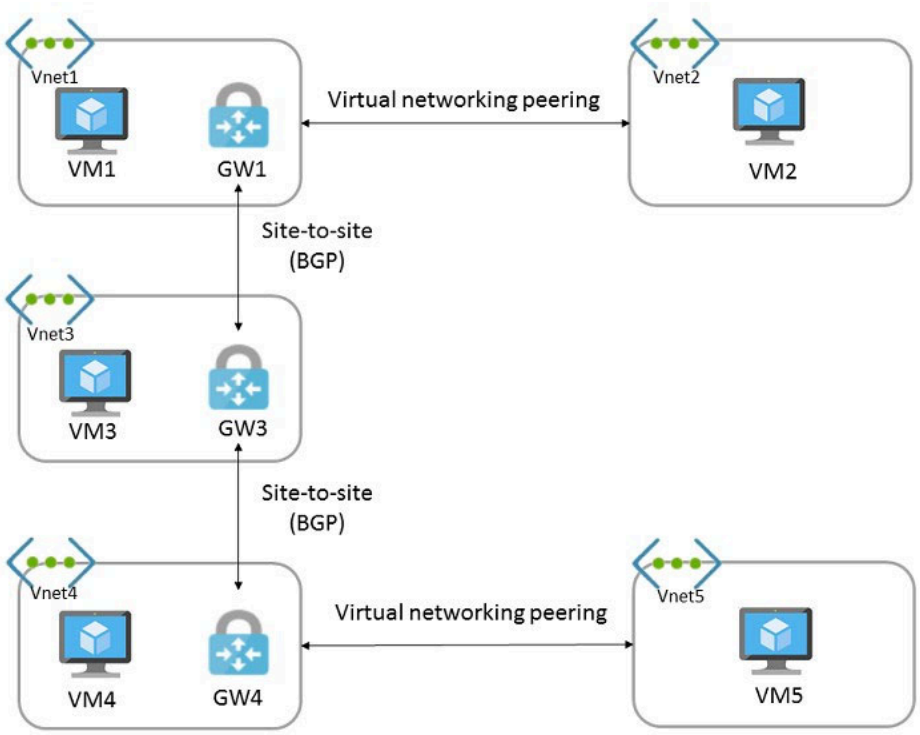
upvoted 3 times

Question #11 *Topic 1*

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.

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



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**

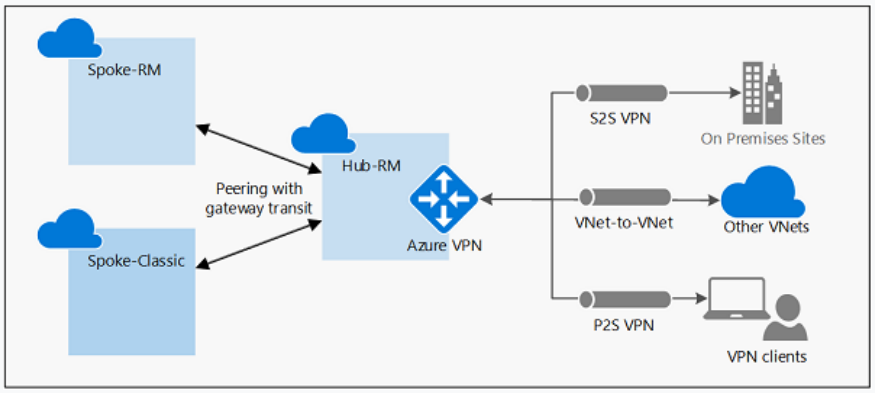
Answer Area:

Statements	Yes	No
VM1 and VM4 can communicate.	○	○
VM2 and VM4 can communicate.	○	○
VM1 and VM5 can communicate.	○	○

Suggested Answer:

Answer Area:

Statements	Yes	No
VM1 and VM4 can communicate.	◯	◯
VM2 and VM4 can communicate.	◯	◯
VM1 and VM5 can communicate.	◯	◯



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

[Removed] Highly Voted 3 years, 8 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 31 times

[Removed] Highly Voted 3 years, 8 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.it blocks communication from VNET5 to VNET4 but allows VNET4 to VNET5How about the the return traffic VNET5 to VNET4 ?How about the the return traffic VNET5 to VNET4 ? - No need to care about the returnThat'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.Could you pls clarify? This is referring the vnet peering settings not NSGHow about you read Microsoft documentation for a change ? Instead of expecting being certified by spoonfeeding you the responses : https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering Disabling 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. YYY- 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 31 times

Aiwa23 3 years, 8 months ago

it blocks communication from VNET5 to VNET4 but allows VNET4 to VNET5How about the the return traffic VNET5 to VNET4 ?How about the the return traffic VNET5 to VNET4 ? - No need to care about the returnThat'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.Could you pls clarify? This is referring the vnet peering settings not NSGHow about you read Microsoft documentation for a change ? Instead of expecting being certified by spoonfeeding you the responses : https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering Disabling 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. YYY- 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 7 times

Aiwa23 3 years, 8 months ago

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

upvoted 7 times

Pratheeshp 3 years ago

How about the the return traffic VNET5 to VNET4 ?How about the the return traffic VNET5 to VNET4 ? - No need to care about the return

upvoted 2 times

Pratheeshp 3 years ago

How about the the return traffic VNET5 to VNET4 ?

upvoted 2 times

xRiot007 1 year, 7 months ago

How about the the return traffic VNET5 to VNET4 ? - No need to care about the return

upvoted 1 times

[Removed] 3 years, 8 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

[Removed] 3 years, 8 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.Could you pls clarify? This is referring the vnet peering settings not NSGHow about you read Microsoft documentation for a change ? Instead of expecting being certified by spoonfeeding you the responses : https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering Disabling 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. YYY- 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

A_way 3 years, 8 months ago

Could you pls clarify? This is referring the vnet peering settings not NSGHow about you read Microsoft documentation for a change ? Instead of expecting being certified by spoonfeeding you the responses : https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering Disabling 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. YYY- 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 6 times

A_way 3 years, 8 months ago

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

upvoted 6 times

sapien45 3 years, 8 months ago

How about you read Microsoft documentation for a change ? Instead of expecting being certified by spoonfeeding you the responses :

https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering

Disabling 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. YYY

upvoted 2 times

sapien45 3 years, 8 months ago

How about you read Microsoft documentation for a change ? Instead of expecting being certified by spoonfeeding you the responses : https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering Disabling 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. YYY- 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

fourfour 3 years ago

- 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

Alessandro365 3 years, 8 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 12 times

Rowdy_47 Most Recent 1 year, 1 month ago

Answer is YYY the "Traffic to remote virtual network" only applies to traffic between peered VNets.

upvoted 2 times

Asher 1 year, 1 month ago

Y = VM 1 can reach VM 4 via site-to-site which will have routing Y = peering on VNET2 is set to use remote gateway and VNET1 is set to use it's gateway for transit N = although VNET4 and 5 are peered, peerings are not transitive so a peering between vnet1 and 5 would be needed for this to work? Block on VNET 5 can be ignored as it won't apply to return traffic only traffic originated from VNET5?

upvoted 2 times

nabeel79 1 year, 6 months ago

YYY is worked

upvoted 1 times

Hullstar 2 years ago

there isn't a peering configuration for VNet3 and the default is not to allow. Wouldn't the answer be NYN

upvoted 1 times

sam881989 2 years, 4 months 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 10 times

Opala79 2 years, 5 months ago

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

upvoted 3 times

Opala79 2 years, 5 months ago

I think it would be NNN because the option "Use remote gateway" of VNET 1 is disabled, someone disagrees ?I think this should be the answer. Someone need to confirm.This is correct because going by the possible data flow between the VNets, the three options have to be routed through Vnet1, of which the `use of remote's gateway` (VNet3 S2S) is not permittedI think so

upvoted 3 times

lvz 2 years, 2 months ago

I think this should be the answer. Someone need to confirm.

upvoted 1 times

pattj2 1 year, 7 months ago

This is correct because going by the possible data flow between the VNets, the three options have to be routed through Vnet1, of which the `use of remote's gateway` (VNet3 S2S) is not permitted

upvoted 1 times

Aydin 2 years ago

I think so

upvoted 1 times

Verytutos 2 years, 8 months ago

Appeared on Exam 05 Sep 2023

upvoted 3 times

Oklama 2 years, 11 months ago

YYY is correct

upvoted 1 times

arnaudhelin 3 years, 1 month 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.so what is your find man?

upvoted 7 times

arnaudhelin 3 years, 1 month 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

lvz 2 years, 2 months ago

so what is your find man?

upvoted 2 times

mm2 3 years, 3 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

tester2023 3 years, 3 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.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 7 times

tester2023 3 years, 3 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 7 times

asdasd123123iu 2 years, 10 months 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 3 years, 3 months 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 differnt vnet, such as vnet1, thus (bidirectional) communication between them its not possible.

upvoted 7 times

TJ001 3 years, 4 months ago

YYY seems right

upvoted 1 times

MyPractice 3 years, 5 months ago

This came in Dec 2022

upvoted 1 times

geuser 3 years, 5 months ago

I say YYN No becuase: 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 5 times

Question #12 *Topic 1*

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.

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

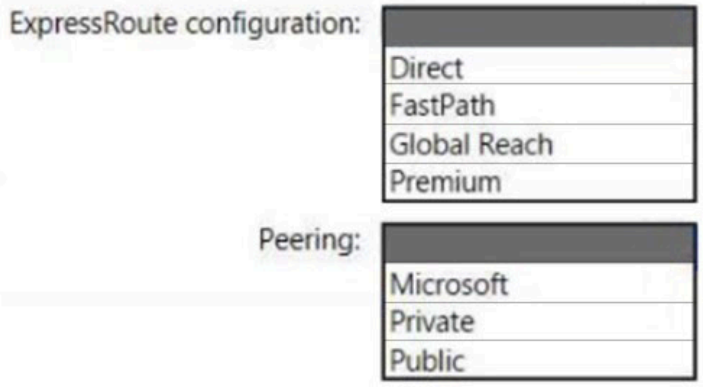
How should you configure the network? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

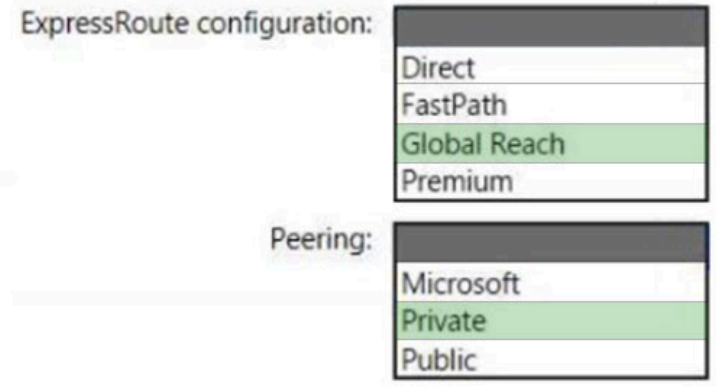
Name	Azure region	Datacenter
ERC1	East US	New York
ERC2	West US2	Seattle

Answer Area



Suggested Answer:

Answer Area



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

MCCC454 Highly Voted 2 years, 3 months ago

On exam 7 februari 2024

upvoted 7 times

ironbornson Highly Voted 2 years, 9 months 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 obiously

upvoted 6 times

SSETH78 Most Recent 1 year, 8 months ago

Both the location are within Geopolitical region "North America" as mentioned at https://learn.microsoft.com/en-us/azure/expressroute/expressroute-locations-providers?tabs=america%2Ca-c%2Ca-k#locations Then why do we need to have "Global reach" facility and pay high charges? Express route of type "Premum" would serve the purpose. isnt it?

upvoted 2 times

NextBrand 2 years, 1 month ago

Across on-premises connectivity with ExpressRoute Global Reach By enabling ExpressRoute Global Reach, you can exchange data across your on-premises sites through your ExpressRoute circuits. For instance, suppose you have two private data centers, one in California and one in Texas, each connected to an ExpressRoute circuit in their respective regions. You can use ExpressRoute Global Reach to link your data centers with these circuits, and your cross data-center traffic uses the Microsoft network. https://learn.microsoft.com/en-us/azure/expressroute/expressroute-introduction

upvoted 2 times

bakamon 2 years, 11 months ago

:: Global Reach :: Private

upvoted 1 times

Himank20 3 years 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 3 years, 4 months ago

En examen 20/01/2023

upvoted 3 times

Tightbot 3 years, 5 months ago

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

upvoted 2 times

Takloy 3 years, 6 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 3 years, 7 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.East US and West US does not fall in the same geopolitical,,,,East US and East US 2 maythat's not right, they are indeed under the same geopolitical region - check here https://learn.microsoft.com/en-us/azure/expressroute/expressroute-locationsI agree. Geoppolitical 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 2 times

sikbeats 3 years, 7 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 3 years, 4 months ago

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

upvoted 1 times

TJ001 3 years, 4 months ago

East US and West US does not fall in the same geopolitical,,,,East US and East US 2 maythat's not right, they are indeed under the same geopolitical region - check here https://learn.microsoft.com/en-us/azure/expressroute/expressroute-locationsI agree. Geoppolitical 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

mauchi 3 years, 3 months ago

that's not right, they are indeed under the same geopolitical region - check here https://learn.microsoft.com/en-us/azure/expressroute/expressroute-locationsI agree. Geoppolitical 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 2 times

mauchi 3 years, 3 months 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 3 years, 2 months ago

I agree. Geoppolitical 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 3 years, 8 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 3 years, 8 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 2 times

DerekKey 3 years, 8 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 3 years, 8 months ago

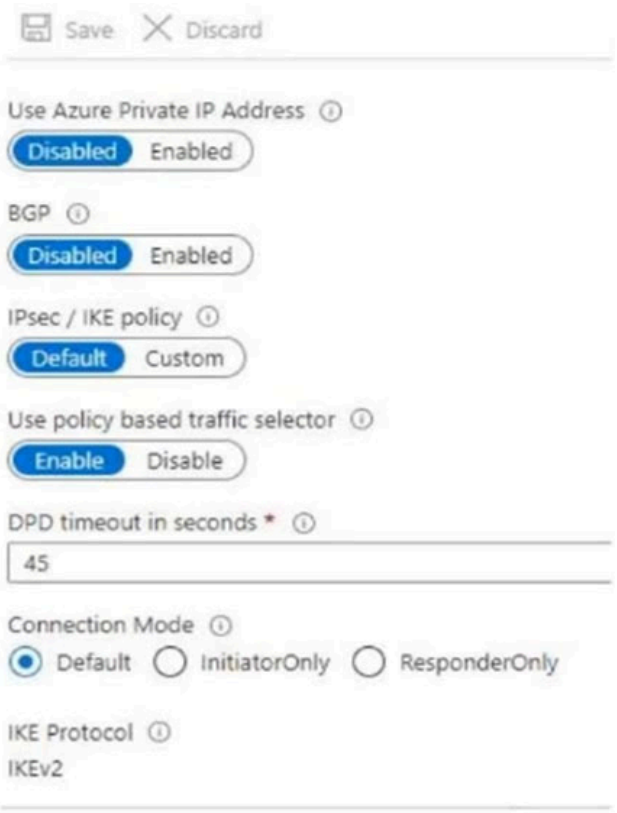
Looks correct. To confirm the second question - https://docs.microsoft.com/en-us/azure/expressroute/expressroute-howto-set-global-reach.

upvoted 2 times

Question #13 *Topic 1*

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.

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.

Suggested 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 (91%) B (9%)

RageshBethapudi Highly Voted 4 years, 2 months ago
correct answer is D. https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-connect-multiple-policybased-rm-ps
upvoted 17 times

jilguens Highly Voted 4 years, 2 months ago

D is correct

upvoted 6 times

dho2009 Most Recent 6 months, 2 weeks ago

using custom IPsec/IKE policy, you can use a route-based VPN gateway and connect to multiple policy-based VPN/firewall devices

upvoted 1 times

679956a 8 months, 3 weeks ago

Key here is that on-premises POLICY-based VPN needs to communicated to AZ ROUTE-based VPN and this requires to configure 'custom IPsec/IKE policy' and enable 'PolicyBasedTrafficSelectors'

upvoted 1 times

620b351 2 years, 1 month ago

Correct answerd is D. BGP is not mandatory to have a S2S VPN.

upvoted 1 times

vDreams 3 years, 2 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 3 years, 7 months ago

Correct answer is D

upvoted 1 times

Chezzer83 3 years, 7 months ago

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

upvoted 2 times

where2go 3 years, 7 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 3 years, 8 months 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 3 years, 9 months 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 3 years, 10 months ago

En examen 20/01/2023

upvoted 2 times

mm2 3 years, 10 months 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 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 3 years, 10 months 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 3 years, 10 months ago

Not have to set BGP if onpremise is act/stanby

upvoted 1 times

Andre369 3 years, 11 months ago

correct answer is D. https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-connect-multiple-policybased-rm-ps

upvoted 1 times

JRodJ 3 years, 11 months 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

Question #14 *Topic 1*

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.

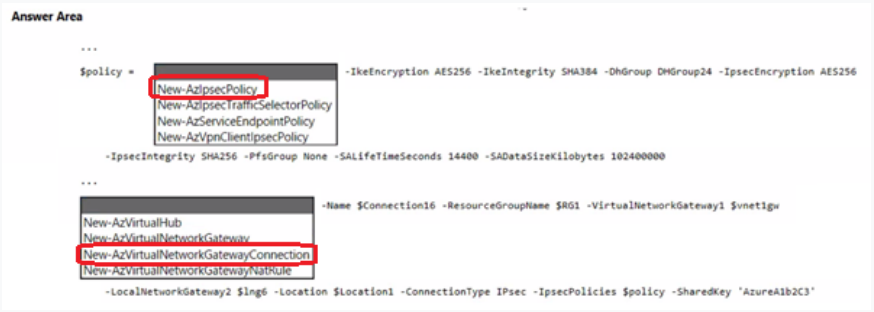
How should you complete the PowerShell script? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

```
...
$policy = [                              ] -IkeEncryption AES256 -IkeIntegrity SHA384 -DhGroup DHGroup24 -IpsecEncryption AES256
          [New-AzIpsecPolicy             ]
          [New-AzIpsecTrafficSelectorPolicy]
          [New-AzServiceEndpointPolicy   ]
          [New-AzVpnClientIpsecPolicy    ]
    -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'
```

Suggested Answer:



Goofer Highly Voted 3 years, 4 months ago

1 = New-AzIpsecPolicy 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-1Thanks - agreed

upvoted 19 times

Goofer Highly Voted 3 years, 4 months ago

1 = New-AzIpsecPolicy 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 19 times

nabeel79 Most Recent 1 year, 6 months ago

1 - New-AzIpsecPolicy

2 - New-AzVirtualNetworkGatewayConnection

upvoted 2 times

nabeel79 1 year, 6 months ago

New-AzIpsecPolicy and NewVirtualNetworkGatewayConnection

upvoted 1 times

_Cris 2 years, 8 months ago

appears on exam, 19 Sept 2023

upvoted 3 times

SLGUY 2 years, 8 months ago

Appeared on Exam 26 Aug 2023

upvoted 2 times

Billabongs 2 years, 10 months 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 2 times

Rajan395 3 years, 3 months ago

answer looks correct

upvoted 3 times

liono 3 years, 4 months ago

Given Answer is correct

upvoted 1 times

TJ001 3 years, 4 months ago

Given answers looks good

upvoted 1 times

Aunehwet79 3 years, 4 months ago

Thanks - agreed

upvoted 1 times

Goofer 3 years, 4 months ago

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

upvoted 1 times

Question #15 *Topic 1*

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 = [                          ] -Name "HQ" -ResourceGroupName "ForcedTunneling"
          Get-AzLocalNetworkGateway
          Get-AzNatGateway
          Get-AzNetworkVirtualAppliance
          Get-AzVirtualNetworkGateway

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

Suggested Answer:

Answer Area

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

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

nabeel79 Most Recent 1 year, 6 months ago

Get-AzLocalNetworkGateway

AzVirtualNetworkGatewayDefaultSite

upvoted 2 times

Verytutos 2 years, 2 months ago

Appeared on Exam 05 Sep 2023

upvoted 3 times

dani999 2 years, 9 months ago

Correct answer :

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

$VirtualGateway = Get-AzVirtualNetworkGateway -Name "ContosoVirtualGateway"

Set-AzVirtualNetworkGatewayDefaultSite -GatewayDefaultSite $LocalGateway -VirtualNetworkGateway $VirtualGateway

upvoted 4 times

liono 2 years, 10 months ago

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

upvoted 2 times

DavidSapery Highly Voted 2 years, 10 months 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 18 times

Question #16 *Topic 1*

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

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?

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

A. VNet-to-VNet VPN connections

B. peering

C. service endpoints

D. route tables

Suggested Answer: *B*

Community vote distribution

B (100%)

3f92a3c Most Recent 8 months ago

My answer is B

upvoted 1 times

nabeel79 1 year, 6 months ago

Peering

upvoted 2 times

admyn1997 2 years, 1 month ago

Peering with transit gateway.

upvoted 1 times

unciax 3 years, 2 months ago

Appeared on Exam 28 Aug 2023

upvoted 3 times

ronin201 3 years, 4 months ago

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

upvoted 4 times

Rick0304 3 years, 6 months ago

Peering is the correct answer!

upvoted 2 times

ESAJRR 3 years, 7 months ago

Peering is correct!

upvoted 2 times

mVic 3 years, 9 months ago

Peering is correct.

upvoted 4 times

Rajan395 3 years, 9 months ago

Correct. VNET peering is the answer.

upvoted 3 times

liono 3 years, 10 months ago

VNET Peering!

upvoted 1 times

krishnadasns96 3 years, 10 months ago

Correct, Peering

upvoted 3 times

Question #17 *Topic 1*

Your company has an office in New York.

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

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?

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

A. one ExpressRoute Premium circuit

B. two ExpressRoute Premium circuits

C. four ExpressRoute Standard circuits

D. one ExpressRoute Standard circuit

Suggested Answer: *A*

Community vote distribution

A (100%)

sumandev Highly Voted 3 years, 10 months ago

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

upvoted 13 times

OrangeSG Highly Voted 3 years ago

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 8 times

nabeel79 Most Recent 1 year, 6 months ago

Express Route Premium SKU provides ability to connect from on-premises any other Azure regions

upvoted 1 times

Ganchev 2 years ago

Why we can't use ER Local SKU to connect NY to VNET1, which has a Global VNET Peering with VNET2, 3 and 4?

upvoted 1 times

_Cris 3 years, 1 month ago

appears on exam, 19 Sept 2023

upvoted 3 times

SLGUY 3 years, 2 months ago

Appeared on Exam 26 Aug 2023

upvoted 6 times

charrua86 3 years, 3 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 5 times

Pratheeshp 3 years, 6 months 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 2 times

Rafael1984 3 years, 7 months ago

I think is D because you must be minimized cost

upvoted 2 times

Rafael1984 3 years, 7 months ago

I think is D because you must be minimized costER Standard SKU doesn't allow you to connect across a geopolitical area. Hence, it is A ref: https://eighty20solutions.com.au/azure-expressroute/This is a much better explanation compared to MS garble!

upvoted 2 times

ryswick7 3 years, 7 months 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 5 times

ryswick7 3 years, 7 months 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/This is a much better explanation compared to MS garble!

upvoted 5 times

jarz 3 years, 6 months ago

This is a much better explanation compared to MS garble!

upvoted 2 times

ESAJRR 3 years, 7 months ago

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 3 years, 8 months ago

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

upvoted 1 times

SeanPan 3 years, 9 months ago

A is correct

upvoted 2 times

dani999 3 years, 9 months ago

A is correct

upvoted 4 times

liono 3 years, 10 months ago

One ExpressRoute circuit is required for the office with premium SKU

upvoted 1 times

DeepMoon 3 years, 10 months 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

Question #18 *Topic 1*

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

Suggested Answer: *C*

Community vote distribution

C (100%)

DavidSapery Highly Voted 3 years, 10 months 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 41 times

nabeel79 Most Recent 1 year, 6 months ago

Selected Answer: C

Generation2 VpnGw4AZ Max. 100* Max

upvoted 1 times

Nabgre 2 years, 1 month ago

The correct answer is C - VpnGw4 which support up to 100 S2S/VNet-to-VNet

Tunnels

upvoted 1 times

Pixan 3 years 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 2 times

Lazylinux 3 years ago

Selected Answer: C

I C

as per

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

upvoted 2 times

Rick0304 3 years, 6 months ago

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

upvoted 2 times

ESAJRR 3 years, 7 months 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 10 times

wooyourdaddy 3 years, 8 months 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 4 times

dani999 3 years, 9 months ago

Selected Answer: C

VpnGw4AZ Max. 100 s2s

Zone-redundant is support

upvoted 4 times

sserna 3 years, 10 months ago

En examen 20/01/2023

upvoted 2 times

liono 3 years, 10 months ago

Correct! SKU4

upvoted 2 times

DavidSapery Highly Voted 3 years, 10 months 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 41 times

DeepMoon 3 years, 10 months ago

Ditto.

upvoted 2 times

Question #19 *Topic 1*

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

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?

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

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.

Suggested Answer: *D*

Community vote distribution

D (100%)

DeepMoon Highly Voted 2 years, 10 months 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 19 times

DeepMoon Highly Voted 2 years, 10 months 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-overviewyou 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 providedI don't understand why everyone is fixed on D. The question doesn't state that VM2 in the VNet in a different region need to be added to the backend pool. They just need to be able to reach LB1 in VNet1.

upvoted 19 times

ConanBarb 2 years, 1 month 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 7 times

ConanBarb 2 years, 1 month 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 providedI don't understand why everyone is fixed on D. The question doesn't state that VM2 in the VNet in a different region need to be added to the backend pool. They just need to be able to reach LB1 in VNet1.

upvoted 7 times

haxaffee 1 year, 11 months ago

I don't understand why everyone is fixed on D. The question doesn't state that VM2 in the VNet in a different region need to be added to the backend pool. They just need to be able to reach LB1 in VNet1.

upvoted 1 times

daemon101 2 years, 3 months 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/this, IMHO, is the right reasoning behind D - Standard SKU, not Basicagree 100%, the question is not about cross region load balancing, but about supportability of the front end of the LB.

upvoted 11 times

daemon101 2 years, 3 months 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 11 times

ConanBarb 2 years, 1 month ago

this, IMHO, is the right reasoning behind D - Standard SKU, not Basicagree 100%, the question is not about cross region load balancing, but about supportability of the front end of the LB.

upvoted 3 times

ConanBarb 2 years, 1 month ago

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

upvoted 3 times

ar407 2 years ago

agree 100%, the question is not about cross region load balancing, but about supportability of the front end of the LB.

upvoted 1 times

windowsmodulesinstallerworker Most Recent 1 year, 5 months ago

reminder that both vm1 and vm2 have to be in a single availability set for this question to make sense, since basic sku supports only vms in a single availability set to be added to the backend pool

upvoted 1 times

nabeel79 1 year, 6 months ago

Basic sku won't support cross-region traffic

upvoted 1 times

ConanBarb 2 years, 1 month ago

Global VNet Peering now supports Standard Load Balancer

upvoted 3 times

khanda 2 years, 7 months ago

Azure Standard Load Balancer supports cross-region load balancing.

upvoted 4 times

ESAJRR 2 years, 7 months ago

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 2 years, 10 months ago

Correct. Change SKU to Standard.

upvoted 3 times

Stevy_nash 2 years, 10 months ago

we should also change the SKU of VMs' IP adresses to standard or remove themThe question didn't mention that the VMs have public IP addresses.

upvoted 4 times

Stevy_nash 2 years, 10 months ago

Selected Answer: D

we should also change the SKU of VMs' IP adresses to standard or remove them

upvoted 4 times

Neostar 2 years, 8 months ago

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

upvoted 1 times

TT924 2 years, 10 months ago

Selected Answer: D

Standard ILB is supported via Global VNet Peering

Standard ILB is supported via Global VNet Peering

upvoted 2 times

TT924 2 years, 10 months ago

Standard ILB is supported via Global VNet Peering Standard ILB is supported via Global VNet Peeringhttps://learn.microsoft.com/en-us/azure/load-balancer/skus#skus

upvoted 2 times

TT924 2 years, 10 months ago

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

upvoted 1 times

Question #20 *Topic 1*

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).

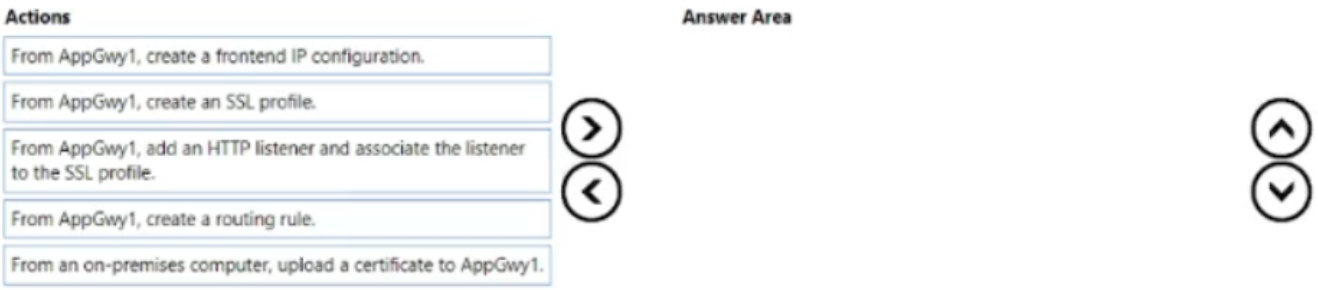
You have an Azure subscription.

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.



Suggested Answer:



aklas Highly Voted 3 years, 6 months 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.Agree. However must be some mistake in answer related with listener, because there is no possibility to sign SSL profile to HTTP, only HTTPS.Agree. In this link is added the routing rule: https://learn.microsoft.com/en-us/azure/application-gateway/mutual-authentication-powershelldisagreed. routing Rule had been configured, as mentioned in the questionthat routing rule is for another HTTP listener this answer is correct based on the given information stating you have already completed the following • Configure an HTTP listener • Associate a routing rule with the listener so the focus here is the mutual auth configuration steps, and adjusting the routing rule or creating a new rule to match the new listener would be required. The revealed solution would be correct if there were no actions already been taken.To asssociate the SSL profile with a listener you need the SSL profile and the frontend IP

upvoted 35 times

aklas Highly Voted 3 years, 6 months 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 35 times

Antviss Most Recent 7 months, 1 week ago

Upload the CA Cert: The gateway needs the public key to "know" who the trusted issuer is.

Create the SSL Profile: This is the container where you tell Azure, "Hey, please demand a client certificate and check it against that CA cert I just uploaded."

Add/Configure the Listener: You link the listener to that SSL Profile. This is the moment the "HTTP Listener" (resource type) is configured to handle the secure handshake.

Create the Routing Rule: The final bridge that tells the authenticated traffic where to go on the backend.

upvoted 2 times

asdasd123123iu 3 years, 4 months 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

asdasd123123iu 3 years, 4 months 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.Agree. In this link is added the routing rule: https://learn.microsoft.com/en-us/azure/application-gateway/mutual-authentication-powershell

upvoted 3 times

rcristiano 7 months, 2 weeks ago

Resposta oficial do exame: 1. From AppGw1, create a frontend IP configuration

2. From an on-premises computer, upload a certificate to AppGw1

3. From AppGw1, create an SSL profile

4. From AppGw1, add an HTTP listener and associate the listener to the SSL profile

upvoted 1 times

Drummer 1 year, 5 months ago

Step 1: From an on-prem computer, upload a certificate to AppGwy1

Step 2: From AppGwy1, create an SSL profile

Step 3: From AppGwy1, add an HTTP listener and associate the listener with the SSL profile

Step 4: From AppGwy1, create a fronten IP Configuration

upvoted 1 times

Eddie_Sli 2 years, 3 months ago

disagreed. routing Rule had been configured, as mentioned in the question

upvoted 1 times

Eddie_Sli 2 years, 3 months ago

disagreed. routing Rule had been configured, as mentioned in the questionthat routing rule is for another HTTP listener this answer is correct based on the given information stating you have already completed the following • Configure an HTTP listener • Associate a routing rule with the listener so the focus here is the mutual auth configuration steps, and adjusting the routing rule or creating a new rule to match the new listener would be required. The revealed solution would be correct if there were no actions already been taken.

upvoted 1 times

windowsmodulesinstallerworker 1 year, 6 months ago

You need to upload the cert first since it is then referenced when creating the ssl profile. And after that creating a listener must reference the ssl profile. Lastly you create a route as illustrated in the powershell example.

1. upload cert

2. create ssl profile

3. add listener

4. create routing rule

https://learn.microsoft.com/en-us/azure/application-gateway/mutual-authentication-powershell#configure-client-authentication

https://learn.microsoft.com/en-us/azure/application-gateway/mutual-authentication-powershell#configure-the-rule

The frontend IP is already there since you need it when creating a listener and a previous HTTP listener was already created so the frontend ip config must exist

upvoted 2 times

a250fb0 1 year, 9 months ago

Step 1: From an on-prem computer, upload a certificate to AppGwy1

Step 2: From AppGwy1, create an SSL profile

Step 3: From AppGwy1, add an HTTP listener and associate the listener with the SSL profile

Step 4: From AppGwy1, create a routing rule

upvoted 5 times

Eddie_Sli 2 years, 3 months ago

fontend IP, create SSL profile, upload a cert, associate the listener to the profile

upvoted 1 times

harshit101 3 years, 9 months ago

what is going on here?

upvoted 12 times

harshit101 3 years, 9 months ago

what is going on here?Bweakfast

upvoted 12 times

Lazylinux 3 years 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 6 times

ConanBarb 3 years, 1 month 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 2 times

voldemort123 3 years, 1 month ago

such discussions, much confusion

upvoted 3 times

_Cris 3 years, 1 month ago

appears on exam, 19 Sept 2023

upvoted 1 times

pijp 3 years, 2 months ago

thanks for the feedback

upvoted 1 times

Feliphus 2 years ago

To asssociate the SSL profile with a listener you need the SSL profile and the frontend IP

upvoted 1 times

grimrodd 2 years, 3 months ago

that routing rule is for another HTTP listener this answer is correct based on the given information stating you have already completed the following

• Configure an HTTP listener

• Associate a routing rule with the listener

so the focus here is the mutual auth configuration steps, and adjusting the routing rule or creating a new rule to match the new listener would be required.

The revealed solution would be correct if there were no actions already been taken.

upvoted 1 times

SLGUY 3 years, 2 months ago

Appeared on Exam 26 Aug 2023thanks for the feedback

upvoted 3 times

SLGUY 3 years, 2 months ago

Appeared on Exam 26 Aug 2023

upvoted 3 times

DCor2022 3 years, 2 months ago

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

upvoted 3 times

khanda 3 years, 7 months ago

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

upvoted 1 times

rj_289 3 years, 7 months ago

Given answer is correct!

upvoted 3 times

Aziza_Adam 3 years, 9 months ago

The given answer is correct

upvoted 3 times

kienvu 3 years, 9 months 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

kienvu 3 years, 9 months 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 ProfileThis 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 6 times

omgMerrick 3 years, 9 months 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 3 years, 9 months ago

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

upvoted 6 times

tryhard97 3 years, 9 months ago

help answer plz

upvoted 1 times

Kalzonee3611 2 years, 7 months ago

Bweakfast

upvoted 4 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 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.

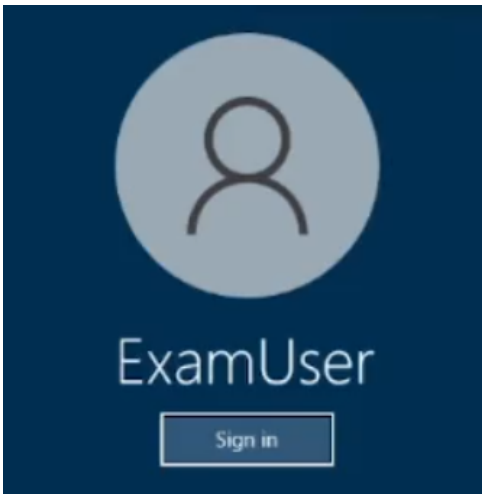
The on-premises network has the following configuration:

• 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.


ExamUser
Sign in

Suggested 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.

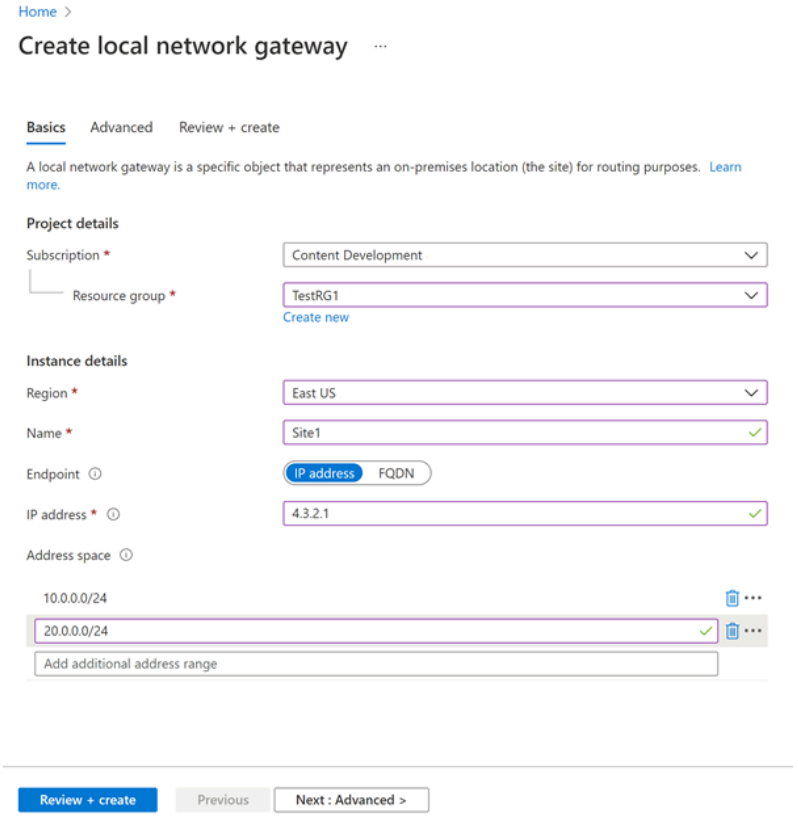
Step 1: From the Azure portal, in Search resources, services, and docs (G+/) type local network gateway. Locate local network gateway under Marketplace in the search results and select it. This opens the Create local network gateway page.

Step 2: On the Create local network gateway page, on the Basics tab, specifiy 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.



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 2 years, 7 months ago

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

upvoted 6 times

Ozarsif Most Recent 1 year, 3 months ago

as of july, 2025, there is no labs anymore

upvoted 3 times

nabeel79 1 year, 6 months ago

need to create a Local Network Gateway

upvoted 1 times

Lazylinux 2 years ago

Yep Given answer 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
-

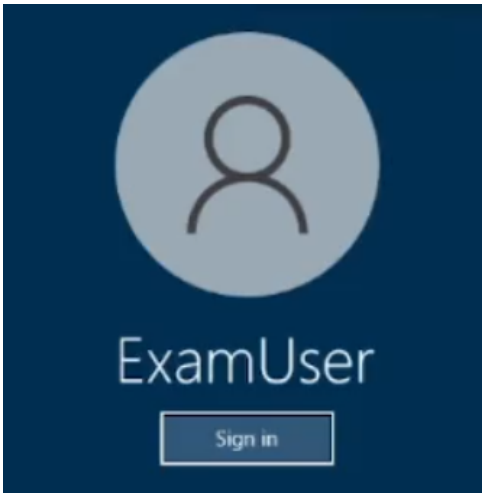
If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678
-

You need to ensure that 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.



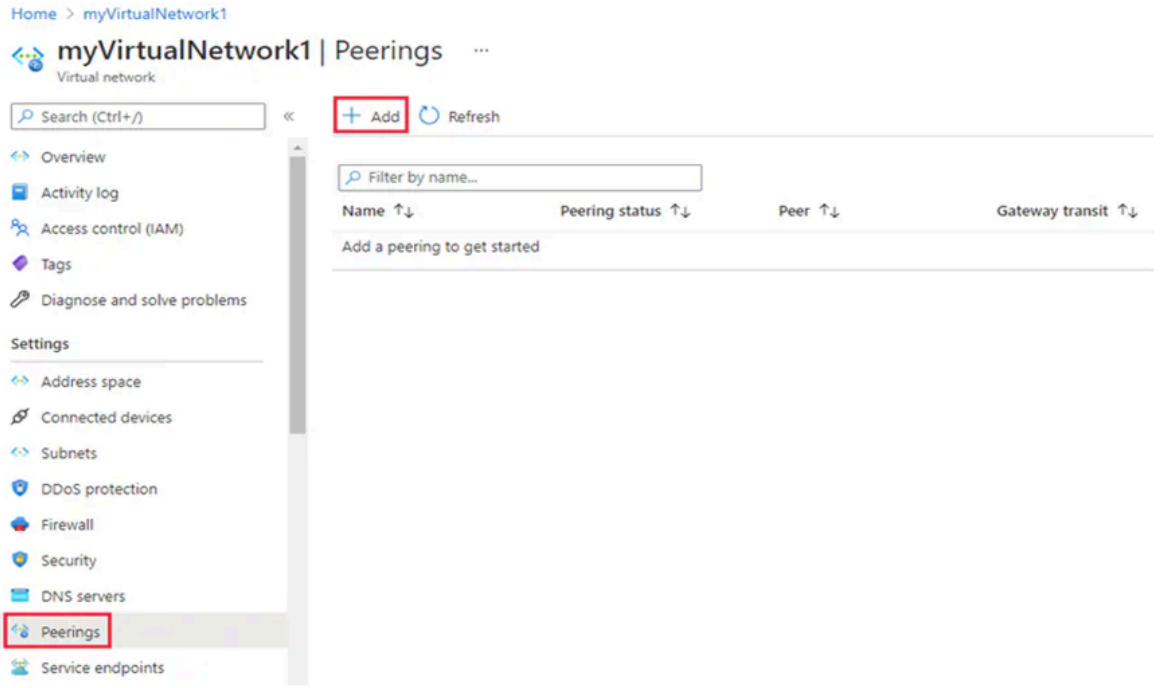
Suggested Answer:

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

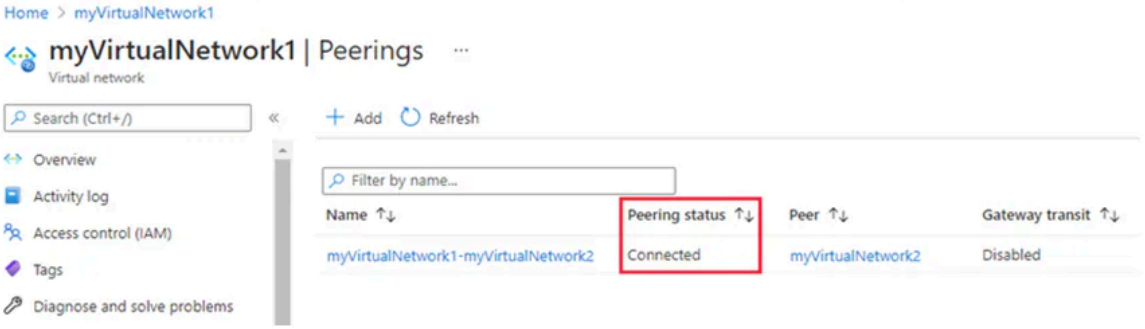
Step 1: In the search box at the top of the Azure portal, look for VNET2. When VNET2 appears in the search results, select it.

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

Ozarsif Most Recent 1 year, 3 months ago
as of july, 2025, there was no labs
upvoted 3 times

nabeel79 1 year, 6 months ago
peering the HubNet1 to VNet2 and 3
upvoted 1 times

DGUI 3 years, 4 months ago

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

upvoted 1 times

Lazylinux 3 years, 4 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 commentsFollowing 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-psdisagreed. VNET peering, no need to be configured for both VNETs, set it up on one VNET, it will peer with the other one.By default peerings are not transient.

upvoted 1 times

Lazylinux 3 years, 4 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 3 years, 4 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

Eddie_Sli 2 years, 3 months ago

disagreed. VNET peering, no need to be configured for both VNETs, set it up on one VNET, it will peer with the other one.

upvoted 1 times

grimrodd 2 years, 3 months ago

By default peerings are not transient.

upvoted 1 times

thor04 3 years, 5 months ago

Do we need to create the connection for VPN site-to-site ?No we dont, see my comments

upvoted 1 times

thor04 3 years, 5 months ago

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

upvoted 1 times

Lazylinux 3 years, 4 months ago

No we dont, see my comments

upvoted 1 times

Question #23 *Topic 1*

HOTSPOT
-

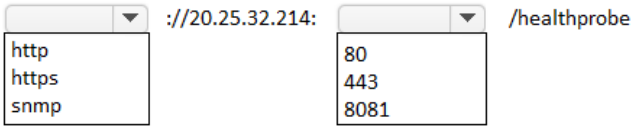
You have an Azure subscription that contains a virtual network gateway named VNetGwy1. VNetGwy1 has a public IP address of 20.25.32.214.

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.

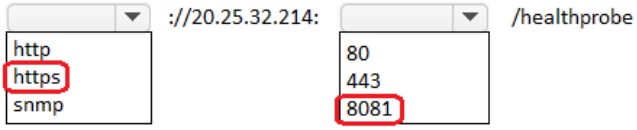
NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:

Answer Area



Jayr4 Most Recent 7 months, 2 weeks ago

The reason we use HTTP instead of HTTPS for the Azure VPN Gateway health probe is because of how Microsoft designed the probe endpoint:

The health probe is a lightweight diagnostic endpoint, not a user-facing service.

It's exposed on port 8081 and only responds to HTTP requests.

It doesn't support HTTPS because the probe isn't meant for secure data transfer — it simply returns a status code (like 200 OK) to confirm the gateway is alive.

Using HTTPS would imply certificate validation and encryption, which isn't necessary for this internal monitoring function.

upvoted 1 times

nabeel79 1 year, 6 months ago

https://publicaip:8081

upvoted 1 times

ckyap Highly Voted 2 years, 1 month 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 11 times

Question #24 *Topic 1*

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

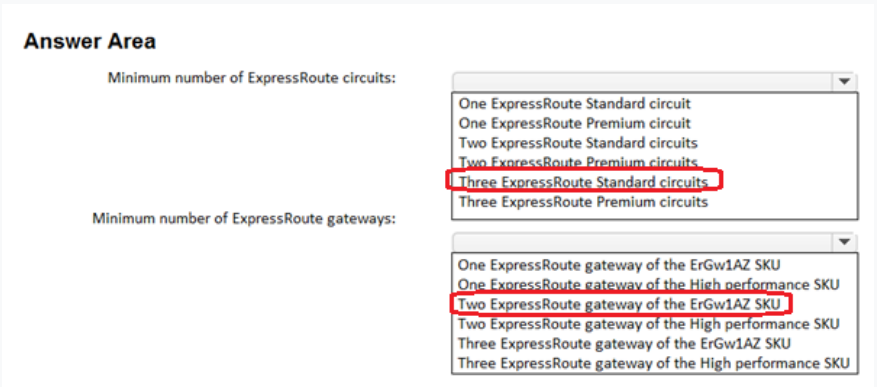
Minimum number of ExpressRoute circuits:

- 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

Suggested Answer:



bakamon Highly Voted 3 years, 5 months ago

Answer : --> One ExpressRoute Standard circuit --> One ExpressRoute gateway of the ErGw1AZ SKU

upvoted 41 times

thekhijir Most Recent 1 year, 11 months ago

For requirement of 1000 Mbps, ErGw1AZ is the most cost-effective choice while ensuring zone redundancy. 1ER Circuit required.

ErGw1AZ: This SKU supports up to 1 Gbps and is designed for availability zone deployments, providing high availability and resiliency.

ErGw2AZ: If you anticipate needing more bandwidth in the future, this SKU supports up to 2 Gbps and also offers zone redundancy.

ErGw3AZ: This SKU supports up to 3 Gbps and is suitable if you expect significant growth in your bandwidth needs.

upvoted 1 times

CiscoTerminator 3 years, 3 months ago

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

upvoted 3 times

CiscoTerminator 3 years, 3 months ago

You need zone-redundant gateways so 1 Standard circuit won't do.When deploying an ErGw1AZ, it is possible to define its zone availability as "Zone-Redundant"?Yes, it is. Look at https://learn.microsoft.com/en-us/azure/expressroute/expressroute-about-virtual-network-gateways?source=docs Zone-redundant gateways use specific new gateway SKUs for ExpressRoute gateway: - ErGw1AZ (1 Gbps) - ErGw2AZ (2 Gbps) - ErGw3AZ (10 Gbps) - ErGwScale (from 1 to 40 Gbps) Note: I was so much time thinking the xAZ number was the number AZs supported by the Er GW and not the capacityFor your current requirement of 1000 Mbps, ErGw1AZ is the most cost-effective choice while ensuring zone redundancy. ErGw1AZ: This SKU supports up to 1 Gbps and is designed for availability zone deployments, providing high availability and resiliency. ErGw2AZ: If you anticipate needing more bandwidth in the future, this SKU supports up to 2 Gbps and also offers zone redundancy. ErGw3AZ: This SKU supports up to 3 Gbps and is suitable if you expect significant growth in your bandwidth needs.

upvoted 3 times

thekhijir 2 years, 10 months ago

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

upvoted 2 times

chpsilva02 2 years, 3 months ago

Standard/ERGw1Az 1 Gbps 500 4000

High Performance/ERGw2Az 2 Gbps 500 9,500

Ultra Performance/ErGw3Az 10 Gbps 500 9,500

ErGwScale (per scale unit) 1 Gbps 500 4,000

upvoted 2 times

erreyesarroyo 2 years, 10 months ago

Guess one and one....

upvoted 1 times

Feliphus 2 years ago

Yes, it is. Look at https://learn.microsoft.com/en-us/azure/expressroute/expressroute-about-virtual-network-gateways?source=docs Zone-redundant gateways use specific new gateway SKUs for ExpressRoute gateway: - ErGw1AZ (1 Gbps) - ErGw2AZ (2 Gbps) - ErGw3AZ (10 Gbps) - ErGwScale (from 1 to 40 Gbps) Note: I was so much time thinking the xAZ number was the number AZs supported by the Er GW and not the capacityFor your current requirement of 1000 Mbps, ErGw1AZ is the most cost-effective choice while ensuring zone redundancy. ErGw1AZ: This SKU supports up to 1 Gbps and is designed for availability zone deployments, providing high availability and resiliency. ErGw2AZ: If you anticipate needing more bandwidth in the future, this SKU supports up to 2 Gbps and also offers zone redundancy. ErGw3AZ: This SKU supports up to 3 Gbps and is suitable if you expect significant growth in your bandwidth needs.

upvoted 2 times

Feliphus 2 years ago

Yes, it is. Look at https://learn.microsoft.com/en-us/azure/expressroute/expressroute-about-virtual-network-gateways?source=docs

Zone-redundant gateways use specific new gateway SKUs for ExpressRoute gateway: - ErGw1AZ (1 Gbps) - ErGw2AZ (2 Gbps) - ErGw3AZ (10 Gbps) - ErGwScale (from 1 to 40 Gbps) Note: I was so much time thinking the xAZ number was the number AZs supported by the Er GW and not the capacity

upvoted 2 times

MCCC454 2 years, 10 months ago

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

upvoted 16 times

Redrum702 2 years, 10 months 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 3 times

_Cris 3 years, 1 month ago

appears on exam, 19 Sept 2023

upvoted 5 times

mabalon 3 years, 2 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 3 years, 2 months ago

Appeared on Exam 26 Aug 2023

upvoted 4 times

charrua86 3 years, 3 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 30 times

bakamon Highly Voted 3 years, 5 months ago

Answer :

--> One ExpressRoute Standard circuit

--> One ExpressRoute gateway of the ErGw1AZ SKU

upvoted 41 times

henryhung 3 years, 7 months 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 3 years, 7 months 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 SKUPlease ignore this ChatGPT 3.5 answer.

upvoted 1 times

thekhijir 2 years, 10 months ago

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

upvoted 2 times

_fvt 3 years, 7 months 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.I tested in lab, deployed an ErGw1AZ in a Region (France Central) with 3Az an I well have 3 Instances of the Public IP and ER Gateway. So the Answer is: - one ErGw1AZ - one Circuit.This correct.Standard or Premium ER CCT?Standard. Premium is viable when it spans over several regions and that is not the case here

upvoted 1 times

_fvt 3 years, 7 months 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 3 years, 7 months ago

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

upvoted 20 times

_fvt 3 years, 7 months ago

I tested in lab, deployed an ErGw1AZ in a Region (France Central) with 3Az an I well have 3 Instances of the Public IP and ER Gateway. So the Answer is: - one ErGw1AZ - one Circuit.This correct.Standard or Premium ER CCT?Standard. Premium is viable when it spans over several regions and that is not the case here

upvoted 20 times

thekhijir 1 year, 11 months ago

For your current requirement of 1000 Mbps, ErGw1AZ is the most cost-effective choice while ensuring zone redundancy.

ErGw1AZ: This SKU supports up to 1 Gbps and is designed for availability zone deployments, providing high availability and resiliency.

ErGw2AZ: If you anticipate needing more bandwidth in the future, this SKU supports up to 2 Gbps and also offers zone redundancy.

ErGw3AZ: This SKU supports up to 3 Gbps and is suitable if you expect significant growth in your bandwidth needs.

upvoted 1 times

aklas 3 years, 6 months 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

jarz 3 years, 6 months ago

Standard or Premium ER CCT?

upvoted 2 times

jarz 3 years, 6 months ago

Standard or Premium ER CCT?Standard. Premium is viable when it spans over several regions and that is not the case here

upvoted 2 times

henryhung 3 years, 7 months 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 2 times

henryhung 3 years, 7 months ago

Please ignore this ChatGPT 3.5 answer.

upvoted 7 times

JohnnyChimpo 3 years, 6 months ago

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

upvoted 2 times

khanda 3 years, 7 months ago

This correct.

upvoted 1 times

Question #25 *Topic 1*

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

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?

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)

A. an internal load balancer

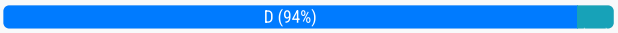
B. Azure Application Gateway

C. a NAT gateway

D. a public load balancer

Suggested Answer: *D*

Community vote distribution



kncappy Highly Voted 2 years, 2 months ago

Public load balancers allow internet traffic to your VMs by translating their private IP addresses to public IP addresses. You can configure your load balancer with a frontend IP address and load balancer rules to define how incoming traffic is distributed. Azure NAT gateways handle outbound traffic, and only packets arriving as a response to an outbound connection can pass through the NAT gateway. Application gateways operate at layer 7 OSI and can only manage web traffic. Since the question is asking for a solution to ensure Internet traffic can reach the VMs, public load balancer is the way to go. https://learn.microsoft.com/en-us/azure/load-balancer/components https://learn.microsoft.com/en-us/azure/nat-gateway/nat-overview

upvoted 14 times

AlfKay Most Recent 4 months, 2 weeks ago

A,C obviously ruled out here due to word internet, while C the nat gateway is being used only for outbound,not otherwise eg inbound.While B is not the answer due to App Gateway is layer 7 and hence it can only route traffic HTTP/S but not layer 4 tcp/udp.hence why D is the answer

upvoted 1 times

40a4d4c 7 months, 3 weeks ago

can be accessed from the internet (NAT Gateway= False)

upvoted 1 times

xRiot007 1 year, 7 months ago

Inbound to a common public IP requires a public Load Balancer. Outbound using a common public IP requires a NAT gateway. So the answer is D - a public load balancer. Example architecture: https://azure.microsoft.com/en-us/products/application-gateway

upvoted 3 times

northgaterebel 1 year, 9 months ago

B. Azure Application Gateway. "Route traffic to back-end server pools with URL path-based routing, and to MULTIPLE web applications using host header-based routing." https://azure.microsoft.com/en-us/products/application-gateway

upvoted 1 times

snehmaithil 1 year, 10 months ago

Public load balancer

upvoted 1 times

KeZhai 2 years, 4 months 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 2 years, 4 months ago

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

Lazylinux 2 years, 6 months ago

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 2 years, 7 months 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 2 years, 11 months ago

why not a nat gateway ?bad idea , just realized that nat gateway can only handle outbound traffic . so it can only be D

upvoted 2 times

Ben_88 2 years, 11 months ago

why not a nat gateway ?

upvoted 2 times

Ben_88 2 years, 11 months ago

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

upvoted 6 times

Oklama 2 years, 11 months ago

Given answer is correct

upvoted 4 times

jamess 2 years, 12 months ago

Why not Azure Application Gateway with different listeners?Because Application Gateway is a layer 7 load balancer, which means it works only with web traffic (HTTP, HTTPS)!Agree, see Notes in: https://learn.microsoft.com/en-us/azure/application-gateway/overview

upvoted 1 times

jamess 2 years, 12 months ago

Why not Azure Application Gateway with different listeners?

upvoted 1 times

GiorgioLDN Highly Voted 2 years, 11 months ago

Because Application Gateway is a layer 7 load balancer, which means it works only with web traffic (HTTP, HTTPS)!Agree, see Notes in: https://learn.microsoft.com/en-us/azure/application-gateway/overview

upvoted 12 times

GiorgioLDN 2 years, 11 months ago

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

upvoted 12 times

DCor2022 2 years, 8 months ago

Agree, see Notes in: https://learn.microsoft.com/en-us/azure/application-gateway/overview

upvoted 2 times

ubdubdoo 3 years 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 3 years ago

Given answer is correct

upvoted 4 times

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.

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):

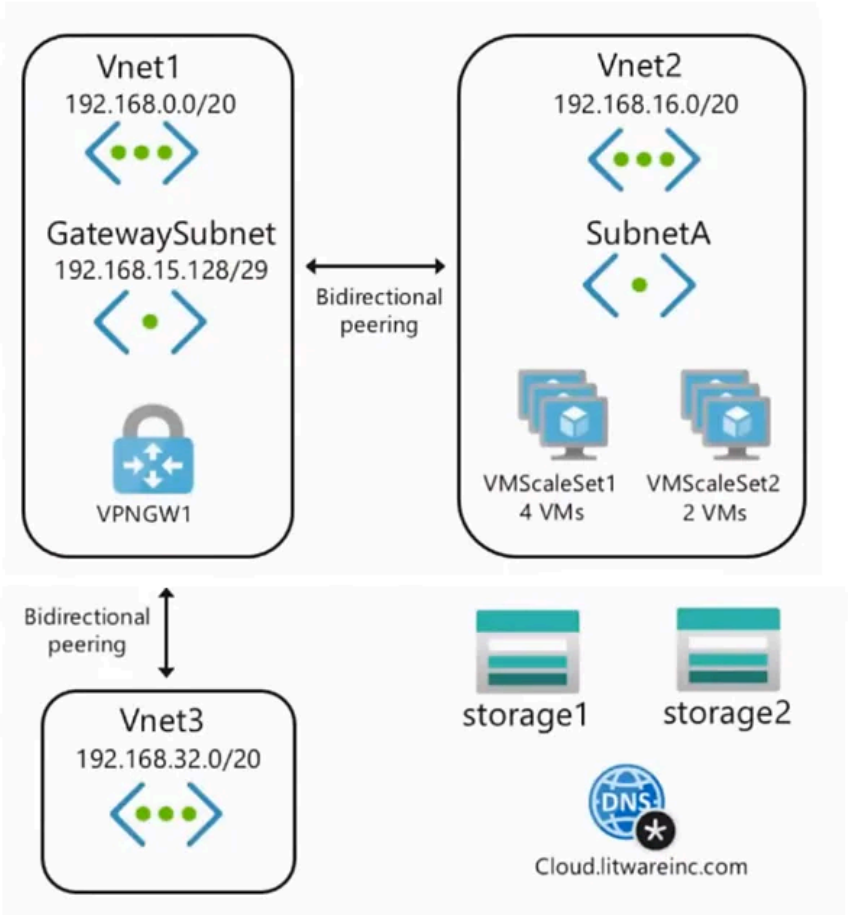
• The storage1 account must be accessible from all on-premises locations without exposing the public endpoint of storage1.
• The storage2 account must be accessible from Vnet2 and Vnet3 without exposing the public endpoint of storage2.

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.

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. 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.

Suggested Answer: *A, E*

Community vote distribution

BE (51%) AE (49%)

azure_dori Highly Voted 3 years, 3 months ago

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-vpngatewaysI fully agree with this explanation

upvoted 16 times

azure_dori Highly Voted 3 years, 3 months 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 16 times

Henk_2025 8 months, 3 weeks ago

I fully agree with this explanation

upvoted 1 times

c71da7e Most Recent 3 months, 3 weeks ago

E is needed for the requirements for the Boston on-premises datacenter. It's the only way to accomplish that. A is needed for the other requirement, which is traffic between vnet2 and vnet3 must be routed through vnet1.

upvoted 2 times

MANAGER24 6 months, 2 weeks ago

AE are correct.

upvoted 2 times

Flankengott_111 8 months, 4 weeks ago

Answer is A and E

upvoted 2 times

784680a 9 months ago

Vnet1 is the hub and Vnet2 & Vnet3 are spokes. The peerings allow traffic from Vnet2 & Vnet3 to the hub which is where the gateway is, hence E is correct for Vnet2 & Vnet3 Peerings are not transitive, so you must enable forwarding in the hub to allow traffic between vnet2 & Vnet3 to pass through it. Hence A is correct. All those saying B,E are incorrect.

upvoted 2 times

shimizu 9 months, 3 weeks ago

AE are correct. VNET 1 acts as hub and forwards traffic from VNET2 and VNET3 act as spokes

upvoted 4 times

MarkMac 11 months, 2 weeks ago

It would definitely help if the wording actually matched the configuration settings. These need to be updated.

upvoted 1 times

Enarsi_Guru 1 year, 7 months ago

Too much yapping and yet the question is so simple

upvoted 1 times

1322d93 1 year, 7 months ago

what do they mean 'remote virtual network'? On premises?

upvoted 2 times

Feliphus 2 years ago

INHO, I propose this correct answer, you need A-D-E-F to allow the connection between Vnet2 and Vnet3. F is a new option to complete the answer - A. On the peering from Vnet1, select Allow for "Traffic forwarded" from remote virtual network. - 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 - F. On the peering from Vnet1, select Use "this" virtual network's Gateway or Route Server

upvoted 1 times

620b351 2 years, 1 month ago

The correct answer is A & E.

upvoted 2 times

Eddie_Sli 2 years, 3 months ago

AE is the correct answer

upvoted 3 times

SKachroo 2 years, 11 months ago

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

upvoted 4 times

Lazylinux 3 years ago

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

bp_a_user 3 years, 1 month 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 3 times

hogehogehoge 3 years ago

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

upvoted 2 times

bp_a_user 3 years, 1 month 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...and here a concrete example: https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-peering-gateway-transitBE i mean

upvoted 3 times

bp_a_user 3 years, 1 month 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 3 years, 1 month ago

...and here a concrete example: https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-peering-gateway-transitBE i mean

upvoted 1 times

bp_a_user 3 years, 1 month ago

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

upvoted 2 times

bp_a_user 3 years, 1 month ago

BE i mean

upvoted 4 times

bp_a_user 3 years, 1 month ago

we have here a hub-spoke toplogy: why is no NAV/Firewall required?I mean NVA

upvoted 2 times

derp12352 3 years, 3 months 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

bp_a_user 3 years, 1 month ago

I mean NVA

upvoted 2 times

Feliphus 2 years ago

IMHO You would B, if you would have another Vnets in cascade, for example, named Vnet2b or Vnet3b peered to Vnet2 or Vnet3 respectively

upvoted 1 times

Question #27 *Topic 1*

HOTSPOT
-

You have an Azure subscription.

You plan to use Azure Virtual WAN.

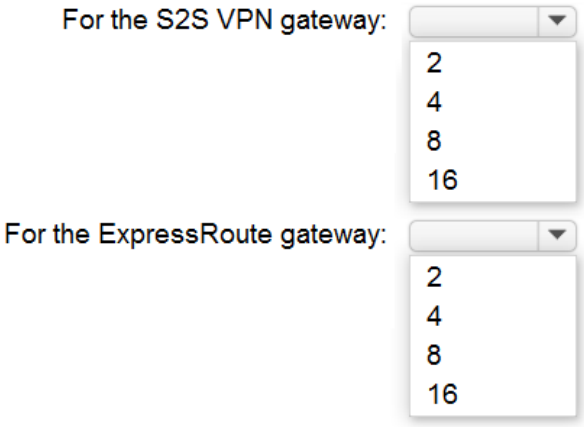
You need to deploy a virtual WAN hub that meets the following requirements:

- 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.

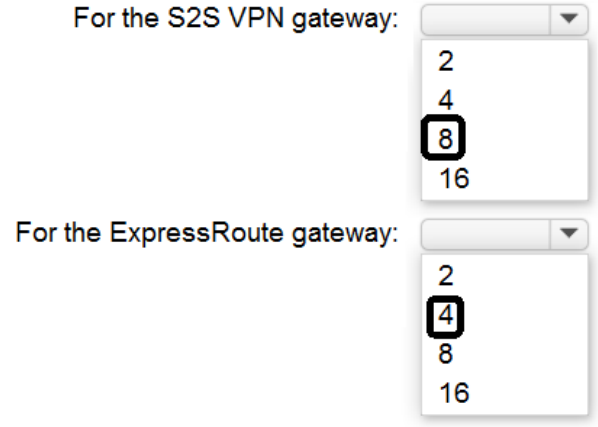
NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:

Answer Area



Acaer Highly Voted 2 years, 8 months 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-performancedid you have this in your examI 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 23 times

Acaer Highly Voted 2 years, 8 months 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 23 times

ohi Most Recent 1 year, 6 months ago

On a second note, we are using a virtual hub and each scale unit is x2. Meaning for 1 scale unit of vpn you have 500Mbps x2 this instance 0 and instance 1 allowing you to support 1Gbp per scale unit. So it should be 4S2S and 2 Exr

upvoted 1 times

sunsetblvdfightclub 2 years, 2 months ago

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://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-faq#what-are-virtual-wan-gateway-scale-units

upvoted 2 times

ConanBarb 2 years, 7 months 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 2 years, 8 months ago

did you have this in your exam

upvoted 1 times

Question #28 *Topic 1*

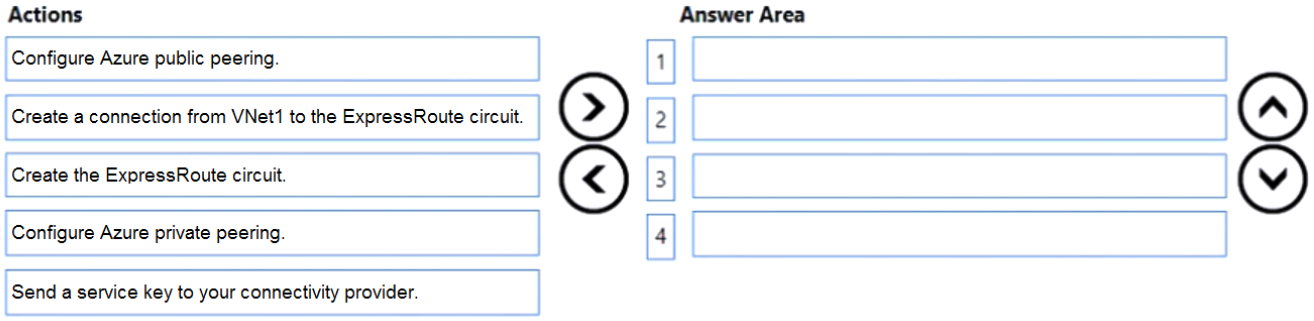
DRAG DROP
-

You have an on-premises network.

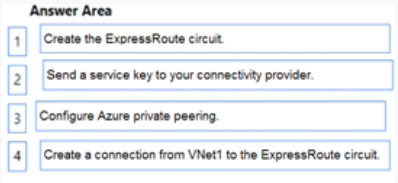
You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains an ExpressRoute gateway.

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.



Suggested Answer:



3fd1c62 Highly Voted 2 years, 3 months ago

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

upvoted 14 times

Lazylinux 2 years, 6 months ago

Given answer is correct as per

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

upvoted 1 times

Opiate 2 years, 6 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 2 years, 7 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 2 years, 8 months ago

appears on exam, 19 Sept 2023

upvoted 2 times

jmt97 2 years, 8 months 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 2 years, 8 months ago

should step3 switch with step 4? first you have to have the connection, then you can have peering

upvoted 2 times

Acaer Highly Voted 2 years, 8 months 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 16 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.

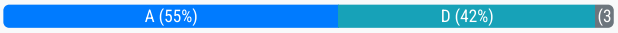
B. Add an additional VPN gateway to the Azure subscription.

C. Create an additional virtual hub.

D. Increase the number of gateway scale units.

Suggested Answer: *D*

Community vote distribution



linux2022 Most Recent 4 months ago

Selected Answer: D

The correct Answer is D.

It is specifically designed to increase throughput without creating new resources.

upvoted 1 times

af7b10d Highly Voted 2 years, 4 months ago

Selected Answer: A

D. Increase the number of gateway scale units: Is incorrect

Unsupported for Basic SKU: The Basic SKU does not support increasing gateway scale units to achieve higher throughput. This option is more relevant for Standard or higher SKUs.

Because of this I believe the answer is A, we need to upgrade the virtual WAN to Standard SKU first.

upvoted 7 times

af7b10d 2 years, 4 months ago

D. Increase the number of gateway scale units: Is incorrect Unsupported for Basic SKU: The Basic SKU does not support increasing gateway scale units to achieve higher throughput. This option is more relevant for Standard or higher SKUs. Because of this I believe the answer is A, we need to upgrade the virtual WAN to Standard SKU first.Basic is the vWan not GW...check descriptionAnd it's basic because it's not using more than S2S to connect

upvoted 7 times

AlfKay 4 months, 2 weeks ago

Selected Answer: A

D is not an option,basic cant increase the number of scale gateway units.

upvoted 1 times

CJL 2 years, 2 months ago

Basic is the vWan not GW...check description

upvoted 2 times

CJL 2 years, 2 months ago

Basic is the vWan not GW...check descriptionAnd it's basic because it's not using more than S2S to connect

upvoted 2 times

AlfKay 4 months, 3 weeks ago

Selected Answer: A

agreed with A. D is not the answer, since basic vwan gateway throughput cant be scale in basic. B Add Additional VPN is also not option since basic can only have one VPN or single S2S.

upvoted 1 times

bouth 5 months, 3 weeks ago

Selected Answer: A

Basic does not support upgrading scaling units

upvoted 1 times

MANAGER24 6 months, 2 weeks ago

Selected Answer: D

D. Increase the number of scale units

upvoted 1 times

neymarie 8 months, 1 week ago

Selected Answer: A

basic SKU can not change

upvoted 1 times

Henk_2025 8 months, 3 weeks ago

Selected Answer: A

A: correct answer

Basic Virtual WAN doesn't support adjusting gateway scale units to increase throughput. If you need higher aggregate throughput, upgrade to Standard Virtual WAN. For more information about gateway scale units, see About Virtual WAN gateway settings.

https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about

upvoted 2 times

Flankengott_111 8 months, 4 weeks ago

Selected Answer: A

only in Standard-SKU you can increase scale units

upvoted 1 times

784680a 9 months ago

Selected Answer: A

You cannot increase the scale units of the Azure Virtual WAN basic SKU, hence D incorrect and answer is A

upvoted 1 times

Rowdy_47 1 year ago

Selected Answer: A

You cannot increase the scale units of the Azure Virtual WAN basic SKU, therefore you must upgrade to standard

upvoted 2 times

Chezzer83 1 year, 4 months ago

Selected Answer: A

Im inclined to go with A for this as you cant increase the scale units on a Basic vWAN SKU.

upvoted 1 times

Kaumru 1 year, 7 months ago

Selected Answer: D

D is correct.

Basic or Standard Azure VWAN only determines the types of resources that can be created within a hub, including the type of gateways that can be created (site-to-site VPN, point-to site User VPN, and ExpressRoute).

Hence regardless if its basic or standard, the supported scale unit (throughput aggregate) is 20-GBPS.

https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-faq

upvoted 1 times

CallMeHerb 1 year, 8 months ago

Selected Answer: A

The answer is definitely A. Basic SKU maxes out at 1Gb/s

upvoted 1 times

a250fb0 1 year, 9 months ago

Selected Answer: A

A. Upgrade the virtual WAN to the Standard SKU.

Here's why:

Standard SKU: Upgrading to the Standard SKU increases the throughput capacity and provides additional features and capabilities compared to the Basic SKU.

Minimal Administrative Effort: This option requires less configuration and management compared to adding additional VPN gateways or creating additional virtual hubs

upvoted 1 times

GabiBT 1 year, 10 months ago

Selected Answer: U

La opción correcta sería actualizar la WAN virtual a la SKU estándar. Esto te permitirá aumentar el rendimiento de la puerta de enlace de red virtual más allá del límite de 1 Gbps que tiene la WAN virtual básica. La actualización a la SKU estándar es la solución que minimiza el esfuerzo administrativo y cumple con el requisito de aumentar el rendimiento a 3 Gbps. Ya que la WAN virtual básica no permite aumentar el número de unidades de escalado.

upvoted 1 times

Asheesh22 1 year, 11 months ago

Selected Answer: A

Increase the number of gateway scale units: Is incorrect

upvoted 1 times

Feliphus 2 years ago

And it's basic because it's not using more than S2S to connect

upvoted 1 times

UR 3 years, 1 month ago

Selected Answer: D

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

upvoted 2 times

Acaer Highly Voted 3 years, 2 months 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 11 times

Question #30 *Topic 1*

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)

Suggested Answer: *B*

Community vote distribution

B (100%)

singhindra Most Recent 11 months, 2 weeks ago

Selected Answer: B

Correct Answer: B

upvoted 2 times

xRiot007 1 year, 7 months ago

Selected Answer: B

B - an NVA

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

upvoted 1 times

thekhijir 2 years, 1 month ago

Selected Answer: B

B. A Network Virtual Appliance (NVA)

upvoted 1 times

Diamante22 2 years, 2 months ago

B parece correta

upvoted 1 times

trashbox 2 years, 6 months 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 Highly Voted 2 years, 8 months 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 6 times

HOTSPOT
-

You have the Azure resources shown in the following table.

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.

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

Answer Area

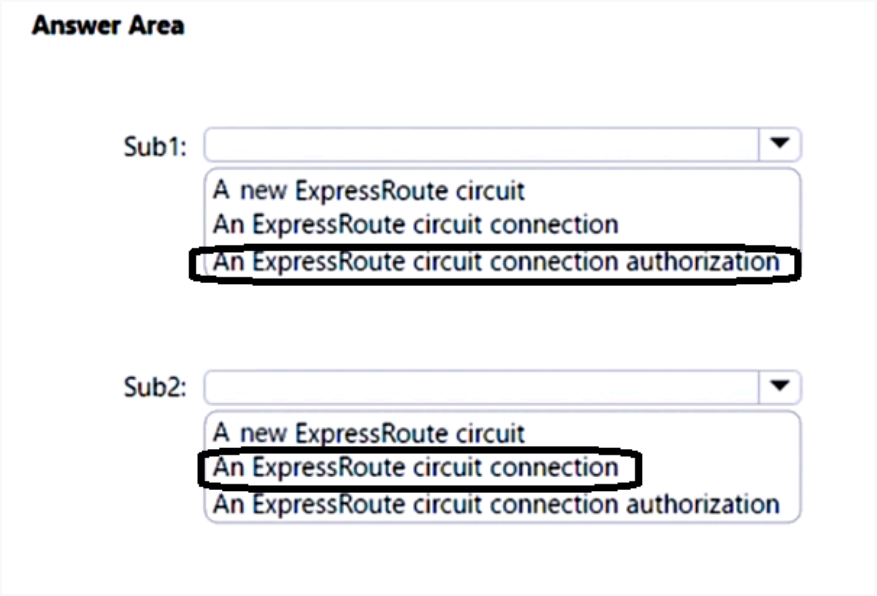
Sub1:

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

Suggested Answer:



VinceWho Most Recent 4 days ago

Answer is correct but the question doesn't make sense at all. Two VNET's can siply be connected using VNET peering.

upvoted 1 times

Eddie_Sli 2 years, 3 months ago

Correct

upvoted 1 times

Lazylinux 3 years 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

Verytutos Highly Voted 3 years, 2 months ago

Appeared on Exam 05 Sep 2023

upvoted 5 times

gabrielcor 3 years, 2 months ago

Correct

upvoted 2 times

Acaer Highly Voted 3 years, 2 months 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 13 times

Question #32 *Topic 1*

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

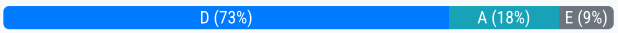
C. Ultra performance

D. ErGw3AZ

E. ErGw2AZ

Suggested Answer: *D*

Community vote distribution



karthickG Highly Voted 3 years ago

D is correct. ErGw3Az and Ultra Performance SKU supports FastPath. ErGw3Az is Zone-redundant, but not Ultra Performance SKU.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#gatewaysErGw3Az and Ultra Performance SKU and it supports FastPath. ErGw2Az is Zone-redundant and High Performance SKU but it doesn't support FastPathhttps://learn.microsoft.com/en-us/azure/expressroute/expressroute-about-virtual-network-gateways#gatewayfeaturesupport

upvoted 20 times

karthickG Highly Voted 3 years ago

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

upvoted 20 times

Neffo 2 years, 10 months 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 4 times

Feliphus 2 years ago

ErGw3Az and Ultra Performance SKU and it supports FastPath. ErGw2Az is Zone-redundant and High Performance SKU but it doesn't support FastPath

upvoted 2 times

Feliphus 2 years ago

ErGw3Az and Ultra Performance SKU and it supports FastPath. ErGw2Az is Zone-redundant and High Performance SKU but it doesn't support FastPathhttps://learn.microsoft.com/en-us/azure/expressroute/expressroute-about-virtual-network-gateways#gatewayfeaturesupport

upvoted 2 times

Feliphus 2 years ago

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

upvoted 1 times

AlfKay Most Recent 4 months, 3 weeks ago

D is correct. Fastpath can only supported by these gateways, Ultraperformance, ErGw3Az and ErGwScale minimum 10 scale unit. Ultraperformance is not an AZ(zone redundant) gateway,thus leaving us with obvious choice here, that is ErGw3Az. Refer to https://learn.microsoft.com/en-us/azure/expressroute/about-fastpath

upvoted 1 times

784680a 9 months ago

A. ErGw1AZ: This SKU is a basic version of the gateway and does not support high throughput or zone redundancy, so it wouldn't meet the requirement of minimizing downtime in case of failure. B. High performance: While this SKU offers high throughput, it does not support zone redundancy and is not designed for the specific need of minimizing downtime due to datacenter failure. C. Ultra performance: This SKU is more suitable for extremely high-throughput scenarios (such as massive data transfers), but it also does not support zone redundancy like ErGw2AZ does. D. ErGw3AZ: While this SKU does support ExpressRoute FastPath, it provides more capacity and higher throughput than required for most scenarios. It may not be necessary unless your organization requires extremely high performance, which increases costs unnecessarily.

upvoted 1 times

ohi 1 year, 6 months ago

https://learn.microsoft.com/en-us/azure/expressroute/about-fastpath

upvoted 1 times

Davidf 1 year, 8 months ago

Ultra performance does not allow zone redundant

upvoted 1 times

LearnICC 1 year, 10 months ago

For FastPath answers C and D are correct. As downtime should be minimized we need ErGw*AZ, so D is correct

upvoted 1 times

bobothewiseman 1 year, 11 months ago

FastPath not supported by ergw1az:

upvoted 1 times

bewavos102 1 year, 11 months ago

D is correct since A and E don't support FastPath.

upvoted 1 times

thekhijir 1 year, 11 months ago

ErGw1AZ: FastPath not supported. https://learn.microsoft.com/en-us/azure/expressroute/expressroute-about-virtual-network-gateways

upvoted 1 times

bobothewiseman 1 year, 12 months ago

D is correct. ErGw3Az and Ultra Performance SKU supports FastPath.

upvoted 1 times

manhattan 2 years ago

ErGw1AZ is not supported for Fastpath, so answer is D https://learn.microsoft.com/en-us/azure/expressroute/expressroute-about-virtual-network-gateways#gatewayfeaturesupport

upvoted 1 times

620b351 2 years, 2 months ago

Selected Answer: A

I guess the answer is A, this is because it shows to minimise cost as well. Both ErGw1AZ and ErGw3AZ are correct, but when it comes to cost, I guess A is the answer.

upvoted 2 times

620b351 2 years, 2 months ago

I guess the answer is A, this is because it shows to minimise cost as well. Both ErGw1AZ and ErGw3AZ are correct, but when it comes to cost, I guess A is the answer.Only the following SKUs support FastPath: - Ultra Performance - ErGw3AZ

upvoted 2 times

JManuel 1 year, 10 months ago

Only the following SKUs support FastPath: - Ultra Performance - ErGw3AZ

upvoted 1 times

MHy2k 2 years, 6 months ago

D is correct. Ultra Performance SKU/ErGw3Az supports FastPath

upvoted 3 times

HOTSPOT

-

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

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.

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

Answer Area

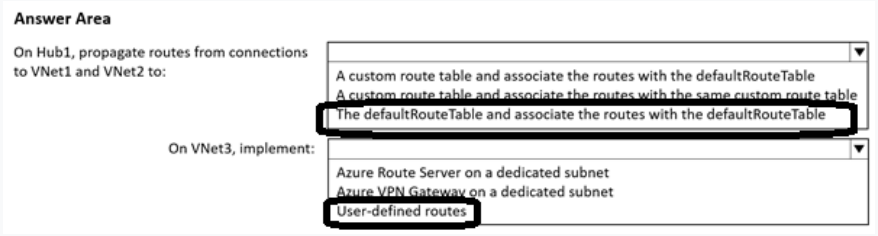
On Hub1, propagate routes from connections to VNet1 and VNet2 to:

- 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

Suggested Answer:



Anonymous Highly Voted 2 years, 4 months ago

Everything you need to know can be found in this section: https://learn.microsoft.com/en-us/azure/virtual-wan/scenario-bgp-peering-hub. An extract:

The following steps are required when BGP peering isn't used on the virtual hub:

Virtual hub configuration

On the Hub 1's defaultRouteTable, configure static route for VNET5 (subnet 10.2.1.0/24) pointing to VNET2 connection.

On Hub 1's virtual network connection for VNET2, configure static route for VNET5 pointing to VNET2 NVA IP (subnet 10.2.0.5).

On Hub 1, propagate routes from connections for VNET1 and VNET2 to the defaultRouteTable, and associate them to the defaultRouteTable.

Virtual network configuration

On VNET5, set up a user-defined route (UDR) to point to VNET2 NVA IP.

upvoted 5 times

ieboaix Highly Voted 2 years, 10 months ago

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

upvoted 9 times

MostafaNawar 2 years, 10 months 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 2 times

Question #34 *Topic 1*

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

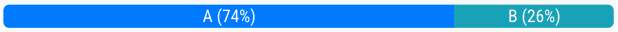
B. ErGw3AZ

C. ErGw2AZ

D. High performance

Suggested Answer: *B*

Community vote distribution



amitnahmias Highly Voted 2 years, 9 months ago

only ErGw3AZ and Ultra Performance are supported by FastPath. However, you cannot upgrade from Standard to ErGw3AZ. so answer is AYou can, but with a longer downtown as compared to Ultra Performance SKU.https://learn.microsoft.com/en-us/azure/expressroute/gateway-migration You can now migrate an ExpressRoute Standard gateway to ErGw3AZ using Azure's "Seamless Gateway Migration", which deploys a new gateway in the same subnet and transfers configurations automatically.

upvoted 23 times

amitnahmias Highly Voted 2 years, 9 months ago

Selected Answer: A

only ErGw3AZ and Ultra Performance are supported by FastPath. However, you cannot upgrade from Standard to ErGw3AZ.

so answer is A

upvoted 23 times

Bl4d3 1 year, 1 month ago

Selected Answer: A

ErGw2AZ and ErGw3AZ: These are newer, zone-redundant SKUs that do support FastPath, but they provide significantly higher throughput (20 Gbps and 40 Gbps, respectively) and come at a higher cost.

Ultra performance: This is the standard high-throughput SKU (10 Gbps) and is the minimum requirement to enable FastPath.

To minimize downtime, you would perform an in-place resize of your existing gateway. Since the request is simply to enable FastPath without other specified performance requirements, the most appropriate and cost-effective choice is the Ultra Performance SKU.

upvoted 1 times

ohi 1 year, 6 months ago

Selected Answer: B

Gateway Migration tool makes ErGw3Az the correct answer

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

upvoted 3 times

cryptonite 1 year, 8 months ago

Selected Answer: B

For FastPath, the options are between A and B, but I'll go with B.

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

From the comments, this link that everyone who chose A refers to was updated in Jan 2025 to show that:

If you want to upgrade your gateway to a higher-capacity gateway SKU, you can use the Seamless Gateway Migration tool in either the Azure portal or PowerShell. The following upgrades are supported:

Non-Az-enabled SKU on Basic IP to Non-Az-enabled SKU on Standard IP

Non-Az-enabled SKU on Basic IP to Az-enabled SKU on Standard IP

Non-Az-enabled SKU on Standard IP to Az-enabled SKU on Standard IP

Also, in this other link updated in March 2025, Microsoft recommends "migrating to an Az-enabled SKU for enhanced reliability and high availability" - which addresses the criteria to minimise downtime.

https://learn.microsoft.com/en-us/azure/expressroute/gateway-migration

upvoted 3 times

tc0369 1 year, 8 months ago

Selected Answer: B

B

FastPath ->narrow down the choices to A & B.

Minimize downtime -> indicate seamless gateway migration, which only support the below 3 cases. But from the question, can't tell if it's baisc or standard IP, so upgrade to az-enabled gw is more acceptable.

Non-Az-enabled SKU on Basic IP to Non-az enabled SKU on Standard IP.

Non-Az-enabled SKU on Basic IP to Az-enabled SKU on Standard IP.

Non-Az-enabled SKU on Standard IP to Az-enabled SKU on Standard IP.

upvoted 2 times

GabiBT 1 year, 10 months ago

Selected Answer: A

La opción correcta sería A. Ultra Performance. Sin embargo, si también necesitas alta disponibilidad y resiliencia, ErGw3AZ sería la mejor opción, ya que está habilitado para zonas de disponibilidad (AZ), proporcionando mayor redundancia.

upvoted 1 times

nk_exam 1 year, 11 months ago

Selected Answer: A

A is correct

upvoted 1 times

felipeaol 2 years, 3 months ago

Selected Answer: A

Standard to High Performance

Standard to Ultra Performance

High Performance to Ultra Performance

ErGw1Az to ErGw2Az

ErGw1Az to ErGw3Az

ErGw2Az to ErGw3Az

Default to Standard

upvoted 4 times

Eddie_Sli 2 years, 3 months ago

amitnahmias is correct, Answer: A

upvoted 1 times

ajinkyap 2 years, 4 months ago

Selected Answer: A

As mentioned by others, we cannot upgrade standard to AZ SKU. answer is A

upvoted 1 times

thekhijir 2 years, 7 months ago

Selected Answer: A

If you want to upgrade your gateway to a higher capacity gateway SKU, you can use the Resize-AzVirtualNetworkGateway PowerShell cmdlet or perform the upgrade directly in the ExpressRoute virtual network gateway configuration page in the Azure portal. The following upgrades are supported:

Standard to High Performance

Standard to Ultra Performance

High Performance to Ultra Performance

ErGw1Az to ErGw2Az

ErGw1Az to ErGw3Az

ErGw2Az to ErGw3Az

Default to Standard

upvoted 2 times

BigV00 2 years, 8 months ago

Selected Answer: A

As explained by an other user you can only transition from Standard to Ultra Performance

upvoted 1 times

2278345 Most Recent 4 months, 1 week ago

You can, but with a longer downtown as compared to Ultra Performance SKU.

upvoted 1 times

youngjosephm 2 years, 9 months ago

Selected Answer: B

Ultra Performance will support the FastPath but I think the criteria "Must minimize down time" implies you need to go with an AZ SKU and ErGw3AZ is the only one that support FastPath

upvoted 4 times

JManuel 1 year, 10 months ago

https://learn.microsoft.com/en-us/azure/expressroute/gateway-migration

You can now migrate an ExpressRoute Standard gateway to ErGw3AZ using Azure's "Seamless Gateway Migration", which deploys a new gateway in the same subnet and transfers configurations automatically.

upvoted 3 times

youngjosephm 2 years, 9 months ago

Selected Answer: B

Ultra Performance will support the FastPath but I think the criteria "Must minimize down time" implies you need to go with an AZ SKU and ErGw3AZ is the only one that support FastPath

upvoted 4 times

Jackdisuin 2 years, 9 months 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

thekhijir 2 years, 7 months ago

There is no option to go from standard to ErGw3AZ

If you want to upgrade your gateway to a higher capacity gateway SKU, you can use the Resize-AzVirtualNetworkGateway PowerShell cmdlet or perform the upgrade directly in the ExpressRoute virtual network gateway configuration page in the Azure portal. The following upgrades are supported:

Standard to High Performance

Standard to Ultra Performance

High Performance to Ultra Performance

ErGw1Az to ErGw2Az

ErGw1Az to ErGw3Az

ErGw2Az to ErGw3Az

Default to Standard

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

upvoted 2 times

Jackdisuin 2 years, 9 months 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-gatewaysCould be both To configure FastPath, the virtual network gateway must be either: Ultra Performance ErGw3AZ https://learn.microsoft.com/en-us/azure/expressroute/about-fastpathTo configure FastPath, the virtual network gateway must be either: Ultra Performance ErGw3AZ https://learn.microsoft.com/en-us/azure/expressroute/about-fastpath

upvoted 2 times

MCCC454 2 years, 9 months 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 2 times

MCCC454 2 years, 9 months 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-fastpathTo configure FastPath, the virtual network gateway must be either: Ultra Performance ErGw3AZ https://learn.microsoft.com/en-us/azure/expressroute/about-fastpath

upvoted 2 times

thekhijir 2 years, 7 months ago

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

Question #35 *Topic 1*

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

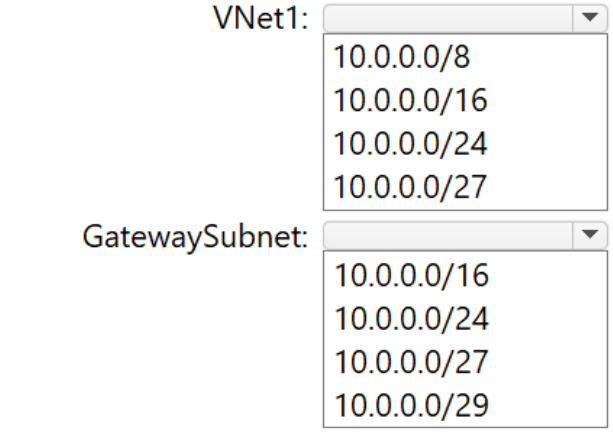
You need to recommend which subnet masks to assign to VNet1 and GatewaySubnet. The solution must meet the following requirements:

• 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.

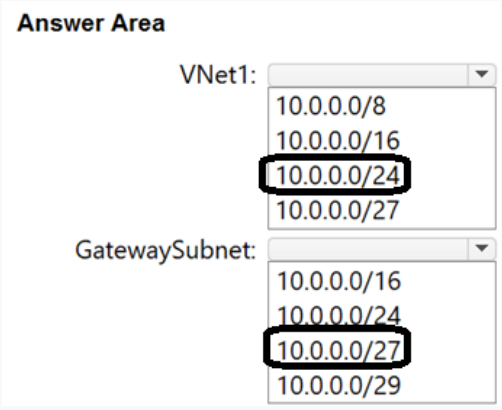
NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:

Answer Area



Jackdisuin Highly Voted 2 years, 9 months ago

Maximize the number of available IP addresses on VNet1 10.0.0.0/16 Minimize the number of available IP addresses on GatewaySubnet 10.0.0.0/27Está correto: VNet1 - Correto → 10.0.0.0/16 (VNET) GatewaySubnet - Correto → 10.0.0.0/27 (SUBNET) Incorreto - VNet1 10.0.0.0/8 → Because overlap with local address 10.1.0.0/16. 10.0.0.0/24 → Need to maximize the number of available IP addresses in VNet1. 10.0.0.0/27 → Need to maximize the number of available IP addresses in VNet1. Note: What may cause confusion is that the question refers to VNet (Address Space) and not SUBNet. Therefore, the VNet should be 10.0.0.0/16 where multiple subnets can be created, which includes the GatewaySubnet 10.0.0.0/27. The smallest gateway subnet recommended by MS is /27.

upvoted 28 times

Jackdisuin Highly Voted 2 years, 9 months 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 28 times

itmaster 2 years, 2 months ago

Maximize the number of available IP addresses on VNet1, so I don't see a problem with 10.0.0.0/24

upvoted 2 times

BradFelmey 2 years, 2 months ago

Although the question doesn't mention which gateway SKU is to be chosen, it DOES say that route-based policy is a requirement, and since the gateway Basic SKU does not support BGP, we can surmise that a non-Basic SKU must be chosen. Ref. this matrix for BGP support by gateway SKU:

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

If we accept this premise, then the documentation further states the *only* gateway SKU which supports a /29 is the Basic SKU, which we have determined cannot be chosen. All other gateway SKUs have a minimum requirement of /27. Reference this section:

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

Since 10.1/16 and 10.0/16 do not overlap, but 10.0/8 do, the correct selection for the maximum VNet is 10.0/16, and the given answer to the question is in error.

upvoted 5 times

uridex 2 years, 9 months ago

10.0.0.0/16 - largest that doesn't overlap with on-prem address 10.0.0.0/27 - the minimum for gateway subnet

upvoted 13 times

uridex 2 years, 9 months ago

10.0.0.0/16 - largest that doesn't overlap with on-prem address 10.0.0.0/27 - the minimum for gateway subnetYou can create a gateway subnet as small as /29, we recommend that you create a gateway subnet of /27 or larger https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-vpn-faq

upvoted 13 times

620b351 2 years, 2 months ago

it is obvious that the answer is 10.0.0.0/16. so that it will start from 10.0.0.0 to 10.0.255.255. This is the maximum amount. Why /29 is not the answer is explained very well by the others.

upvoted 3 times

Octocon 2 years, 8 months ago

"While it's possible to create a gateway subnet as small as /29 (applicable to the Basic SKU only), all other SKUs require a gateway subnet of size /27 or larger (/27, /26, /25 etc.). You might want to create a gateway subnet larger than /27 so that the subnet has enough IP addresses to accommodate possible future configurations."

https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings

As we are only creating a s2s wouldn't we would be minimizing the addresses used by using a /29 ?

The only thing is the sku isn't specified.

upvoted 3 times

fodocel235 2 years, 9 months ago

VNet1: 10.0.0.0/24 GatewaySubnet: 10.0.0.0/29, when you are making use of the Basic SKU. With the Basic SKU, you can setup a S2S VPN connection. 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. While it's possible to create a gateway subnet as small as /29 (applicable to the Basic SKU only), all other SKUs require a gateway subnet of size /27 or larger (/27, /26, /25 etc.). You might want to create a gateway subnet larger than /27 so that the subnet has enough IP addresses to accommodate possible future configurations. https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings Generation1 Basic, Max 10 S2S tunnels https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngatewaysSorry, VNet can be 10.0.0.0/16. So answer is then 10.0.0.0/16 and 10.0.0.0/29.You can create a gateway subnet as small as /29, we recommend that you create a gateway subnet of /27 or larger https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-vpn-faq

upvoted 4 times

fodocel235 2 years, 9 months ago

VNet1: 10.0.0.0/24 GatewaySubnet: 10.0.0.0/29, when you are making use of the Basic SKU. With the Basic SKU, you can setup a S2S VPN connection.

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. While it's possible to create a gateway subnet as small as /29 (applicable to the Basic SKU only), all other SKUs require a gateway subnet of size /27 or larger (/27, /26, /25 etc.). You might want to create a gateway subnet larger than /27 so that the subnet has enough IP addresses to accommodate possible future configurations. https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings

Generation1 Basic, Max 10 S2S tunnels https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways

upvoted 4 times

fodocel235 2 years, 9 months ago

Sorry, VNet can be 10.0.0.0/16. So answer is then 10.0.0.0/16 and 10.0.0.0/29.You can create a gateway subnet as small as /29, we recommend that you create a gateway subnet of /27 or larger https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-vpn-faq

upvoted 4 times

fodocel235 2 years, 9 months ago

Sorry, VNet can be 10.0.0.0/16. So answer is then 10.0.0.0/16 and 10.0.0.0/29.

upvoted 4 times

thekhijir 2 years, 7 months ago

You can create a gateway subnet as small as /29, we recommend that you create a gateway subnet of /27 or larger

https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-vpn-faq

upvoted 4 times

Leinad78 2 years, 9 months ago

Why not 10.0.0.0/29 for Gatewaysubnet?

upvoted 2 times

Leinad78 2 years, 9 months ago

Why not 10.0.0.0/29 for Gatewaysubnet?Mimimum for GatewaySubnet is /27You can create a gateway subnet as small as /29, we recommend that you create a gateway subnet of /27 or larger https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-vpn-faq

upvoted 2 times

HoangNam2711 2 years, 9 months ago

Mimimum for GatewaySubnet is /27

upvoted 1 times

poullb Most Recent 2 years, 1 month ago

Está correto:

VNet1 - Correto → 10.0.0.0/16 (VNET)

GatewaySubnet - Correto → 10.0.0.0/27 (SUBNET)

Incorreto - VNet1

10.0.0.0/8 → Because overlap with local address 10.1.0.0/16.

10.0.0.0/24 → Need to maximize the number of available IP addresses in VNet1.

10.0.0.0/27 → Need to maximize the number of available IP addresses in VNet1.

Note:

What may cause confusion is that the question refers to VNet (Address Space) and not SUBNet. Therefore, the VNet should be 10.0.0.0/16 where multiple subnets can be created, which includes the GatewaySubnet 10.0.0.0/27.

The smallest gateway subnet recommended by MS is /27.

upvoted 4 times

UncleBenzz 2 years, 9 months ago

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

upvoted 7 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.

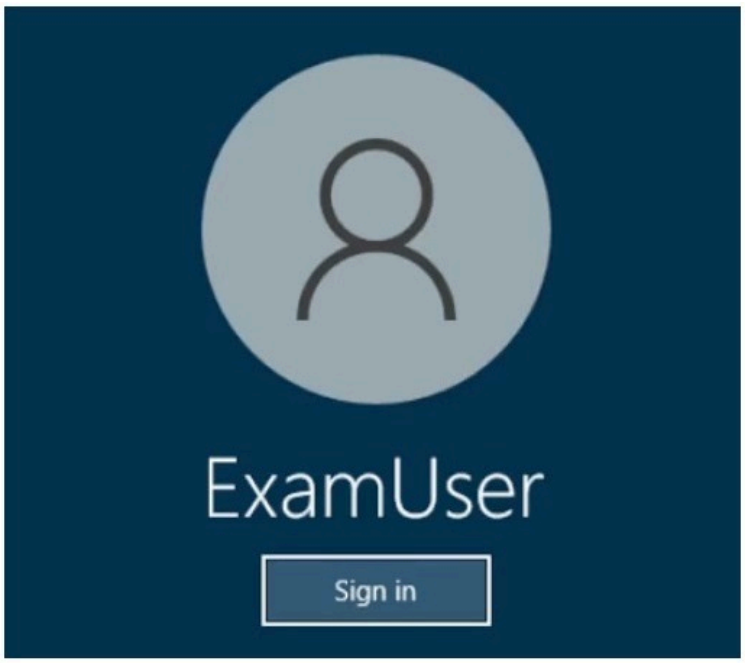
The following information is for technical support purposes only:

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.



Suggested 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 backpool 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.

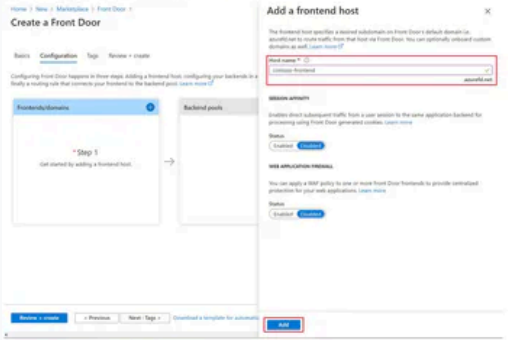
Step 2: On the Compare offerings page, select Explore other offerings. Then select Azure Front Door (classic). Then select Continue.

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.

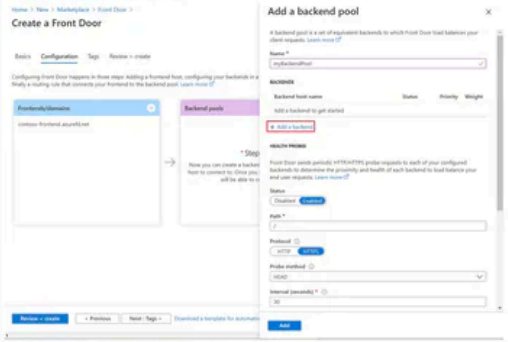
Step 5: For Host name, type a globally unique hostname. For example, contoso-frontend. Select Add



Next, set up a backend pool.

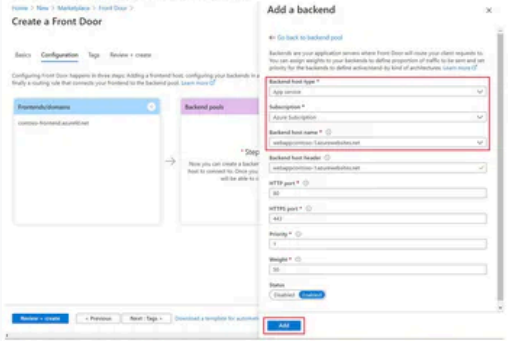
Step 1: Still in Create a Front Door, in Backend pools, select + to open the Add a backend pool page.

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



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.



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

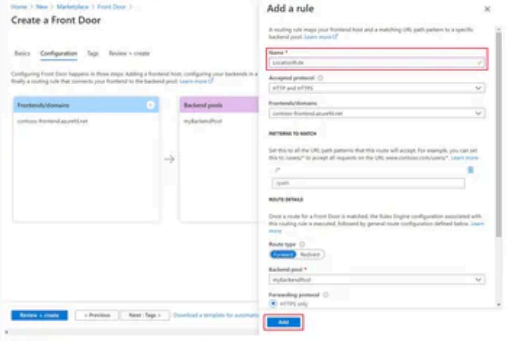
Step 5: Select Add on the Add a backend pool page to finish the configuration of the backend pool.

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.

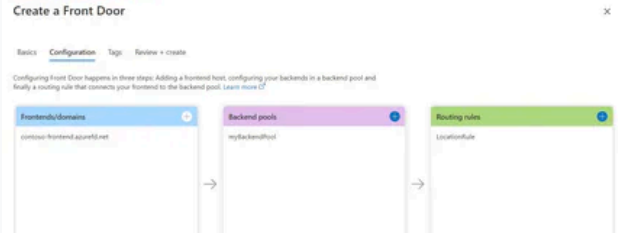
Step 1: Still in Create a Front Door, in Routing rules, select + to set up a routing rule.

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.





cerifyme85 Highly Voted 2 years, 8 months ago

This looks more like Traffic Manager to me.. using performance routing Plus it says DNS hostnames (Servers) and not applications (or urls) Plus Azure TMs are cheaper. https://learn.microsoft.com/en-us/azure/architecture/guide/technology-choices/load-balancing-overview#https-vs-non-https:~:text=DNS%2Dbased%20traffic%20load%20balancer%20thatI think we don't have enough information to be 100% sure, according to your link, if we tray to answer all the decision blocks: - Web application ? (HTTP/HTTPs) -> Unknown - Internet Facing application? -> Unknown - Global/Deployed in multiple regions? -> Yes - Do you require SSL offload or application-layer processing per request? -> Unknown - Hosting - PaaS, IaaS, AKS -> Yes - Do you require performance acceleration? - Unknown Azure Front Door is the unique option for Hosting - PaaS, IaaS, AKS And the extra information are the backend servers can be reach by unique FQDN and we want to sent the request to the backserver with lower latencythe key element should be HTTP/s (front door) or Non HTTP/s (traffic manager) because Front door and Traffic manager are both global services. but as you said we don't have enough info...

upvoted 15 times

cerifyme85 Highly Voted 2 years, 8 months ago

This looks more like Traffic Manager to me.. using performance routing Plus it says DNS hostnames (Servers) and not applications (or urls) Plus Azure TMs are cheaper. https://learn.microsoft.com/en-us/azure/architecture/guide/technology-choices/load-balancing-overview#https-vs-non-https:~:text=DNS%2Dbased%20traffic%20load%20balancer%20that

upvoted 15 times

Feliphus 2 years ago

I think we don't have enough information to be 100% sure, according to your link, if we tray to answer all the decision blocks: - Web application ? (HTTP/HTTPs) -> Unknown - Internet Facing application? -> Unknown - Global/Deployed in multiple regions? -> Yes - Do you require SSL offload or application-layer processing per request? -> Unknown - Hosting - PaaS, IaaS, AKS -> Yes - Do you require performance acceleration? - Unknown

Azure Front Door is the unique option for Hosting - PaaS, IaaS, AKS

And the extra information are the backend servers can be reach by unique FQDN and we want to sent the request to the backserver with lower latency

upvoted 2 times

Feliphus 2 years ago

I think we don't have enough information to be 100% sure, according to your link, if we tray to answer all the decision blocks: - Web application ? (HTTP/HTTPs) -> Unknown - Internet Facing application? -> Unknown - Global/Deployed in multiple regions? -> Yes - Do you require SSL offload or application-layer processing per request? -> Unknown - Hosting - PaaS, IaaS, AKS -> Yes - Do you require performance acceleration? - Unknown Azure Front Door is the unique option for Hosting - PaaS, IaaS, AKS And the extra information are the backend servers can be reach by unique FQDN and we want to sent the request to the backserver with lower latencythe key element should be HTTP/s (front door) or Non HTTP/s (traffic manager) because Front door and Traffic manager are both global services. but as you said we don't have enough info...

upvoted 2 times

manhattan 1 year, 10 months ago

the key element should be HTTP/s (front door) or Non HTTP/s (traffic manager) because Front door and Traffic manager are both global services. but as you said we don't have enough info...

upvoted 1 times

MarkMac Most Recent 11 months, 1 week ago

Agreed with others that this could be either, but with the lack of detail and mentioning minimizing cost, Traffic Manager makes the most sense.

upvoted 1 times

Ozarsif 1 year, 3 months ago

as of august, 2025, there is no labs anymore

upvoted 4 times

a250fb0 1 year, 9 months ago

To route users to the server with the lowest latency while minimizing costs, you should use Azure Traffic Manager

upvoted 2 times

Eddie_Sli 2 years, 3 months ago

do we have those labs in the real exam?Did you attend the exam and get any lab questions? Thanks

upvoted 3 times

Eddie_Sli 2 years, 3 months ago

do we have those labs in the real exam?

upvoted 3 times

Raghu_Muthu 2 years, 2 months ago

Did you attend the exam and get any lab questions? Thanks

upvoted 3 times

ajinkyap 2 years, 4 months ago

It should be TM and not FD

upvoted 1 times

zuzmo483 2 years, 5 months ago

Yeah, Front Door could be more costly considering all the features it has. I would go with a Performance type Traffic Manager profile, that support different geo locations based on the lowest latency, then add External Endpoints with FQDN.

upvoted 4 times

zpack 2 years, 7 months ago

I don't believe that Azure Front Door will be saving costs when compared to Traffic Manager

upvoted 1 times

balota9153 2 years, 9 months ago

The solution must minimize costs. the answer will be front door

upvoted 2 times

balota9153 2 years, 9 months ago

The solution must minimize costs. the answer will be front doorno its not, traffic manager is cheaper and does the job.

upvoted 2 times

maikel87 2 years, 5 months ago

no its not, traffic manager is cheaper and does the job.

upvoted 4 times

Question #37 *Topic 1*

HOTSPOT
-

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

You need to implement hybrid connectivity between an on-premises network and VNet1. The solution must meet the following requirements:

• All cross-premises network traffic must traverse an ExpressRoute circuit.
• All cross-premises network traffic must be encrypted by using a Site-to-Site (S2S) VPN.

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

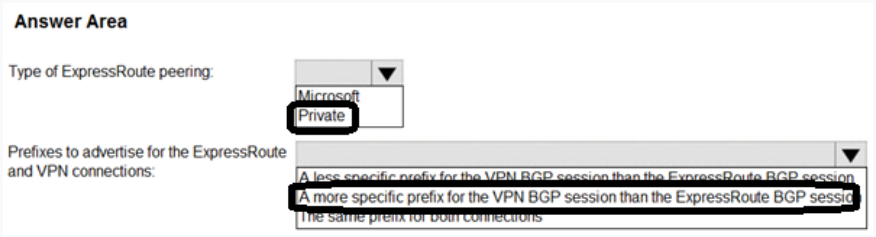
NOTE: Each correct selection is worth one point.

Answer Area

Type of ExpressRoute peering: [▼]
- Microsoft
- Private

Prefixes to advertise for the ExpressRoute and VPN connections: [▼]
- A less specific prefix for the VPN BGP session than the ExpressRoute BGP session
- A more specific prefix for the VPN BGP session than the ExpressRoute BGP session
- The same prefix for both connections

Suggested Answer:



Gaz_ Highly Voted 1 year, 9 months ago

Private and more specific for the VPN. ExpressRoute is private only, not encrypted.Agree. This should be a s2s vpn connection over ER private peering solution. Advertise more specific prefixes on the VPN BGP session for the VPN-connected network. https://learn.microsoft.com/en-us/azure/vpn-gateway/site-to-site-vpn-private-peering#routing

upvoted 5 times

Gaz_ Highly Voted 1 year, 9 months ago

Private and more specific for the VPN. ExpressRoute is private only, not encrypted.

upvoted 5 times

679956a Most Recent 8 months, 2 weeks ago

https://learn.microsoft.com/en-us/azure/vpn-gateway/site-to-site-vpn-private-peering#routing

it says

"If you advertise the same prefixes over both ExpressRoute and VPN connections, Azure will use the ExpressRoute path directly without VPN protection."

Thats wait is required.

So - private and same

upvoted 1 times

doshen 1 year, 9 months ago

Agree. This should be a s2s vpn connection over ER private peering solution. Advertise more specific prefixes on the VPN BGP session for the VPN-connected network.

https://learn.microsoft.com/en-us/azure/vpn-gateway/site-to-site-vpn-private-peering#routing

upvoted 2 times

mraznathani 1 year, 9 months ago

The same prefix for both connections.

upvoted 1 times

HOTSPOT

-

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

You have devices that run either Windows or macOS. The devices connect to VGW1 by using the OpenVPN protocol.

Which virtual networks can each device access? To answer, select the appropriate options in the answer area.

Name	Configuration
VNet1	Peers with VNet2 Has the Allow gateway transit setting enabled Contains an Azure VPN gateway named VGW1 that has BGP disabled
VNet2	Peers with VNet1 Has the Use remote gateway setting enabled
VNet3	Connected to VNet1 via a Site-to-Site (S2S) VPN connection

Answer Area

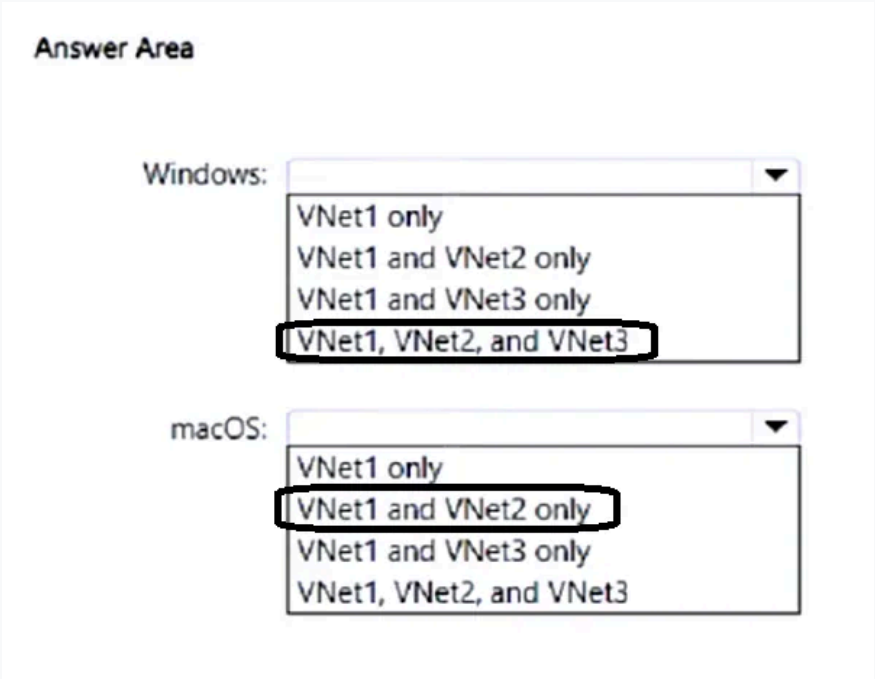
Windows:

- VNet1 only
- VNet1 and VNet2 only
- VNet1 and VNet3 only
- VNet1, VNet2, and VNet3

macOS:

- VNet1 only
- VNet1 and VNet2 only
- VNet1 and VNet3 only
- VNet1, VNet2, and VNet3

Suggested Answer:



NK203 Highly Voted 1 year, 11 months ago

Both answer is VNet1,VNet2,VNet3No. should be 1 and 2 only since OpenVPN doesn't support S2Syeah, it could be, it seems a weird question anyway, maybe it misses a protocol/settings info statement in the questions...

upvoted 16 times

NK203 Highly Voted 1 year, 11 months ago

Selected Answer: D

Both answer is VNet1,VNet2,VNet3

upvoted 16 times

GohanF2 Most Recent 1 month, 1 week ago

VNet1: Both devices connect directly to VGW1, which is in VNet1.

VNet2: VNet1 and VNet2 are peered correctly for gateway transit:

- VNet1: Allow gateway transit = Enabled

- VNet2: Use remote gateway = Enabled

Therefore, P2S clients can access the directly peered VNet2.

VNet3: This is the trap. VNet3 is connected to VNet1 through an S2S VPN, but BGP is disabled on VGW1. Microsoft states that for P2S clients to reach additional VNets through S2S connectivity, BGP must be used.

So, answer is Vnet1 and Vnet2 only for both scenarios.

upvoted 1 times

windowsmodulesinstallerworker 1 year, 5 months ago

just a reminder that this question is presupposing that the connection to vnet1 is route based

upvoted 1 times

nexus2020 3 months, 1 week ago

"Multiple VNets connected using an S2S VPN

In this example, the Point-to-Site VPN gateway connection is for VNet1. VNet1 is connected to VNet2 using a Site-to-Site VPN connection. VNet2 is connected to VNet3 using a Site-to-Site VPN connection. There is no direct peering or Site-to-Site VPN connection between VNet1 and VNet3. All Site-to-Site connections aren't running BGP for routing.

Clients using Windows, or another supported OS, can only access VNet1. To access additional VNets, BGP must be used."

upvoted 1 times

Ghelderz 1 year, 7 months ago

As per https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-point-to-site-routing#multis2s to access Virtual Networks that are connected to another Virtual Network using S2S VPN, BGP must be used.

Therefore, only VNET 1 and VNET 2 are accessible by both Windows AND Non-Windows clients.

upvoted 12 times

c9348c7 1 year, 5 months ago

BGP disabled so all protocol's P2S users cannot connect to VNET3 both of question , VNET 1 and VNET 2 only

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

upvoted 6 times

c9348c7 1 year, 5 months ago

BGP disabled so all protocol's P2S users cannot connect to VNET3 both of question , VNET 1 and VNET 2 only https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-point-to-site-routing"Multiple VNets connected using an S2S VPN In this example, the Point-to-Site VPN gateway connection is for VNet1. VNet1 is connected to VNet2 using a Site-to-Site VPN connection. VNet2 is connected to VNet3 using a Site-to-Site VPN connection. There is no direct peering or Site-to-Site VPN connection between VNet1 and VNet3. All Site-to-Site connections aren't running BGP for routing. Clients using Windows, or another supported OS, can only access VNet1. To access additional VNets, BGP must be used."

upvoted 7 times

098a37e 1 year, 8 months ago

VNet1 and VNet2 only, S2S does not support OpenVPN. Answer is B for both.

upvoted 6 times

Kaumru 1 year, 7 months ago

I agree with this

upvoted 3 times

098a37e 1 year, 8 months ago

VNet1 and VNet2 only, S2S does not support OpenVPN. Answer is B for both.I agree with this

upvoted 6 times

Lozo2020 1 year, 1 month ago

No. should be 1 and 2 only since OpenVPN doesn't support S2S

upvoted 1 times

manhattan 1 year, 10 months ago

yeah, it could be, it seems a weird question anyway, maybe it misses a protocol/settings info statement in the questions...

upvoted 2 times

Question #39 *Topic 1*

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

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 that Vnet1 must have?

Name	Type	Description
Vnet1	Virtual network	*None*
Subnet1	subnet	Hosted in Vnet1
Subnet2	subnet	Hosted in Vnet1
GatewaySubnet	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

A. 2

B. 3

C. 4

D. 5

Suggested Answer: *C*

Community vote distribution

B (55%) C (45%)

Jor466077 Highly Voted 1 year, 11 months ago

Cannot deploy in GatewaySugnet, and if deployed in Subnet1 or Subnet2 VM1 or VM2 will start accessing the Internet by using the NAT GW IP address. Thus, a new subnet (4th) is needed.Nat gateway will not process traffic of vm's that have their own public IPhttps://learn.microsoft.com/en-us/azure/nat-gateway/nat-overview A NAT gateway can't be deployed in a gateway subnet.But NAT gateway cannot be used with Basic SKU public IP addresses. "Basic 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 resources exist. Basic load balancer and basic public IP can be upgraded to standard to work with a NAT gateway." https://learn.microsoft.com/en-us/azure/nat-gateway/nat-overview Does it change the answer to 3 ?

upvoted 12 times

Jor466077 Highly Voted 1 year, 11 months ago

Selected Answer: C

Cannot deploy in GatewaySugnet, and if deployed in Subnet1 or Subnet2 VM1 or VM2 will start accessing the Internet by using the NAT GW IP address. Thus, a new subnet (4th) is needed.

upvoted 12 times

784680a Most Recent 8 months ago

Nat gateway will not process traffic of vm's that have their own public IP

upvoted 1 times

NK203 1 year, 11 months ago

https://learn.microsoft.com/en-us/azure/nat-gateway/nat-overview A NAT gateway can't be deployed in a gateway subnet.

upvoted 3 times

e6d6bf4 1 year, 11 months ago

But NAT gateway cannot be used with Basic SKU public IP addresses. "Basic 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 resources exist. Basic load balancer and basic public IP can be upgraded to standard to work with a NAT gateway." https://learn.microsoft.com/en-us/azure/nat-gateway/nat-overview Does it change the answer to 3 ?

upvoted 2 times

mohsim 1 year, 10 months ago

NAT gateway doesn't require a subnet itself, only require a subne to be associated with. So the answer is 3

upvoted 8 times

1f0f262 1 year, 2 months ago

ChatGPT said answer is C.

upvoted 1 times

fran199 1 year, 2 months ago

answer is correct

upvoted 1 times

Zorro2003 1 year, 2 months ago

Answer: C. 4 Why: A NAT gateway is associated at the subnet level. Any subnet associated with a NAT gateway uses the NAT gateway's public IPs for all outbound traffic—even VMs that have their own public IPs. Since VM1 (Subnet1) and VM2 (Subnet2) must keep using their own public IPs, the NAT gateway cannot be attached to either of those subnets. You need an additional subnet for the NAT gateway association. Together with the existing GatewaySubnet, VNet1 must have four subnets.

upvoted 2 times

Patel777 1 year, 4 months ago

No additional subnet is required for NAT gateway.

upvoted 3 times

beskar 1 year, 6 months ago

NAT Gateways are not configured in a way where they are placed into a subnet. So an additional subnet is not needed for the NAT Gateway.

upvoted 3 times

windowsmodulesinstallerworker 1 year, 6 months ago

NAT gateway is only associated with a subnet it does not need to be deployed to one like a VNG for example. This means that no additional subnets are required.I agree. Watching any youtube video of someone creating a NAT Gateway will show that it is not placed into a subnet. It is only associated with subnets that it will perform outbound NAT for.

upvoted 4 times

windowsmodulesinstallerworker 1 year, 6 months ago

Selected Answer: B

NAT gateway is only associated with a subnet it does not need to be deployed to one like a VNG for example. This means that no additional subnets are required.

upvoted 4 times

beskar 1 year, 6 months ago

I agree. Watching any youtube video of someone creating a NAT Gateway will show that it is not placed into a subnet. It is only associated with subnets that it will perform outbound NAT for.

upvoted 1 times

Diounaidou 1 year, 8 months ago

Cannont deploy Nat gatway in GatewaySubnet and in subnet where basic resource exists. therefore we need another subnet

upvoted 1 times

Gaz_ 1 year, 9 months ago

Selected Answer: C

NAT gateway can't be used with subnets where basic resources exist. A NAT gateway can't be deployed in a gateway subnet. https://learn.microsoft.com/en-us/azure/nat-gateway/nat-overview

upvoted 1 times

Gaz_ 1 year, 9 months ago

NAT gateway can't be used with subnets where basic resources exist. A NAT gateway can’t be deployed in a gateway subnet. https://learn.microsoft.com/en-us/azure/nat-gateway/nat-overviewYou can still deploy it to Subnet2, which has a VM with a Standard IP and not set it up to manage the IP of the VM. No need to create a new subnet in this scenario

upvoted 1 times

xRiot007 1 year, 7 months ago

You can still deploy it to Subnet2, which has a VM with a Standard IP and not set it up to manage the IP of the VM. No need to create a new subnet in this scenario

upvoted 1 times

bobothewiseman 1 year, 9 months ago

• Since VM1 and VM2 will retain their public IPs, NAT Gateway will not manage their outbound traffic. • No additional subnets are required to deploy the NAT Gateway. • Therefore, VNet1 only needs 3 subnets: Subnet1, Subnet2, and the existing GatewaySubnet.Spot on

upvoted 4 times

bobothewiseman 1 year, 9 months ago

Selected Answer: B

• Since VM1 and VM2 will retain their public IPs, NAT Gateway will not manage their outbound traffic. • No additional subnets are required to deploy the NAT Gateway. • Therefore, VNet1 only needs 3 subnets: Subnet1, Subnet2, and the existing GatewaySubnet.

upvoted 4 times

784680a 8 months ago

Spot on

upvoted 1 times

mohsim 1 year, 10 months ago

Actually since we can't associate the NAT Gateway to any of the other three subnets, then a fourth subnet is required.

upvoted 4 times

GabiBT 1 year, 10 months ago

Yo solo veo que necesitemos 3 subredes no entiendo porque necesitaríamos una 4a Subnet1 y Subnet2 son necesarias para hospedar VM1 y VM2, respectivamente, cada una con su propia dirección IP pública. GatewaySubnet es necesaria para implementar la puerta de enlace NAT. Cual seria la 4 ???I'm not so good with Spanish I'll try with English :-) You need a 4th subnet because if you connect NAT gateway with the subnet 1-2 the VMs will use the public IP of the NAT gateway. you can't attach a NAT gateway to a Gatewaysubnet too, so you need a fourth subnet. read this ""The NAT gateway takes precedence over a load balancer, regardless of the outbound rules. The gateway also takes precedence over public IP addresses that are assigned directly to VMs."" https://learn.microsoft.com/en-us/azure/architecture/networking/guide/well-architected-network-address-translation-gateway#operational-excellence

upvoted 3 times

GabiBT 1 year, 10 months ago

Selected Answer: B

Yo solo veo que necesitemos 3 subredes no entiendo porque necesitaríamos una 4a Subnet1 y Subnet2 son necesarias para hospedar VM1 y VM2, respectivamente, cada una con su propia dirección IP pública. GatewaySubnet es necesaria para implementar la puerta de enlace NAT. Cual seria la 4 ???

upvoted 3 times

manhattan 1 year, 10 months ago

I'm not so good with Spanish I'll try with English :-) You need a 4th subnet because if you connect NAT gateway with the subnet 1-2 the VMs will use the public IP of the NAT gateway. you can't attach a NAT gateway to a Gatewaysubnet too, so you need a fourth subnet. read this ""The NAT gateway takes precedence over a load balancer, regardless of the outbound rules. The gateway also takes precedence over public IP addresses that are assigned directly to VMs."" https://learn.microsoft.com/en-us/azure/architecture/networking/guide/well-architected-network-address-translation-gateway#operational-excellence

upvoted 1 times

Question #40 *Topic 1*

DRAG DROP

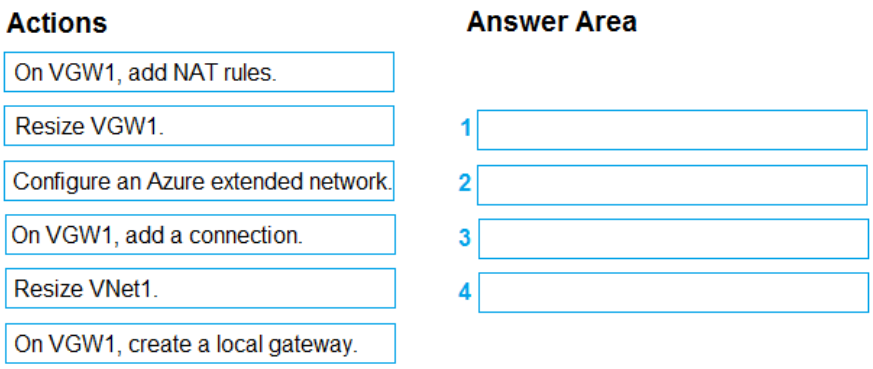
-

You have 100 on-premises servers with IP addresses from the 10.0.0.0/24 IP address space.

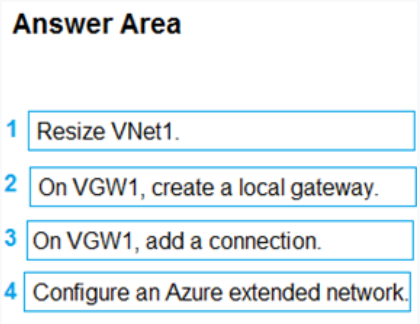
You have an Azure subscription that contains a virtual network named VNet1, an Azure VPN gateway named VGW1, and 100 virtual machines. VNet1 has an IP address space of 10.0.0.0/22. VGW1 uses the VpnGw1 SKU.

You need to ensure that the Azure virtual machines and the on-premises servers can communicate by using VGW1. The solution must minimize administrative effort.

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.



Suggested Answer:



Gambito11 1 year, 10 months ago

I think the given answer it's correct: -1 Resize Vnet1 (for example to 10.0.1.0/24 so we don't need NAT rules) -2 Create local gw -3 Add connection -4 Azure extended networkYou can't resize the VNET as it is in use.

upvoted 5 times

Gambito11 1 year, 10 months ago

I think the given answer it's correct: -1 Resize Vnet1 (for example to 10.0.1.0/24 so we don't need NAT rules) -2 Create local gw -3 Add connection -4 Azure extended network

upvoted 5 times

DC095 Most Recent 10 months, 2 weeks ago

The Nat Rules must be created before the connection as they are link/referenced when creating the connection

1. Resize VGW1

2. Create Local GW

3. Create Nat Rules

3 Add a connection (Link NAT Rules)

https://learn.microsoft.com/en-us/azure/vpn-gateway/nat-howto

upvoted 1 times

xRiot007 1 year, 7 months ago

1. Resize to VGW1 to VpnGw2 or higher

2. Create Local GW

3. Create NAT rules

4. Add a connection

Ref: https://learn.microsoft.com/en-us/azure/vpn-gateway/nat-howto#part-1-create-vnet-and-gateways

upvoted 4 times

Patel777 1 year, 4 months ago

Resize VGW1.

On VGW1, create a local gateway.

On VGW1, add NAT rules.

On VGW1, add a connection.

upvoted 3 times

Patel777 1 year, 4 months ago

Resize VGW1. On VGW1, create a local gateway. On VGW1, add NAT rules. On VGW1, add a connection.The Nat Rules must be created before the connection as they are link/referenced when creating the connection 1. Resize VGW1 2. Create Local GW 3. Create Nat Rules 3 Add a connection (Link NAT Rules) https://learn.microsoft.com/en-us/azure/vpn-gateway/nat-howto

upvoted 3 times

pattj2 1 year, 7 months ago

Your answer is almost correct, the order is

- Resize VGW1 because only VpnGW2 VpnGw5, VpnGw2AZ-5AZ allow for NAT rules

- On VGW1, create a local gateway

- On VGW1, add NAT rules

- On VGW1, add a connection

A note in https://learn.microsoft.com/en-us/azure/vpn-gateway/nat-howto#part-1-create-vnet-and-gateways clear states that the note should be the last step

upvoted 4 times

SilverFox22 1 year, 8 months ago

I think any answer that involves resizing the VNet is too much admin effort. Instead, its:

1. Resize VGW1 (Upgrade to at least VpnGw2 to enable NAT support.)

2. On VGW1, create a local gateway (Defines the on-premises network in Azure.)

3. On VGW1, add a connection (Establishes the Site-to-Site VPN tunnel.)

4. On VGW1, add NAT rules (Resolves overlapping IP conflicts.)

upvoted 2 times

Diounaidou 1 year, 8 months ago

- Azure VPN Gateway NAT supports the scenario to connect on-premises networks or branch offices to an Azure virtual network with overlapping IP addresses. - NAT is supported on the following SKUs: VpnGw2~5, VpnGw2AZ~5AZ. Correct answer should be: 1- Resize VGW1 2- On VGW1, Configure Local network gateway 3- on VGW1, add a connection 4- On VGW1, add Nat rules https://learn.microsoft.com/en-us/azure/vpn-gateway/nat-overview

upvoted 3 times

Diounaidou 1 year, 8 months ago

- Azure VPN Gateway NAT supports the scenario to connect on-premises networks or branch offices to an Azure virtual network with overlapping IP addresses. - NAT is supported on the following SKUs: VpnGw2~5, VpnGw2AZ~5AZ. Correct answer should be: 1- Resize VGW1 2- On VGW1, Configure Local network gateway 3- on VGW1, add a connection 4- On VGW1, add Nat rules https://learn.microsoft.com/en-us/azure/vpn-gateway/nat-overviewYour answer is almost correct, the order is - Resize VGW1 because only VpnGW2 VpnGw5, VpnGw2AZ-5AZ allow for NAT rules - On VGW1, create a local gateway - On VGW1, add NAT rules - On VGW1, add a connection A note in https://learn.microsoft.com/en-us/azure/vpn-gateway/nat-howto#part-1-create-vnet-and-gateways clear states that the note should be the last step

upvoted 3 times

NK203 1 year, 11 months ago

Selected Answer: D

1.On VGW1, create a local gateway. 2.On VGW1, add a connection. 3.On VGW1, add NAT rules. 4.Configure an Azure extended network

upvoted 3 times

NK203 1 year, 11 months ago

1.On VGW1, create a local gateway. 2.On VGW1, add a connection. 3.On VGW1, add NAT rules. 4.Configure an Azure extended networkI think the given answer it's correct: -1 Resize Vnet1 (for example to 10.0.1.0/24 so we don't need NAT rules) -2 Create local gw -3 Add connection -4 Azure extended networkthis is correct.1. On VGW1, create a local gateway 2. On VGW1, add NAT rules 3. On VGW1, add a connection 4. Configure an Azure extended network. Resize Vnet will affect existing resource, like VM and gateway subnet. NAT rules must be created before creating connections https://learn.microsoft.com/en-us/azure/vpn-gateway/nat-howtochange answer to 1. resize VGW 2. On VGW1 create LGW 3. add NAT 4. Add connection NAT supprot VPNGW2 - VPNGW5

upvoted 3 times

Ghelderz 1 year, 7 months ago

You can't resize the VNET as it is in use.

upvoted 4 times

D10SJoker Highly Voted 1 year, 11 months ago

I think the given answer it's correct: -1 Resize Vnet1 (for example to 10.0.1.0/24 so we don't need NAT rules) -2 Create local gw -3 Add connection -4 Azure extended networkthis is correct.

upvoted 10 times

D10SJoker Highly Voted 1 year, 11 months ago

I think the given answer it's correct: -1 Resize Vnet1 (for example to 10.0.1.0/24 so we don't need NAT rules) -2 Create local gw -3 Add connection -4 Azure extended network

upvoted 10 times

doshen 1 year, 9 months ago

1. On VGW1, create a local gateway 2. On VGW1, add NAT rules 3. On VGW1, add a connection 4. Configure an Azure extended network. Resize Vnet will affect existing resource, like VM and gateway subnet. NAT rules must be created before creating connections https://learn.microsoft.com/en-us/azure/vpn-gateway/nat-howto

upvoted 2 times

doshen 1 year, 9 months ago

1. On VGW1, create a local gateway 2. On VGW1, add NAT rules 3. On VGW1, add a connection 4. Configure an Azure extended network. Resize Vnet will affect existing resource, like VM and gateway subnet. NAT rules must be created before creating connections https://learn.microsoft.com/en-us/azure/vpn-gateway/nat-howtochange answer to 1. resize VGW 2. On VGW1 create LGW 3. add NAT 4. Add connection NAT supprot VPNGW2 - VPNGW5

upvoted 2 times

doshen 1 year, 9 months ago

change answer to

1. resize VGW

2. On VGW1 create LGW

3. add NAT

4. Add connection

NAT supprot VPNGW2 - VPNGW5

upvoted 2 times

Gambito11 1 year, 10 months ago

this is correct.

upvoted 1 times

DRAG DROP

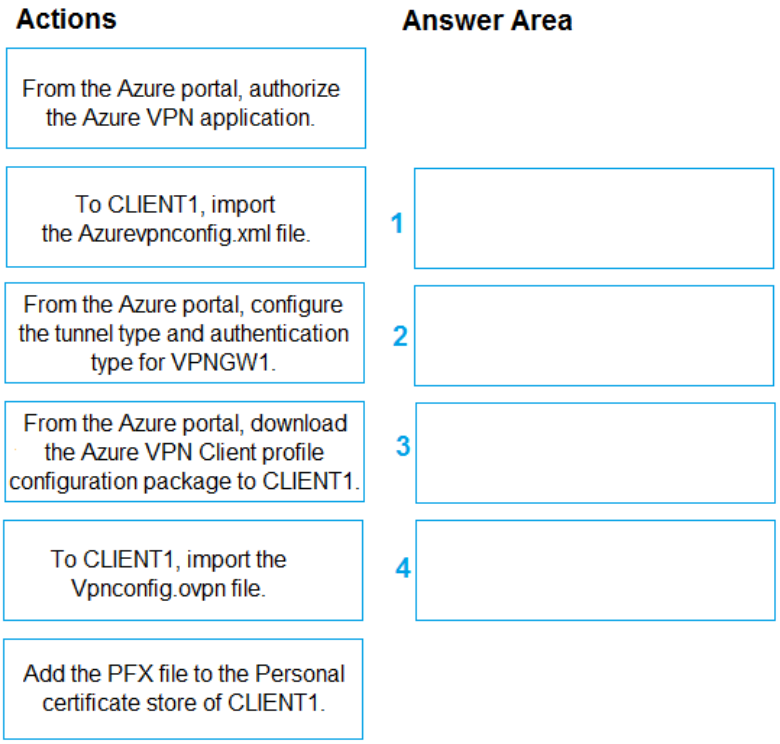
-

You have a computer named CLIENT1 that runs Windows 11 and has the Azure VPN Client installed.

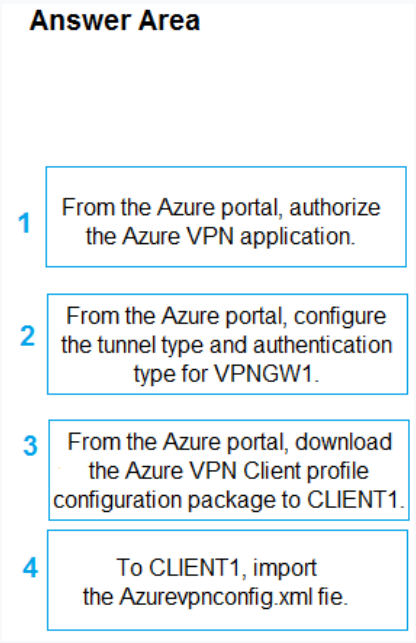
You have an Azure virtual network gateway named VPNGW1.

You need to ensure that you can connect CLIENT1 to VPNGW1. The solution must support Microsoft Entra authentication.

Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer are and arrange them in the correct order.



Suggested Answer:



VinceWho Most Recent 4 days ago

After digging in to it it seems that the Entra ID authentication requires OpenVPN protocol on the gateway side but it also requires the Azure VPN Client on the client side. You cannot use the public OpenVPN software because that cannot handle the interactive Entra ID modern authentication process. Since you are using Azure VPN Client, you need to import the xml file. The ovpn file can only be read by the OpenVPN software.

upvoted 1 times

sismer 1 year, 9 months ago

From the Azure portal, authorize the Azure VPN application. This step allows CLIENT1 to authenticate using Microsoft Entra ID. From the Azure portal, configure the tunnel type and authentication type for VPNGW1. This ensures VPNGW1 supports Microsoft Entra authentication. From the Azure portal, download the Azure VPN Client profile configuration package to CLIENT1. This package contains the necessary settings for CLIENT1 to connect. To CLIENT1, import the Vpnconfig.ovpn file. This step completes the configuration, allowing CLIENT1 to establish a VPN connection.import azurevpnconfig.xml. ovpn file is used for point-to-site configurationThis is a P2S connection. The Entra Authentication requirements dictate that the tunnel type be set to OpenVPNThe docs mention .xml file and not .ovpn https://learn.microsoft.com/en-us/azure/vpn-gateway/point-to-site-vpn-client-certificate-windows-azure-vpn-client#connection-requirementsThe Key is the Entra authentication requirement. OpenVPN is required for Entra Auth.

upvoted 3 times

sismer 1 year, 9 months ago

From the Azure portal, authorize the Azure VPN application.

This step allows CLIENT1 to authenticate using Microsoft Entra ID. From the Azure portal, configure the tunnel type and authentication type for VPNGW1.

This ensures VPNGW1 supports Microsoft Entra authentication. From the Azure portal, download the Azure VPN Client profile configuration package to CLIENT1.

This package contains the necessary settings for CLIENT1 to connect. To CLIENT1, import the Vpnconfig.ovpn file.

This step completes the configuration, allowing CLIENT1 to establish a VPN connection.

upvoted 3 times

GohanF2 1 month, 1 week ago

answers are correct. I believe that this appeared on exam 2026

upvoted 1 times

Patel777 1 year, 4 months ago

import azurevpnconfig.xml. ovpn file is used for point-to-site configurationThis is a P2S connection. The Entra Authentication requirements dictate that the tunnel type be set to OpenVPN

upvoted 1 times

Patel777 1 year, 4 months ago

import azurevpnconfig.xml. ovpn file is used for point-to-site configuration

upvoted 1 times

easy_t 10 months, 3 weeks ago

Keyword: "Azure VPN Client + Microsoft Entra"

Excluded:

- Add the PFX file to the Personal certificate store of CLIENT1 (No need personal certificate)

- To CLIENT1, import the Vpnconfig.ovpn file (Third-party OpenVPN)

Step:

1. From the Azure portal, configure the tunnel type and authentication type for VPNGW1.

2. From the Azure portal, authorize the Azure VPN application.

3. From the Azure portal, download the Azure VPN Client profile configuration package to CLIENT1.

4. To CLIENT1, import the Azurevpnconfig.xml file.

https://learn.microsoft.com/en-us/azure/vpn-gateway/point-to-site-vpn-client-certificate-windows-azurehttps://www.examtopics.com/discussions/microsoft/view/153014-exam-az-700-topic-1-question-41-discussion/#-vpn-client#connection-requirements

upvoted 2 times

rdj17629 Highly Voted 1 year, 9 months ago

The docs mention .xml file and not .ovpn https://learn.microsoft.com/en-us/azure/vpn-gateway/point-to-site-vpn-client-certificate-windows-azure-vpn-client#connection-requirements

upvoted 8 times

rdj17629 Highly Voted 1 year, 9 months ago

The docs mention .xml file and not .ovpn https://learn.microsoft.com/en-us/azure/vpn-gateway/point-to-site-vpn-client-certificate-windows-azure-vpn-client#connection-requirementsThe Key is the Entra authentication requirement. OpenVPN is required for Entra Auth.

upvoted 8 times

DC095 11 months, 2 weeks ago

This is a P2S connection. The Entra Authentication requirements dictate that the tunnel type be set to OpenVPN

upvoted 1 times

DC095 11 months, 2 weeks ago

The Key is the Entra authentication requirement. OpenVPN is required for Entra Auth.

upvoted 1 times

Question #42 *Topic 1*

HOTSPOT
-

You have an on-premises server named Server1 that runs Windows Server and has the DNS Server role installed.

You have an Azure subscription that contains two virtual networks named VNet1 and VNet2. VNet1 contains an Azure Firewall instance named FW1. VNet1 peers with VNet2.

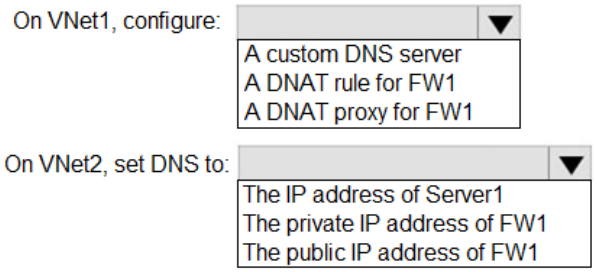
The on-premises network is connected to VNet1 by using ExpressRoute. The on-premises network is inaccessible from VNet2.

You need to ensure that virtual machines connected to VNet2 use Server1 to perform name resolution. The solution must minimize administrative effort.

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

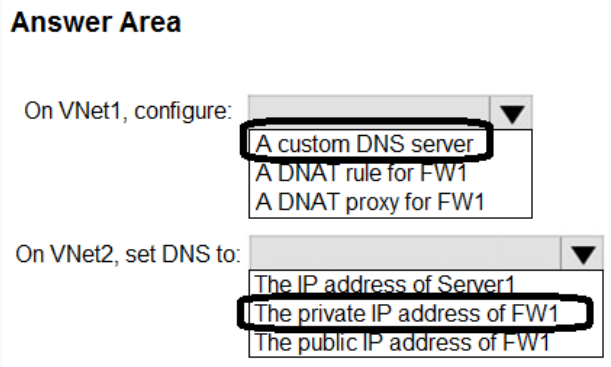
NOTE: Each correct answer is worth one point.

Answer Area



Suggested Answer:

Answer Area



NK203 Highly Voted 1 year, 11 months ago

Selected Answer: D

a custom dns server & pirvate IP

upvoted 10 times

Zorro2003 1 year, 1 month ago

On VNet1: enable DNS Proxy for FW1

On VNet2: set DNS to the private IP address of FW1

 This way, VMs in VNet2 send DNS queries to FW1, and FW1 forwards them to Server1 (on-premises).

Minimal effort, no extra DNAT rules needed.

upvoted 3 times

lakinduchandula 1 year, 10 months ago

in the question also saying that "VNet2 use Server1 to perform name resolution", couldn't we use the fw dnat rule to pass dns queries to ip address of server1. then we can set the private addr of fw1 as the vnet2 vm dns.

could you please comment on this?

upvoted 2 times

Zorro2003 1 year, 2 months ago

Final Answer:

On VNet1, configure: A DNS proxy for FW1

On VNet2, set DNS to: The private IP address of FW1

Why:

VNet2 cannot reach the on-prem network directly, so its VMs can't query Server1 themselves. Enabling DNS proxy on Azure Firewall (FW1) makes the firewall listen on port 53 and forward DNS queries to an upstream server—here, Server1 over ExpressRoute. Pointing VNet2's DNS to FW1's private IP sends queries across the VNet peering to FW1, which resolves them through Server1 and returns the answers.

This minimizes admin effort and avoids DNAT (public inbound only) or configuring VNet1's custom DNS (which wouldn't make FW1 a DNS listener).

upvoted 1 times

manhattan 1 year, 10 months ago

I believe that DNAT proxy is an typo, to me "DNAT proxy" doesn't make sense. I think that the answer would rather be "DNS proxy" You can configure Azure Firewall to act as a DNS proxy. A DNS proxy is an intermediary for DNS requests from client virtual machines to a DNS server https://learn.microsoft.com/en-us/azure/firewall/dns-details

upvoted 4 times

bobothewiseman 1 year, 10 months ago

I think the amswer is DNAT rule for FW1 and the Private IP adress of FW1. • Setting a custom DNS server on VNet1 would require all resources within VNet1 to use that DNS server (Server1 in this case).

upvoted 1 times

bobothewiseman 1 year, 10 months ago

I think the amswer is DNAT rule for FW1 and the Private IP adress of FW1. • Setting a custom DNS server on VNet1 would require all resources within VNet1 to use that DNS server (Server1 in this case).I was wrong! Should be custom DNS server and the Private IP address of FW1 DNAT is uses for public-facing inbound traffic

upvoted 1 times

DC095 10 months, 2 weeks ago

VNET 2 cannot communicate with the on-prem network. "DNAT Proxy" is a typo. It is supposed to be DNS Proxy, so you would setup the DNS Proxy on the Azure Firewall to point to Server 1 and then configure VNET 2 to use the private IP of the Firewall as its DNS server

upvoted 1 times

windowsmodulesinstallerworker 1 year, 6 months ago

dnat proxy = DNS PROXY its a mistake in the question

upvoted 1 times

PentalT2 1 year, 7 months ago

"When you use Azure Firewall as a DNS proxy, you can configure your clients to point to the private IP address of the firewall, and configure the firewall to forward requests to a DNS server, such as an on-premises server reachable via ExpressRoute."

A

upvoted 3 times

Vhailor 1 year, 3 months ago

why second question is not ip address of server1? this server is the dnsVNET 2 cannot communicate with the on-prem network. "DNAT Proxy" is a typo. It is supposed to be DNS Proxy, so you would setup the DNS Proxy on the Azure Firewall to point to Server 1 and then configure VNET 2 to use the private IP of the Firewall as its DNS server

upvoted 1 times

Vhailor 1 year, 3 months ago

why second question is not ip address of server1? this server is the dns

upvoted 1 times

doshen 1 year, 9 months ago

DNAT support translate FW private IP to private IP.

"Each rule in the NAT rule collection can then be used to translate your firewall public or private IP address and port to a private IP address and port."

https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-dnat

upvoted 1 times

a250fb0 1 year, 9 months ago

On VNet1:

Set custom DNS server to the IP address of Server1,

On VNet2:

Set custom DNS server to the private IP address of FW1

upvoted 1 times

bobothewiseman 1 year, 9 months ago

DNAT for FW1 a Private IP adress of FW1. • Setting a custom DNS server on VNet1 would require all resources within VNet1 to use that DNS server (Server1 in this case).I was wrong! Should be custom DNS server and the Private IP address of FW1 DNAT is uses for public-facing inbound trafficDNAT support translate FW private IP to private IP. "Each rule in the NAT rule collection can then be used to translate your firewall public or private IP address and port to a private IP address and port." https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-dnat

upvoted 2 times

bobothewiseman 1 year, 9 months ago

DNAT for FW1 a Private IP adress of FW1.

• Setting a custom DNS server on VNet1 would require all resources within VNet1 to use that DNS server (Server1 in this case).

upvoted 2 times

bobothewiseman 1 year, 9 months ago

I was wrong! Should be custom DNS server and the Private IP address of FW1 DNAT is uses for public-facing inbound trafficDNAT support translate FW private IP to private IP. "Each rule in the NAT rule collection can then be used to translate your firewall public or private IP address and port to a private IP address and port." https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-dnat

upvoted 3 times

Henk_2025 Most Recent 8 months, 2 weeks ago

correct

upvoted 1 times

nhr2 1 year, 10 months ago

Configure on Azure Firewall (FW1): Create a DNS proxy. Azure Firewall DNS proxy allows you to forward DNS requests to the desired DNS server (Server1, in this case). This ensures that all DNS traffic from VNet2 can reach Server1 through FW1. Configure on VNet2: Configure virtual network settings to use FW1 as the DNS server. You configure VNet2 to use FW1's private IP address as the DNS server. This directs all DNS queries from VNet2 virtual machines to Azure Firewall, which then forwards the queries to Server1.question did not mention the Firewall DNS Proxy being enabled or forwarding to Server1, so the correct answer is: On VNet1: A custom DNS server On VNet2: The IP address of Server1correct

upvoted 2 times

nhr2 1 year, 10 months ago

Configure on Azure Firewall (FW1): Create a DNS proxy.

Azure Firewall DNS proxy allows you to forward DNS requests to the desired DNS server (Server1, in this case). This ensures that all DNS traffic from VNet2 can reach Server1 through FW1. Configure on VNet2: Configure virtual network settings to use FW1 as the DNS server.

You configure VNet2 to use FW1's private IP address as the DNS server. This directs all DNS queries from VNet2 virtual machines to Azure Firewall, which then forwards the queries to Server1.

upvoted 2 times

Patel777 1 year, 4 months ago

question did not mention the Firewall DNS Proxy being enabled or forwarding to Server1, so the correct answer is: On VNet1: A custom DNS server On VNet2: The IP address of Server1correct

upvoted 2 times

Patel777 1 year, 4 months ago

question did not mention the Firewall DNS Proxy being enabled or forwarding to Server1, so the correct answer is: On VNet1: A custom DNS server On VNet2: The IP address of Server1

upvoted 2 times

NK203 Highly Voted 1 year, 11 months ago

Selected Answer: D

a custom dns server & pirvate IP

upvoted 10 times

lakinduchandula 1 year, 10 months ago

in the question also saying that "VNet2 use Server1 to perform name resolution", couldn't we use the fw dnat rule to pass dns queries to ip address of server1.

then we can set the private addr of fw1 as the vnet2 vm dns.

could you please comment on this?

upvoted 2 times

manhattan 1 year, 10 months ago

I believe that DNAT proxy is an typo, to me "DNAT proxy" doesn't make sense.

I think that the answer would rather be "DNS proxy"

You can configure Azure Firewall to act as a DNS proxy. A DNS proxy is an intermediary for DNS requests from client virtual machines to a DNS server

https://learn.microsoft.com/en-us/azure/firewall/dns-details

upvoted 4 times

bobothewiseman 1 year, 9 months ago

I was wrong! Should be custom DNS server and the Private IP address of FW1 DNAT is uses for public-facing inbound traffic

upvoted 1 times

Question #43 *Topic 1*

HOTSPOT
-

You create an ExpressRoute circuit named ERC1 that is enabled by your connectivity provider.

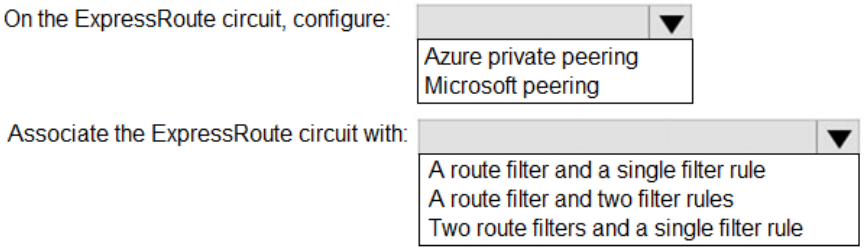
You need to ensure that the routes for Azure Backup and Azure Cosmos DB are advertised to the on-premises network via ECR1.

The solution must minimize administrative effort.

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

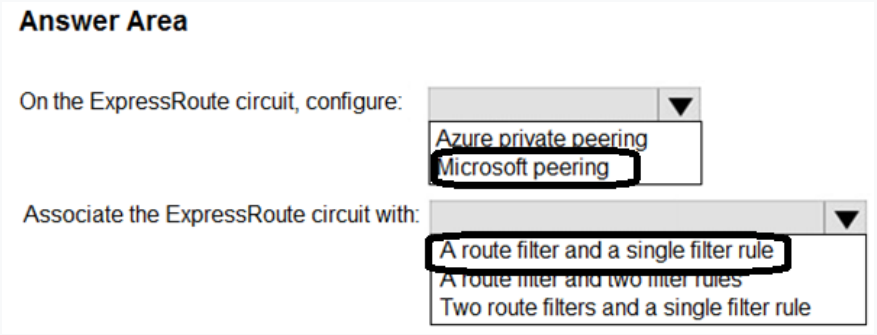
NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:

Answer Area



NK203 Highly Voted 1 year, 11 months ago

Microsoft peering and Single filter ruleNo, you cannot use a single route filter with a single filter rule if you need access to multiple Azure services like Azure Backup and Azure Cosmos DB. Each Azure Service Has a Unique BGP Community Value. A single filter rule in a route filter can only specify one BGP community value. Therefore, a single rule cannot encompass multiple services. https://learn.microsoft.com/en-us/azure/expressroute/how-to-routefilter-portal"Microsoft peering and Single filter rule" There is only one rule available, but with several possibilities. So one rule but you configure service for backup and Cosmos DB.and they are named "rules", check the link above. a route filter and two filter rules is correct in my opinionyou create 1 rule filter (as Azure resource), inside the rule filter you manage the (one and only) rule with "manage rule" button and select "Allowed service communities"

upvoted 10 times

NK203 Highly Voted 1 year, 11 months ago

Selected Answer: D

Microsoft peering and Single filter rule

upvoted 10 times

Raheal Most Recent 1 year, 3 months ago

one route filter and two filter rules is typically the best choice for:

Minimizing administrative effort

Accessing multiple Microsoft services

Keeping costs low

upvoted 2 times

JManuel 1 year, 10 months ago

No, you cannot use a single route filter with a single filter rule if you need access to multiple Azure services like Azure Backup and Azure Cosmos DB. Each Azure Service Has a Unique BGP Community Value. A single filter rule in a route filter can only specify one BGP community value. Therefore, a single rule cannot encompass multiple services. https://learn.microsoft.com/en-us/azure/expressroute/how-to-routefilter-portal

upvoted 5 times

JManuel 1 year, 10 months ago

No, you cannot use a single route filter with a single filter rule if you need access to multiple Azure services like Azure Backup and Azure Cosmos DB. Each Azure Service Has a Unique BGP Community Value. A single filter rule in a route filter can only specify one BGP community value. Therefore, a single rule cannot encompass multiple services. https://learn.microsoft.com/en-us/azure/expressroute/how-to-routefilter-portal"Microsoft peering and Single filter rule" There is only one rule available, but with several possibilities. So one rule but you configure service for backup and Cosmos DB.and they are named "rules", check the link above. a route filter and two filter rules is correct in my opinionyou create 1 rule filter (as Azure resource), inside the rule filter you manage the (one and only) rule with "manage rule" button and select "Allowed service communities"

upvoted 5 times

azuri 1 year, 4 months ago

Explanation:

When Microsoft peering is configured on an ExpressRoute circuit, Microsoft edge routers establish BGP sessions with your edge routers.

No routes are advertised to your network by default.

To receive route advertisements for specific services like Microsoft 365 or public Azure services, you must associate a route filter with your ExpressRoute circuit.

A route filter defines an allowed list of BGP community values, and only prefixes corresponding to these values are advertised to your network.

For example, if you want to access Exchange Online through your ExpressRoute circuit, you would add the BGP community value for Exchange Online to the route filter rule.

In summary:

You need one route filter resource.

This route filter can only have one rule.

This rule must be of type 'Allow'.

The rule can include a list of BGP community values associated with the services you want to access

upvoted 4 times

LearnICC 1 year, 10 months ago

"Microsoft peering and Single filter rule" There is only one rule available, but with several possibilities. So one rule but you configure service for backup and Cosmos DB.

upvoted 1 times

bobothewiseman 1 year, 9 months ago

MS peering

a Route filter and a Single filter rule

upvoted 2 times

manhattan 1 year, 10 months ago

and they are named "rules", check the link above. a route filter and two filter rules is correct in my opinion

upvoted 1 times

Knight_Of_Peace 1 year, 9 months ago

Suggested answer is:

- Microsoft Peering because its connected to Azure Service and not Virtual Network.

- One route filter with one filter rule because route filter can have only one rule as confirmed in the following link:

https://learn.microsoft.com/en-us/azure/expressroute/how-to-routefilter-portal#:~:text=A%20route%20filter%20can%20have%20only%20one%20rule%2C%20and%20the%20rule%20must%20be%20of%20type%20%27Allow%27.%20This%20rule%20can%20have%20a%20list%20of%20BGP%20community%20values%20associated%20with%20it.

Same link confirm that servers can be assigned to the one rule, so can add both of the Azure Backup and Azure Cosmos DB to the same rule.

https://learn.microsoft.com/en-us/azure/expressroute/how-to-routefilter-portal#:~:text=Select%20the%20services%20you%20want%20to%20connect%20to%20from%20the%20drop%2Ddown%20list%20and%20save%20the%20rule%20when%20done.

upvoted 3 times

LearnICC 1 year, 10 months ago

"Microsoft peering and Single filter rule"

There is only one rule available, but with several possibilities. So one rule but you configure service for backup and Cosmos DB.

upvoted 1 times

manhattan 1 year, 10 months ago

and they are named "rules", check the link above.

a route filter and two filter rules is correct in my opinion

upvoted 1 times

LearnICC 1 year, 8 months ago

you create 1 rule filter (as Azure resource), inside the rule filter you manage the (one and only) rule with "manage rule" button and select "Allowed service communities"

upvoted 3 times

Question #44 *Topic 1*

HOTSPOT

-

You plan to implement an Azure Virtual WAN named VWAN1 that will contain a hub named Hub1. VWAN1 will include the virtual networks shown in the following table.

You need to ensure that hosts connected to VNet1 can communicate with hosts connected to VNet3.

How should you configure the routing tables for VWAN1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Name	IP address space	Description
VNet1	10.1.0.0/24	Connected directly to Hub1 by using a connection named Conn1
VNet2	10.2.0.0/24	Connected directly to Hub1 by using a connection named Conn2 and hosting a Network Virtual Appliance (NVA) named NVA2 that has an IP address of 10.2.0.5
VNet3	10.2.3.0/24	Connected to VNet2 by using a virtual network peering named Peering1

Answer Area

Default route table:
- From destination 10.2.0.0/16 to next hop Conn2
- From destination 10.2.3.0/24 to next hop 10.2.0.5
- From destination eastusconn to next hop 10.2.0.0/16

Route table for Conn1:
- From destination 10.2.0.0/16 to next hop Conn2
- From destination 10.2.3.0/24 to next hop 10.2.0.5
- From destination eastusconn to next hop 10.2.0.0/16

Suggested Answer:

Answer Area

Default route table: From destination 10.2.0.0/16 to next hop Conn2

Route table for Conn1: From destination 10.2.3.0/24 to next hop 10.2.0.5

windowsmodulesinstallerworker 1 year, 6 months ago

From destination 10.2.3.0/24 to next hop 10.2.0.5 - this is because the default route table will instruct all traffic to go to the NVA if they want to reach vnet3, since its connected by a peering only there needs to be an NVA in VNET2 in order to forward traffic to VNET3.

From destination 10.2.0.0/16 to next hop Conn2 - This is to direct the traffic (for all 10.2.x.x destinations) from VNET1 to the hub where the default route table then applies.

upvoted 1 times

windowsmodulesinstallerworker 1 year, 6 months ago

From destination 10.2.3.0/24 to next hop 10.2.0.5 - this is because the default route table will instruct all traffic to go to the NVA if they want to reach vnet3, since its connected by a peering only there needs to be an NVA in VNET2 in order to forward traffic to VNET3. From destination 10.2.0.0/16 to next hop Conn2 - This is to direct the traffic (for all 10.2.x.x destinations) from VNET1 to the hub where the default route table then applies.delete this comment. it's totally wrong

upvoted 1 times

windowsmodulesinstallerworker Most Recent 1 year, 5 months ago

delete this comment. it's totally wrong

upvoted 1 times

NK203 1 year, 11 months ago

Selected Answer: D

vnet2-conn2 ,vnet3-nva2

upvoted 3 times

NK203 1 year, 11 months ago

vnet2-conn2 ,vnet3-nva2Default Route Table: From destination 10.2.3.0/24 to next hop 10.2.0.5 Route Table for Conn1: From destination 10.2.0.0/16 to next hop Conn2Correction!!!! Given answer is correct

upvoted 3 times

bobothewiseman 1 year, 10 months ago

Default Route Table: From destination 10.2.3.0/24 to next hop 10.2.0.5

Route Table for Conn1: From destination 10.2.0.0/16 to next hop Conn2

upvoted 4 times

bobothewiseman 1 year, 10 months ago

Default Route Table: From destination 10.2.3.0/24 to next hop 10.2.0.5 Route Table for Conn1: From destination 10.2.0.0/16 to next hop Conn2Correction!!!! Given answer is correct

upvoted 4 times

bobothewiseman 1 year, 10 months ago

Correction!!!! Given answer is correct

upvoted 4 times

Question #45 *Topic 1*

HOTSPOT

-

You have 50 on-premises networks. Each network contains a server that runs Windows Server.

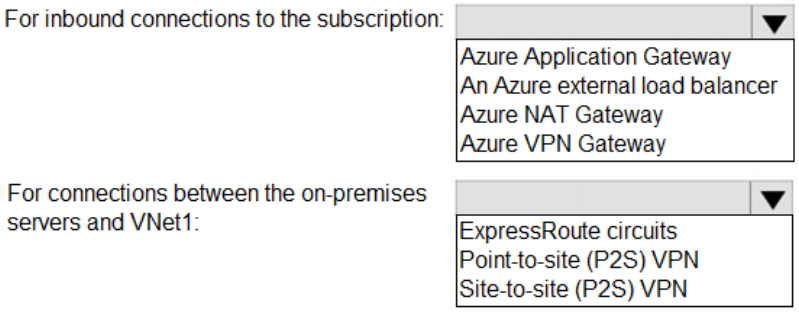
You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains a database server named DB1.

You plan to deploy an app named App1 that will be hosted on the on-premises servers and will connect to DB1 by using Azure Network Adapter.

What should you use to support the Azure Network Adapter connections to VNet1? To answer, select the appropriate options in the answer area.

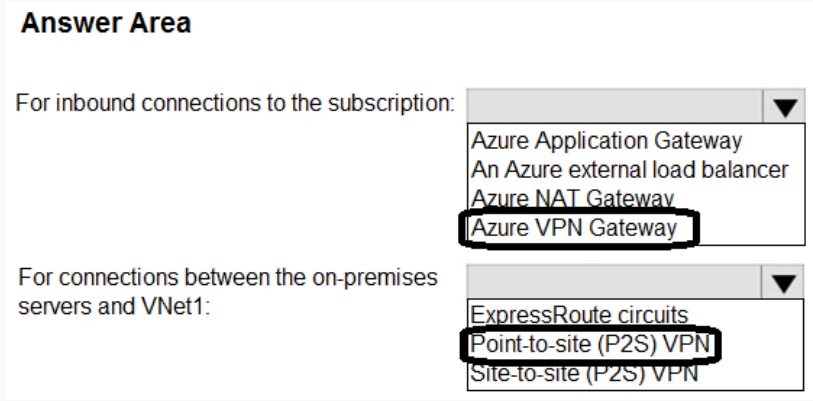
NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:

Answer Area



NK203 Highly Voted 1 year, 11 months ago

Selected Answer: D

Azure VPN Gateway & P2S

upvoted 16 times

GohanF2 Most Recent 1 month, 1 week ago

it is point to site for the servers and azure vpn gateway.

ExpressRoute, it is designed for broader private connectivity between networks, not the per-server Azure Network Adapter feature.

Site-to-site VPN, connects entire networks/sites, not individual Windows Server hosts through Azure Network Adapter.

Application Gateway / Load Balancer / NAT Gateway, do not terminate Azure Network Adapter VPN connections.

upvoted 1 times

exam2301 1 year, 10 months ago

Why not S2S VPN?in this scenario we have a few on-prem servers to connect to the virtual Network , so P2S is more efficient in this scenario

upvoted 2 times

exam2301 1 year, 10 months ago

Why not S2S VPN?

upvoted 2 times

MarkMac 11 months, 1 week ago

Sounds like there are 50 servers in need of this config, so P2S doesn't seem ideal.

Azure VPN w/ S2S?

upvoted 1 times

Zorro2003 1 year, 2 months ago

Answer:

For inbound connections to the subscription: Azure VPN Gateway

For connections between the on-premises servers and VNet1: Point-to-site (P2S) VPN

Why: Azure Network Adapter (from Windows Admin Center) connects Windows Server to an Azure VNet using a P2S VPN, which requires an Azure VPN Gateway in the VNet to terminate those connections.

upvoted 1 times

Krishlab 1 year, 8 months ago

Answers: Azure VPN Gateway and Express route circuits.

upvoted 1 times

NK203 Highly Voted 1 year, 11 months ago

Selected Answer: D

Azure VPN Gateway & P2S

upvoted 16 times

c9348c7 1 year, 5 months ago

in this scenario we have a few on-prem servers to connect to the virtual Network , so P2S is more efficient in this scenario

upvoted 2 times

manhattan 1 year, 11 months ago

yes, azure VPN Gateway and P2S as for the steps included here:

https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/azure/use-azure-network-adapter

upvoted 6 times

Question #46 *Topic 1*

You have an on-premises network.

You have an Azure subscription that contains a virtual network.

You have an ExpressRoute service provider.

You plan to connect the Azure virtual network and the on-premises network by using an ExpressRoute circuit.

You create a new ExpressRoute circuit.

You need to provision the new circuit.

Which information should you provide to the service provider?

A. the IKEv2 shared key

B. the certificate

C. the public IP address

D. the service key

Suggested Answer: *D*

Community vote distribution

D (100%)

nabeel79 Most Recent 1 year, 6 months ago

Selected Answer: D

service key

upvoted 2 times

a250fb0 1 year, 9 months ago

Selected Answer: D

To provision the new ExpressRoute circuit, you should provide the service provider with the service key

upvoted 2 times

addy_1011 Highly Voted 1 year, 11 months ago

Selected Answer: D

https://learn.microsoft.com/en-us/azure/expressroute/expressroute-circuit-peerings#circuits

upvoted 13 times

Question #47 *Topic 1*

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

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

You plan to connect Server1 to VNet1 by using Azure Network Adapter.

You need to minimize how long it takes to deploy the adapter to Server1.

What should you create first?

A. a route server

B. an Azure Bastion host

C. a private endpoint

D. an Azure VPN gateway

Suggested Answer: *D*

Community vote distribution

D (100%)

Zorro2003 Most Recent 1 year, 2 months ago

Selected Answer: D

Correct Answer: D. an Azure VPN gateway

You want to connect Server1 (on-premises) to VNet1 using Azure Network Adapter.

Azure Network Adapter creates a Point-to-Site (P2S) VPN connection automatically.

To establish this VPN connection, Azure needs a VPN Gateway in the target virtual network.

upvoted 3 times

bobothewiseman 1 year, 11 months ago

Selected Answer: D

https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/azure/use-azure-network-adapter

upvoted 3 times

manhattan 1 year, 11 months ago

Selected Answer: D

Considering that in the Microsoft process (here attached) for Azure Network adapter a VPN Gateway is included and usually it is not a quick task to do, I'd say the answer D seems correct.

https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/azure/use-azure-network-adapter

upvoted 3 times

Question #48 *Topic 1*

HOTSPOT
-

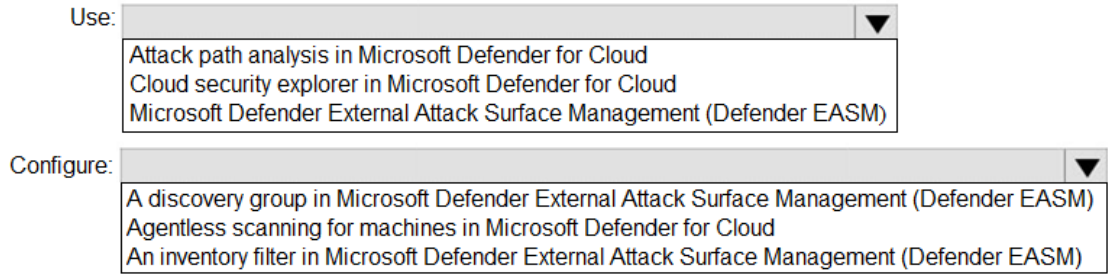
You have an Azure subscription. The subscription contains 500 virtual machines that run either Windows 11 or Linux.

You need to identify which Linux virtual machines are accessible from the internet. The solution must minimize administrative effort.

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

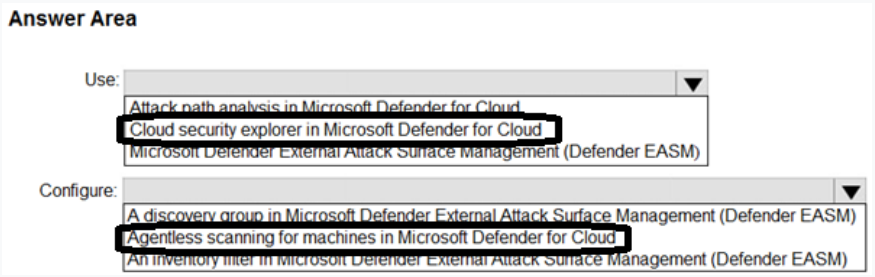
NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:

Answer Area



Krishlab Most Recent 1 year, 8 months ago

Use: Defender easm

configure: agentless scanning

upvoted 1 times

nhr2 Highly Voted 1 year, 10 months ago

Use:

Microsoft Defender External Attack Surface Management (Defender EASM)

Configure:

A discovery group in Microsoft Defender External Attack Surface Management (Defender EASM)

upvoted 8 times

NK203 1 year, 11 months ago

Use:Microsoft Defend Extenanl Attack Surface Management Configure:discovery group

upvoted 4 times

NK203 1 year, 11 months ago

Use:Microsoft Defend Extenanl Attack Surface Management Configure:discovery groupMicrosoft Defender External Attack Surface Management (Defender EASM): Provides an inventory of all external-facing assets and determine which are accessible from the internet, including virtual machines. It minimizes administrative effort by automating discovery and categorization of resources. Discovery group in Defender EASM: Enables identification and monitoring of external-facing assets based on the subscription and resource configuration, such as virtual machines. https://learn.microsoft.com/en-us/azure/external-attack-surface-management/overview https://learn.microsoft.com/en-us/azure/external-attack-surface-management/discovering-your-attack-surface

upvoted 4 times

JManuel Highly Voted 1 year, 10 months ago

Microsoft Defender External Attack Surface Management (Defender EASM): Provides an inventory of all external-facing assets and determine which are accessible from the internet, including virtual machines. It minimizes administrative effort by automating discovery and categorization of resources.

Discovery group in Defender EASM: Enables identification and monitoring of external-facing assets based on the subscription and resource configuration, such as virtual machines.

https://learn.microsoft.com/en-us/azure/external-attack-surface-management/overview

https://learn.microsoft.com/en-us/azure/external-attack-surface-management/discovering-your-attack-surface

upvoted 12 times

manhattan 1 year, 11 months ago

Selected Answer: B

Just to be able to add comments

upvoted 4 times

Question #49 *Topic 1*

You have an instance of Azure Web Application Firewall (WAF) on Azure Front Door.

You plan to create a WAF rule that will block high rates of requests from a single IP address.

You need to query Log Analytics to identify the optimal threshold for the rule.

Which table should you query in Log Analytics?

A. AZFWThreatIntel

B. AzureDiagnostics

C. SecurityDetection

D. AGWFirewallLogs

Suggested Answer: *B*

Community vote distribution

B (100%)

sbaeurle Most Recent 1 year, 1 month ago

Selected Answer: B

AzureDiagnostics table can be filtered like:

AzureDiagnostics

| where Category == "FrontdoorWebApplicationFirewallLog"

upvoted 2 times

a250fb0 1 year, 9 months ago

Selected Answer: B

To identify the optimal threshold for a WAF rule that will block high rates of requests from a single IP address, you should query the AzureDiagnostics table in Log Analytics

upvoted 3 times

Jor466077 Highly Voted 1 year, 11 months ago

Selected Answer: B

Correct answer.

https://learn.microsoft.com/en-us/azure/web-application-firewall/shared/application-ddos-protection#waf-log-analysis

upvoted 6 times

DRAG DROP

-

Your on-premises network contains two subnets named Subnet and Subnet2. Subnet2 contains a Hyper-V host that contains two virtual machines named VM1 and VM2. VM1 and VM2 are connected to Subnet2.

You have an Azure virtual network named VNet1 that contains GatewaySubnet and a subnet named VSubnet1. VNet1 is connected to the on-premises network by using a Site-to-Site (S2S) VPN connection.

You plan to migrate VM1 to VNet1 and maintain the existing IP address of VM1. VM2 will remain on Subnet2.

You need to prepare the environment to ensure that VM1 can communicate with VM2 once the migration is complete.

Which five 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.

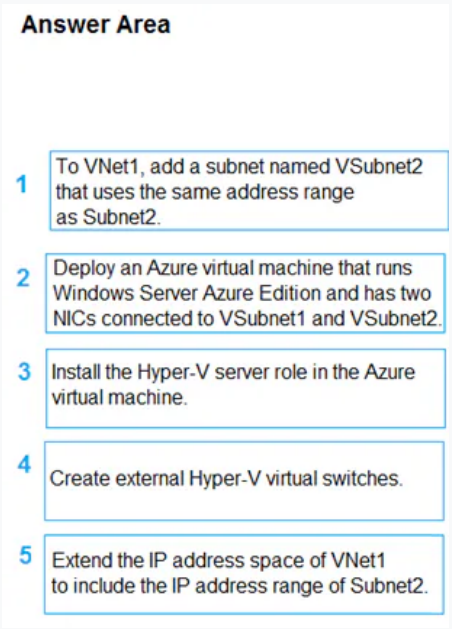
Actions

- Install the Hyper-V server role in the Azure virtual machine.
- Create external Hyper-V virtual switches.
- Extend the IP address space of VNet1 to include the IP address range of Subnet1.
- To VNet1, add a subnet named VSubnet2 that uses the same address range as Subnet1.
- Extend the IP address space of VNet1 to include the IP address range of Subnet2.
- To VNet1, add a subnet named VSubnet2 that uses the same address range as Subnet2.
- Deploy an Azure virtual machine that runs Windows Server Azure Edition and has two NICs connected to VSubnet1 and VSubnet2.

Answer Area

1.
2.
3.
4.
5.

Suggested Answer:



Makaveli1 Highly Voted 1 year, 10 months ago

1. Extend the IP address space of VNet1 to include the IP address range of Subnet2. 2. To VNet1, add a subnet named VSubnet2 that uses the same address range as Subnet2. 3. Deploy an Azure virtual machine that runs Windows Server Azure Edition and has two NICs connected to VSubnet1 and VSubnet2 4. Install the Hyper-V server role in the Azure virtual machine. 5. Create external Hyper-V virtual switches.Seems to be the process as explained here: https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/azure/azure-extended-network

upvoted 14 times

Makaveli1 Highly Voted 1 year, 10 months ago

1. Extend the IP address space of VNet1 to include the IP address range of Subnet2. 2. To VNet1, add a subnet named VSubnet2 that uses the same address range as Subnet2. 3. Deploy an Azure virtual machine that runs Windows Server Azure Edition and has two NICs connected to VSubnet1 and VSubnet2 4. Install the Hyper-V server role in the Azure virtual machine. 5. Create external Hyper-V virtual switches.

upvoted 14 times

MarkMac Most Recent 11 months, 1 week ago

Is MS trying to train people in unlikely unique scenarios? Have the extra conversation and convince the VM owner to change the IP and set this up according to stable, sound architecture instead of having to create and maintain a complex infrastructure like this.

upvoted 1 times

Saba53 1 year, 8 months ago

1. To VNet1, add a subnet named VSubnet2 that uses the same address range as Subnet2. 2. Deploy an Azure virtual machine that runs Windows Server Azure Edition and has two NICs connected to VSubnet1 and VSubnet2.

3. Install the Hyper-V server role in the Azure virtual machine.

4. Create external Hyper-V virtual switches.

5. Extend the IP address space of VNet1 to include the IP address range of Subnet2.

upvoted 2 times

NK203 1 year, 11 months ago

When you click Discussion button,no answer option :A,B,C,D can be choosed. So you cannot add a comment and submit.I just edit html to add these 4 options and provide a answer .Then others can add comment.Corrected Sequence: 1. To VNet1, add a subnet named VSubnet2 that uses the same address range as Subnet2. 2. Deploy an Azure virtual machine that runs Windows Server Azure Edition and has two NICs connected to VSubnet1 and VSubnet2. 3. Install the Hyper-V server role in the Azure virtual machine. 4. Create external Hyper-V virtual switches. 5. Extend the IP address space of VNet1 to include the IP address range of Subnet2.

upvoted 5 times

NK203 1 year, 11 months ago

Selected Answer: D

When you click Discussion button,no answer option :A,B,C,D can be choosed. So you cannot add a comment and submit.I just edit html to add these 4 options and provide a answer .Then others can add comment.

upvoted 5 times

Gaz_ 1 year, 9 months ago

Seems to be the process as explained here: https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/azure/azure-extended-network

upvoted 1 times

NK203 1 year, 11 months ago

1 To Vnet1,add VSubnet2 ...as Subnet1 2 Deploy an Azure Vm 3 Install the.. 4 Create external 5 Extend the IP...Subnet2

upvoted 2 times

NK203 1 year, 11 months ago

1 To Vnet1,add VSubnet2 ...as Subnet1 2 Deploy an Azure Vm 3 Install the.. 4 Create external 5 Extend the IP...Subnet2First one should be replaced by "To Vnet1,add VSubnet2 ...as Subnet2"Corrected Sequence: 1. To VNet1, add a subnet named VSubnet2 that uses the same address range as Subnet2. 2. Deploy an Azure virtual machine that runs Windows Server Azure Edition and has two NICs connected to VSubnet1 and VSubnet2. 3. Install the Hyper-V server role in the Azure virtual machine. 4. Create external Hyper-V virtual switches. 5. Extend the IP address space of VNet1 to include the IP address range of Subnet2.thisis correcthow do you expect to extend the vnet address space after you've allready included the address space via the subnet to the vnet? It dosen't work that way. First you have to modify the address space of the VNET, then you can add the subnnetBut wouldn't you have to extend the IP address space of VNet1 before you can create the VSubnet2 which has to have the same address range as Subnet2. You can't create the VSubnet2 without having the addresses available in the VNet1. So Extend the IP...Subnet2 should be first, no?

upvoted 2 times

NK203 1 year, 10 months ago

First one should be replaced by "To Vnet1,add VSubnet2 ...as Subnet2"

upvoted 3 times

bobothewiseman 1 year, 10 months ago

Corrected Sequence: 1. To VNet1, add a subnet named VSubnet2 that uses the same address range as Subnet2. 2. Deploy an Azure virtual machine that runs Windows Server Azure Edition and has two NICs connected to VSubnet1 and VSubnet2. 3. Install the Hyper-V server role in the Azure virtual machine. 4. Create external Hyper-V virtual switches. 5. Extend the IP address space of VNet1 to include the IP address range of Subnet2.thisis correcthow do you expect to extend the vnet address space after you've allready included the address space via the subnet to the vnet? It dosen't work that way. First you have to modify the address space of the VNET, then you can add the subnnet

upvoted 3 times

Jurka 1 year, 10 months ago

But wouldn't you have to extend the IP address space of VNet1 before you can create the VSubnet2 which has to have the same address range as Subnet2. You can't create the VSubnet2 without having the addresses available in the VNet1. So Extend the IP...Subnet2 should be first, no?

upvoted 2 times

NK203 1 year, 10 months ago

First one should be replaced by "To Vnet1,add VSubnet2 ...as Subnet2"

upvoted 3 times

windowsmodulesinstallerworker 1 year, 5 months ago

how do you expect to extend the vnet address space after you've allready included the address space via the subnet to the vnet? It dosen't work that way. First you have to modify the address space of the VNET, then you can add the subnnet

upvoted 2 times

Anonymouse1312 1 year, 9 months ago

thisis correct

upvoted 1 times

manhattan 1 year, 10 months ago

Thanks for your sequence, it should be correct

https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/azure/azure-extended-network

upvoted 2 times

bobothewiseman 1 year, 10 months ago

Corrected Sequence:

1. To VNet1, add a subnet named VSubnet2 that uses the same address range as Subnet2.

2. Deploy an Azure virtual machine that runs Windows Server Azure Edition and has two NICs connected to VSubnet1 and VSubnet2.

3. Install the Hyper-V server role in the Azure virtual machine.

4. Create external Hyper-V virtual switches.

5. Extend the IP address space of VNet1 to include the IP address range of Subnet2.

upvoted 2 times

Question #51 *Topic 1*

You have an on-premises datacenter named Site1 that contains a firewall named FW1. FW1 connects to the internet.

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

You plan to connect Site1 to Hub1 by using a site-to-site connection.

You need to configure the site-to-site connection to FW1.

What should you create in VWAN1?

Name	Type	Description
VNet1	Virtual network	*None*
VWAN1	Azure Virtual WAN	Standard Virtual WAN connected to Hub1
Hub1	Azure Virtual WAN hub	Contains a Site-to-Site (S2S) VPN gateway

A. a VPN site

B. a virtual network connection

C. a network virtual appliance (NVA)

D. a User VPN configuration

Suggested Answer: *A*

Community vote distribution

A (100%)

Jor466077 Highly Voted 1 year, 11 months ago

Correct. https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-site-to-site-portal#site

upvoted 6 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
-

Proseware, Inc. is a financial services company that has a main office in New York City and a branch office in San Francisco.

Existing Environment. Hybrid Environment

Proseware has an on-premises Active Directory Domain Services (AD DS) forest named corp.proseware.com that syncs with a Microsoft Entra tenant named proseware.com.

Proseware has an Azure subscription that is linked to proseware.com.

Proseware has an internal certification authority (CA).

Existing Environment. Network Infrastructure

The offices contain the resources shown in the following table.

NYCNet connects to Azure by using an ExpressRoute circuit.

SFONet connects to Azure by using a Site-to-Site (S2S) VPN.

Existing Environment. Azure Resources

The Azure subscription contains the virtual networks and subnets shown in the following table.

The subscription contains four virtual machines named VM1, VM2, VM3, and VM4. VM1 and VM2 host an app named App1.

VM3 and VM4 host a web app named App2 that is accessed by using a FQDN of app2.proseware.com. Users access app2.proseware.com by

using HTTP or HTTPS.

VM1, VM2, and VM4 are connected to SpokeVNet.

The subscription contains Application Gateway resources shown in the following table.

The subscription contains an Azure Front Door Standard profile named FD1. FD1 contains a single origin group that targets APPGW1 by using the default endpoint name.

HubVNet connects to NYCNet by using an ExpressRoute gateway named ERGW1.

Planned Changes and Requirements. Planned Changes

Proseware plans to implement the following changes:

• Deploy an Azure Private DNS Resolver named PRDNS1 to HubVNet and link PRDNS1 to SpokeVNet.
• Create a DNS forwarding ruleset named DNSRS1 and associate DNSRS1 with PRDNS1.
• Deploy Azure Virtual Network Manager and implement the following rules:
- Allow inbound connections on TCP port 3389 from the on-premises networks to SUBNET-JUMPHOSTS.
- Block inbound connections on TCP port 80 from the internet to SpokeVNet.
• Ensure that Azure Virtual Network Manager rules take precedence over conflicting NSG rules.
• Deploy two network virtual appliances (NVAs) named NVA1 and NVA2 to HubVNet.
• Deploy a gateway load balancer named LBGW1 to HubVNet.
• Configure LBGW1 to inspect traffic on TCP ports 443, 1433, and 1434 from LBS1 by using NVA1 and NVA2.
• Ensure that all the traffic to App2 is processed by using FD1.

Planned Changes and Requirements. Connectivity requirements

Proseware identifies the following connectivity requirements:

• Minimize the complexity of the Azure Virtual Network Manager deployment.
• Route traffic between NYCNet and SFONet via the ExpressRoute circuit and the S2S VPN.
• Ensure that remote users on Windows 11 devices can connect to HubVNet by using a Point-to-Site (P2S) VPN and their proseware.com credentials.

Planned Changes and Requirements. Security requirements

Proseware identifies the following security requirements:

• Whenever possible, use the internal CA.
• Ensure that all connections routed via APPGW1 use end-to-end encryption.
• Ensure that user connections to Azure-hosted apps use end-to-end encryption.
• Ensure that all inbound internet traffic to app2.proseware.com is routed via FD1.
• Prevent devices that connect to NYCNet from accessing Azure services that use private endpoints.
• Enable the virtual machines that connect to HubVNet and SpokeVNet to access Azure services that use private endpoints.

Planned Changes and Requirements. General requirements

Proseware identifies the following general requirements:

• Minimize the IP address space required to deploy platform-managed resources to the virtual networks.
• From SpokeVNet, resolve name resolution requests for the azure.proseware.com namespace and the corp.proseware.com namespace by using PRDNS1.
• Whenever possible, minimize administrative effort.

You need to configure the P2S VPN to meet the connectivity requirements.

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

NOTE: Each correct selection is worth one point.

Name	Type	Office	Description
NYCNet	On-premises network	New York City	IP address space of 192.168.0.0/22
SFONet	On-premises network	San Francisco	IP address space of 192.168.100.0/22
NYCDNS1	Server	New York City	DNS server that runs Windows Server 2019 and has an IP address of 192.168.0.100

Name	Type	Location	Description
HubVNet	Virtual network	East US Azure region	IP address space of 10.0.0.0/20 peered to SpokeVNet
SpokeVNet	Virtual network	East US Azure region	IP address space of 10.0.16.0/20 peered to HubVNet
VPNGW1	Virtual network gateway	HubVNet	Active-passive resiliency, in the Generation 2, VpnGw3 SKU that has the default ASN connected to SFONet
SUBNET-PE	Subnet	HubVNet	Used for private endpoints
SUBNET-JUMPHOSTS	Subnet	HubVNet	Used for jump hosts
SUBNET-APPGW1	Subnet	SpokeVNet	Contains an Azure application gateway named APPGW1

Name	Type	Location	Description
APPGW1	Application Gateway	SpokeVNet	In the Azure Web Application Firewall (WAF) V2 SKU Terminates HTTPS connections to a backend pool that contains VM3 and VM4
APPGW1-NSG1	Network security group (NSG)	East US region	Associated with SUBNET-APPGW1
APPGW1-WAFPolicy	Azure Web Application Firewall (WAF) policy	East US region	Applied to APPGW1

Answer Area

For VPNGW1, set Tunnel type to:

- IKEv2
- OpenVPN (SSL)
- SSTP (SSL)

For proseware.com:

- Configure an enterprise application.
- Create an app registration.
- Provision a user-assigned managed identity.

Suggested Answer:



Krishlab Highly Voted 1 year, 8 months ago

Correct answers: 1. OpenVPN (SSL) 2. Configure an enterprise application

Reason: 1. The requirement states that remote users on Windows 11 devices must connect using a Point-to-Site (P2S) VPN and their proseware.com credentials (which syncs with Microsoft Entra ID). 2. To enable authentication using Microsoft Entra ID for the P2S VPN, you need to configure an enterprise application in Entra ID.

upvoted 10 times

Krishlab Highly Voted 1 year, 8 months ago

Correct answers: 1. OpenVPN (SSL) 2. Configure an enterprise application Reason: 1. The requirement states that remote users on Windows 11 devices must connect using a Point-to-Site (P2S) VPN and their proseware.com credentials (which syncs with Microsoft Entra ID). 2. To enable authentication using Microsoft Entra ID for the P2S VPN, you need to configure an enterprise application in Entra ID.This is correct.

upvoted 10 times

GohanF2 Most Recent 1 year, 6 months ago

This is correct.

upvoted 1 times

Question #53 *Topic 1*

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. URL rewrite rules

B. path-based rules

C. listeners

D. HTTP settings

Suggested Answer: *A*

Community vote distribution

A (100%)

40a4d4c Most Recent 7 months, 3 weeks ago

Selected Answer: A

Azure Application Gateway supports:

• Header modification

• Server variable manipulation

upvoted 1 times

Krishlab Highly Voted 1 year, 8 months ago

Selected Answer: A

URL rewrite rules allow you to modify request and response headers, including adding, removing, or modifying server variables in the response header.

upvoted 7 times

Question #54 *Topic 1*

HOTSPOT
-

You have an on-premises network.

You have an Azure subscription that contains two virtual networks named VNet1 and VNet2. VNet1 is peered with VNet2.

The on-premises network is connected to VNet1 by using an ExpressRoute circuit named Circuit1.

You need to recommend a solution to improve the routing performance between the on-premises network and the virtual networks. The solution must minimize costs.

Which configurations should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Configure the ExpressRoute route circuit to use:
- ExpressRoute FastPath
- ExpressRoute Global Reach
- ExpressRoute Metro
- ExpressRoute Premium

For the virtual networks:
- Connect VNet2 directly to Circuit1.
- Remove the peering between VNet1 and VNet2.
- Upgrade the SKU of each virtual network.
- Update the route tables.

Suggested Answer:

Answer Area

Configure the ExpressRoute route circuit to use:
- ExpressRoute FastPath
- **ExpressRoute Global Reach**
- ExpressRoute Metro
- ExpressRoute Premium

For the virtual networks:
- **Connect VNet2 directly to Circuit1.**
- Remove the peering between VNet1 and VNet2.
- Upgrade the SKU of each virtual network.
- Update the route tables.

GohanF2 Most Recent 1 month, 1 week ago

I will chose to use FastPath and to connect the Vnet2 dirctly to the circuit.

upvoted 1 times

de3ca78 8 months, 3 weeks ago

Correct answers:

Configure the ExpressRoute route circuit to use: ExpressRoute FastPath

For the virtual networks: Connect VNet2 directly to Circuit1

upvoted 2 times

GiJoe1987 1 year ago

Choose ExpressRoute FastPath for the route circuit, and Update the route tables for the virtual networks.

Reason: FastPath reduces hops and latency for ExpressRoute traffic; updating route tables (UDRs) lets you control/advertise optimal routes to the VNets without creating extra gateways or connections, keeping cost minimal.

upvoted 3 times

CheMetto Highly Voted 1 year, 1 month ago

Global Reach extend the capabilities to go into other region. In my Opinion is FastPath which bypass the vpngw (so improve the routing performance because you remove 1 hop) and connect Vnet2 directly to the circuit

upvoted 17 times

Question #55 *Topic 1*

You have an on-premises datacenter named DC1 that contains two routers.

You have an Azure subscription. The subscription contains a virtual network named VNet1 and a zone-redundant ExpressRoute virtual network gateway named GW1 that uses the ErGw3Az SKU. GW1 is attached to VNet1

DC1 is connected to VNet1 by using an ExpressRoute Standard circuit named Circuit1. The DC1 routers are configured as endpoints for Circuit1. Circuit1 traffic traverses two physical links.

During a link outage, the connection takes three minutes to fail over.

You need to ensure that failovers between the links take less than one second.

What should you do?

A. For Circuit1, select FastPath.

B. On the routers, configure Bidirectional Forwarding Detection (BFD).

C. For GW1, change SKU to UltraPerformance.

D. For GW1, set Active-active mode to Enabled.

Suggested Answer: *B*

Community vote distribution

B (100%)

Flankengott_111 Most Recent 8 months, 4 weeks ago

Selected Answer: B

the routers are checking the BGP-Timer with Keepalive 60s

upvoted 1 times

CheMetto 1 year, 1 month ago

Selected Answer: B

BFD is correct.

https://learn.microsoft.com/en-us/azure/expressroute/expressroute-bfd

upvoted 2 times

Question #56 *Topic 1*

HOTSPOT
-

Your company has an Azure subscription that contains a virtual network named VNet1 and an Azure VPN gateway named vGW1.

The company has 50 users that have Windows 11 devices.

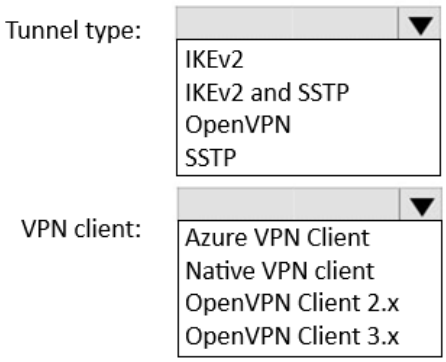
You need to ensure that the users can access the resources on VNet1. The solution must meet the following requirements:

• Ensure that the users can establish Point-to-Site (P2S) VPN connections to vGW1.
• Ensure that the users can authenticate by using only their Microsoft Entra credentials.

Which type of tunnel should you configure, and which VPN client should you configure on the users' devices? To answer, select the appropriate options in the answer area.

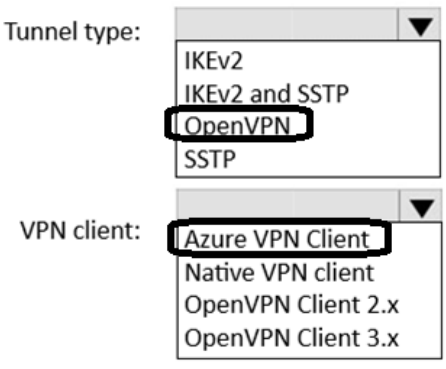
NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:

Answer Area



Gregsenn Most Recent 8 months, 1 week ago

Correct.

OpenVPN and Azure VPN Client.

https://learn.microsoft.com/en-us/azure/vpn-gateway/point-to-site-entra-vpn-client-windows

upvoted 1 times

Question #1 *Topic 2*

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

Suggested 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 4 years, 1 month 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

AmalMOQ Highly Voted 4 years, 1 month 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.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-routingAgree!
upvoted 12 times

Verytutos Most Recent 2 years, 2 months ago
Appeared on Exam 05 Sep 2023
upvoted 2 times

SLGUY 2 years, 2 months ago
Appeared on Exam 26 Aug 2023
upvoted 1 times

khanda 2 years, 7 months 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 2 years, 8 months 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 2 years, 9 months ago
correct
upvoted 1 times

HasanHHH 3 years, 1 month 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 3 years, 2 months ago

Selected Answer: B

Since you implemented VNET peering later, you n3ed to download and install VPN client to get topology changes.

upvoted 1 times

hogs 3 years, 3 months ago

Appeared on exam Aug2022

upvoted 1 times

kogunribido 3 years, 4 months ago

Appeared on exam 6/27/2022

upvoted 1 times

Edward1 3 years, 7 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

Ben_Dover2 3 years, 9 months ago

Selected Answer: B

download VPN config and reconnect

upvoted 3 times

AckeyGraham 3 years, 9 months ago

Would help if there was more context to such a question, presuming like an exam than 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 3 years, 10 months ago

Download the p2s configuration file and reconnect is the solution.

So correct answer here is, NO.

upvoted 2 times

AidenYoukhana 3 years, 10 months ago

Selected Answer: B

Correct: NO.

upvoted 2 times

RandomUser 4 years, 1 month ago

Correct

upvoted 1 times

liono 2 years, 10 months ago

Agree!

upvoted 1 times

FunkyB 3 years, 2 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

Question #2 *Topic 2*

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

Suggested 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%)

Verytutos Most Recent 2 years, 2 months ago
Appeared on Exam 05 Sep 2023
upvoted 2 times

SLGUY 2 years, 2 months ago
Appeared on Exam 26 Aug 2023
upvoted 3 times

Rajan395 2 years, 9 months ago
Correct Answer! re-downloading of the client is required as topology changed

.
upvoted 1 times

HasanHHH 3 years, 1 month 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 3 years, 4 months ago
Appeared on exam 6/27/2022
upvoted 2 times

Edward1 3 years, 7 months ago
Selected Answer: B
Correct!
upvoted 1 times

Takloy Highly Voted 3 years, 10 months ago
Selected Answer: B
Solution: Download the P2S configuration package, install it on the client device and reconnect.

Answer: NO
upvoted 11 times

aftab7500 3 years, 11 months ago

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

upvoted 4 times

Charl 4 years ago

Correct!

upvoted 2 times

Question #3 *Topic 2*

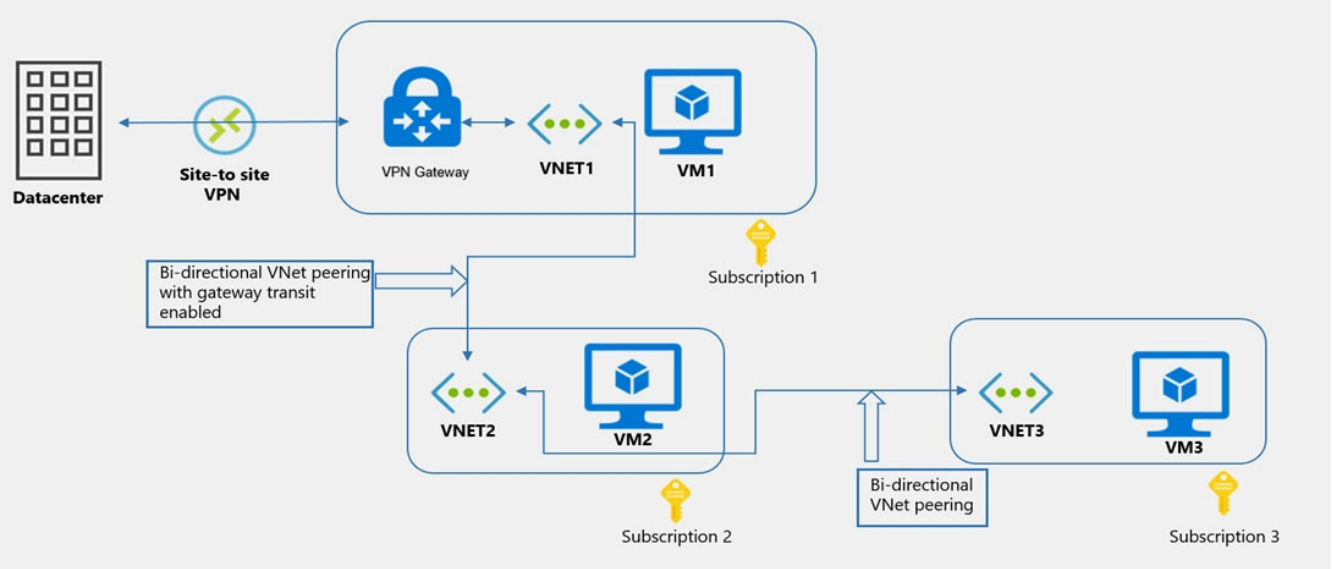
HOTSPOT -

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

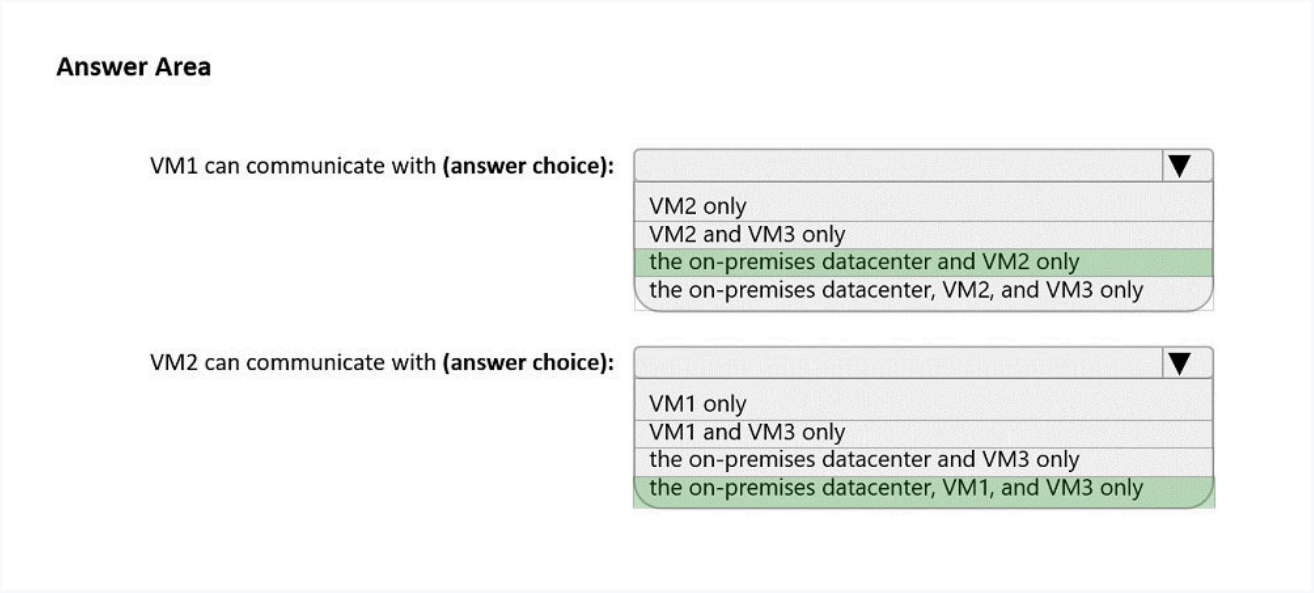
VM1 can communicate with **(answer choice):**

- 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

Suggested Answer:



Reference: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-peering-gateway-transit?toc=/azure/virtual-network/toc.json

RickMorais Highly Voted 4 years ago
Given answers are correct
upvoted 52 times

Vivek_Dwivedi Highly Voted 4 years ago
Use Remote gateway in VNET 2 peering is not mentioned. Which means VM2 can connect only to Vm1 and Vm3.
upvoted 20 times

Vivek_Dwivedi 4 years ago
Use Remote gateway in VNET 2 peering is not mentioned. Which means VM2 can connect only to Vm1 and Vm3.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 diagramThat 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 20 times

kpallivishal 3 years, 10 months 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 9 times

sallymaher 3 years, 10 months 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

Lazylinux Most Recent 2 years ago
Given answer is correct
upvoted 4 times

Verytutos 2 years, 2 months ago
Appeared on Exam 05 Sep 2023
upvoted 3 times

fsgsfgs 2 years, 3 months ago
Given answers are correct
upvoted 4 times

khanda 2 years, 7 months ago
Given answer is correct.
upvoted 4 times

liono 2 years, 10 months ago

Correct.

upvoted 4 times

Goofer 2 years, 10 months ago

VNET1 and VNET2 do not have a router configured to route trafic to another VNET VNET2 and VNET3 do not have UDR configured to route trafic to the router. VM1 --> on-premises and vm2 VM2 --> VM1 and VM3

upvoted 1 times

Bill831231 3 years ago

what if for the S2S VPN without BGP enabled? VM2 can still communicate with On-premise?

upvoted 1 times

HasanHHH 3 years, 1 month 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 11 times

sapien45 3 years, 1 month 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 2 times

AdityaGupta 3 years, 2 months ago

Correct Answer

upvoted 1 times

1particle 3 years, 3 months ago

Correct. VM2 uses VM1's gateway to reach the Datacenter.

upvoted 1 times

unclegrandfather 3 years, 4 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

unclegrandfather 3 years, 4 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.Can you advise whether it varies due to the placement of the "VPN Gateway" on the graph? TIA

upvoted 2 times

WickedMJ 3 years, 3 months ago

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

upvoted 1 times

wsrudmen 3 years, 6 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 3 years, 7 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 3 years, 8 months ago

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

upvoted 2 times

Question #4 *Topic 2*

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

Suggested Answer: *A, D, E*
Reference: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-for-azure-services

Community vote distribution
ADE (89%)

GohanF2 Most Recent 1 month, 1 week ago

Selected Answer: ADE

I agree with JSOC_DXB, AD DS also requires its own subnet. Worst case scenario, its too discard if this option does not appear. However, this question appears on the exam , I took it 2 weeks ago and it does not give AD DS as an option.

upvoted 1 times

d0bermannn Highly Voted 4 years, 3 months ago

Selected Answer: ADE

all GW types and Bastion must have dedicated subnets

upvoted 14 times

d0bermannn 4 years, 3 months ago

all GW types and Bastion must have dedicated subnetsNice answer. THanks

upvoted 14 times

JSOC_DXB 1 year, 7 months ago

Selected Answer: ABE

It's a bad question, AD DS also requires its own Subnet:

https://learn.microsoft.com/en-us/entra/identity/domain-services/network-considerations

"A managed domain must be deployed in its own subnet. Using an existing subnet, gateway subnet, or remote gateways settings in the virtual network peering is unsupported."

upvoted 2 times

Krishlab 1 year, 8 months ago

Selected Answer: ABE

C. Azure Private Link (Does NOT require a dedicated subnet)

Private Link does not require a dedicated subnet; it can be deployed in an existing subnet.

However, a dedicated subnet is recommended in some cases for better isolation.

 D. Azure Application Gateway v2 (Does NOT require a dedicated subnet)

Can be deployed in an existing subnet, but it must have at least a /27 CIDR block.

A dedicated subnet is recommended but not strictly required.

upvoted 1 times

ESAJRR 3 years, 1 month 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 3 years, 2 months ago

Selected Answer: ADE

Correct

upvoted 1 times

liono 3 years, 4 months ago

Given answers are correct.

upvoted 1 times

nostromer89 3 years, 5 months 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 4 times

Webfacat33 3 years, 5 months ago

Selected Answer: ADE

It's correct

upvoted 1 times

HasanHHH 3 years, 7 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 4 times

kevino81 3 years, 7 months ago

Selected Answer: ADE

correct

upvoted 1 times

Alessandro365 3 years, 8 months ago

Selected Answer: ADE

ADE are correct

upvoted 1 times

AdityaGupta 3 years, 8 months ago

Selected Answer: ADE

Aure Bastion, Azure Application Gateway, VNET Gateway and Azure Firewall need dedicated subnet

upvoted 3 times

Jitusrit 3 years, 9 months ago

Selected Answer: ADE

ADE are correct.

upvoted 2 times

1particle 3 years, 9 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 5 times

unclegrandfather 3 years, 10 months ago

Appeared on exam 6/28/22

upvoted 3 times

aldanetcloud 3 years, 11 months ago

Selected Answer: ADE

ade correct answer

upvoted 3 times

lasmas 3 years, 11 months ago

Selected Answer: ADE

ADE seems correct

upvoted 3 times

jpfsm 3 years, 12 months ago

Selected Answer: ADE

Correct

upvoted 3 times

milan92stankovic 4 years, 1 month ago

Selected Answer: ADE

Correct answers are A,D & E

upvoted 3 times

rockethack 4 years, 2 months ago

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

upvoted 3 times

thekhijir 2 years, 1 month ago

Nice answer. THanks

upvoted 1 times

az4o2n 4 years, 3 months ago

Selected Answer: ADE

The answer is correct, looking at the MS documents under Network resource

support evidence https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-for-azure-services#services-that-can-be-deployed-into-a-virtual-network

upvoted 4 times

Ben_Dover2 4 years, 3 months ago

ADE for sure ... B - ADS makes no reason at all

upvoted 3 times

Joshalom 4 years, 3 months ago

on exam 6/2/2022

upvoted 1 times

sleekdunga 4 years, 3 months ago

ADE is the correct answer. While you can Azure-AD & Azure Privatelink within a subnet, they do not require dedicated subnets.

upvoted 3 times

Takloy 4 years, 4 months ago

The Answers are correct!

A. Azure Bastion

D. Azure Application Gateway v2

E. VPN gateway

upvoted 2 times

Acrophat 4 years, 5 months ago

This link denotes that Azure AD DS services are deployed to a dedicated subnet. It's odd that the provided document link is not updated to reflect this.

https://docs.microsoft.com/en-us/azure/active-directory-domain-services/tutorial-configure-networking

upvoted 1 times

Cshekmen 4 years, 5 months ago

Selected Answer: ADE

Given explanation is correct

upvoted 4 times

3tallah 4 years, 6 months ago

Selected Answer: ABE

Azure Active Directory Domain Services (Azure AD DS) managed domain is deployed into an Azure virtual network subnet. This virtual network subnet should only be used for the managed domain resources provided by the Azure platform.

upvoted 4 times

devpool 4 years, 5 months ago

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-for-azure-services#services-that-can-be-deployed-into-a-virtual-network

ADE is correct.

upvoted 4 times

walkwolf3 4 years, 6 months ago

ADE

Is a dedicated subnet required for Private Link service? No. Private Link service doesn't require a dedicated subnet

https://docs.microsoft.com/en-us/azure/private-link/private-link-faq

upvoted 3 times

Opiate 4 years, 6 months ago

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-for-azure-services details "Services than can be deployed into a virtual network" not required.

upvoted 2 times

srikanth1987 Highly Voted 4 years, 7 months ago

yes..ADE is the correct

answer.

upvoted 32 times

Question #5 *Topic 2*

HOTSPOT -
You have an Azure private DNS zone named contoso.com that is linked to the virtual networks shown in the following table.

The links have auto registration enabled.
You create the virtual machines shown in the following table.

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:

Name	IP address
Vnet1	10.1.0.0/16
Vnet2	10.2.0.0/16

Name	IP address
VM1	10.1.10.10
VM2	10.2.10.10
VM3	10.2.10.11

.

Answer Area

Statements	Yes	No
VM2 will resolve vm1.contoso.com to 10.1.10.10	◯	◯
Deleting VM1 will delete all VM1 records automatically	◯	◯
Changing the IP address of VM3 will update the DNS record of VM3 automatically	◯	◯

Suggested Answer:

Answer Area

Statements	Yes	No
VM2 will resolve vm1.contoso.com to 10.1.10.10	○	○
Deleting VM1 will delete all VM1 records automatically	○	○
Changing the IP address of VM3 will update the DNS record of VM3 automatically	○	○

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 4 years, 10 months 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 41 times

walkwolf3 Highly Voted 5 years 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 34 times

walkwolf3 5 years 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.walkwolf3 - your described results should mean that the answer is N,N,YAgree 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.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?There is no possibility to change ip address without rebooting vm so DNS will be updated automatically.So are you saying answer 3 should be Yes as it registers itself after a reboot?if it comes back and registers, then the answer is YES right?

upvoted 34 times

Royce341 4 years, 3 months ago

walkwolf3 - your described results should mean that the answer is N,N,Y

upvoted 10 times

wooyourdaddy 3 years, 8 months 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

wooyourdaddy 3 years, 8 months 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.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?There is no possibility to change ip address without rebooting vm so DNS will be updated automatically.

upvoted 2 times

Apptech 3 years, 7 months 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?There is no possibility to change ip address without rebooting vm so DNS will be updated automatically.

upvoted 2 times

Apptech 3 years, 7 months 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 3 years, 3 months ago

There is no possibility to change ip address without rebooting vm so DNS will be updated automatically.

upvoted 1 times

JamRackie 5 years ago

So are you saying answer 3 should be Yes as it registers itself after a reboot?

upvoted 5 times

yokoka2259 4 years, 12 months ago

if it comes back and registers, then the answer is YES right?

upvoted 4 times

40a4d4c Most Recent 7 months, 3 weeks ago

NNY Manual record overrides auto-registration >>>N Auto-registered records only >>> N New record is created automatically >>> Y

upvoted 2 times

Flankengott_111 8 months, 3 weeks ago

NNY - auto registration enabled for VM3 / VNET2

upvoted 1 times

Zorro2003 1 year, 2 months ago

The correct set is No / No / Yes — not N/N/N. 1) VM2 resolves vm1.contoso.com to 10.1.10.10 → No. There's a manual A record for VM1 → 10.1.10.9 in the private zone. With auto-registration also creating 10.1.10.10, the record set contains two A records. Resolution is not guaranteed to return 10.1.10.10 only. 2) Deleting VM1 deletes all VM1 records → No. Deleting the VM removes the auto-registered entry, but the manually created record remains. 3) Changing VM3's IP auto-updates its DNS record → Yes. With auto-registration enabled on the VNet link, Azure Private DNS updates A/PTR records when a VM's NIC private IP changes (whether the NIC allocation is dynamic or static). This doesn't depend on setting a static IP inside the guest OS (which is unsupported in Azure). So when you change VM3's NIC private IP, its DNS record is updated automatically.

upvoted 2 times

TheBlob 2 years, 4 months ago

NNY I see there a lot of misconception on the 3rd question. Configuring a 'static' IP Address to VM3; this still applied Azure DHCP. Essentially it only creates a DHCP scope reservation in the Azure DHCP. Hence the DNS record is update automatically. Now if you question how the IP Address is changed, read the sentence closely; it says, 'of VM3' and not 'on VM3'. Just my two cents.

upvoted 3 times

SnowmanPapi 2 years, 5 months ago

NYY. I've tested this in a lab. 1. Adding a manual entry overrides the auto-registered entry VM1 had previously, so answer is NO because it will resolve to the new entry that was manually added. 2. Deleting the VM auto-deleted the entry (it appears it checks the status of the VMs NIC), so answer is YES. 3. Changing the IP address of the [NIC] VM deleted the entry and then it re-added a new entry with the updated IP. (I've just tested this on 02/06/2024) Thank you all for your contributions

upvoted 4 times

Techbiz 3 years, 1 month ago

The answer given is correct

upvoted 1 times

voldemort123 3 years, 1 month 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 3 years, 1 month ago

appears on exam, 19 Sept 2023

upvoted 1 times

SLGUY 3 years, 2 months ago

Appeared on Exam 26 Aug 2023

upvoted 3 times

ESAJRR 3 years, 7 months ago

Answer is correct, N,N,N, lab tested too.

upvoted 1 times

AzureLearner01 3 years, 8 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 3 years, 9 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 9 times

Rajan395 3 years, 9 months ago

Answer is No, NO and YES

upvoted 5 times

zukako 3 years, 10 months ago

I think q3 is Yes because for VM, azure manage the DNS record automatically

upvoted 4 times

Kevmeister 3 years, 12 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.Answer NNY, probado en labA 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 10 times

Kevmeister 3 years, 12 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 10 times

Gambito11 1 year, 10 months ago

Answer NNY, probado en lab

upvoted 1 times

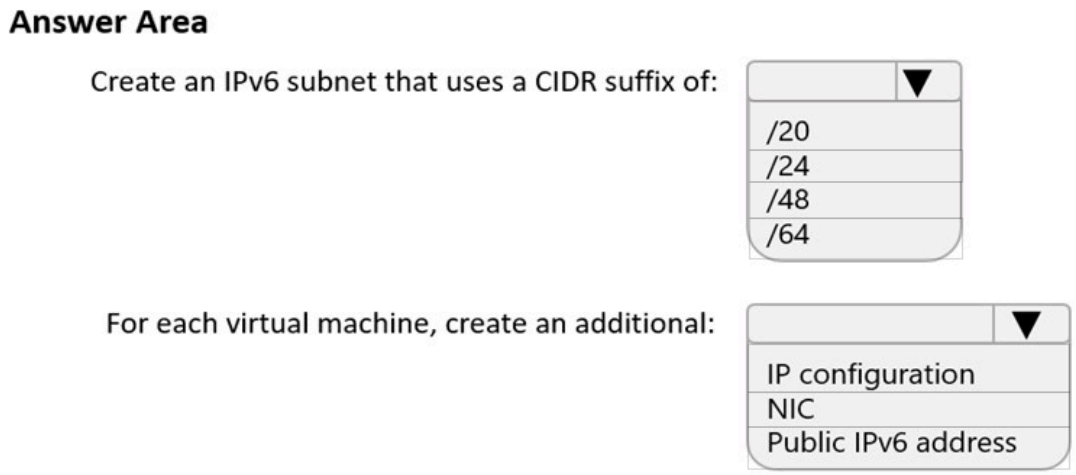
Kevmeister 3 years, 12 months ago

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.

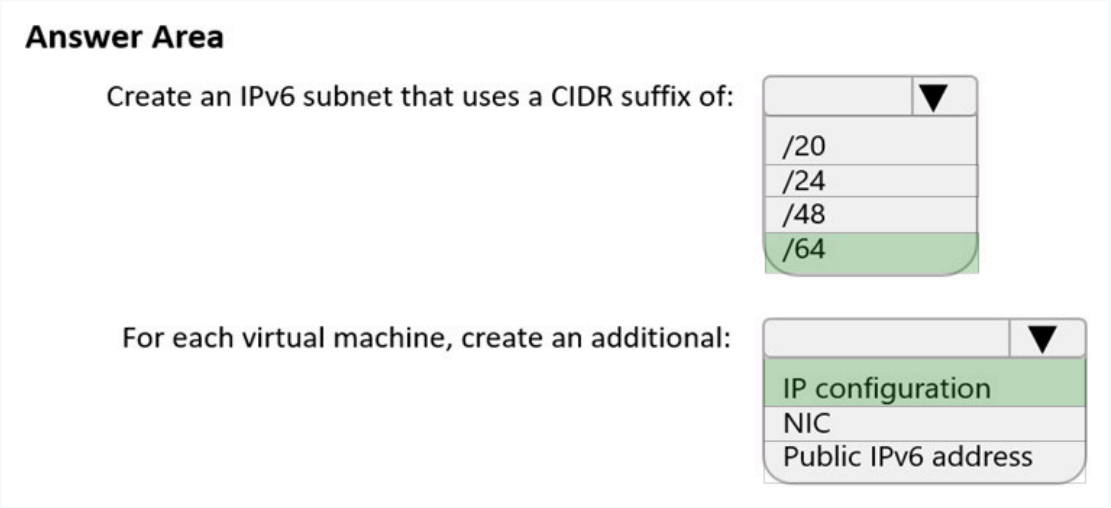
upvoted 2 times

Question #6 *Topic 2*

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:



Suggested Answer:



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 5 years 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 31 times

Wesgo Highly Voted 5 years 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-powershellYour 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.The correct answer was even embedded in his powershell script "Add-AzNetworkInterfaceIpConfig" Implying IP Configurations at the NIC level.I didnt understand. how can public ipv6 be correct. It is IP configuration as per your explanation as well

upvoted 31 times

Windows98 5 years 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.The correct answer was even embedded in his powershell script "Add-AzNetworkInterfaceIpConfig" Implying IP Configurations at the NIC level.

upvoted 8 times

Windows98 5 years 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 8 times

sleekdunga 4 years, 9 months ago

The correct answer was even embedded in his powershell script "Add-AzNetworkInterfaceIpConfig" Implying IP Configurations at the NIC level.

upvoted 6 times

ian2387 4 years, 7 months ago

I didnt understand. how can public ipv6 be correct. It is IP configuration as per your explanation as well

upvoted 7 times

jelley 5 years 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 20 times

40a4d4c Most Recent 7 months, 3 weeks ago

/64 IP configuration - {Public IPv6 Not required for internal communication}

upvoted 1 times

Zorro2003 1 year, 2 months ago

Answer: Create an IPv6 subnet with CIDR: /64 For each virtual machine, create an additional: IP configuration Why: In Azure, IPv6 subnets must use a /64 prefix. To give a VM an IPv6 private address on a dual-stack subnet, you add an additional IPv6 IP configuration to its NIC (no extra NIC or public IPv6 is needed), which also avoids allocating extra IPv4 addresses.

upvoted 6 times

ZQasqas 2 years, 2 months ago

First question is: /64 https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/ipv6-overview Second question is: IP configurations Add IPv6 configuration to virtual machine: https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/add-dual-stack-ipv6-vm-portal?tabs=azureportal#add-ipv6-configuration-to-virtual-machine

upvoted 2 times

_Cris 3 years, 1 month ago

appears on exam, 19 Sept 2023

upvoted 2 times

Billabongs 3 years, 4 months 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 3 years, 9 months 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 exsisting one that uses the old subnet

upvoted 1 times

LeonTH 3 years, 9 months ago

maledetti

upvoted 5 times

liono 3 years, 10 months ago

Given answers are correct!

upvoted 1 times

yamapan 3 years, 11 months ago

URL is outdated; this islatest https://learn.microsoft.com/en-US/azure/load-balancer/ipv6-add-to-existing-vnet-powershell

upvoted 2 times

HasanHHH 4 years, 1 month 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 7 times

Pradh 4 years, 2 months ago

100% CORRECT ANSWER : /64 & IP Configuration .

upvoted 6 times

Pradh 4 years, 2 months ago

100% CORRECT ANSWER : /64 & IP Configuration .100% unhelpful comment

upvoted 6 times

sapien45 4 years, 1 month ago

100% unhelpful comment

upvoted 24 times

hogs 4 years, 3 months ago

Appeared on exam Aug2022

upvoted 3 times

1particle 4 years, 3 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 7 times

unclegrandfather 4 years, 4 months ago

Appeared on exam 6/28/22

upvoted 2 times

kogunribido 4 years, 4 months ago

Appeared on exam 6/27/2022

upvoted 2 times

Question #7 *Topic 2*

HOTSPOT -

You plan to deploy Azure Virtual WAN.

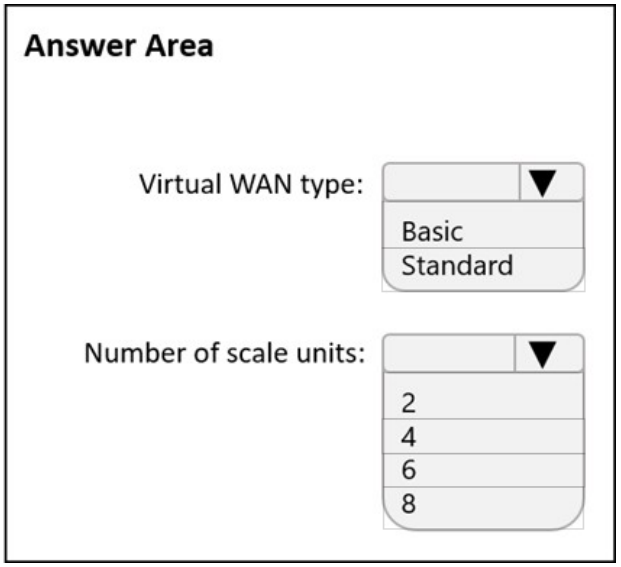
You need to deploy a virtual WAN hub that meets the following requirements:

- ✑ 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

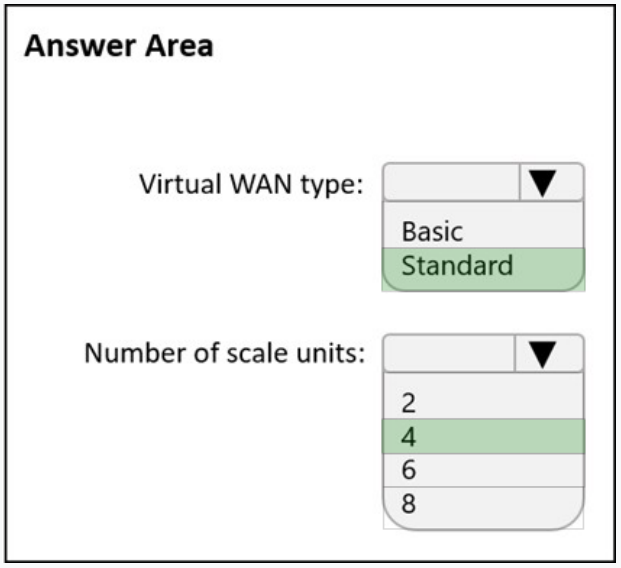
What should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Suggested Answer:



Reference: https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about

Bharat Highly Voted 4 years, 1 month 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-architecturehttps://www.azure.cn/en-us/pricing/details/virtual-wan/

upvoted 45 times

Bharat Highly Voted 4 years, 1 month 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 45 times

Mirek 4 years, 1 month ago

https://www.azure.cn/en-us/pricing/details/virtual-wan/

upvoted 7 times

walkwolf3 4 years 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 33 times

walkwolf3 4 years 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-architectureGreat link !

upvoted 33 times

sapien45 3 years, 1 month ago

Great link !

upvoted 2 times

Lazylinux Most Recent 2 years ago

Given answer is correct

upvoted 3 times

Techbiz 2 years, 1 month ago

The given answer is correct, Basic WANs don't support expressroutes

upvoted 1 times

raffykian 2 years, 2 months ago

this is on my exam today 8/23

upvoted 1 times

daemon101 2 years, 4 months 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 2 years, 4 months 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-faqI 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

daemon101 2 years, 4 months 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 2 years, 5 months ago

Correct Answer : :: Standard :: 4

upvoted 1 times

DeepMoon 2 years, 11 months 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.Each scale unit represents 500Mbps of VPN throughput.ER Scale units are 2GBps, 500Mbps is for P2S & S2S.https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-faq#what-are-virtual-wan-gateway-scale-units

upvoted 1 times

DeepMoon 2 years, 11 months 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

khanda 2 years, 7 months ago

Each scale unit represents 500Mbps of VPN throughput.ER Scale units are 2GBps, 500Mbps is for P2S & S2S.

upvoted 1 times

khanda 2 years, 7 months ago

Each scale unit represents 500Mbps of VPN throughput.

upvoted 1 times

GBAU 2 years ago

ER Scale units are 2GBps, 500Mbps is for P2S & S2S.

upvoted 1 times

charrua86 2 years, 3 months ago

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

upvoted 1 times

HasanHHH 3 years, 1 month 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 3 years, 3 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 3 years, 3 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 3 years, 3 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 3 years, 8 months ago

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

upvoted 1 times

KranthiChaitanya 3 years, 9 months ago

Came on exam 28/Jan/22

upvoted 1 times

Acrophat 4 years ago

ExpressRoute gateways are provisioned in units of 2 Gbps. 1 scale unit = 2 Gbps with support up to 10 scale units = 20 Gbps.
https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-expressroute-portal#hub

upvoted 4 times

Wesgo 4 years ago

1) Of course Standard. Basic does not support ExpressRoute. 2) ExpressRoute Scale Unit3 $0.42/hour 2 Gbps per Scale Unit
https://azure.microsoft.com/en-us/pricing/details/virtual-wan/

upvoted 6 times

WorkHardBeProud 4 years 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-unitsYes the first answer is indeed Standard as it needs to support Express route. But for the Scale unit I don't this we are talking about ExpressRoute but Azure WAN, then it should be 8 to support 8gbps. Link where you can find AzWan Scale Units / Traffic: https://learn.microsoft.com/en-us/azure/virtual-wan/hub-settings

upvoted 5 times

WorkHardBeProud 4 years 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 5 times

_fvt 2 years, 7 months ago

Yes the first answer is indeed Standard as it needs to support Express route. But for the Scale unit I don't this we are talking about ExpressRoute but Azure WAN, then it should be 8 to support 8gbps. Link where you can find AzWan Scale Units / Traffic: https://learn.microsoft.com/en-us/azure/virtual-wan/hub-settings

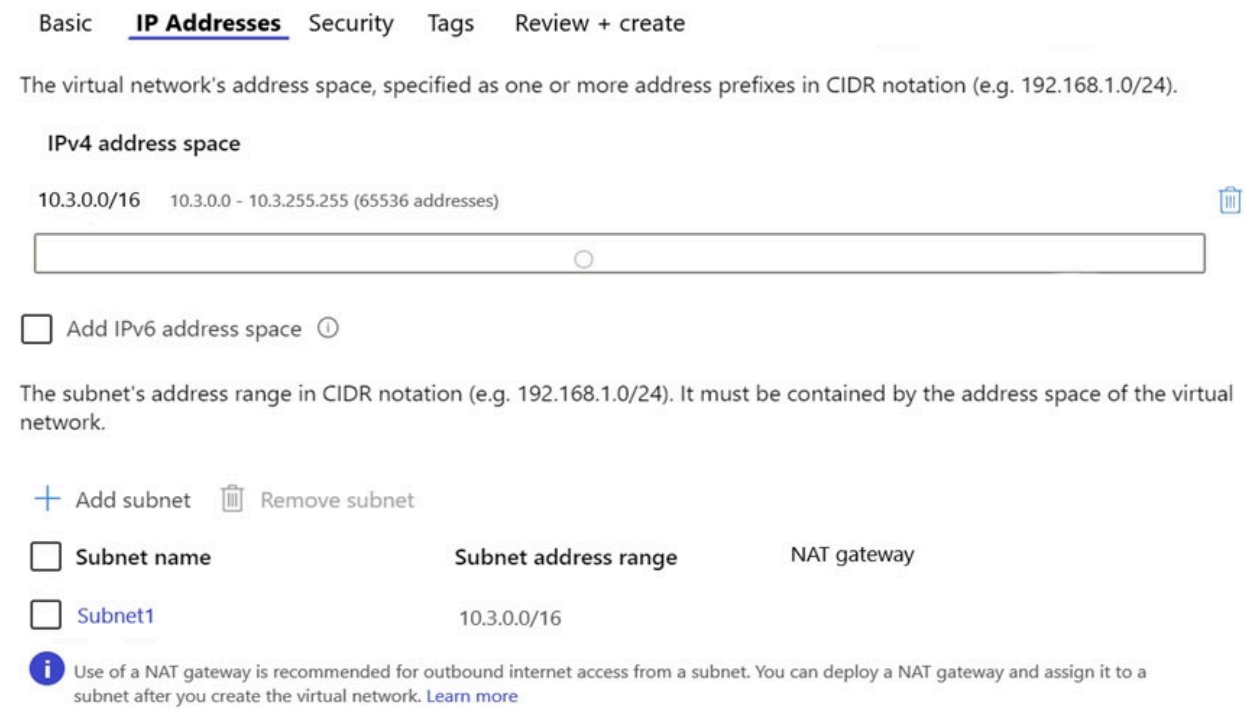
upvoted 1 times

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

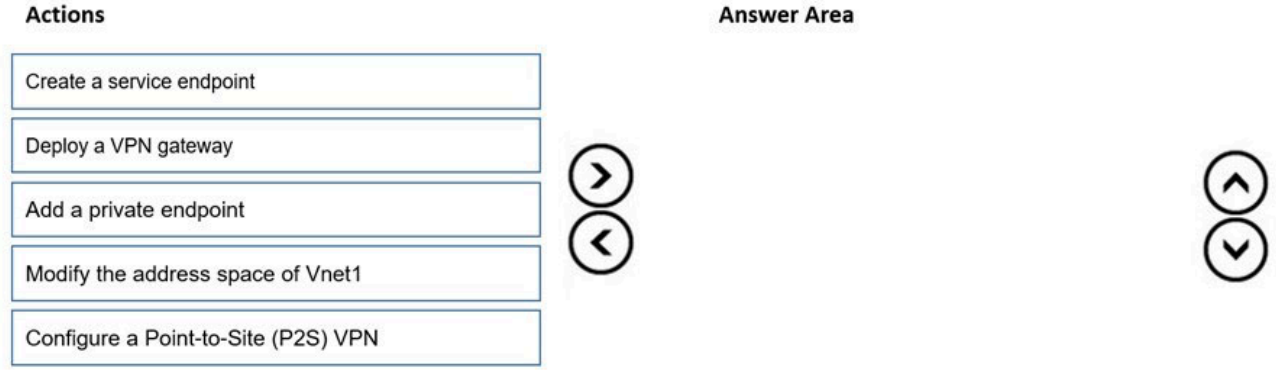
The IP Addresses settings for Vnet1 are configured as shown in the exhibit.



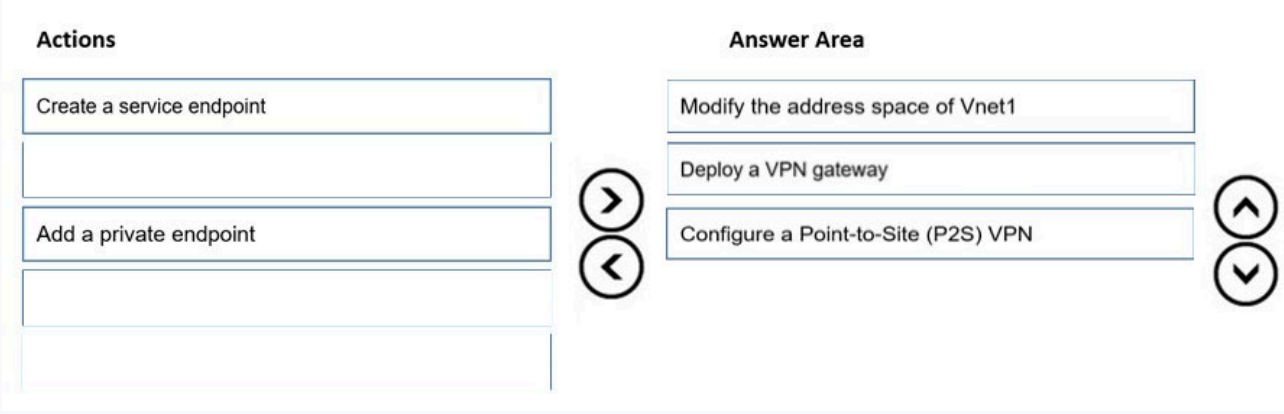
You need to ensure that you can integrate WebApp1 and Vnet1.

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:



Suggested Answer:



Reference: https://docs.microsoft.com/en-us/azure/app-service/web-sites-integrate-with-vnet#gateway-required-vnet-integration

tkoutanis Highly Voted 4 years 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 59 times

tkoutanis Highly Voted 4 years 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-integrationNew Link --> https://learn.microsoft.com/en-us/azure/app-service/configure-gateway-required-vnet-integration

upvoted 59 times

beskar Most Recent 1 year, 5 months ago

New Link --> https://learn.microsoft.com/en-us/azure/app-service/configure-gateway-required-vnet-integration

upvoted 1 times

walkwolf3 4 years 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 17 times

Lazylinux 2 years 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-integrationthis is the future and hence question maybe too old now https://learn.microsoft.com/en-us/azure/app-service/overview-vnet-integration

upvoted 3 times

Lazylinux 2 years 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 3 times

Lazylinux 2 years 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 3 times

homer_simpson 2 years, 1 month 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 3 times

bp_a_user 2 years, 1 month ago

The provided link https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration#gateway-required-vnet-integratio seems not to mention VPN? Is the question outdated?

upvoted 1 times

azure_2563 2 years, 3 months ago

Guy's any video is available to this problem?

upvoted 1 times

tester2023 2 years, 9 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 6 times

AdityaGupta 3 years, 2 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 4 times

1particle 3 years, 3 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 3 years, 3 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

derrrp 3 years, 3 months ago

Remember: Modify the VNET so you can add the VPN. Add the VPN. Then configure it.

upvoted 6 times

unclegrandfather 3 years, 4 months ago

Appeared on exam 6/28/22

upvoted 1 times

ash21 3 years, 5 months ago

The mentioned answer is correct, https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration.

upvoted 1 times

Stanley3427 3 years, 5 months ago

the answer is 413, this question will not use vpn services

upvoted 2 times

petermogaka91 3 years, 6 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 3 years, 7 months ago

The answers are correct. Virtual network integration doesn't enable your apps to be accessed privately.

upvoted 1 times

WorkHardBeProud 4 years ago

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-vnet-integration

upvoted 1 times

Question #9 *Topic 2*

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.

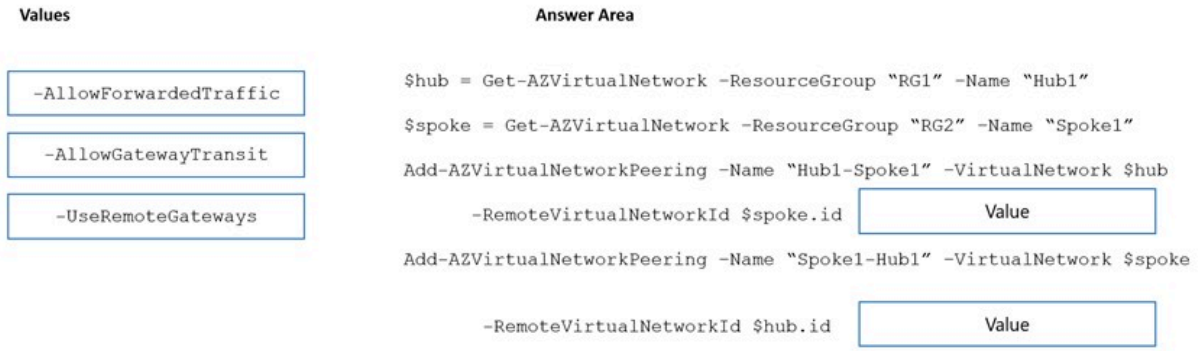
You are implementing peering between Hub1 and Spoke1.

You need to ensure that a virtual machine connected to Spoke1 can connect to the on-premises network through Hub1.

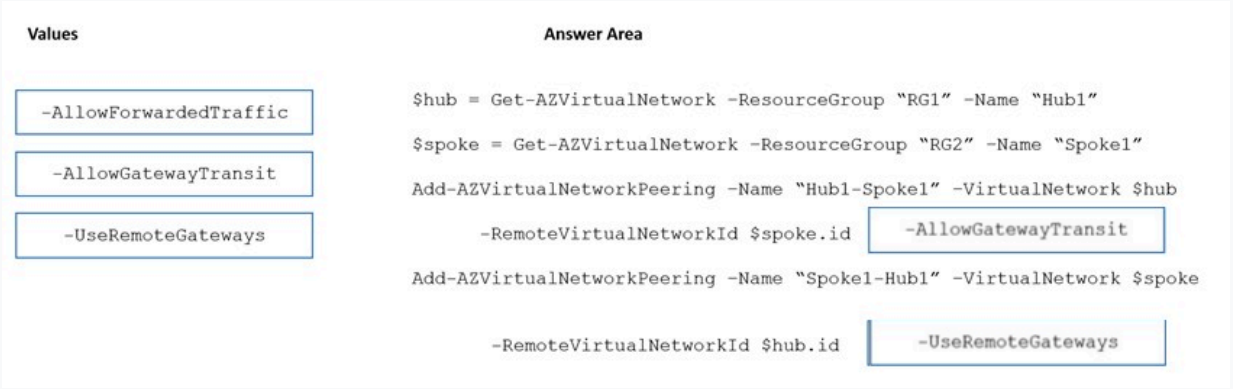
How should you complete the PowerShell script? To answer, drag the appropriate values to the correct targets. Each value may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Suggested Answer:



Reference: https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke?tabs=cli#virtual-network-peering

Bharat Highly Voted 4 years, 7 months ago

The answer is correct. However, this is a better reference: https://docs.microsoft.com/en-us/azure/firewall/tutorial-hybrid-ps

upvoted 31 times

Bharat Highly Voted 4 years, 7 months ago

The answer is correct. However, this is a better reference: https://docs.microsoft.com/en-us/azure/firewall/tutorial-hybrid-psFrom 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 -UseRemoteGatewaysNo, 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 31 times

jeepTango123456 3 years, 9 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 -UseRemoteGatewaysNo, 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 9 times

jeepTango123456 3 years, 9 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 9 times

MrBlueSky 3 years, 1 month 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 3 times

walkwolf3 4 years, 6 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 22 times

kikocu 2 years, 4 months 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-transitThis URL is the best

upvoted 5 times

kikocu 2 years, 4 months 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 5 times

RabbitB Most Recent 1 year, 12 months ago

This URL is the best

upvoted 2 times

Sant25 2 years, 4 months 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 2 times

Lazylinux 2 years, 6 months ago

Given answer is correct AT Hub side, we AllowGatewayTransit AT Spoke side, we need UseRemoteGateway

upvoted 1 times

MikeSA 2 years, 11 months ago

Confusing because the second part could be either allowforwarded or useremotegateways. Seems to be missing one of the options. # Peer spoke to hub Add-AzVirtualNetworkPeering -Name SpoketoHub -VirtualNetwork $VNetSpoke -RemoteVirtualNetworkId $VNetHub.Id -AllowForwardedTraffic -UseRemoteGateways

upvoted 2 times

Himank20 3 years 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 3 years, 3 months 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

sapien45 3 years, 7 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 3 years, 8 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 3 times

derrrp 3 years, 9 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 4 years, 1 month ago

The answers are correct.

upvoted 1 times

jj22222 4 years, 1 month ago

on test April 10 2022

upvoted 1 times

Joshalom 4 years, 3 months ago

on exam 6/2/2022

upvoted 1 times

Joshalom 4 years, 3 months ago

on exam 28/1/2022

upvoted 1 times

Takloy 4 years, 4 months 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

prepper666 4 years, 6 months ago

Are these the wrong way around? $hub.id should allow gateway transit and $spoke.id should use remote gateway.

upvoted 5 times

prepper666 4 years, 6 months ago

Are these the wrong way around? $hub.id should allow gateway transit and $spoke.id should use remote gateway.I think, ExamTopics answer is correct onlyI thought that as well, but we have to pay attention to the PS command. On the 1st box we are creating the peering on the Hub VNET which will have the Allow Gateway In Transit Enabled. On the 2nd box we are creating the peering on the Spoke VNET which needs to Use the Remote Gateway.

upvoted 5 times

yokoka2259 4 years, 6 months ago

I think, ExamTopics answer is correct only

upvoted 1 times

DatBroNZ 4 years, 5 months ago

I thought that as well, but we have to pay attention to the PS command. On the 1st box we are creating the peering on the Hub VNET which will have the Allow Gateway In Transit Enabled. On the 2nd box we are creating the peering on the Spoke VNET which needs to Use the Remote Gateway.

upvoted 6 times

Question #10 *Topic 2*

DRAG DROP -

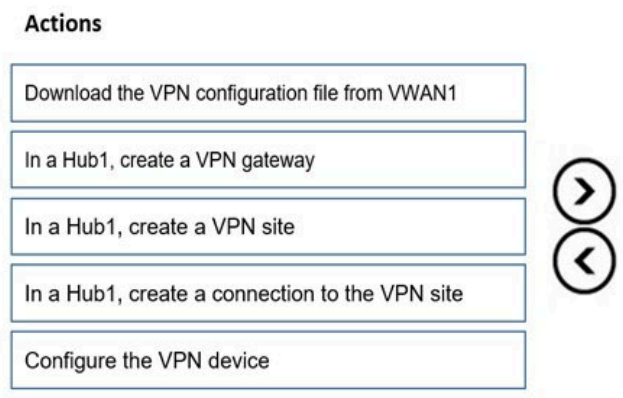
You have three on-premises sites. Each site has a third-party VPN device.

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.

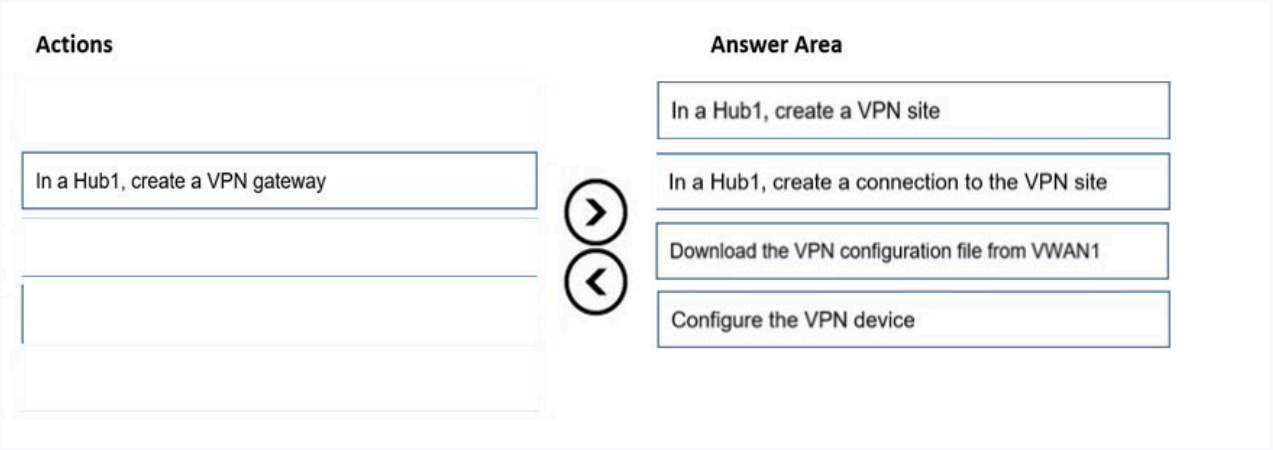
You need to connect the third site to the other two sites by using Hub1.

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:



Suggested Answer:



Reference: https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-site-to-site-portal

derrrp Highly Voted 3 years, 3 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 65 times

derrrp Highly Voted 3 years, 3 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.your way of explaining stuff is so funny but I it thx (^_^)

upvoted 65 times

Stevy_nash 2 years, 10 months ago

your way of explaining stuff is so funny but I it thx (^_^)

upvoted 3 times

srikanth1987 4 years ago

Answer is correct. As already two VPN S2S are formed, means that, VGW is there.

upvoted 40 times

srikanth1987 4 years ago

Answer is correct. As already two VPN S2S are formed, means that, VGW is there.You're right.Right!

upvoted 40 times

Takloy 3 years, 3 months ago

You're right.

upvoted 1 times

jeffangel28 3 years, 3 months ago

Right!

upvoted 1 times

Zorro2003 Most Recent 1 year, 2 months ago

Order (top → bottom): In Hub1, create a VPN site In Hub1, create a connection to the VPN site Download the VPN configuration file from vWAN1 Configure the VPN device Reason: Hub1 already has a VPN gateway (it connects two sites). To add the third site, define it as a VPN site, create a connection from the hub to that site, then download the config and apply it to the on-premises VPN device.

upvoted 1 times

Techbiz 2 years, 1 month 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

Rajan395 2 years, 9 months ago

Correct Answer

upvoted 1 times

sujay1982 3 years, 2 months ago

Right Answer

upvoted 2 times

GGbis 3 years, 4 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 3 years, 8 months ago

On exam 3/3/2022

upvoted 4 times

rockethack 3 years, 8 months ago

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

upvoted 4 times

KranthiChaitanya 3 years, 9 months ago

Came on exam 28/Jan/22

upvoted 2 times

AidenYoukhana 3 years, 10 months ago

CORRECT ANSWER.

upvoted 2 times

JoMa 3 years, 11 months ago

Correct answer

upvoted 4 times

Question #11 *Topic 2*

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

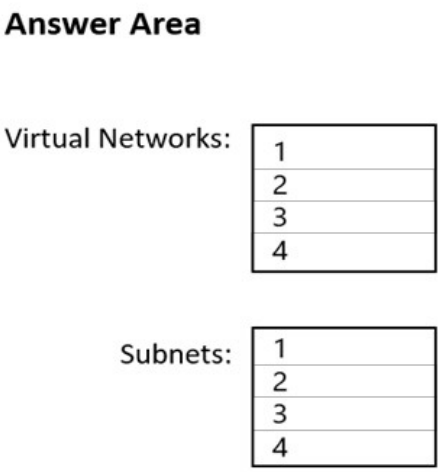
App Service and SQL Managed Instance will be delegated to create resources in virtual networks.

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.

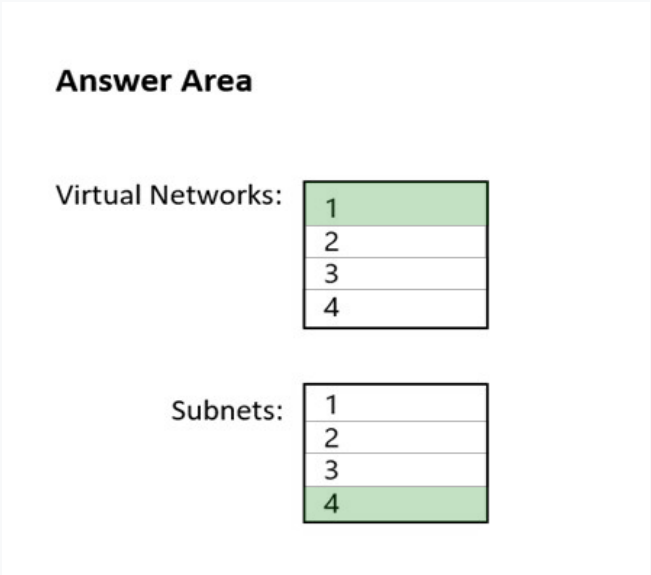
What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Suggested Answer:



Reference: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-for-azure-services#services-that-can-be-deployed-into-a-virtual-network

prepper666 Highly Voted 4 years, 6 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.you better get some experience before shouting so loud lolWrong. An app service needs its own dedicated subnet. Web API Management-Dedicated Subnet-Yes Web Apps-Dedicated Subnet-Yes App Service Environment-Dedicated Subnet-Yes Azure Logic Apps-Dedicated Subnet-YesFor Azure WebApp, we need to add webapp-integration subnet. https://docs.microsoft.com/en-us/azure/app-service/networking/nat-gateway-integrationApp service needs Vnet -> "App Service (...) will be delegated to create resources in virtual networks."

upvoted 17 times

prepper666 Highly Voted 4 years, 6 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 17 times

Ajdlfasudfo0 3 years, 5 months ago

you better get some experience before shouting so loud lol

upvoted 3 times

HasanHHH 3 years, 7 months ago

Wrong. An app service needs its own dedicated subnet. Web API Management-Dedicated Subnet-Yes Web Apps-Dedicated Subnet-Yes App Service Environment-Dedicated Subnet-Yes Azure Logic Apps-Dedicated Subnet-Yes

upvoted 1 times

leonmflai4exam 4 years, 2 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

volto 2 years, 8 months ago

App service needs Vnet -> "App Service (...) will be delegated to create resources in virtual networks."

upvoted 1 times

Madball 4 years 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 11 times

87aef5e Most Recent 7 months, 1 week ago

1 VNet and 3 Subnets

upvoted 1 times

nhr2 1 year, 10 months ago

Virtual Network: All resources can share a single virtual network to minimize costs. Subnets: Subnet 1: For the Virtual Machine. Subnet 2: For the Azure App Service (delegated for App Service resources). Subnet 3: For the Virtual Network Gateway (GatewaySubnet). Subnet 4: For the Azure SQL Managed Instance (delegated for SQL resources).

upvoted 1 times

NSF2 2 years, 4 months 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 3 years, 2 months 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 3 years, 2 months 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)I like that!

upvoted 2 times

Libaax01 3 years, 2 months 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 2 times

RabbitB 1 year, 12 months ago

I like that!

upvoted 1 times

Rajan395 3 years, 3 months ago

Given answer is correct.

upvoted 1 times

sapien45 3 years, 7 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 3 years, 8 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 3 years, 9 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 3 years, 10 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 3 years, 12 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

bmulvIT 4 years, 2 months ago

On exam today 3/3/2022

upvoted 1 times

rockethack 4 years, 2 months ago

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

upvoted 1 times

Beitran 4 years, 2 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

TonytheTiger 4 years, 4 months ago

On the Exam 01/14/2022

upvoted 3 times

Question #12 *Topic 2*

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

Suggested 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%)

ajinkyap Most Recent 2 years, 4 months ago
Selected Answer: A
correct ans
upvoted 1 times

Verytutos 3 years, 2 months ago
Appeared on Exam 05 Sep 2023
upvoted 1 times

Rajan395 3 years, 9 months ago
Given answer is correct
upvoted 1 times

yyts 4 years, 1 month ago
Does Windows10 work with IKEv2 P2S VPN?
upvoted 2 times

jilguens 4 years, 2 months ago
Selected Answer: A
right a
upvoted 1 times

d0bermannn Highly Voted 4 years, 9 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 12 times

AckeyGraham 4 years, 9 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 4 years, 9 months ago
correct....on exam 28/1/2022
upvoted 1 times

AidenYoukhana 4 years, 10 months ago

CORRECT ANSWER.

upvoted 1 times

Cova16 4 years, 12 months ago

correct

upvoted 1 times

prepper666 5 years ago

Agreed. Initial config was downloaded before vNet1 and vNet2 were peered.

upvoted 1 times

Sbgani 5 years ago

correct

upvoted 4 times

Question #13 *Topic 2*

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.

Suggested Answer: *C, D*
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%)

CristianM99 Most Recent 2 years, 3 months ago
Selected Answer: CD
C and D
upvoted 2 times

Whatsamattr81 Highly Voted 3 years, 5 months ago
C and D... whilst E looks correct, it isnt 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, id probably skip the dns proxy stuff and just put forwarders in but the question and possible answers don't mention that scenario.
upvoted 10 times

Whatsamattr81 3 years, 5 months ago
C and D... whilst E looks correct, it isnt 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, id probably skip the dns proxy stuff and just put forwarders in but the question and possible answers don't mention that scenario.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 10 times

AzureLearner01 2 years, 8 months 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 3 years, 1 month 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 3 years, 2 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 foward 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 you 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 conficure your on-prem DNS server with forwarder to Azure DNS VM.

upvoted 7 times

erima21 Highly Voted 3 years, 2 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 17 times

Takloy 3 years, 3 months ago

Can someone explain why the answers are CD?

I thought E would be one of the answers.

upvoted 2 times

john6732 3 years, 3 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 3 years, 4 months ago

A version of this question appeared on the exam. Make sure you know WHY these are correct

upvoted 2 times

kinder2 3 years, 5 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 3 years, 5 months ago

Selected Answer: CD

C and D are correct.

upvoted 4 times

MrBlueSky 2 years, 7 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

mdnick 3 years, 6 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 3 years, 6 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 3 years, 6 months ago

A & E would be better options?

upvoted 2 times

jkklim 3 years, 6 months ago

ae - the answer

upvoted 1 times

jamelia1303 3 years, 7 months ago

better explanation : https://azure.microsoft.com/en-us/blog/new-enhanced-dns-features-in-azure-firewall-now-generally-available/

upvoted 2 times

Question #14 *Topic 2*

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

Suggested Answer: *A*
Reference: https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview

Community vote distribution
A (100%)

SOMINAZURE Highly Voted 2 years, 2 months ago
Selected Answer: A
yes correct
upvoted 6 times

sellamibassem 2 years, 2 months ago
A is correct
upvoted 1 times

Rajan395 2 years, 3 months ago
A is correct for sure
upvoted 1 times

degiro 2 years, 6 months ago
Selected Answer: A
Answer is correct.
upvoted 1 times

Prutser2 2 years, 7 months ago
Selected Answer: A
for sure
upvoted 1 times

Jawad1462 2 years, 7 months ago
Selected Answer: A
Answer is correct A
upvoted 1 times

Alessandro365 2 years, 8 months ago
Selected Answer: A
A, correct answer
upvoted 1 times

AdityaGupta 2 years, 8 months ago
Selected Answer: A
Undoubtly A, Internal Load Balancer.
upvoted 1 times

naidu 2 years, 8 months ago
Yes Correct answer
upvoted 2 times

Villaran 2 years, 8 months ago
Selected Answer: A
A. internal load balancers
upvoted 2 times

HOTSPOT -

You have an Azure subscription.

You have the on-premises sites shown the following table.

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:

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

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

Suggested 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 3 years, 8 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 17 times

raffykian Most Recent 2 years, 8 months ago

on exam 8-23

upvoted 2 times

omgMerrick 3 years, 3 months ago

Given answer is correct. https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about#basicstandard

upvoted 4 times

Rajan395 3 years, 3 months ago

Answer is correct. Basic sku supports Site-to-Site only

upvoted 3 times

Jawad1462 3 years, 7 months ago

That's correct

upvoted 3 times

fun_and_games 3 years, 8 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 3 years, 8 months ago

This is correct.

upvoted 3 times

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.

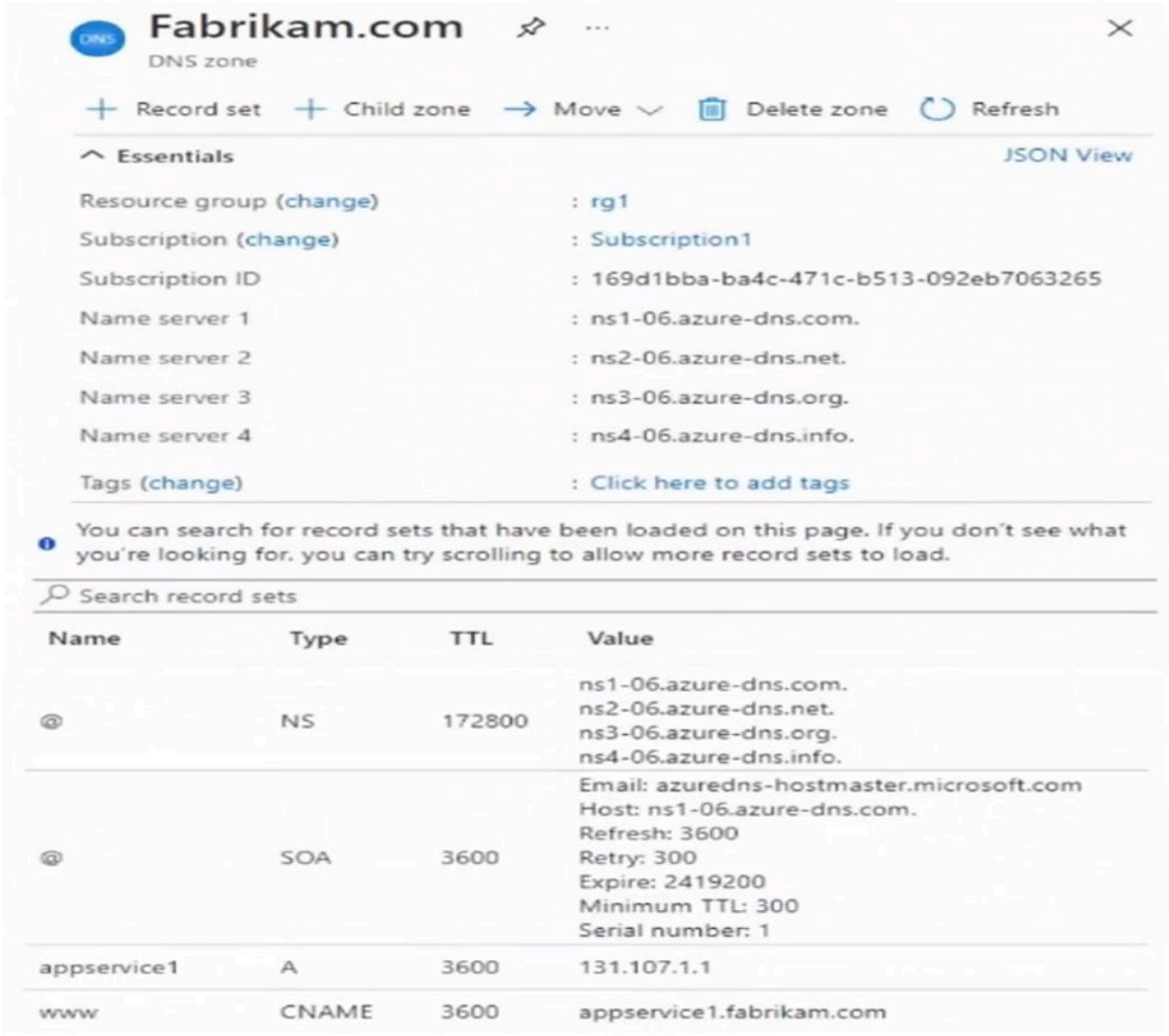
You have a private DNS zone named fabrikam.com. The zone is configured as shown in the Private DNS Zone exhibit.

You have a virtual network link configured as shown in the Virtual Network Link 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:


Fabrikam.com
DNS zone
Record set
Child zone
Move
Delete zone
Refresh
Essentials
JSON View
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
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
@ 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

Fabrikam.com

Private DNS zone

+ Record set → Move 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

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

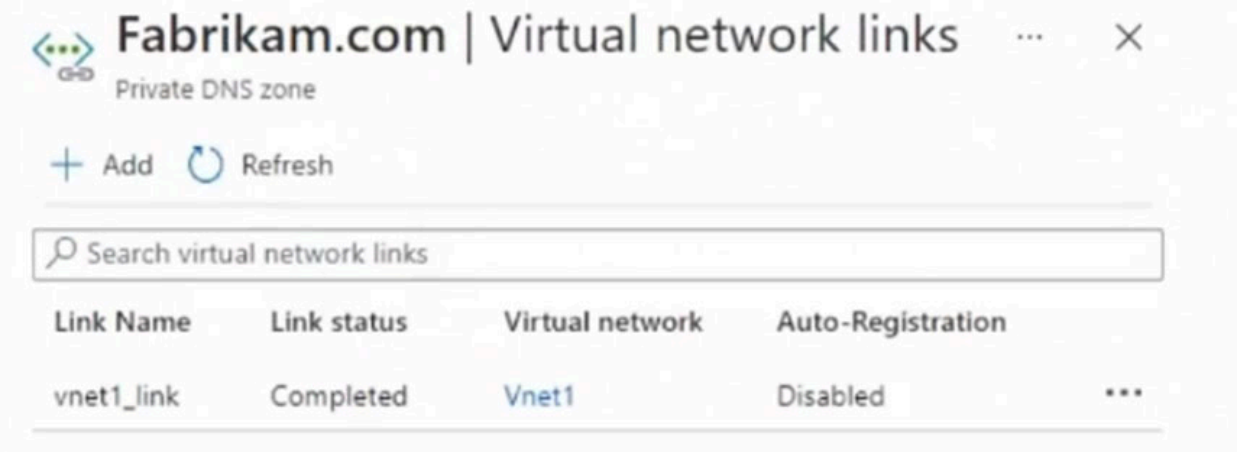
Subscription ID : 169d1bba-ba4c-471c-b513-092eb7063265

Tags (change) : Click here to add tags

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



Answer Area

Statements	Yes	No
Queries for www. fabrikam.com from the internet are resolved to 131.107.1.1.	○	○
Queries for server1.fabrikam.com can be resolved from the internet.	○	○
Queries for www. fabrikam.com from Vnet2 are resolved to 131. 107.100. 10.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
Queries for www. fabrikam.com from the internet are resolved to 131.107.1.1.	○	○
Queries for server1.fabrikam.com can be resolved from the internet.	○	○
Queries for www. fabrikam.com from Vnet2 are resolved to 131. 107.100. 10.	○	○

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 3 years, 2 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 40 times

wsrudmen Highly Voted 3 years, 6 months ago

CORRECT!!

upvoted 13 times

Techbiz Most Recent 2 years, 1 month ago

Answer and explanation given are correct

upvoted 1 times

_fvt 2 years, 7 months 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 Shoud 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 2 years, 9 months ago

absolutely correct.

upvoted 1 times

DeepMoon 2 years, 10 months 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 3 times

DeepMoon 2 years, 10 months 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.Look carefully there's a host-A record for appservice1 in Public DNS Zone.

upvoted 3 times

Skankhunt 2 years, 9 months ago

Look carefully there's a host-A record for appservice1 in Public DNS Zone.

upvoted 6 times

Prutser2 3 years, 1 month ago

correct,

upvoted 1 times

jeffangel28 3 years, 3 months ago

Given answer and explanation is correct

upvoted 2 times

Question #17 *Topic 2*

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

Suggested 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 4 years, 5 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 43 times

pinchocr Highly Voted 4 years, 5 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 subnetIt is correct, 3 different subnets are needed for each availability zone and vnet since the premise is that in case of failure of 2 zones, the APPs continue working.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 eeach Vnet/subnet).. and because NAT GW is zonal, we will have to multiply that by 3 = 6 NAT GW 2 subnets/ 6 NAT GWCorrection: 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-gatewayThis 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.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 43 times

Gambito11 1 year, 11 months ago

It is correct, 3 different subnets are needed for each availability zone and vnet since the premise is that in case of failure of 2 zones, the APPs continue working.

upvoted 1 times

Komy 4 years, 4 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 eeach Vnet/subnet).. and because NAT GW is zonal, we will have to multiply that by 3 = 6 NAT GW 2 subnets/ 6 NAT GWCorrection: 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-gatewayThis 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 11 times

Komy 4 years, 4 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 eeach 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 11 times

Komy 4 years, 4 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 32 times

Komy 4 years, 4 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-gatewayThis 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 32 times

john6732 4 years, 4 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 8 times

sapien45 4 years, 1 month 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 4 times

Jorex 4 years, 6 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 23 times

Jorex 4 years, 6 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)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-resiliency1 subnet can have only 1 nat gateway, so 6 subnets are required for 6 nat gateway.Multiple NAT gateways can't be attached to a single subnet.You cant attach multiple NAT gateways to a single subnet.

upvoted 23 times

Goofer 3 years, 10 months 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

Arkadeep 4 years, 4 months ago

1 subnet can have only 1 nat gateway, so 6 subnets are required for 6 nat gateway.

upvoted 11 times

Sanaz90 4 years, 2 months ago

Multiple NAT gateways can't be attached to a single subnet.

upvoted 3 times

khanda 3 years, 7 months ago

You cant attach multiple NAT gateways to a single subnet.

upvoted 1 times

MarkMac Most Recent 11 months, 1 week ago

2 subnets / 2 NGWs. To support outgoing Internet traffic over the NGW during a zonal failure, the NGW would have to Standard V2. Exam Q doesn't specify, but should.

upvoted 2 times

Zorro2003 1 year, 2 months ago

Minimum number of subnets: 2 Minimum number of Virtual Network NAT instances: 2 Why: Subnets aren't zonal—one subnet can contain VMs in all three AZs. So each VNet needs only one subnet for its 12 VMs → 2 subnets total (one per VNet). A NAT gateway is scoped to a VNet and can't be shared across VNets. To keep outbound connectivity for both App1 (VNet1) and App2 (VNet2) even during zone failures, deploy a zone-redundant NAT gateway per VNet → 2 NAT gateways.

upvoted 1 times

windowsmodulesinstallerworker 1 year, 5 months ago

its 6 and 6 every zone has to have a nat gateway and a subnet

https://azure.microsoft.com/en-us/blog/ensure-zone-resilient-outbound-connectivity-with-nat-gateway/

upvoted 2 times

windowsmodulesinstallerworker 1 year, 5 months ago

its 6 and 6 every zone has to have a nat gateway and a subnet https://azure.microsoft.com/en-us/blog/ensure-zone-resilient-outbound-connectivity-with-nat-gateway/This is correct, whey you create de NAT Gateway you have to choose the zone, in this case 3 resources per zone and per vnet. 6 in total.

upvoted 2 times

cassucena 1 year ago

This is correct, whey you create de NAT Gateway you have to choose the zone, in this case 3 resources per zone and per vnet. 6 in total.

upvoted 1 times

Nagachn 1 year, 6 months ago

May i know the final correct answer?

upvoted 1 times

manhattan 2 years ago

answers given are correct! this is a tricky, questions, it is not asking to span the subnet among regions but among availability zones! look here: 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. https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview#virtual-networks-and-availability-zones

upvoted 3 times

thekhijir 2 years ago

Each virtual network (VNet1 and VNet2) should have at least one subnet per application. Azure Virtual Network NAT (NAT gateway) operates at the subnet level, and for each subnet, you can associate a NAT gateway. You don't need a separate subnet for each availability zone, because the subnets themselves span all availability zones. Therefore: You need one subnet for VNet1 for App1. You need one subnet for VNet2 for App2. To ensure availability in case two zones fail, you need to deploy one NAT gateway per virtual network. Azure NAT gateways are zone-redundant by default, meaning that a single NAT gateway can span multiple zones and provide high availability across all the zones in a region. You need one NAT gateway for VNet1 (App1). You need one NAT gateway for VNet2 (App2). Total: 2 NAT gateways (1 per VNet).https://azure.microsoft.com/en-us/products/azure-nat-gateway/#faq Assign your NAT gateway resource to one or more subnets in a virtual network and add at least one public IP address or prefix.So one nat can have more relevant subnets.Are you sure a subnet can span all availability zones ? First time I read it The subnet is created in only one availabiliy zone, it's a non-zonal redudant resource, that's the basement to set 3 subnets and one subnet in every availabity zone

upvoted 6 times

thekhijir 2 years ago

Each virtual network (VNet1 and VNet2) should have at least one subnet per application. Azure Virtual Network NAT (NAT gateway) operates at the subnet level, and for each subnet, you can associate a NAT gateway.

You don't need a separate subnet for each availability zone, because the subnets themselves span all availability zones. Therefore:

You need one subnet for VNet1 for App1. You need one subnet for VNet2 for App2.

To ensure availability in case two zones fail, you need to deploy one NAT gateway per virtual network. Azure NAT gateways are zone-redundant by default, meaning that a single NAT gateway can span multiple zones and provide high availability across all the zones in a region.

You need one NAT gateway for VNet1 (App1). You need one NAT gateway for VNet2 (App2). Total: 2 NAT gateways (1 per VNet).

upvoted 6 times

NK203 1 year, 11 months ago

https://azure.microsoft.com/en-us/products/azure-nat-gateway/#faq Assign your NAT gateway resource to one or more subnets in a virtual network and add at least one public IP address or prefix.So one nat can have more relevant subnets.

upvoted 1 times

Feliphus 2 years ago

Are you sure a subnet can span all availability zones ? First time I read it The subnet is created in only one availabiliy zone, it's a non-zonal redudant resource, that's the basement to set 3 subnets and one subnet in every availabity zone

upvoted 1 times

DGriff 2 years, 4 months ago

This is a quote from the guide "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." In this case, there are two different availability zones. Each zone has a NAT gateway mapping VMs (subnets) from both zones (resiliency; availability). Thus, if one zone gateway fails, the other zone NAT provides outbound connectivity for VMs in the down zone.

upvoted 1 times

AlainChk 2 years, 4 months ago

In my opinion, we may also deploy one subnet spanning 3 zones, and one nonzonal NAT gateway per application. So in total 2 subnets and 2 nonzonal NAT Gateways. Quote from Azure: If no zone is selected at the time that the NAT gateway resource is deployed, the NAT gateway is placed in no zone by default. When NAT gateway is placed in no zone, Azure places the resource in a zone for you. There isn't visibility into which zone Azure chooses for your NAT gateway. After NAT gateway is deployed, zonal configurations can't be changed. No zone NAT gateway resources, while still zonal resources can be associated to public IP addresses from a zone, no zone, or that are zone-redundant.

upvoted 1 times

p7vpki7qz 2 years, 4 months ago

A] 3 subnets in VNet1, one for each availability zone. Same for VNet2. So total is 6. B] 1 NAT gateway for VNet1 that is zone-redundant, covering all three subnets/zones. Same for VNet2. So 2 in total.

upvoted 1 times

RemmyT 2 years, 6 months ago

The optimal solution : 6 subnets & 3 NAT Gateways (vnet1 & vnet 2 are in the same region). 1. NAT Gateway has high availability only into one zone 2. If the zone that goes down is also the zone in which NAT gateway has been deployed then all outgoing traffic from virtual machines across all zones will be blocked. 3. A subnet cannot have more than one NAT gateway attached to it and it is not possible to set up multiple NAT gateways on a single subnet. https://azure.microsoft.com/en-us/blog/ensure-zone-resilient-outbound-connectivity-with-nat-gateway/ Scenario 3: Deploy zonal NAT gateways with zonally configured VMSS for optimal zone resiliency What is the optimal solution then for creating a secure, resilient, and scalable outbound setup? The solution is to deploy a VMSS in each availability zone, configure each to their own respective subnet and then attach each subnet to a zonal NAT gateway resource In our case: select 6 subnets & 6 VNATA NAT GW can be associated only to subnets from one vnet. Error when trying to associate a subnet from VNet2: The NAT gateway NAT-GW-Z1 cannot be associated with this subnet because it is associated with a subnet in the virtual network VNet1. So the answers is : 6 subnets & 6 NAT GW

upvoted 2 times

RemmyT 2 years, 6 months ago

The optimal solution : 6 subnets & 3 NAT Gateways (vnet1 & vnet 2 are in the same region).

1. NAT Gateway has high availability only into one zone 2. If the zone that goes down is also the zone in which NAT gateway has been deployed then all outgoing traffic from virtual machines across all zones will be blocked. 3. A subnet cannot have more than one NAT gateway attached to it and it is not possible to set up multiple NAT gateways on a single subnet.

https://azure.microsoft.com/en-us/blog/ensure-zone-resilient-outbound-connectivity-with-nat-gateway/

Scenario 3: Deploy zonal NAT gateways with zonally configured VMSS for optimal zone resiliency

What is the optimal solution then for creating a secure, resilient, and scalable outbound setup? The solution is to deploy a VMSS in each availability zone, configure each to their own respective subnet and then attach each subnet to a zonal NAT gateway resource

In our case: select 6 subnets & 6 VNAT

upvoted 2 times

RemmyT 2 years, 6 months ago

A NAT GW can be associated only to subnets from one vnet. Error when trying to associate a subnet from VNet2: The NAT gateway NAT-GW-Z1 cannot be associated with this subnet because it is associated with a subnet in the virtual network VNet1. So the answers is : 6 subnets & 6 NAT GW

upvoted 3 times

Dholkawala 2 years, 8 months ago

In Azure, subnets are not inherently zone-redundant. While Azure NAT Gateway can be deployed across availability zones for redundancy, subnets themselves do not automatically span multiple zones unless explicitly configured to do so. Therefore, to ensure that an outage of 2 zones does not impact the workload, you would need to create subnets that are zone-redundant by spanning them across multiple availability zones within the region. In this scenario, with three availability zones, it would be advisable to create at least 3 subnets per virtual network (VNet1 and VNet2) to achieve zone redundancy and ensure high availability for the workloads hosted in each subnet1 6 subnets/ 2 NAT GW

upvoted 3 times

NSF2 2 years, 10 months 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 3 years 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 8 times

groox 3 years, 2 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 3 years, 3 months ago

We cannot associate multiple NAT Gatways 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 Gatways.If No. Then 6 Subnets + 6 NAT Gateways.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.So if we consider the most effective method then 6 Subnets + 6 NAT Gateways would be the most fulfilling answer for this question.

upvoted 2 times

mein17 3 years, 3 months ago

We cannot associate multiple NAT Gatways 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 Gatways.

upvoted 2 times

mein17 3 years, 3 months ago

If No. Then 6 Subnets + 6 NAT Gateways.

upvoted 2 times

mein17 3 years, 3 months ago

If No. Then 6 Subnets + 6 NAT Gateways.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.So if we consider the most effective method then 6 Subnets + 6 NAT Gateways would be the most fulfilling answer for this question.

upvoted 2 times

mein17 3 years, 2 months 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.So if we consider the most effective method then 6 Subnets + 6 NAT Gateways would be the most fulfilling answer for this question.

upvoted 1 times

mein17 3 years, 2 months 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 3 years, 2 months 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 7 times

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:

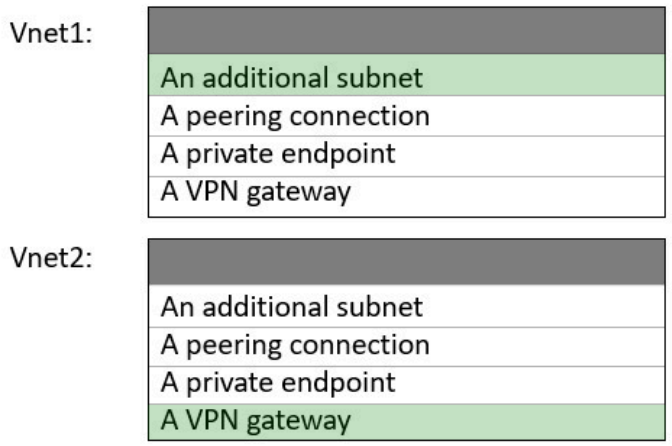
An additional subnet
A peering connection
A private endpoint
A VPN gateway

Vnet2:

An additional subnet
A peering connection
A private endpoint
A VPN gateway

Suggested Answer:

Answer Area:



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 4 years, 2 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 necesarily mean you have a VPN gate created, it just means you created a subnet called GatewaySubnet).

upvoted 31 times

Cristoicach91 Highly Voted 4 years, 2 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 necesarily mean you have a VPN gate created, it just means you created a subnet called GatewaySubnet).not to mention "minimize costs"; peering is free.Thanks Cristoicach91 !why do I need a vpn gateway? 1) new app gateway for webapp1 2) peering this is minimizing the costs and a faster solution for sure..sorry I made a mess mixing up two questions....message above need to be deleted

upvoted 31 times

Flacky_Penguin32 3 years, 11 months ago

not to mention "minimize costs"; peering is free.

upvoted 3 times

sapien45 4 years, 1 month ago

Thanks Cristoicach91 !

upvoted 2 times

manhattan 1 year, 11 months ago

why do I need a vpn gateway? 1) new app gateway for webapp1 2) peering this is minimizing the costs and a faster solution for sure..sorry I made a mess mixing up two questions....message above need to be deleted

upvoted 3 times

manhattan 1 year, 11 months ago

why do I need a vpn gateway? 1) new app gateway for webapp1 2) peering this is minimizing the costs and a faster solution for sure..

upvoted 3 times

manhattan 1 year, 10 months ago

sorry I made a mess mixing up two questions....message above need to be deleted

upvoted 1 times

leaviu1 3 years, 10 months 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 29 times

leaviu1 3 years, 10 months 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.)but, from the same document - limitation: - The app and the virtual network must be in the same region. Not in this case. WebApp1 - East US vNET2 - West US So, the only solution is v VPN gateway for vNET2.the limitation is for the vnet you are integrating the app service with. not the peering connection to another vnet, that can be globalThis is the answer as it says minimizing costs and the public doc says integration allows access to include global peering connections.

upvoted 29 times

stillface 1 year, 11 months ago

but, from the same document - limitation: - The app and the virtual network must be in the same region. Not in this case.

WebApp1 - East US vNET2 - West US

So, the only solution is v VPN gateway for vNET2.

upvoted 1 times

stillface 1 year, 11 months ago

but, from the same document - limitation: - The app and the virtual network must be in the same region. Not in this case. WebApp1 - East US vNET2 - West US So, the only solution is v VPN gateway for vNET2.the limitation is for the vnet you are integrating the app service with. not the peering connection to another vnet, that can be global

upvoted 1 times

windowsmodulesinstallerworker 1 year, 5 months ago

the limitation is for the vnet you are integrating the app service with. not the peering connection to another vnet, that can be global

upvoted 1 times

aklas 3 years, 7 months ago

This is the answer as it says minimizing costs and the public doc says integration allows access to include global peering connections.

upvoted 2 times

xRiot007 1 year, 7 months ago

VNet1 : a subnet (same region) Vnet2: a peering connection.

Virtual network integration supports connecting to a virtual network in the same region. Using virtual network integration enables your app to access: Resources in virtual networks peered to the virtual network your app is integrated with including global peering connections.

Ref: https://learn.microsoft.com/en-us/azure/app-service/overview-vnet-integration

upvoted 2 times

xRiot007 1 year, 7 months ago

VNet1 : a subnet (same region) Vnet2: a peering connection. Virtual network integration supports connecting to a virtual network in the same region. Using virtual network integration enables your app to access: Resources in virtual networks peered to the virtual network your app is integrated with including global peering connections. Ref: https://learn.microsoft.com/en-us/azure/app-service/overview-vnet-integrationVirtual network integration supports connecting to a virtual network in the same region. Using 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.

upvoted 2 times

cassucena Most Recent 11 months, 4 weeks ago

Virtual network integration supports connecting to a virtual network in the same region. Using 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.

upvoted 1 times

DGriff 2 years, 4 months ago

At first glance you would look at VNet-to-VNet, however the focus is AppServices connectivity to both VNet. Therefore integration between AppService and Virtual networks requires a unique subnet. Note. The virtual network integration feature has no extra charge for use beyond the App Service plan pricing tier charges. On the other side is a required -gateway to enable Vnet to connect.

upvoted 1 times

NSF2 2 years, 9 months ago

I were the architect, I would use peering between VNETs as opposed to a `VPN or private end points can be created in VNET1 to reach out to services in VNET2. I dont agree with the answer given in box 2

upvoted 4 times

AzureLearner01 3 years, 8 months 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 3 times

AzureLearner01 3 years, 8 months 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.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

AzureLearner01 3 years, 8 months 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 6 times

Skankhunt 3 years, 9 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 Vnet2It mentions minimizing cost. The most cost effective way to achieve the goal is to use a new subnet (for app integration) + peering

upvoted 3 times

Skankhunt 3 years, 9 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 3 years, 7 months 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 3 times

Rajan395 3 years, 9 months ago

exam topic answer seem to be correct

upvoted 1 times

TJ001 3 years, 10 months 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 correctIf 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

TJ001 3 years, 10 months 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 3 years, 10 months 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 3 years, 10 months ago

Answer: An additional subnet ------> Regional virtual network integration: When you connect to virtual networks in ---> the same region 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 3 years, 11 months 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 6 times

Flacky_Penguin32 3 years, 11 months 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'.not to mention "minimize costs"; peering is free.having the gateway subnet is irrelevant, its meant to confuse.

upvoted 1 times

Flacky_Penguin32 3 years, 11 months 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 3 years, 11 months ago

having the gateway subnet is irrelevant, its meant to confuse.

upvoted 1 times

jellybiscuit 4 years, 1 month 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.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 connectivityThink 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.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

upvoted 4 times

jellybiscuit 4 years, 1 month 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

Aanandan 4 years, 1 month 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

wooyourdaddy 3 years, 8 months 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 2 times

wooyourdaddy 3 years, 8 months 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.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 2 times

wooyourdaddy 3 years, 8 months 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 6 times

AdityaGupta 4 years, 2 months ago

correct.So helpful, truly appreciate your valuable contributions

upvoted 3 times

AdityaGupta 4 years, 2 months ago

correct.

upvoted 3 times

sapien45 4 years, 1 month ago

So helpful, truly appreciate your valuable contributions

upvoted 9 times

HOTSPOT -

You have the Azure App Service app shown in the App Service exhibit.

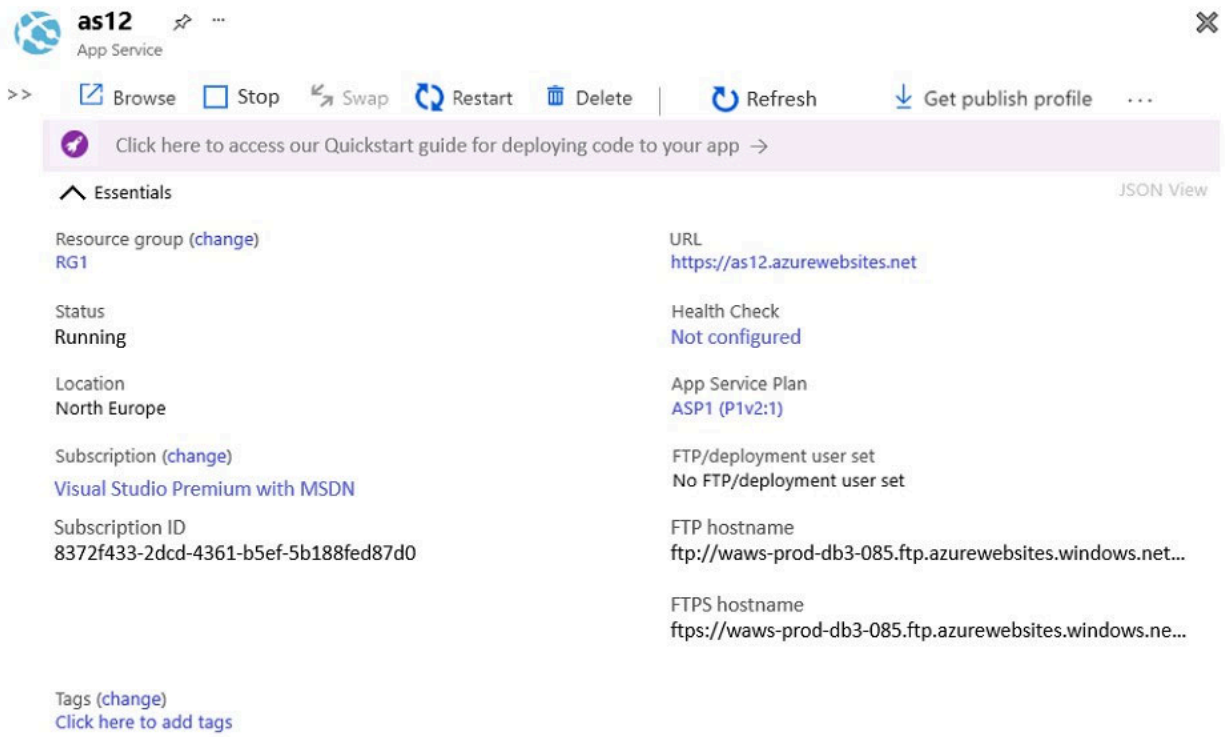
The VNet Integration settings for as12 are configured as shown in the Vnet Integration exhibit.

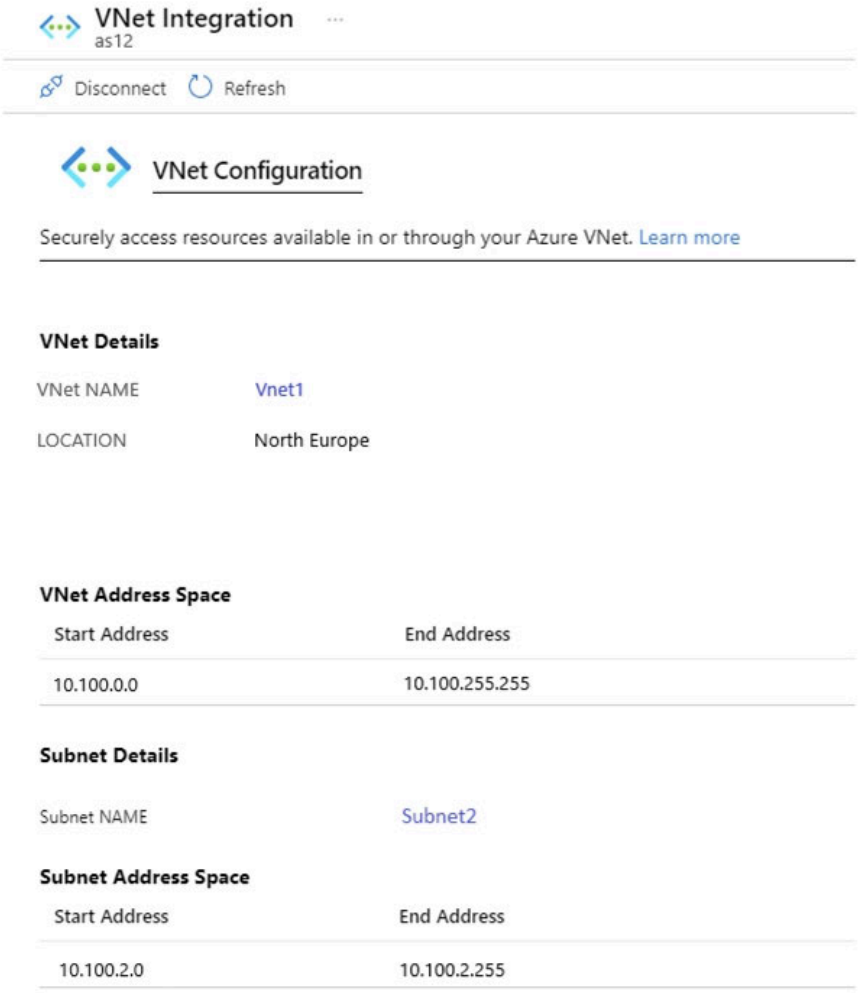
The Private Endpoint connections settings for as12 are configured as shown in the Private Endpoint connections exhibit.

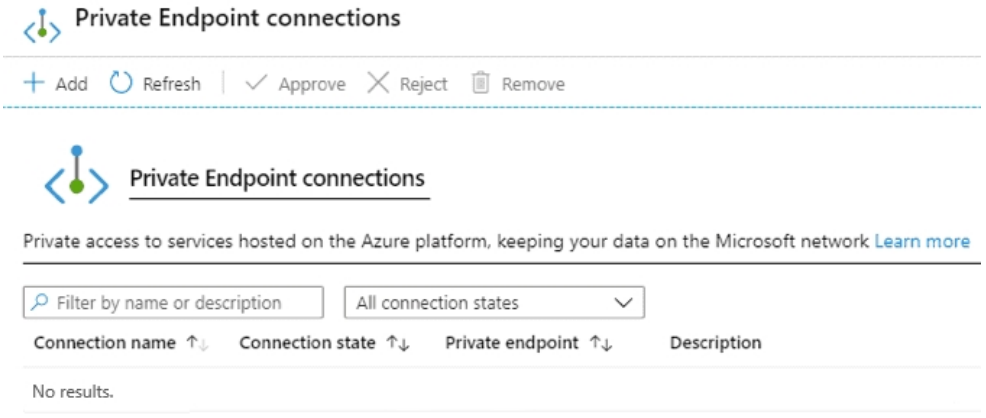
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

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	◯	◯

Suggested 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

AdityaGupta Highly Voted 4 years, 1 month 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.Q3 Should be Yes. Iif you have an app integration subnet within a VNet, it can indeed be accessed from other subnets in the same VNet.

upvoted 22 times

AdityaGupta Highly Voted 4 years, 1 month 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 22 times

thekhijir 1 year, 11 months ago

Q3 Should be Yes. Iif you have an app integration subnet within a VNet, it can indeed be accessed from other subnets in the same VNet.

upvoted 1 times

kimalto452 4 years, 2 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

az700exams Most Recent 7 months, 1 week ago

With multi plan subnet join (MPSJ), you can join multiple App Service plans in to the same subnet. All App Service plans must be in the same subscription but the virtual network/subnet can be in a different subscription. Each instance from each App Service plan requires an IP address from the subnet and to use MPSJ a minimum size of /26 subnet is required. If you plan to join many and/or large scale plans, you should plan for larger subnet ranges. https://learn.microsoft.com/en-us/azure/app-service/overview-vnet-integration

upvoted 1 times

Patel777 1 year, 3 months ago

NYN You can integrate multiple App Service apps (in the same or different App Service Plans) into a delegated subnet, as long as the subnet has capacity.

upvoted 1 times

windowsmodulesinstallerworker 1 year, 6 months ago

the third answer is N, as per microsofts documentation "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. Refer to private endpoint for inbound private access." https://learn.microsoft.com/en-us/azure/app-service/overview-vnet-integration

upvoted 1 times

DumpMaster69 3 years 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 2 times

DumpMaster69 3 years 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 subnetU R clueless, it is YYN and as per others commentsQ3 Should be Yes. If you have an app integration subnet within a VNet, it can indeed be accessed from other subnets in the same VNet.wow look at your lord of all clues. Its NNY

upvoted 2 times

Lazylinux 2 years, 10 months ago

U R clueless, it is YYN and as per others commentsQ3 Should be Yes. If you have an app integration subnet within a VNet, it can indeed be accessed from other subnets in the same VNet.wow look at your lord of all clues. Its NNY

upvoted 3 times

Lazylinux 2 years, 10 months ago

U R clueless, it is YYN and as per others comments

upvoted 3 times

thekhijir 1 year, 11 months ago

Q3 Should be Yes. If you have an app integration subnet within a VNet, it can indeed be accessed from other subnets in the same VNet.

upvoted 1 times

getafix 1 year, 8 months ago

wow look at your lord of all clues. Its NNY

upvoted 1 times

khanda 3 years, 7 months ago

YYN are the correct answers. App will use private IP from the vnet-intergration subnet for outbound calls.

upvoted 2 times

ruirosamendes 3 years, 8 months 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 3 years, 8 months ago

YNN, a Subnet is delegated to an App service plan. without PE it wouldn't use the internal IPs from the VNet.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

AzureLearner01 3 years, 8 months ago

YNN, 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 3 years, 8 months 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 3 years, 9 months 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 3 years, 10 months 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 3 years, 11 months 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

Cristoicach91 4 years, 2 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.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.You were right the first time. There is no PE configured.

upvoted 1 times

Cristoicach91 4 years, 2 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 4 years, 2 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 2 times

Cristoicach91 4 years, 2 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.You were right the first time. There is no PE configured.

upvoted 2 times

jellybiscuit 4 years, 1 month ago

You were right the first time. There is no PE configured.

upvoted 1 times

Question #20 *Topic 2*

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.

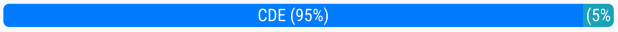
D. Create virtual network connections.

E. Remove the existing virtual network peerings.

F. Redeploy GW1.

Suggested Answer: *C, D, E*
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



AdityaGupta Highly Voted 4 years, 1 month ago
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 reploy App Gateway. Since it is VWAN there will be Vnet connection, no VNET peering.There is no new UDRs required as it will be replaced by VWAN Hub Dynamic Routing.Sweet!
upvoted 13 times

AdityaGupta Highly Voted 4 years, 1 month 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 reploy App Gateway. Since it is VWAN there will be Vnet connection, no VNET peering.
upvoted 13 times

a250fb0 1 year, 9 months ago

Selected Answer: BDE

To migrate your hub-and-spoke topology to Azure Virtual WAN while maintaining a single point of ingress from the internet:

Add virtual network peerings (B): This will help connect your existing virtual networks to the Virtual WAN hub, ensuring seamless communication between them.

Create virtual network connections (D): This is necessary to establish connectivity between your virtual networks and the Virtual WAN hub.

Remove the existing virtual network peerings (E): Since Virtual WAN will handle the connectivity, the existing peerings are no longer needed and should be removed to avoid conflicts.

upvoted 1 times

AdityaGupta 4 years, 1 month ago

There is no new UDRs required as it will be replaced by VWAN Hub Dynamic Routing.

upvoted 3 times

AdityaGupta 4 years, 1 month ago

There is no new UDRs required as it will be replaced by VWAN Hub Dynamic Routing.Sweet!

upvoted 3 times

MarkMac Most Recent 11 months, 1 week ago

Thanks for including the link. The Q is way too ambiguous and doesn't mention existing topology at all. It only mentions a hub so you have to assume there are spokes with peerings and the AGW is in one of those.

upvoted 1 times

flurgen248 3 years, 8 months 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 7 times

flurgen248 3 years, 8 months ago

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.Thanks for including the link. The Q is way too ambiguous and doesn't mention existing topology at all. It only mentions a hub so you have to assume there are spokes with peerings and the AGW is in one of those.

upvoted 7 times

thekhijir 1 year, 11 months ago

Sweet!

upvoted 1 times

Question #21 *Topic 2*

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

Suggested 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 4 years, 2 months ago
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 23 times

AdityaGupta Highly Voted 4 years, 1 month ago
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 8 times

ajinkyap Most Recent 2 years, 4 months ago
C is the correct answer adding app gateway is effort sensitive
upvoted 1 times

uridex 2 years, 9 months ago
C is correct not A
upvoted 1 times

Ben_88 3 years, 5 months ago
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 4 times

Oklama 3 years, 5 months ago

C is correct

upvoted 1 times

tomtom2022 3 years, 6 months ago

C is correct

upvoted 1 times

jellybiscuit 4 years, 1 month ago

https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-ha-ports-overview

upvoted 1 times

sapien45 4 years, 1 month ago

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

Alessandro365 4 years, 1 month ago

C is correct

upvoted 2 times

Sayden 4 years, 2 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 2 times

Question #22 *Topic 2*

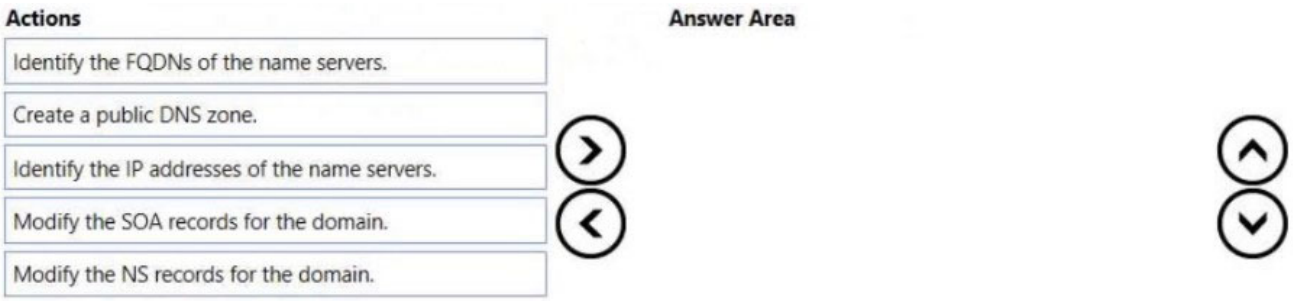
DRAG DROP -

You register a DNS domain with a third-party registrar.

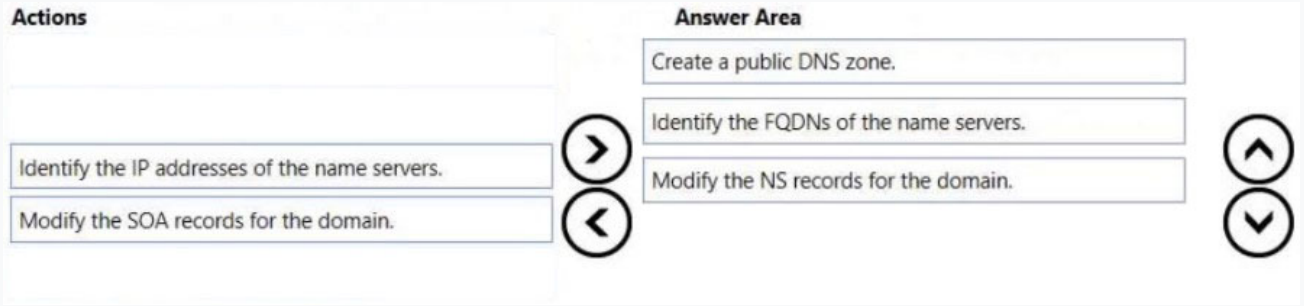
You need to host the DNS zone on Azure.

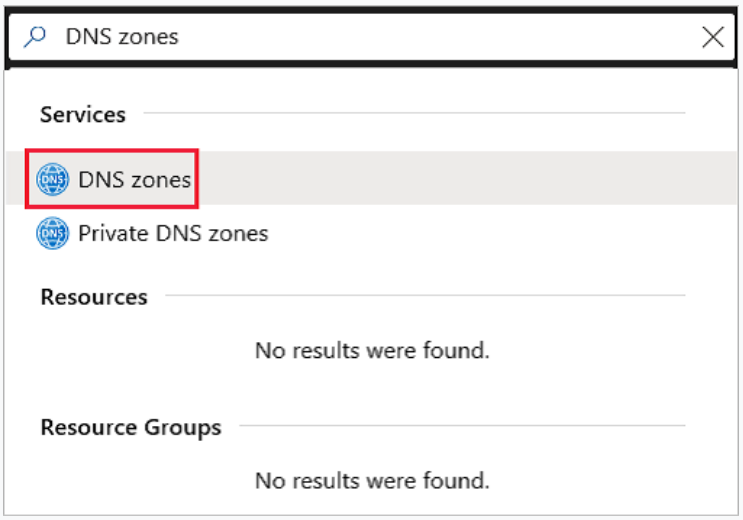
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

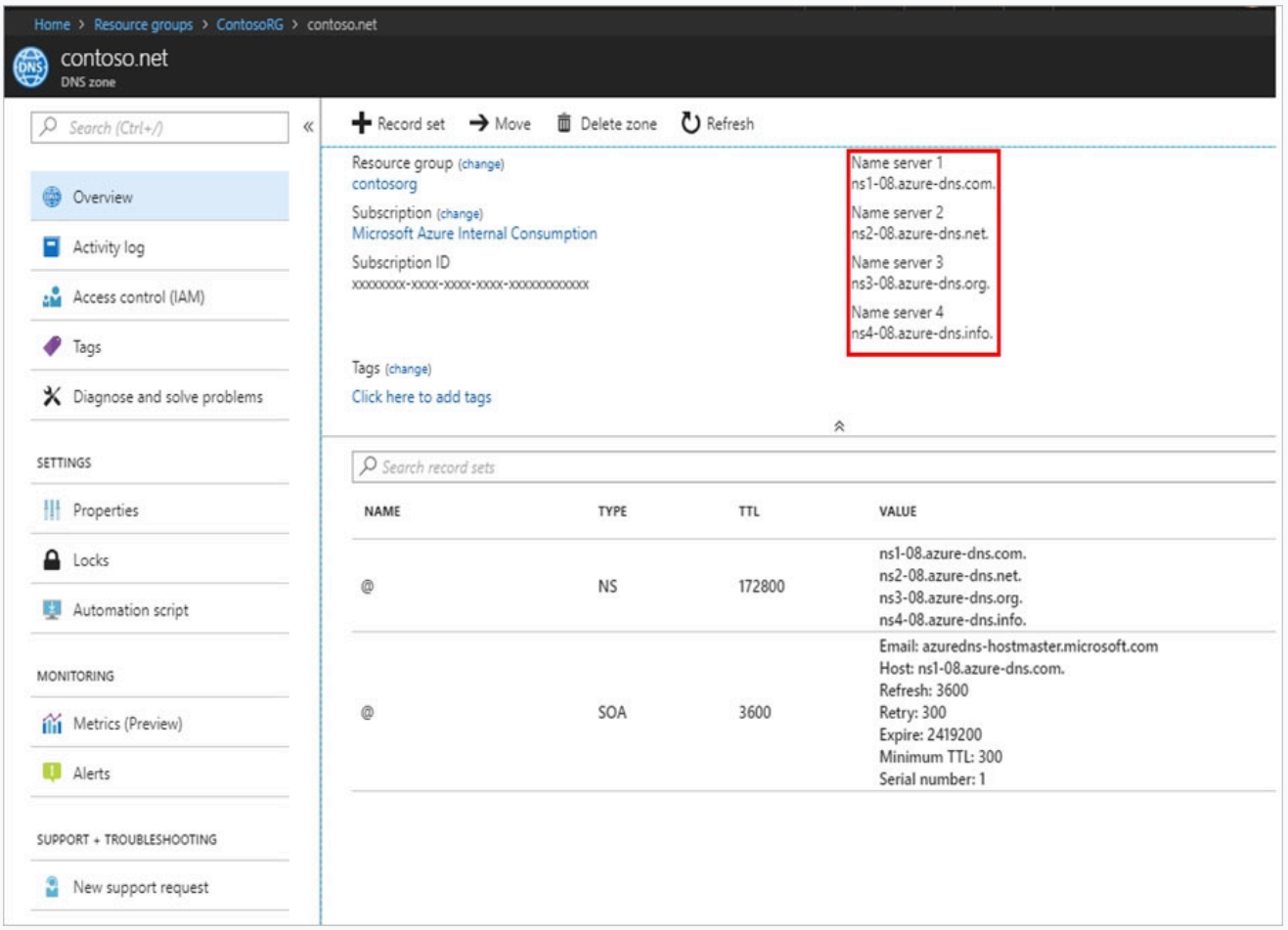
Select and Place:



Suggested Answer:







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: 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 2 years, 8 months ago

The answer is correct. Source: https://learn.microsoft.com/en-us/azure/dns/dns-delegate-domain-azure-dns

upvoted 10 times

Lazylinux Most Recent 2 years ago

Given Answer is correct

upvoted 1 times

Rajan395 2 years, 9 months ago

correct answers

upvoted 2 times

TJ001 2 years, 10 months ago

correct answers

upvoted 1 times

Jawad1462 3 years, 1 month ago

Correct

upvoted 1 times

AdityaGupta 3 years, 1 month ago

Correct : - https://learn.microsoft.com/en-us/azure/dns/dns-delegate-domain-azure-dns

upvoted 4 times

Cristoicach91 3 years, 2 months ago

correct

upvoted 2 times

HOTSPOT -

You have the network topology shown in the Topology exhibit. (Click the Topology tab.)

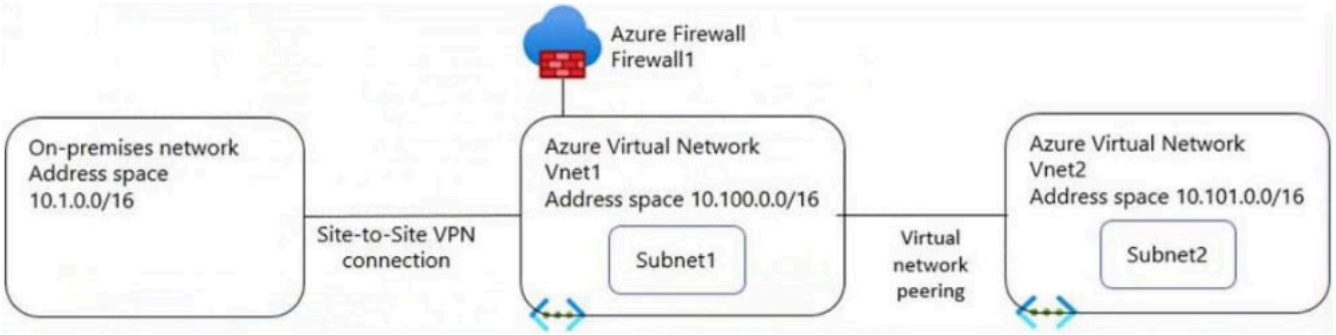
You have the Azure firewall shown in the Firewall1 exhibit. (Click the Firewall1 tab.)

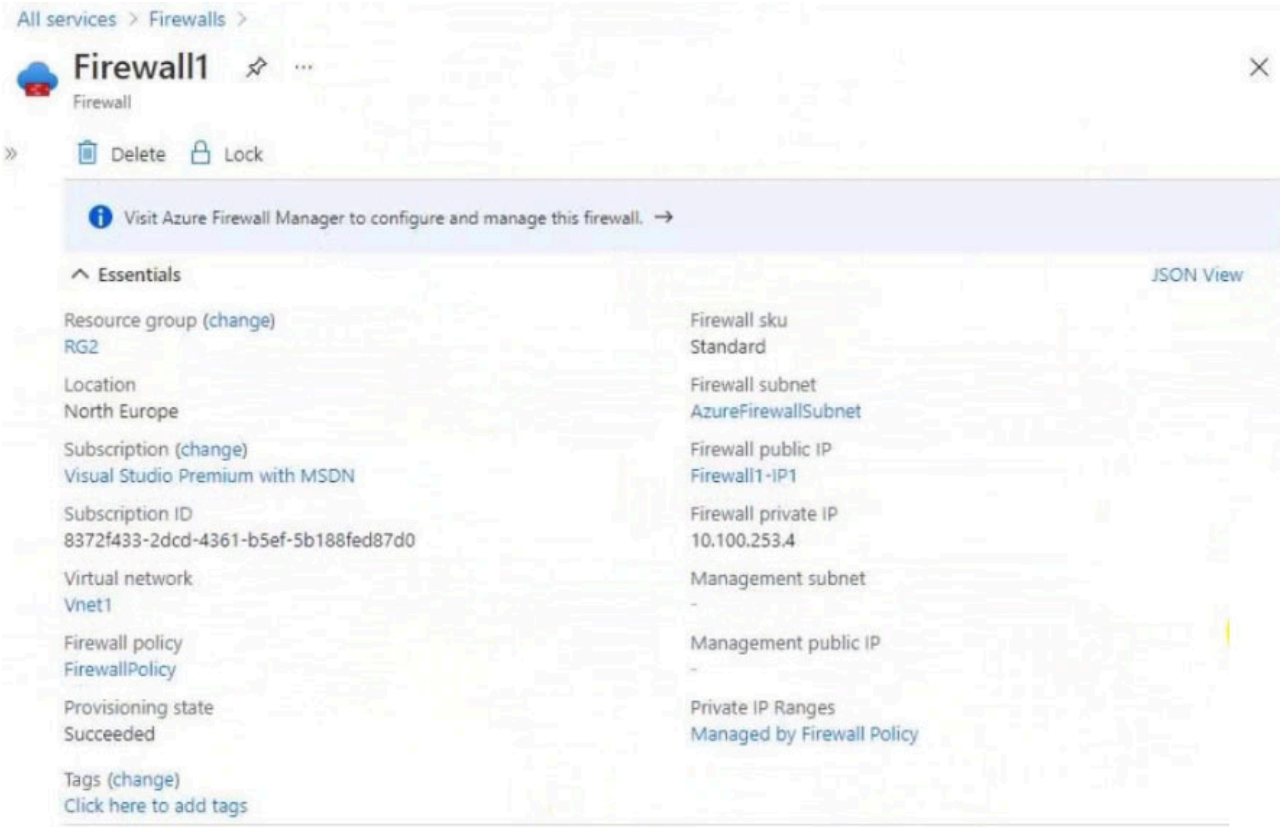
You have the route table shown in the RouteTable1 exhibit. (Click the RouteTable1 tab.)

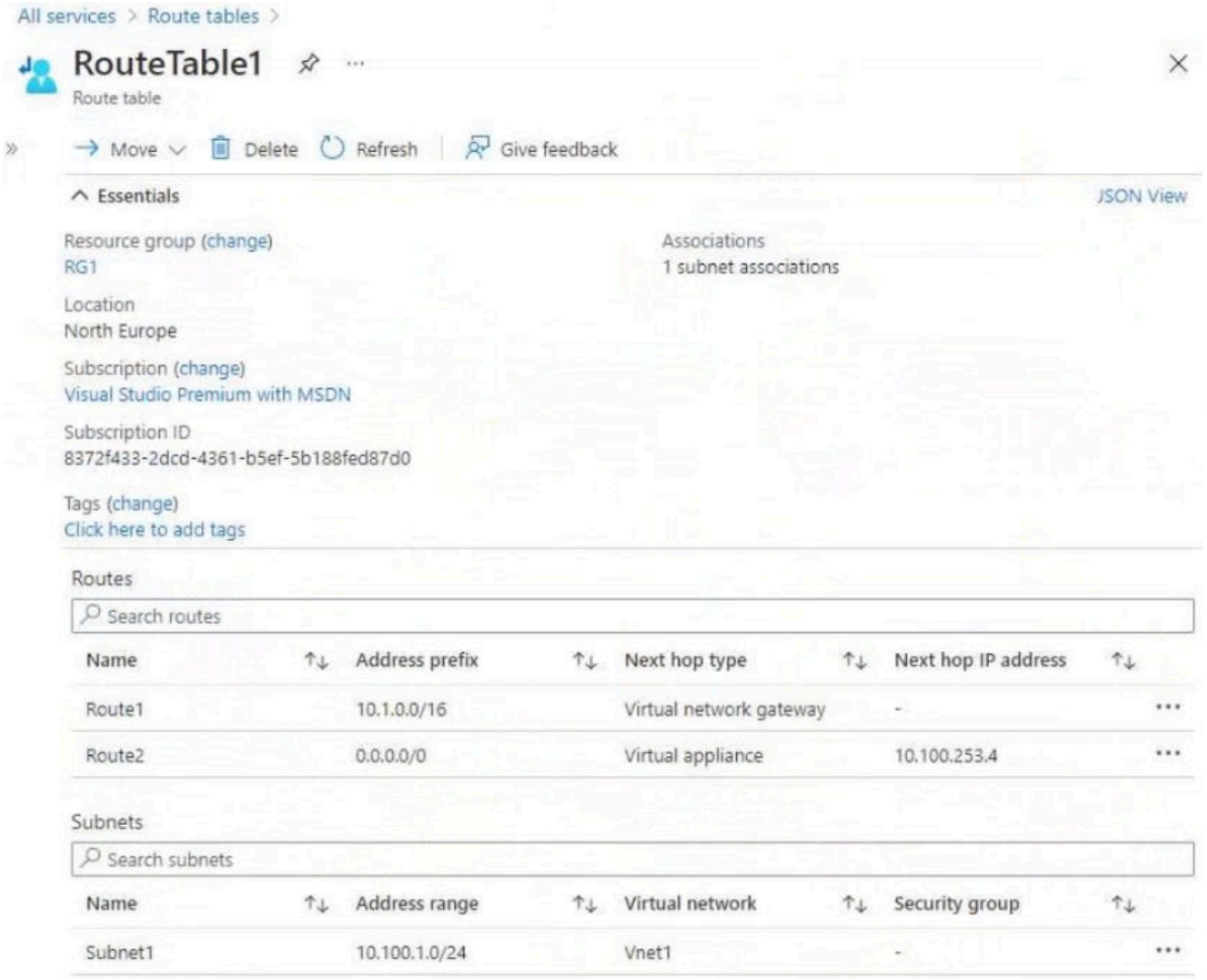
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

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.	○	○
The resources in Subnet1 can connect to the resources in Vnet2.	○	○
The resources in Subnet2 can connect to the internet through Firewall1.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
The resources in Subnet1 can connect to the internet through Firewall1.	○	○
The resources in Subnet1 can connect to the resources in Vnet2.	○	○
The resources in Subnet2 can connect to the internet through Firewall1.	○	○

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 4 years, 2 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 25 times

Sheriboy Highly Voted 4 years, 2 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/firewallLook 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 25 times

AdityaGupta 4 years, 1 month 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 4 years, 1 month 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

620b351 Most Recent 2 years, 2 months ago

Given answer is correct. for the question 2, If the peering is correct, azure distribute traffic automatically. But this is not shown in the route table.

upvoted 2 times

Murad01 2 years, 11 months ago

Appeared on Exam November - 2023

upvoted 1 times

Lazylinux 3 years 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 2 times

Qunlay 3 years, 6 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 3 years, 6 months ago

Correct answer is Y,N,N

upvoted 2 times

_fvt 3 years, 7 months 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 Sunbet 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 3 years, 7 months ago

YNN Y- Will go throuth FW - 0.0.0.0 rout N- subnet2 doesnt have RT N- No route through FW

upvoted 3 times

Rajan395 3 years, 9 months ago

Answers seems to be correct

upvoted 1 times

TJ001 3 years, 10 months ago

YYN Second yes, because peering route take precedence over UDR

upvoted 1 times

DerekKey 3 years, 10 months 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 3 years, 10 months ago

Y Y N- explanation is wrong. The reason is udr is not attached to subnet2

upvoted 1 times

sapien45 4 years, 1 month ago

YNN Route for 0.0.0.0/0 would direct any flow going to VNET2 to go though the Firewall, and therefore going nowhere. There are no routes for peering VNET1-VNET2

upvoted 6 times

sapien45 4 years, 1 month ago

YNN Route for 0.0.0.0/0 would direct any flow going to VNET2 to go though the Firewall, and therefore going nowhere. There are no routes for peering VNET1-VNET2YYN. I stand corrected. The screenshot just show the detail on ONE route table. the resultying routes in EFFECTIVE routes is not shown there, since the two VNETS are peered, VNET peering CDIR range takes priority

upvoted 6 times

sapien45 4 years, 1 month ago

YYN. I stand corrected. The screenshot just show the detail on ONE route table. the resultying routes in EFFECTIVE routes is not shown there, since the two VNETS are peered, VNET peering CDIR range takes priority

upvoted 7 times

Cristoicach91 4 years, 2 months ago

YNN. 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

Question #24 *Topic 2*

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

Suggested 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 2 years, 10 months ago
"You resize the gateway of Vnet1 to a larger SKU" Bro why whould u do that ? are u okay ?
upvoted 10 times

Zorro2003 Most Recent 1 year, 2 months ago
Selected Answer: B
Answer: B. No.

Resizing the VNet1 VPN gateway only increases capacity; it doesn't fix routing.

For a P2S client on VNet1 to reach VNet2, you must ensure peering is set to Allow gateway transit on VNet1 and Use remote gateway on VNet2 and advertise VNet2's prefixes to the P2S clients (so they receive routes to VNet2). A larger SKU won't enable that.
upvoted 1 times

Stevy_nash Highly Voted 2 years, 10 months ago
"You resize the gateway of Vnet1 to a larger SKU"

Bro why whould u do that ? are u okay ?
upvoted 10 times

anishk 2 years, 4 months ago
Bro, why give options
upvoted 1 times

AdityaGupta 3 years, 1 month ago
You need to download VPN client again, since there are topology changes.to download not a VPN client but a VPN client configuration from the gateway
upvoted 4 times

AdityaGupta 3 years, 1 month ago
You need to download VPN client again, since there are topology changes.
upvoted 4 times

Sergovladi 1 year, 10 months ago
to download not a VPN client but a VPN client configuration from the gateway
upvoted 1 times

jilguens 3 years, 2 months ago

Selected Answer: B

correct

upvoted 2 times

Question #25 *Topic 2*

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

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?

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

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

Suggested 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 (87%) A (13%)

IvanMtz Highly Voted 4 years, 1 month ago
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 34 times

jellybiscuit Highly Voted 4 years, 1 month ago
https://learn.microsoft.com/en-us/azure/firewall/firewall-faq#are-there-any-firewall-resource-group-restrictions
upvoted 28 times

TheCloudGuruu Most Recent 6 months, 4 weeks ago
The resource group is a red herring. AF1 is being deployed to RG1, but that doesn't limit which VNet it can use. Resource groups are logical containers — they have no region enforcement on the resources within them. A resource group's location only determines where its metadata is stored. Resources inside a resource group can be in any region.
upvoted 3 times

Patel777 1 year, 4 months ago
Resource group doesn't matter for deployment—the region does.
upvoted 3 times

manhattan 2 years, 1 month ago
Are there any firewall resource group restrictions? Yes. The firewall and VNet must be in the same resource group. The public IP address can be in any resource group. The firewall, VNet, and the public IP address all must be in the same subscription.
upvoted 3 times

ajinkyap 2 years, 4 months ago
https://learn.microsoft.com/en-us/azure/firewall/firewall-faq#are-there-any-firewall-resource-group-restrictions
upvoted 1 times

Lazylinux 3 years ago

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 3 times

Techbiz 3 years, 1 month 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 3 years, 5 months ago

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 5 times

somenick 3 years, 8 months ago

https://learn.microsoft.com/en-us/azure/firewall/firewall-faq#are-there-any-firewall-resource-group-restrictions

upvoted 4 times

Rajan395 3 years, 9 months ago

Correct Answer : C

upvoted 2 times

TJ001 3 years, 10 months ago

>VNET, PIP, FW all in same region and resource group >Firewall subnet should be names AzureFirewallSubnet

upvoted 3 times

Akodo_Shado 3 years, 10 months ago

The firewall, VNet, and the public IP address all must be in the same resource group.

upvoted 4 times

abdulmoiz 3 years, 11 months ago

Should be only Vnet with RG-1

upvoted 1 times

Takloy 3 years, 11 months 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 3 years, 11 months ago

https://learn.microsoft.com/en-us/azure/firewall/firewall-faq#are-there-any-firewall-resource-group-restrictions

upvoted 1 times

HOTSPOT

-

You have two Azure App Service instances that host the web apps shown the following table.

You deploy an Azure 2 that has one public frontend IP address and two backend pools.

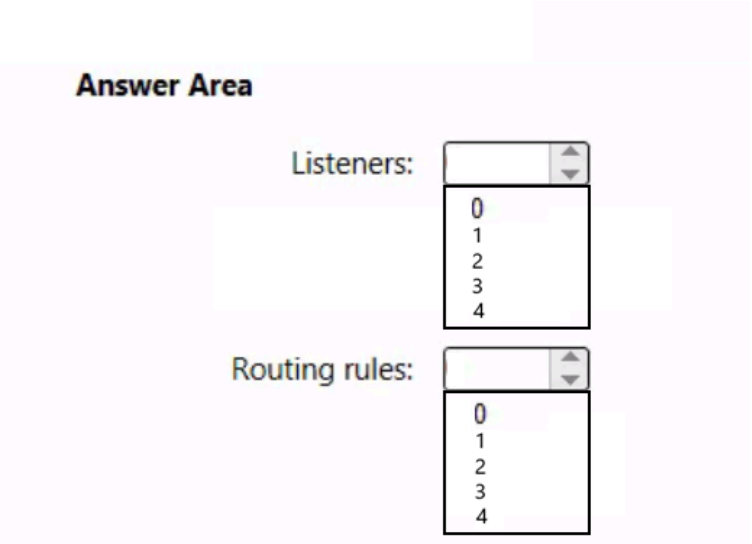
You need to publish all the web apps to the application gateway. Requests must be routed based on the HTTP host headers.

What is the minimum number of listeners and routing rules you should configure? To answer, select the appropriate options in the answer area.

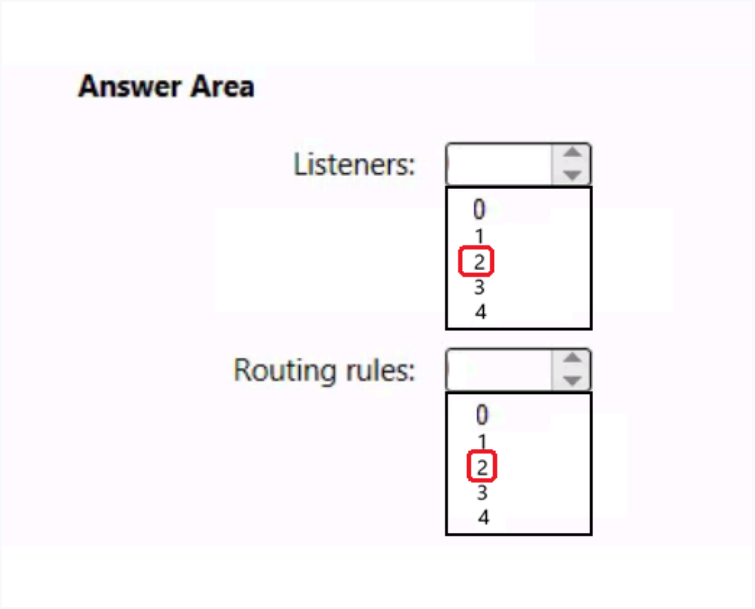
NOTE: Each correct selection is worth one point.

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/

Answer Area



Suggested Answer:



TJ001 Highly Voted 3 years, 4 months 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 22 times

TJ001 Highly Voted 3 years, 4 months 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)the given answer is correct https://learn.microsoft.com/en-us/training/modules/configure-azure-application-gateway/3-determine-routingpls 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 listenersmall 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 selectionWhen 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.The Routing rules are routing based on host headers so path based is not in use. Furthermore, when using path based routing, you can only route between pools and not to individual members of a back end pool.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 IMHOagree - 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 22 times

ieboaix 2 years, 4 months ago

the given answer is correct https://learn.microsoft.com/en-us/training/modules/configure-azure-application-gateway/3-determine-routing

upvoted 1 times

TJ001 3 years, 4 months 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 3 years, 4 months 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 listenersmall 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

TJ001 3 years, 3 months 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 2 times

daemon101 2 years, 10 months 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.The Routing rules are routing based on host headers so path based is not in use. Furthermore, when using path based routing, you can only route between pools and not to individual members of a back end pool.

upvoted 5 times

daemon101 2 years, 10 months 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 5 times

DC095 Most Recent 10 months, 2 weeks ago

The Routing rules are routing based on host headers so path based is not in use. Furthermore, when using path based routing, you can only route between pools and not to individual members of a back end pool.

upvoted 1 times

JohnAvlakiotis 2 years, 11 months 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 4 times

JohnAvlakiotis 2 years, 11 months 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 IMHOagree - 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 4 times

Webesciaki 2 years, 4 months 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

Zeppoonstream 3 years, 1 month ago

what is meant by "You deploy an Azure 2" ??

upvoted 13 times

Zeppoonstream 3 years, 1 month ago

what is meant by "You deploy an Azure 2" ??I guess it's supposed to be Application Gateway Standard V2

upvoted 13 times

daemon101 2 years, 10 months ago

I guess it's supposed to be Application Gateway Standard V2

upvoted 9 times

Zorro2003 1 year, 2 months ago

nswer: Listeners = 2, Routing rules = 2 □ Explanation You have two backend pools (AS1 and AS2) and four web apps across two Azure App Service instances. Since requests must be routed based on the HTTP host header, we need to configure multi-site listeners: Listener 1 → Handles app1.contoso.com and app2.contoso.com → Routes to Backend Pool AS1. Listener 2 → Handles app3.contoso.com and app4.contoso.com → Routes to Backend Pool AS2. Why Only 2 Listeners and 2 Rules One listener per App Service instance. One routing rule per listener, matching the hostnames to the correct backend pool. No need for four listeners or four rules since multiple hostnames can share one listener when they point to the same backend pool.

upvoted 1 times

sam881989 2 years, 4 months 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!Correction. The answer is correct. Path based routing does not work in this situation

upvoted 3 times

sam881989 2 years, 4 months 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 3 times

sam881989 2 years, 4 months ago

Correction. The answer is correct. Path based routing does not work in this situation

upvoted 2 times

NSF2 2 years, 4 months 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 3 times

Lazylinux 2 years, 4 months 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 furtherNow 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 FurtherTherefore 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 httpseting1 with health probe Listener 2- Multi-site (Multiple/wildcard) Hostnames: app3.contoso.com and app4.contoso.co

upvoted 3 times

Lazylinux 2 years, 4 months 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 3 times

Lazylinux 2 years, 4 months 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 FurtherTherefore 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 httpseting1 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 httpseting1 with health probe See below furtherNote: 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 *.constoso.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#allow

upvoted 5 times

Lazylinux 2 years, 4 months 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 5 times

Lazylinux 2 years, 4 months 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 httpseting1 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 httpseting1 with health probe See below further

upvoted 6 times

Lazylinux 2 years, 4 months 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 httpseting1 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 httpseting1 with health probe See below furtherNote: 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 *.constoso.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-fieldBut then the answer is 3 listeners and 3 routing rules if we consider to use multi-site with wildcard? Thanks

upvoted 6 times

Lazylinux 2 years, 4 months 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 *.constoso.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-fieldBut then the answer is 3 listeners and 3 routing rules if we consider to use multi-site with wildcard? Thanks

upvoted 2 times

Lazylinux 2 years, 4 months 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 *.constoso.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 2 times

sirio 2 years, 3 months ago

But then the answer is 3 listeners and 3 routing rules if we consider to use multi-site with wildcard? Thanks

upvoted 3 times

IE17 2 years, 7 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

IE17 2 years, 7 months ago

1 Multi-listener and 2 routing rules... https://learn.microsoft.com/en-us/azure/application-gateway/create-multiple-sites-portalThe URL is a good reference but on same url yo share they're showing 2 routing rule with a Distinct listenner for each rule 2Rules*1Listenner(each) = 2Listenner

upvoted 1 times

c2e9cb4 2 years, 4 months ago

The URL is a good reference but on same url yo share they're showing 2 routing rule with a Distinct listenner for each rule 2Rules*1Listenner(each) = 2Listenner

upvoted 1 times

WMG 3 years, 1 month 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

drprepper_ 3 years, 2 months 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?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 5 times

drprepper_ 3 years, 2 months 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 3 years, 2 months 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 3 years, 2 months 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

Question #27 *Topic 2*

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.

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?

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

A. Recreate LNG1.

B. Reset RTR1.

C. Reset Connection1.

D. Reset GW1.

Suggested Answer: *C*

Community vote distribution

C (100%)

Goofer Highly Voted 3 years, 4 months 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 18 times

bobothewiseman 1 year, 10 months ago

Answer is C. But in reality, you should reset the VPN gateway. Trust me! I have done it multiplr times

upvoted 1 times

Zeinovich 2 years, 8 months ago

why not recreate LNG1? may be the IP or BGP incorrect?

upvoted 2 times

Zeinovich 2 years, 8 months ago

why not recreate LNG1? may be the IP or BGP incorrect?More effort, you need to redeploy the connection as well.That would probably be the next step if resetting does not work. For minimal downtime, disruption and effort, reset C1 and see if the issue is remediated.

upvoted 2 times

LaurentvM 2 years, 3 months ago

More effort, you need to redeploy the connection as well.

upvoted 1 times

xRiot007 Most Recent 1 year, 7 months ago

That would probably be the next step if resetting does not work. For minimal downtime, disruption and effort, reset C1 and see if the issue is remediated.

upvoted 1 times

Oklama 2 years, 11 months ago

The Correct answer is C

upvoted 1 times

sunsetblvdfightclub 3 years, 2 months ago

https://learn.microsoft.com/en-us/azure/vpn-gateway/reset-gateway#reset-a-connection

upvoted 1 times

Rajan395 3 years, 3 months ago

C is correct

upvoted 1 times

DerekKey 3 years, 4 months 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.GW1 is common for multiple connections and it shall incresae the downtime

upvoted 1 times

DerekKey 3 years, 4 months 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 3 years, 4 months ago

GW1 is common for multiple connections and it shall incresae the downtime

upvoted 3 times

Question #28 *Topic 2*

DRAG DROP
-

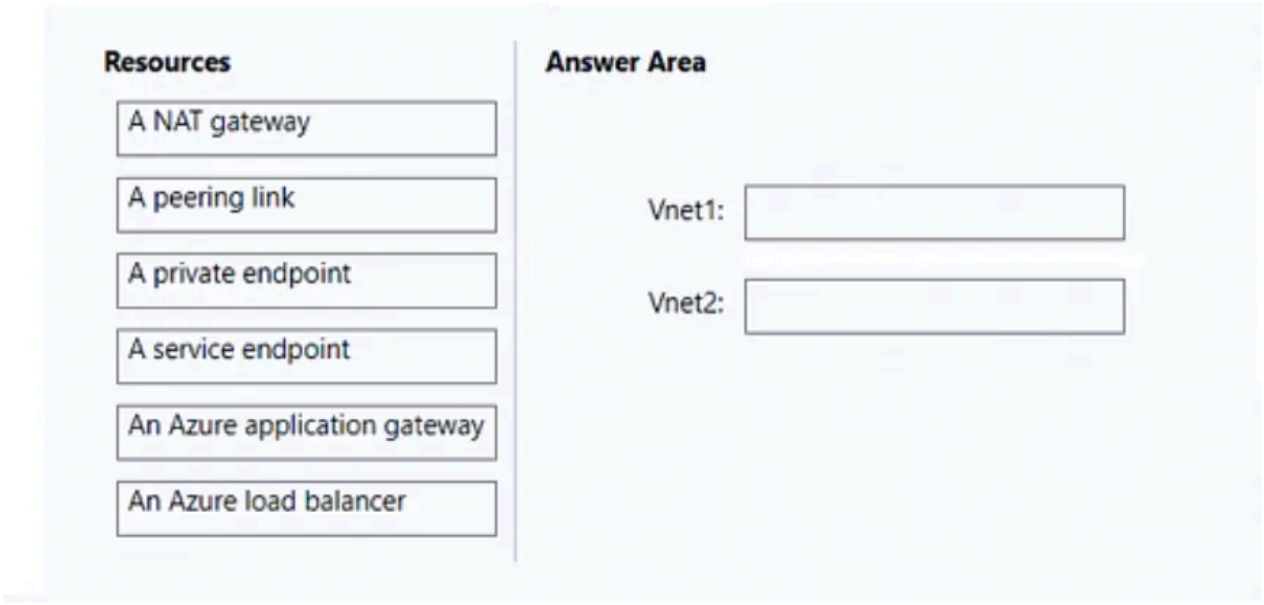
You have an Azure subscription that contains a virtual network named Vnet1 and an Azure SQL database named SQL1. SQL1 has a private endpoint on Vnet1.

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.



Suggested Answer:

Answer Area

Vnet1: A private endpoint

Vnet2: A peering link

Wis10 Highly Voted 3 years, 10 months 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 55 times

Wis10 Highly Voted 3 years, 10 months ago

Correct Answer: - Vnet1 = Standard Load Balancer - Vnet2 = Private Endpoint Justification: https://learn.microsoft.com/en-us/azure/private-link/private-link-service-overview#workflowAgree, SQL already have private endpoint so we need load balancer in VNET1 and private link in VNET2.But question said you need to use an Azure Private Link service.An Azure SQL database (PaaS) does not support Private Link Service. You need a private endpoint instead. This question is a bit tricky. You mainly use a private link service for resources that don't support private endpoints, like apps hosted on VMs (IaaS). That is why you would need a load balancer (IaaS) for such requirement.But what I forgot to mention. The answers are incorrect. I asume you would use the load balancer to connect to the IP Address of the already existing private endpoint. I don't see that described at Microsoft, but I asume it can work.

upvoted 55 times

asdasd123123iu 3 years, 3 months ago

Agree, SQL already have private endpoint so we need load balancer in VNET1 and private link in VNET2.

upvoted 3 times

RabbitB 2 years, 5 months ago

But question said you need to use an Azure Private Link service.

upvoted 2 times

TheBlob 2 years, 4 months ago

An Azure SQL database (PaaS) does not support Private Link Service. You need a private endpoint instead. This question is a bit tricky. You mainly use a private link service for resources that don't support private endpoints, like apps hosted on VMs (IaaS). That is why you would need a load balancer (IaaS) for such requirement.But what I forgot to mention. The answers are incorrect. I asume you would use the load balancer to connect to the IP Address of the already existing private endpoint. I don't see that described at Microsoft, but I asume it can work.

upvoted 1 times

TheBlob 2 years, 4 months ago

An Azure SQL database (PaaS) does not support Private Link Service. You need a private endpoint instead. This question is a bit tricky. You mainly use a private link service for resources that don't support private endpoints, like apps hosted on VMs (IaaS). That is why you would need a load balancer (IaaS) for such requirement.

upvoted 1 times

TheBlob 2 years, 4 months ago

But what I forgot to mention. The answers are incorrect. I asume you would use the load balancer to connect to the IP Address of the already existing private endpoint. I don't see that described at Microsoft, but I asume it can work.

upvoted 1 times

DavidSapery 3 years, 10 months 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 21 times

ninz44 1 year, 8 months ago

Vnet1 - Private Link Vnet2 - Private Endpoint

upvoted 1 times

ninz44 1 year, 8 months ago

Vnet1 - Private Link Vnet2 - Private EndpointCorrection Vnet1 - Peering Link

upvoted 1 times

ninz44 Most Recent 1 year, 8 months ago

Correction Vnet1 - Peering Link

upvoted 1 times

mjk666 2 years, 8 months ago

The question here is how should we put the Azure SQL Database behind the load balancer, we already have an endpoint in the Vnet1 which we don't need then. if it was SQL Server on VMs without endpoint the deploying SLB and PE would make sense

upvoted 2 times

Lazylinux 3 years 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 5 times

Azused 3 years, 2 months 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 5 times

ronin201 3 years, 4 months 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.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 5 times

ronin201 3 years, 4 months 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 5 times

GBAU 3 years 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 3 years, 4 months ago

wrong answer: Vnet1 already has private enpoint. peering links in both vnets must be created

upvoted 7 times

AzureLearner01 3 years, 8 months 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 3 years, 8 months ago

Load balancer Private Link https://learn.microsoft.com/it-it/azure/private-link/private-link-overview

upvoted 2 times

Ayokun 3 years, 8 months ago

Load balancer Private Link https://learn.microsoft.com/it-it/azure/private-link/private-link-overviewSorry 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

Ayokun 3 years, 8 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 3 years, 9 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 7 times

tester2023 3 years, 9 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.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.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-overviewAs 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 7 times

lingxian 3 years, 8 months 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

flurgen248 3 years, 8 months 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 7 times

KeenOnTech 3 years, 2 months 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 2 times

4729 3 years, 9 months ago

VNET1: Private Link VNET2: Private Endpoint

upvoted 7 times

amt2022 3 years, 9 months 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 3 years, 10 months 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 3 years, 10 months ago

VNET1 - Azure Load Balancer - your existing service must be behind a load balancer VNET2 - Private link

upvoted 1 times

Question #29 *Topic 2*

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

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?

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

A. 2

B. 3

C. 4

D. 5

Suggested Answer: *B*

Community vote distribution

C (52%) B (44%) (4

amt2022 Highly Voted 3 years, 9 months ago

Correct Answer : 4 1. GatewaySubnet 2. Subnet 2 3. Subnet 1 with Basic SKU for Public IP 4. NAT Gatway 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 27 times

amt2022 Highly Voted 3 years, 9 months ago

Correct Answer : 4 1. GatewaySubnet 2. Subnet 2 3. Subnet 1 with Basic SKU for Public IP 4. NAT Gatway 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 sectionWhy could you not just deploy the NAT Gateway into the GatewaySubnet?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.GatewaySubnet has nothing to do with NAT Gateway resources. GatewaySubnet is the azure naming convention for subnet used with Virtual Network GatewaysCorrect! When you create a virtual network gateway, the gateway VMs are automatically deployed to the gateway subnet (always named GatewaySubnet), and configured with the settings that you specified. The process can take 45 minutes or more to complete, depending on the gateway SKU that you selected. https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings So you will need a new Subnet for a NAT Gateway. Total: 4 subnets..."Never deploy anything else (for example, more VMs) to the gateway subnet"... https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings#gwsubAnother 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).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.Correction: NATGateway cannot be associated to GatewaySubnet However, NATGat

upvoted 27 times

MrBlueSky 3 years, 7 months ago

Why could you not just deploy the NAT Gateway into the GatewaySubnet?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.GatewaySubnet has nothing to do with NAT Gateway resources. GatewaySubnet is the azure naming convention for subnet used with Virtual Network GatewaysCorrect! When you create a virtual network gateway, the gateway VMs are automatically deployed to the gateway subnet (always named GatewaySubnet), and configured with the settings that you specified. The process can take 45 minutes or more to complete, depending on the gateway SKU that you selected. https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings So you will need a new Subnet for a NAT Gateway. Total: 4 subnets..."Never deploy anything else (for example, more VMs) to the gateway subnet"... https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings#gwsub

upvoted 1 times

MrBlueSky 3 years, 7 months ago

Why could you not just deploy the NAT Gateway into the GatewaySubnet?

upvoted 1 times

jarz 3 years, 6 months 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 4 times

JohnnyChimpo 3 years, 5 months ago

GatewaySubnet has nothing to do with NAT Gateway resources. GatewaySubnet is the azure naming convention for subnet used with Virtual Network GatewaysCorrect! When you create a virtual network gateway, the gateway VMs are automatically deployed to the gateway subnet (always named GatewaySubnet), and configured with the settings that you specified. The process can take 45 minutes or more to complete, depending on the gateway SKU that you selected. https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings So you will need a new Subnet for a NAT Gateway. Total: 4 subnets

upvoted 3 times

JohnnyChimpo 3 years, 5 months ago

GatewaySubnet has nothing to do with NAT Gateway resources. GatewaySubnet is the azure naming convention for subnet used with Virtual Network Gateways

upvoted 3 times

stillface 1 year, 11 months ago

Correct! When you create a virtual network gateway, the gateway VMs are automatically deployed to the gateway subnet (always named GatewaySubnet), and configured with the settings that you specified. The process can take 45 minutes or more to complete, depending on the gateway SKU that you selected. https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings So you will need a new Subnet for a NAT Gateway. Total: 4 subnets

upvoted 1 times

Feliphus 2 years ago

..."Never deploy anything else (for example, more VMs) to the gateway subnet"... https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings#gwsub

upvoted 2 times

tester2023 3 years, 9 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).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.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 3Order 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 6 times

tester2023 3 years, 9 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 6 times

MrBlueSky 3 years, 7 months 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 4 times

MrBlueSky 3 years, 7 months 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.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 3Order 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 4 times

MrBlueSky 3 years, 7 months 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 3Order 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 5 times

MrBlueSky 3 years, 7 months 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 5 times

jarz 3 years, 6 months 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

c2e9cb4 2 years, 10 months ago

This is wrong : a nat gateway dosent require a subnet at all tested on lab ==>corret answer 3

upvoted 6 times

c2e9cb4 2 years, 10 months ago

This is wrong : a nat gateway dosent require a subnet at all tested on lab ==>corret answer 3Every kind of gateway requires subnet! no exceptions! In some cases will be automatically created.Not quite the point. You cannot associate a NAT gateway with any of the existing subnets and meet the requirements for the VMs to continue using their own public IP addresses. A new subnet would be required to meet that requirement.

upvoted 6 times

stillface 1 year, 11 months ago

Every kind of gateway requires subnet! no exceptions! In some cases will be automatically created.

upvoted 1 times

DC095 11 months, 2 weeks ago

Not quite the point. You cannot associate a NAT gateway with any of the existing subnets and meet the requirements for the VMs to continue using their own public IP addresses. A new subnet would be required to meet that requirement.

upvoted 1 times

wooyourdaddy 3 years, 8 months 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 21 times

wooyourdaddy 3 years, 8 months ago

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.Agree +1agree: 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 aboveWe do not need to have a subnet selected for creation of NAT gateway. checked in lab

upvoted 21 times

_NoobMaster69 3 years, 8 months ago

Agree +1

upvoted 1 times

_NoobMaster69 3 years, 8 months ago

Agree +1agree: 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

Webesciaki 2 years, 10 months 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 3 times

ajinkyap 2 years, 4 months ago

We do not need to have a subnet selected for creation of NAT gateway. checked in lab

upvoted 1 times

TheCloudGuruu Most Recent 6 months, 4 weeks ago

No additional subnets needed. The 3 existing subnets are sufficient.

upvoted 1 times

Zorro2003 1 year, 2 months ago

It's 3, not 4. Why: NAT Gateway attaches to existing subnets; it does not require its own/dedicated subnet. You simply associate it to one or more subnets. Microsoft Learn It cannot be deployed in GatewaySubnet and can't be used on subnets with Basic SKU resources (like VM1's Basic public IP). So you'd attach it to Subnet2 only, and leave Subnet1 as-is. Result: Subnet1 + Subnet2 + GatewaySubnet = 3 subnets. Microsoft Learn Docs: NAT overview shows attach-to-subnet behavior and the Basic-SKU incompatibility, plus the restrictionYou're missing the point. No NAT Gateways aren't actually deployed into subnets, but the requirement that the VMs continue to use their ILPIPs means that the Gateway can't be associated with any of the existing subnets. A new one would be required.exactly , so the anwer is C 4 >>> NAT gateway takes precedence over other outbound connectivity methods, including a load balancer, instance-level public IP addresses, and Azure Firewall. https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-outbound-connections

upvoted 1 times

Zorro2003 1 year, 2 months ago

Selected Answer: B

It's 3, not 4.

Why:

NAT Gateway attaches to existing subnets; it does not require its own/dedicated subnet. You simply associate it to one or more subnets. Microsoft Learn

It cannot be deployed in GatewaySubnet and can't be used on subnets with Basic SKU resources (like VM1's Basic public IP). So you'd attach it to Subnet2 only, and leave Subnet1 as-is. Result: Subnet1 + Subnet2 + GatewaySubnet = 3 subnets. Microsoft Learn

Docs: NAT overview shows attach-to-subnet behavior and the Basic-SKU incompatibility, plus the restriction

upvoted 1 times

DC095 11 months, 2 weeks ago

You're missing the point. No NAT Gateways aren't actually deployed into subnets, but the requirement that the VMs continue to use their ILPIPs means that the Gateway can't be associated with any of the existing subnets. A new one would be required.exactly , so the anwer is C 4 >>> NAT gateway takes precedence over other outbound connectivity methods, including a load balancer, instance-level public IP addresses, and Azure Firewall. https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-outbound-connections

upvoted 2 times

DC095 11 months, 2 weeks ago

You're missing the point. No NAT Gateways aren't actually deployed into subnets, but the requirement that the VMs continue to use their ILPIPs means that the Gateway can't be associated with any of the existing subnets. A new one would be required.

upvoted 2 times

Henk_2025 8 months, 2 weeks ago

exactly , so the anwer is C 4 >>> NAT gateway takes precedence over other outbound connectivity methods, including a load balancer, instance-level public IP addresses, and Azure Firewall. https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-outbound-connections

upvoted 1 times

Patel777 1 year, 4 months ago

NAT Gateway doesn't need additional subnet

upvoted 1 times

goos5 1 year, 4 months ago

Answer: A. 2 subnets There are two existing subnets in VNET1: Subnet1 and GatewaySubnet. The question does not specify Subnet2 as hosted on VNET1. VM1 is already accessing the internet with its own Public iP. The NAT Gateway can be deployed to Subnet1. This won't affect the outbound internet traffic flow for VM1.

upvoted 2 times

beskar 1 year, 5 months ago

Three subnets. NAT Gateway does not live inside of a subnet.

upvoted 2 times

windowsmodulesinstallerworker 1 year, 6 months ago

nat gateway DOES NOT require a subnet, it is only associated with one.

upvoted 1 times

bobothewiseman 1 year, 9 months ago

GatewaySubnet 2 Subnet 2 Subnet 1

upvoted 1 times

manny72 2 years, 3 months ago

Azure virtual network NAT doesn't require a subnet, it's rather associated to a subnet, as many have pointed out. It supports multiple public IPs and can be associated to all subnets in a VNET. https://learn.microsoft.com/en-us/azure/nat-gateway/nat-overview There are no subnets required but we can stick to what is already there, that is 3. This is another non-sense Microsoft question. Please stop posting stuff that is creating just a lot of confusion, read the Microsoft documentation if you are not sure...."Can a NAT gateway be deployed without a public IP address or subnet? Yes, a NAT gateway can be deployed without a public IP address or prefix and subnet. However, it's not operational until you attach at least one public IP address or prefix and a subnet."... https://learn.microsoft.com/en-us/azure/nat-gateway/faq

upvoted 7 times

manny72 2 years, 3 months ago

Selected Answer: B

Azure virtual network NAT doesn't require a subnet, it's rather associated to a subnet, as many have pointed out. It supports multiple public IPs and can be associated to all subnets in a VNET. https://learn.microsoft.com/en-us/azure/nat-gateway/nat-overview

There are no subnets required but we can stick to what is already there, that is 3. This is another non-sense Microsoft question. Please stop posting stuff that is creating just a lot of confusion, read the Microsoft documentation if you are not sure.

upvoted 7 times

Feliphus 2 years ago

..."Can a NAT gateway be deployed without a public IP address or subnet? Yes, a NAT gateway can be deployed without a public IP address or prefix and subnet. However, it's not operational until you attach at least one public IP address or prefix and a subnet."... https://learn.microsoft.com/en-us/azure/nat-gateway/faq

upvoted 1 times

efayed 2 years, 3 months ago

To deploy an Azure Virtual Network NAT gateway named Gateway1 while meeting the requirements and minimizing administrative effort, you need to ensure the correct network setup. Given the information: VM1 and VM2 will access the internet using their public IP addresses. You have Vnet1 with Subnet1 and a GatewaySubnet. You need to deploy Gateway1 to Vnet1. The minimum number of subnets required on Vnet1 is 2: Subnet1: This is where VM1 is connected. GatewaySubnet: This is required for deploying the NAT gateway. Therefore, the minimum number of subnets required is 2.

upvoted 2 times

ajinkyap 2 years, 4 months ago

We dont need a subnet for NAT gateway so subnet 1 subnet 2 and gw subnet >> 3 subnets so ans is B

upvoted 2 times

ajinkyap 2 years, 4 months ago

We dont need a subnet for NAT gateway so subnet 1 subnet 2 and gw subnet >> 3 subnets so ans is C

upvoted 1 times

singhaj 2 years, 6 months ago

NAT gateway does not need a subnet to deploy it. But it need to be associated with subnet to which it needs to provide NATing. So answer is 3.

upvoted 1 times

Juan_Ochoa_TI724 2 years, 7 months ago

Only 3 subnets 1. Subnet 1 has an Basic SKU public IP address and the NAT gateway isn't compatible to deploy it in the subnet1 2. GatewaySubnet -- Reserved for VPN GW 3. An additional subnet to deploy the NAT Gateway

upvoted 2 times

HoangNam2711 2 years, 9 months ago

I have created a virtual network with 2 subnets (one is deploying a VM and one is using Subnet Gateway). The NAT Gateway can be created into a subnet deploying a VM, so I think the answer is 3Your answer is 3 and you select C ???

upvoted 1 times

HoangNam2711 2 years, 9 months ago

Selected Answer: C

I have created a virtual network with 2 subnets (one is deploying a VM and one is using Subnet Gateway). The NAT Gateway can be created into a subnet deploying a VM, so I think the answer is 3

upvoted 1 times

HieuDuc 2 years, 5 months ago

Your answer is 3 and you select C ???

upvoted 1 times

galahad 2 years, 9 months ago

According to ChatGPT the answer is 4. Yes, in Azure, a NAT (Network Address Translation) gateway typically requires its own subnet. When you deploy a NAT gateway in Azure, it is associated with a specific subnet in a virtual network. This subnet is referred to as the NAT gateway subnet.

upvoted 1 times

galahad 2 years, 9 months ago

According to ChatGPT the answer is 4. Yes, in Azure, a NAT (Network Address Translation) gateway typically requires its own subnet. When you deploy a NAT gateway in Azure, it is associated with a specific subnet in a virtual network. This subnet is referred to as the NAT gateway subnet.I did a lab to create a NAT gateway without selecting a subnet, there is no need.

upvoted 1 times

ajinkyap 2 years, 4 months ago

I did a lab to create a NAT gateway without selecting a subnet, there is no need.

upvoted 1 times

Question #30 *Topic 2*

HOTSPOT

-

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

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.

The virtual network links in the fabrikam.com DNS zone are configured as shown in the exhibit. (Click the Exhibit tab.)

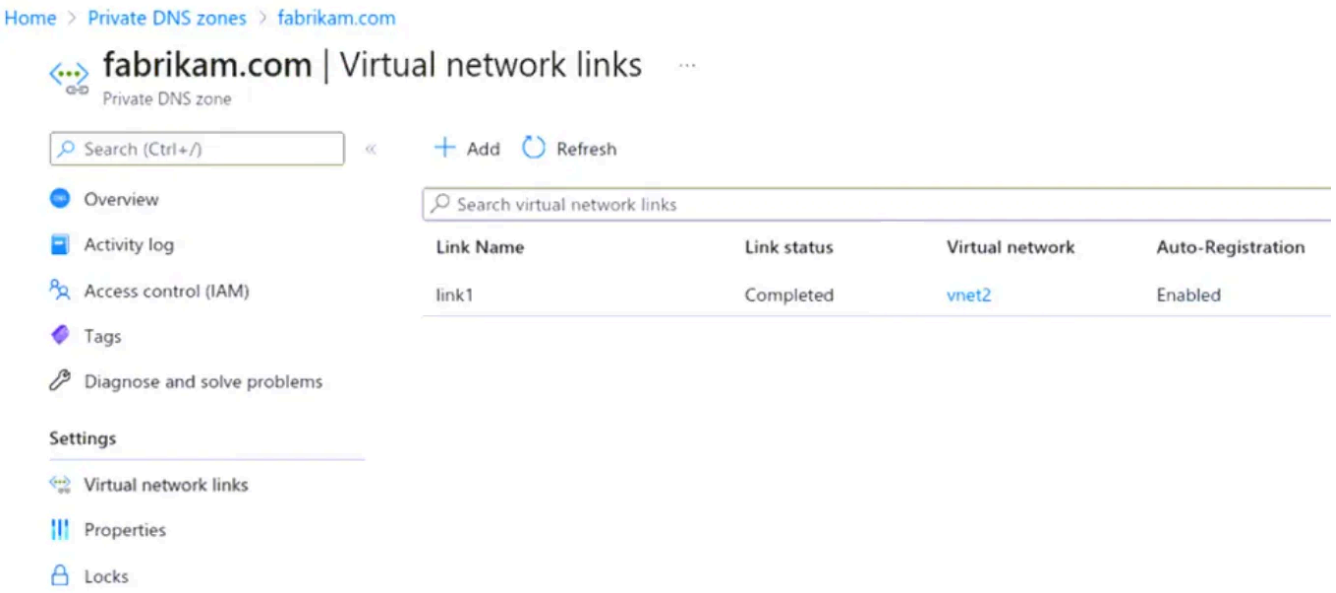
VM5 fails to resolve the IP address for app1.fabrikam.com.

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

NOTE: Each correct selection is worth one point.

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

Name	Type	Value
app1	CNAME	lb1.fabrikam.com
lb1	A	10.3.0.7
vm1	A	10.3.0.4



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.	○	○
Enabling a virtual network link for Vnet3 in the fabrikam.com DNS zone will enable VM5 to resolve app1.fabrikam.com.	○	○
Adding an A record for app1.fabrikam.com to the fabrikam.com DNS zone will enable VM5 to resolve app1.fabrikam.com.	○	○

Suggested Answer:

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.	○	○
Enabling a virtual network link for Vnet3 in the fabrikam.com DNS zone will enable VM5 to resolve app1.fabrikam.com.	○	○
Adding an A record for app1.fabrikam.com to the fabrikam.com DNS zone will enable VM5 to resolve app1.fabrikam.com.	○	○

Zorro2003 Most Recent 1 year, 2 months ago

1 NO → Changing VM5's DNS server won't help because VNet3 (where VM5 is located) isn't linked to the private DNS zone.

2 YES → Linking VNet3 to the fabrikam.com private DNS zone will allow VM5 to resolve app1.fabrikam.com.

3 NO → Adding an A record won't fix the issue since the problem is DNS zone access, not missing records.

upvoted 2 times

thekhijir 1 year, 11 months ago

NYN

N - No Link to VNET3 so another IP from VNET3 [10.4.0.2] has no impact.

Y - Link to VNET3 resolves the issue

N - No impact if there is no link to VNET3

upvoted 3 times

NSF2 2 years, 10 months ago

This is NYN because the problem is that there is no link to VNET3

upvoted 2 times

Murad01 2 years, 11 months ago

Appeared on Exam November - 2023

upvoted 2 times

g_mindset 3 years, 1 month 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 3 years, 4 months 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 enogh because there is no DNS record to VM5, and conflicting DNS records app1.fabricam.com CNAME

upvoted 1 times

Lazylinux 3 years, 4 months 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 app1My 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

Lazylinux 3 years, 4 months 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

Gabaky Highly Voted 3 years, 9 months ago

NYN

10.4.0.2 and 10.4.0.5 are within same subnet that was initially not resolving

upvoted 19 times

Madball Highly Voted 3 years, 9 months 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 50 times

bobg 3 years, 9 months ago

n/y/n . There is no mention of 10.4.0.2 and what it is in the question.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.that's not correct. even with a private dns zone link the vm will still use the azure default dns resolver 168.63.129.16. the ip 10.4.0.2 is just nothing

upvoted 6 times

bobg 3 years, 9 months ago

n/y/n . There is no mention of 10.4.0.2 and what it is in the question.

upvoted 6 times

Aziza_Adam 3 years, 9 months ago

No

Yes

No

upvoted 6 times

Madball 3 years, 9 months 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.that's not correct. even with a private dns zone link the vm will still use the azure default dns resolver 168.63.129.16. the ip 10.4.0.2 is just nothing

upvoted 7 times

Madball 3 years, 9 months 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

windowsmodulesinstallerworker 1 year, 6 months ago

that's not correct. even with a private dns zone link the vm will still use the azure default dns resolver 168.63.129.16. the ip 10.4.0.2 is just nothing

upvoted 1 times

Question #31 *Topic 2*

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.

Suggested Answer: *B*

Community vote distribution

A (100%)

Zorro2003 Most Recent 1 year, 2 months ago

Selected Answer: A

The correct answer is A. Delete Gateway1

Short Explanation

Azure Virtual WAN has its own built-in VPN gateways.

Existing Gateway1 becomes redundant and should be removed.

Branch offices will connect directly to the Virtual WAN hub via Site-to-Site VPN.

Why Not Others

B. P2S VPN → For individual devices, not branch offices.

C. Traffic Manager → Handles DNS load balancing, not VPN routing.

D. Active-active Gateway1 → Increases throughput but doesn't integrate with Virtual WAN.

upvoted 1 times

thekhijir 1 year, 11 months ago

Selected Answer: A

A. Delete GW1

upvoted 1 times

Inderdation Highly Voted 2 years, 8 months ago

Why do so many questions in the sets have wrong answers, and why are they not corrected as well. Wtf is this bs.

upvoted 9 times

Lazylinux 3 years 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 3 years, 2 months 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 3 years, 5 months ago

Selected Answer: A

Correct

upvoted 1 times

tomtom2022 3 years, 6 months ago

Selected Answer: A

A is correct

upvoted 1 times

ayoubneo 3 years, 8 months ago

Selected Answer: A

Correct

upvoted 1 times

AP78 3 years, 8 months ago

Selected Answer: A

Correct

upvoted 1 times

omgMerrick 3 years, 8 months 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 8 times

flurgen248 Highly Voted 3 years, 8 months 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 12 times

Ayokun 3 years, 9 months ago

Enable active - active and then delete.

upvoted 1 times

Ayokun 3 years, 9 months ago

Enable active - active and then delete.Are u ok bro?

upvoted 1 times

drprepper_ 3 years, 8 months ago

Are u ok bro?

upvoted 8 times

samir111 3 years, 9 months ago

Selected Answer: A

delete Gateway1

upvoted 2 times

certacc 3 years, 9 months 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 3 years, 9 months ago

Why p2s ? I would delete GW first!

upvoted 3 times

Bbb78 3 years, 9 months ago

Why p2s ? I would delete GW first!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-vwanI 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 3 times

Ayboum 3 years, 9 months 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-vwanI 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 5 times

Ayboum 3 years, 9 months 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 3 years, 8 months 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

Question #32 *Topic 2*

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

Suggested Answer: *A*

Community vote distribution

A (100%)

omgMerrick Highly Voted 2 years, 8 months 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) attacks4.

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 7 times

omgMerrick Highly Voted 2 years, 8 months ago

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) attacks4. 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/the main point is not that an LB is distributing the traffic but that an Internal LB is always getting its front end IP address from the deployment subnet

upvoted 7 times

WaleedSaleh 2 years, 4 months ago

Selected Answer: A

A. Internal Load Balancers

upvoted 2 times

Sergovladi Most Recent 1 year, 10 months ago

the main point is not that an LB is distributing the traffic but that an Internal LB is always getting its front end IP address from the deployment subnet

upvoted 1 times

flurgen248 2 years, 8 months 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

mVic 2 years, 9 months ago

Selected Answer: A

Internal Load Balancers is the right option.

upvoted 3 times

Ayboum 2 years, 9 months ago

Correct

upvoted 2 times

Ayboum 2 years, 9 months ago

Correctok sir, very good, god bless.

upvoted 2 times

harshit101 2 years, 9 months ago

ok sir, very good, god bless.

upvoted 1 times

Question #33 *Topic 2*

You have an Azure subscription mat contains tour 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

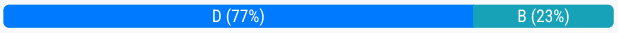
B. Azure Route Server

C. Azure Private Link

D. Azure Firewall

Suggested Answer: *A*

Community vote distribution



Ayboum Highly Voted 3 years, 9 months 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 19 times

Ayboum Highly Voted 3 years, 9 months 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=cliI 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-throughputAgree 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 19 times

679956a Most Recent 8 months, 1 week ago

Selected Answer: D

Azure Route Server (ARS) does not provide transit routing between VNets without a Network Virtual Appliance (NVA)

upvoted 2 times

mammoot 3 years, 9 months 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

mammoot 3 years, 9 months 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-throughputAgree 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 2 times

Zorro2003 1 year, 2 months ago

Selected Answer: D

You're right — Azure Firewall can indeed be the best choice in this hub-and-spoke scenario, especially when you want secure transitive routing between spokes. Let me explain why your reference aligns with Microsoft's recommendations:

upvoted 1 times

Patel777 1 year, 4 months ago

Selected Answer: B

Azure Firewall can be used to support transitive routing via User Defined Routes (UDRs), but it introduces latency and cost, and may not maximize throughput.

upvoted 2 times

xRiot007 1 year, 7 months ago

D - Azure Firewall

Ref: https://learn.microsoft.com/en-us/azure/architecture/networking/architecture/hub-spoke?tabs=cli#spoke-connections-through-azure-firewall-or-nva

upvoted 1 times

cannoe 1 year, 8 months ago

Selected Answer: B

Azure Firewall adds latency due to packet inspection or processing of traffic filtering

upvoted 3 times

a250fb0 1 year, 9 months ago

Selected Answer: B

Azure Route Server simplifies dynamic routing between your network virtual appliance (NVA) and your virtual network. It allows for transitive routing between spokes, which is essential for your requirement of supporting transitive routing

upvoted 2 times

xRiot007 1 year, 7 months ago

"Azure Firewall is not designed for routing purposes" - Who told you that? Wrong

https://learn.microsoft.com/en-us/azure/architecture/networking/architecture/hub-spoke?tabs=cli#spoke-connections-through-azure-firewall-or-nva

upvoted 1 times

Kegomoditswe 2 years ago

isnt the answer A

upvoted 1 times

Kegomoditswe 2 years ago

Why do some say the answer is A OR B

upvoted 1 times

Lazylinux 3 years 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

alinuxguru70 1 year, 11 months ago

Selected Answer: B

A and C are obviously wrong

B. Azure Route Server is purpose built for creating transitive routes. https://learn.microsoft.com/en-us/azure/route-server/route-server-faq

D. Azure Firewall is not designed for routing purposes

upvoted 3 times

alinuxguru70 1 year, 11 months ago

A and C are obviously wrong B. Azure Route Server is purpose built for creating transitive routes. https://learn.microsoft.com/en-us/azure/route-server/route-server-faq D. Azure Firewall is not designed for routing purposes"Azure Firewall is not designed for routing purposes" - Who told you that? Wrong https://learn.microsoft.com/en-us/azure/architecture/networking/architecture/hub-spoke?tabs=cli#spoke-connections-through-azure-firewall-or-nva

upvoted 3 times

Azused 3 years, 2 months 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 3 years, 4 months ago

Selected Answer: D

I think to maximize throughput NVA is the best choice.

upvoted 1 times

daemon101 3 years, 4 months 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 throuhput reference:

https://learn.microsoft.com/en-us/azure/firewall/firewall-faq#:~:text=Azure%20Firewall's%20initial%20throughput%20capacity,100%20Gbps%20for%20Premium%20SKU.

upvoted 3 times

KyDD 3 years, 1 month ago

Agreed and last sentence is the key why choice b not complete.

upvoted 2 times

MrBlueSky 3 years, 7 months 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 3 years, 9 months 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 6 times

omgMerrick 3 years, 9 months 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-network-communications

upvoted 4 times

ronin201 3 years, 4 months 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 approachAgreed and last sentence is the key why choice b not complete.

upvoted 3 times

ronin201 3 years, 4 months 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 3 times

mVic 3 years, 9 months 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 2 times

Bbb78 3 years, 9 months ago

b.Azure Router Service is probably a better answer than VPN GW

upvoted 4 times

Kafura 3 years, 7 months 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 2 times

_fvt 3 years, 7 months 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

Question #34 *Topic 2*

HOTSPOT

-

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

You have the virtual networks shown in the following table.

You have the subnets shown in the following table.

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

NOTE: Each correct selection is worth one point.

Name	Location
RG1	East US
RG2	East US
RG3	UK West

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

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

Statements	Yes	No
Vnet1 can be moved to RG3.	○	○
Three hundred virtual machines can be deployed to the East US Azure region.	○	○
A new virtual network named Vnet2 can be created in RG2 in the East US Azure region.	○	○

Suggested Answer:

Statements	Yes	No
Vnet1 can be moved to RG3.	○	○
Three hundred virtual machines can be deployed to the East US Azure region.	○	○
A new virtual network named Vnet2 can be created in RG2 in the East US Azure region.	○	○

Madball Highly Voted 3 years, 9 months 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.youre wrong. you can deploy two vnets in the same RG, as long as they are in different regions.No you can't, i just tested it on lab!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 28 times

Madball Highly Voted 3 years, 9 months 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 28 times

CheMetto Most Recent 1 year, 1 month ago

So. YNN

For the first one, i create this environment:

Rg1 in the east US

Vnet1 in the east US

Address space 10.0.0.0/16

RG2 in italy North

'SameAddressSpace' in the Italy North

Address Space 10.0.0.0/16

I tried to move vnet1 to RG2 -- the validation gave me ok and when i confirm the move, it moved to RG2.

So it's a Y!

The second one is N! The subnet has only 251 ip address available. You should create a larger subnet/another subnet to accomplish the 300 vm.

The last one is N! I tried to create a new virtual network with the same name and i got "There is already a virtual network with the name 'SameAdressSpace' in the current resource group." (i had already a vnet with the name "SameAdressSpace" (Sorry for the typo :D))

upvoted 1 times

ubdubdoo 3 years, 6 months ago

youre wrong. you can deploy two vnets in the same RG, as long as they are in different regions.No you can't, i just tested it on lab!

upvoted 3 times

ubdubdoo 3 years, 6 months ago

youre wrong. you can deploy two vnets in the same RG, as long as they are in different regions.

upvoted 3 times

Chezzer83 1 year, 3 months ago

This question like many others are so poorly worded. For example expanding or adding a new subnet will allow 300 vms

upvoted 1 times

Omniglass 2 years ago

Can't have the same virtual network name in the same resource group, even if its a different region. Just tested this in a lab.

upvoted 1 times

staffo 3 years, 9 months 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 10 times

staffo 3 years, 9 months 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.Not sure how you tested, must be Azure located in MARS!! sorry we are on Earth!!Thank you for the great insight

upvoted 10 times

bangbang55 2 years, 9 months ago

Madball is right, I just tested in lab. YNN.

You can NOT have 2 VNets of an identical name in the same Resource Group, just tried it.

You can migrate VNets to another region/RG, validation was fine.

upvoted 3 times

Lazylinux 3 years, 4 months ago

Not sure how you tested, must be Azure located in MARS!! sorry we are on Earth!!Thank you for the great insight

upvoted 3 times

Lazylinux 3 years, 4 months ago

Not sure how you tested, must be Azure located in MARS!! sorry we are on Earth!!

upvoted 3 times

Supreem 3 years, 1 month ago

Such poorly written question, especially point 2. Thanks again Microsoft.

upvoted 4 times

Lazylinux 3 years, 4 months 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 4 times

thekhijir 1 year, 11 months ago

I agree but if there are active resources, it's not going to be easy to change the IP. Especially in production environment.

upvoted 1 times

sirio 2 years, 9 months ago

I think we should consider just the information showed in the text, and that the second statement should be interpreted as "300 VMs can be deployed in the existing Vnets in the East US region". Considering that, since Vnet2 is in the West US region, the VMs deployed in the East US should not be just in Vnet1?

upvoted 1 times

Lazylinux 3 years, 4 months 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 3 times

asghs 2 years, 1 month ago

Y: Yes, you can move a VNet to a different resource group even if another VNet with the same IP address range exists in that target resource group. The IP address range overlap is not an issue unless the VNets are peered or need to communicate with each other. N: East Us has Vnet1 and Subnet1-1 which has /24 subnet mask, 256 hosts - 5 azure reserved = 251 hosts Y: All Azure resources have a name. The name must be unique within a scope, that may vary for each resource type. For example, the name of a virtual network must be unique within a resource group, but can be duplicated within a subscription or Azure region. https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-vnet-plan-design-armCan't have the same virtual network name in the same resource group, even if its a different region. Just tested this in a lab.

upvoted 1 times

asghs 2 years, 1 month ago

Y: Yes, you can move a VNet to a different resource group even if another VNet with the same IP address range exists in that target resource group. The IP address range overlap is not an issue unless the VNets are peered or need to communicate with each other. N: East Us has Vnet1 and Subnet1-1 which has /24 subnet mask, 256 hosts - 5 azure reserved = 251 hosts Y: All Azure resources have a name. The name must be unique within a scope, that may vary for each resource type. For example, the name of a virtual network must be unique within a resource group, but can be duplicated within a subscription or Azure region.

https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-vnet-plan-design-arm

upvoted 1 times

Himank20 3 years, 6 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 5 times

Lazylinux 3 years, 4 months 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 4 times

Anonymous 3 years, 6 months 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 6 times

crypto700 3 years, 6 months ago

You are right... just tested in the Lab

YNN

upvoted 4 times

crypto700 3 years, 6 months 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

crypto700 3 years, 6 months 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.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.You are right... just tested in the Lab YNN

upvoted 1 times

[Removed] 3 years, 6 months 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 6 times

P3r 1 year, 11 months ago

Thank you for the great insight

upvoted 2 times

c2e9cb4 2 years, 10 months ago

No you can't, i just tested it on lab!

upvoted 3 times

jarz 3 years, 6 months 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 7 times

Question #35 *Topic 2*

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
-

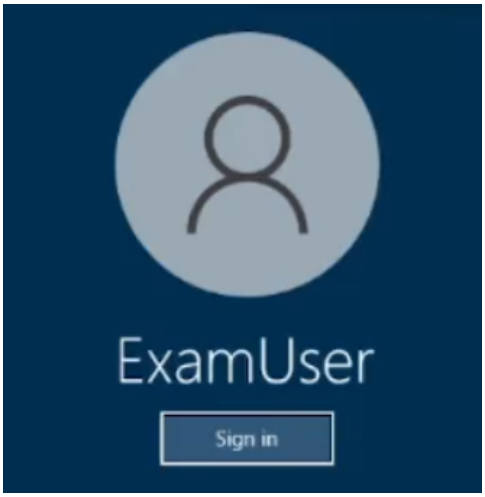
If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

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.



Suggested 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

Ozarsif Most Recent 1 year, 3 months ago
as of august, 2025, there is no labs anymore
upvoted 2 times

Lazylinux 2 years, 6 months ago
Yep Just deploy Azure NAT Gateway and nothing else
upvoted 1 times

trashbox 2 years, 6 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 2 times

Question #36 *Topic 2*

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
-

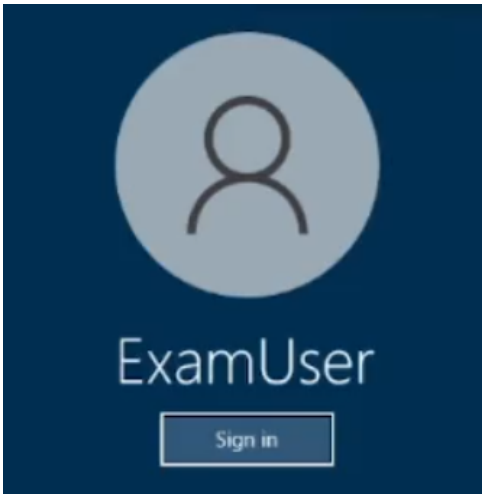
If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

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.



Suggested 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 2 years, 8 months ago
/23 can fit 507 addresses. 512 hosts - 5 reserved = 507. The reserved ip address are .0 .1 .2 .3 and .255
upvoted 10 times

Ozarsif Most Recent 1 year, 3 months ago
as of august, 2025, there is no labs anymore
upvoted 2 times

Nagachn 1 year, 6 months ago
How do we know which vnet subnet4-3 belongs to? because we can't directly go to the subnets 4- 3. First navigate to the vnet and then choose the subnets
upvoted 1 times

NahIgotPride 2 years, 6 months 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 2 years, 7 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 2 years, 8 months ago
/23 subnet won't be able to have 507 hosts, as azure reserves 5 IP addresses. You need /22 subnet.
upvoted 4 times

Sein 2 years, 8 months ago
/23 subnet won't be able to have 507 hosts, as azure reserves 5 IP addresses. You need /22 subnet.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?2^9= 512 512-5 = 507
upvoted 4 times

VeryOldITGuy 2 years, 3 months 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?2^9= 512 512-5 = 507
upvoted 2 times

VeryOldITGuy 2 years, 3 months 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 2 times

cda26aa 2 years ago

2^9= 512 512-5 = 507

upvoted 1 times

Question #37 *Topic 2*

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

Suggested Answer: *A*

Community vote distribution

A (100%)

Zorro2003 Most Recent 1 year, 2 months ago

Selected Answer: A

The correct answer is:

A. internal load balancers

Explanation: Internal Load Balancers (ILBs) require private IP addresses within the subnet because they distribute traffic among resources inside the virtual network.

Azure DDoS Protection (B) is applied at the virtual network level and doesn't require IPs in subnets.

Service endpoint policies (C) are configurations applied to subnets but do not consume IP addresses.

Service endpoints (D) extend VNet connectivity but don't require dedicated IP addresses either.

So, when planning IP addressing for Azure subnets, you must allocate IP addresses for internal load balancers.

upvoted 1 times

Henryjb3 2 years, 4 months ago

Repeat question.

upvoted 3 times

NSF2 2 years, 4 months 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 2 years, 6 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 2 years, 6 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 2 years, 6 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

Question #38 *Topic 2*

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
-

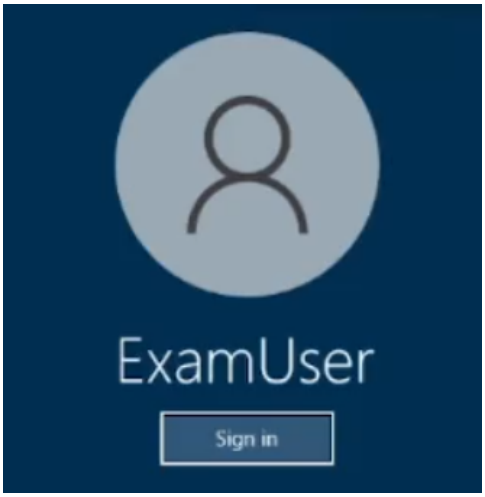
If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

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.



Suggested Answer:

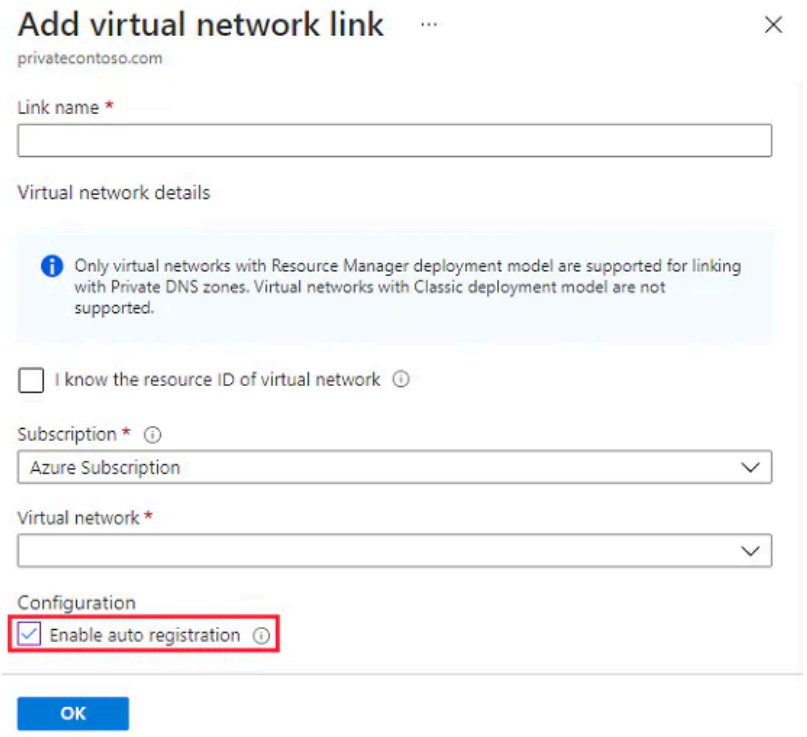
What is the auto registration feature in Azure DNS private zones?
The Azure DNS private zones auto registration feature manages DNS records for virtual machines deployed in a virtual network. When you link a virtual network with a private DNS zone with this setting enabled, a DNS record gets created 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.



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

Ozarsif Most Recent 1 year, 3 months ago
as of august, 2025, there is no labs anymore
upvoted 1 times

beeee12 2 years, 2 months ago
https://learn.microsoft.com/en-us/azure/dns/private-dns-virtual-network-links
upvoted 1 times

Lazylinux 2 years, 6 months ago
Yep create 2 virtual links to private DNS zone for Vnet 1 and 2 and enable Auto-registration for both
upvoted 4 times

lzariqi 2 years, 8 months ago

Answer is right.

upvoted 2 times

Question #39 *Topic 2*

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
-

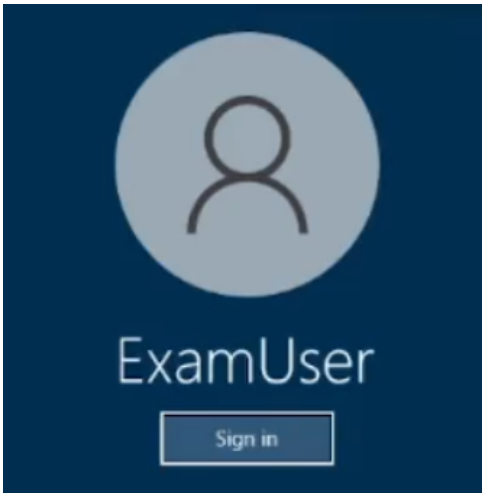
If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

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.



Suggested Answer:

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

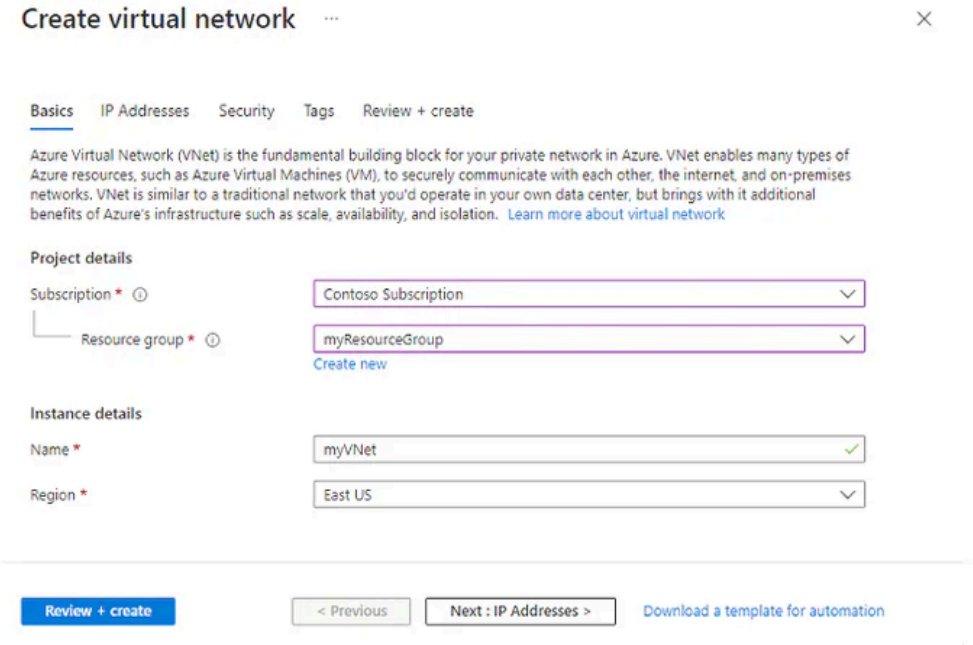
Create a virtual network

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.

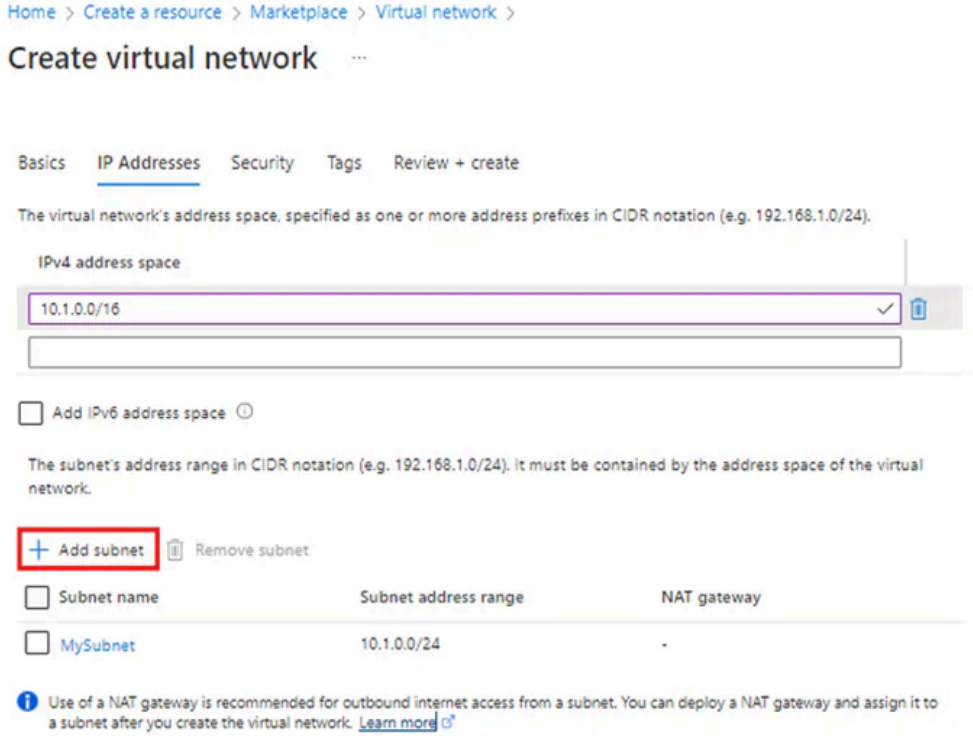
Step 3: In the Virtual Network page, select Create.

Step 4: In Create virtual network, enter or select this information in the Basics tab:



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:



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 Highly Voted 2 years, 3 months 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.10.5.1.0/16 is not valid CIDR. Hence use 10.5.1.0/24. A default subnet 10.5.1.0 - 10.5.1.55 will be created automatically. No need to add subnetYou can use either a 10.5.0.0/16 or 10.0.0.0/8 CIDRs for the Vnet addresses and a 10.5.1.0/24 as the subnet address range

upvoted 9 times

mein17 Highly Voted 2 years, 3 months 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 9 times

bobothewiseman 1 year, 10 months ago

10.5.1.0/16 is not valid CIDR. Hence use 10.5.1.0/24. A default subnet 10.5.1.0 - 10.5.1.55 will be created automatically. No need to add subnet

upvoted 1 times

bobothewiseman 1 year, 10 months ago

10.5.1.0/16 is not valid CIDR. Hence use 10.5.1.0/24. A default subnet 10.5.1.0 - 10.5.1.55 will be created automatically. No need to add subnetYou can use either a 10.5.0.0/16 or 10.0.0.0/8 CIDRs for the Vnet addresses and a 10.5.1.0/24 as the subnet address range

upvoted 1 times

pattj2 1 year, 7 months ago

You can use either a 10.5.0.0/16 or 10.0.0.0/8 CIDRs for the Vnet addresses and a 10.5.1.0/24 as the subnet address range

upvoted 1 times

Crazysaffer 2 years, 5 months ago

Remember to select the right location. (France Central Azure region)

upvoted 5 times

Ozarsif Most Recent 1 year, 3 months ago

as of august, 2025, there is no labs anymore

upvoted 2 times

Question #40 *Topic 2*

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
-

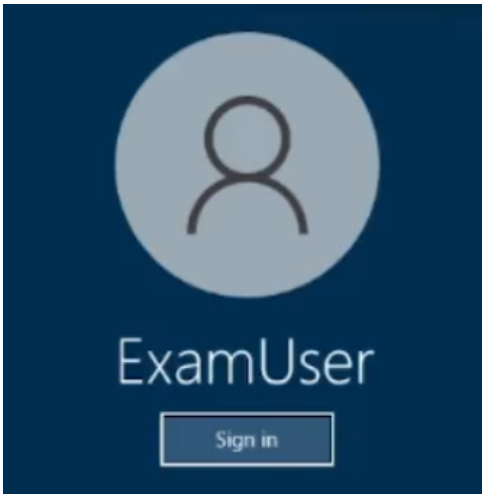
If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

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.

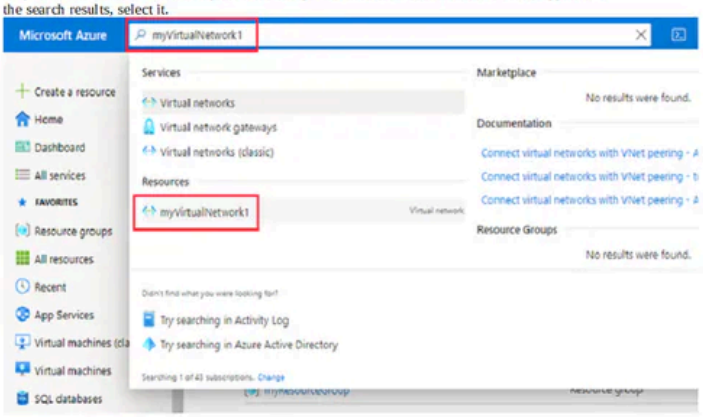
To complete this task, sign in to the Azure portal.



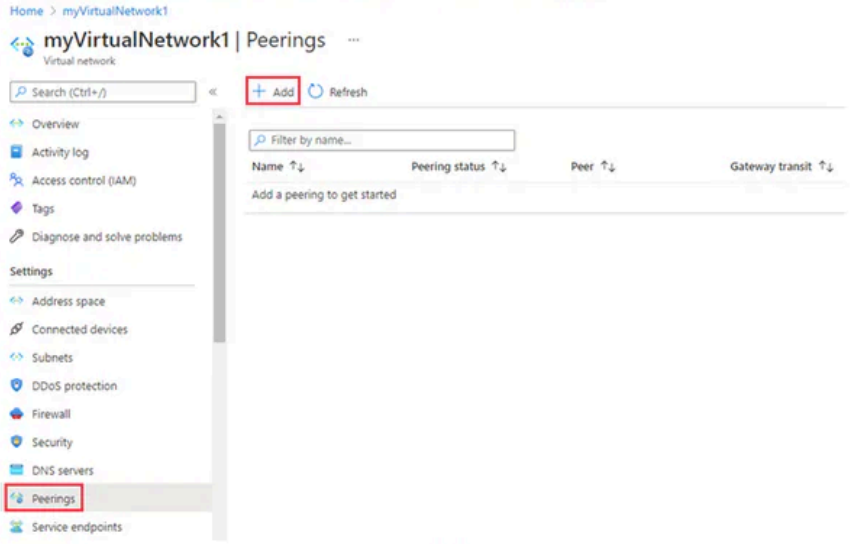
Suggested Answer:

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:

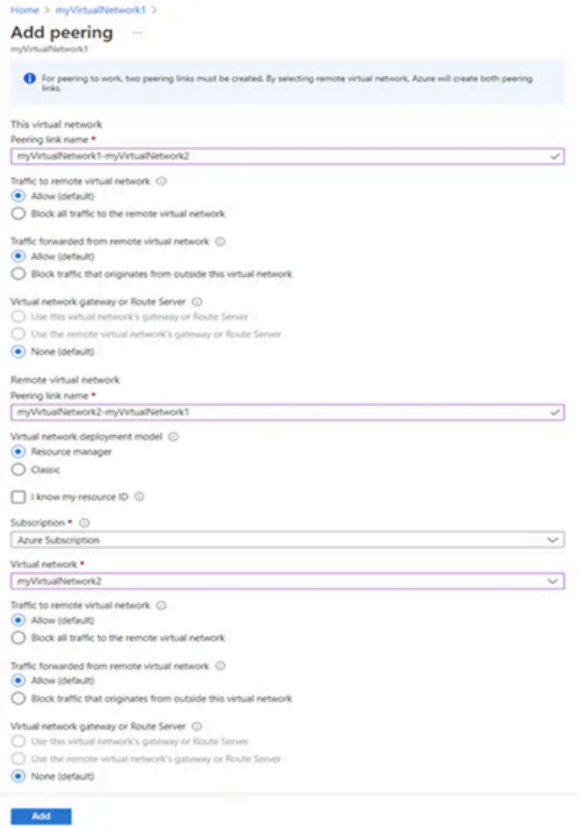


Step 3: Enter or select the following information, accept the defaults for the remaining settings, and then select Add.

* ..

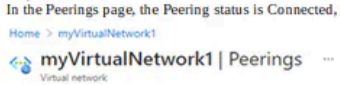
* Virtual network

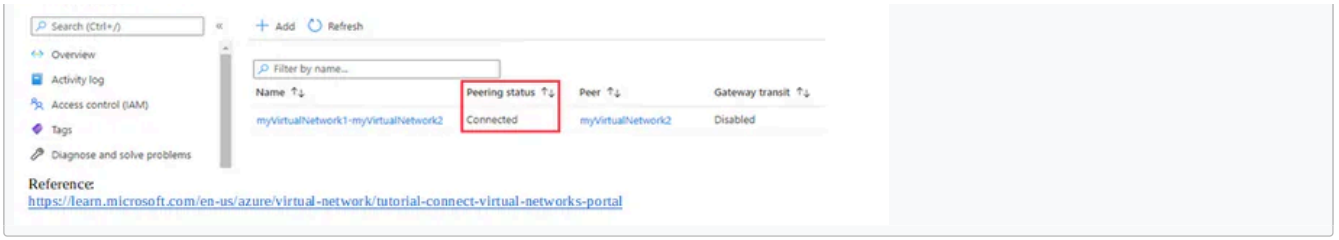
Select VNET2 for the name of the remote virtual network. The remote virtual network can be in the same region of VNET1 or in a different region.



Step 4: Click Add

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





Ozarsif Most Recent 1 year, 3 months ago

as of august, 2025, there is no labs anymore

upvoted 2 times

vanrell 2 years, 1 month ago

Correct.

upvoted 2 times

Question #41 *Topic 2*

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
-

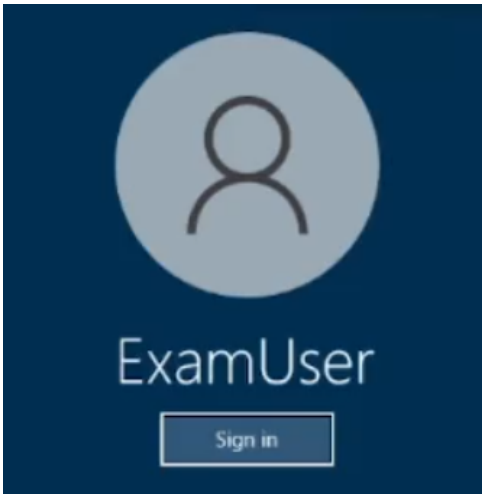
If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

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.



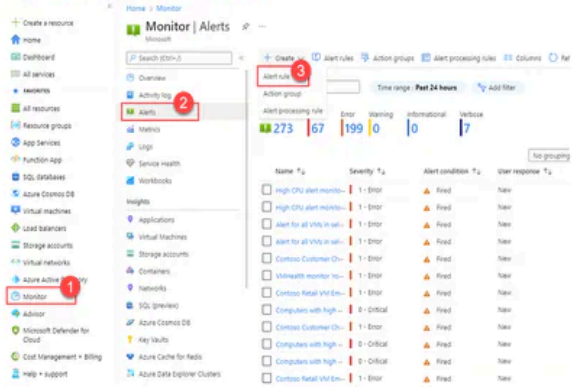
Suggested Answer:

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.

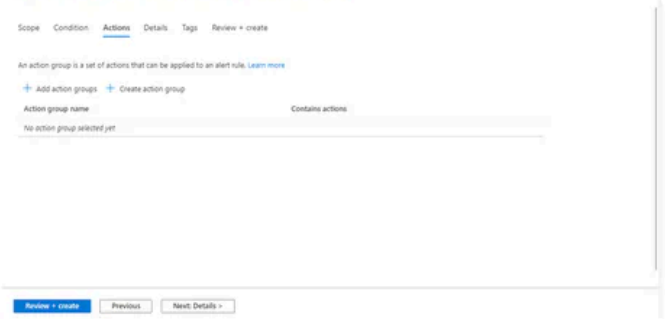
Step 6: Select Next: Condition at the bottom of the page.

Step 7: On the Select a signal pane, filter the list of signals by using the signal type and monitor service

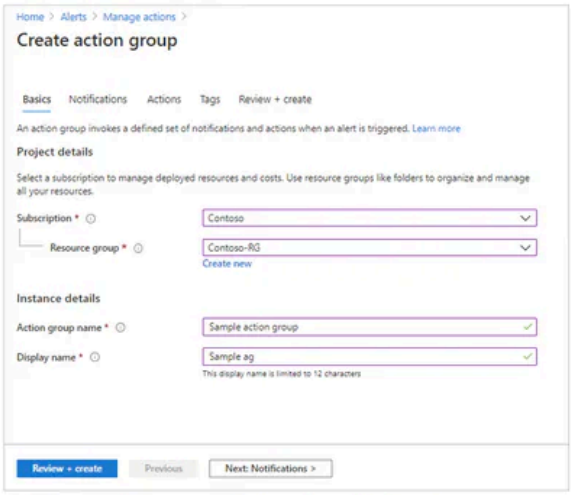
* Signal type: The type of alert rule you're creating.
We select Activity log

* 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.

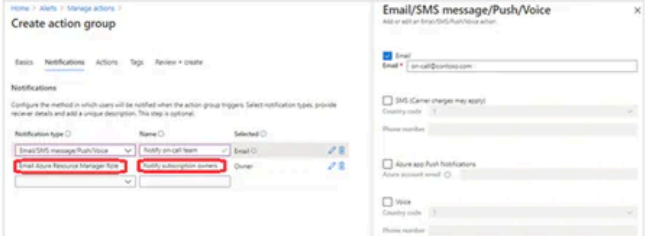


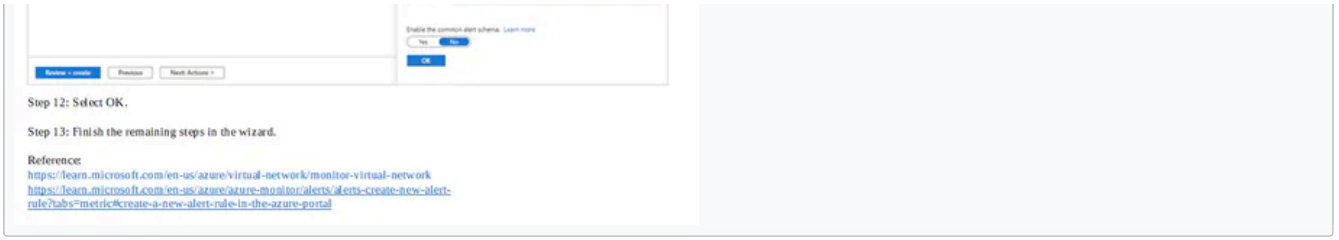
Step 9: Configure basic action group settings



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





Lazylinux Highly Voted 3 years 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 25 times

Lazylinux Highly Voted 3 years 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> DONESweet!

upvoted 25 times

thekhijir 2 years ago

Sweet!

upvoted 1 times

ABIYGK 3 years, 5 months 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 12 times

ABIYGK 3 years, 5 months 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+CreateIncorrect 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 12 times

Lazylinux 3 years 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 7 times

Ozarsif Most Recent 1 year, 3 months ago

as of august, 2025, there is no labs anymore

upvoted 2 times

Question #42 *Topic 2*

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
-

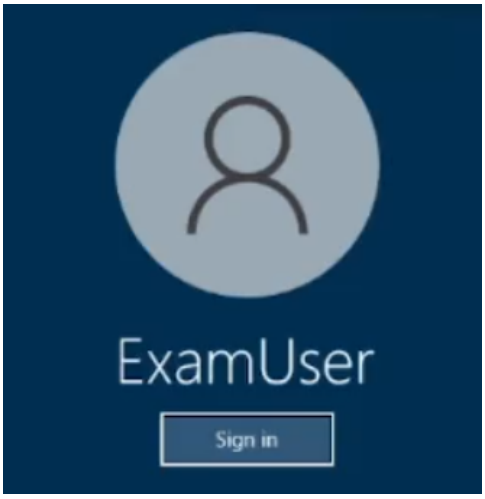
If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

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.



Suggested Answer:

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.

Create a diagnostic setting to send resource logs to a Log Analytics workspace or to a Storage Account.

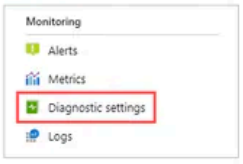
Archiving logs and metrics to a Storage account is useful for audit, static analysis, or backup. Compared to using Azure Monitor Logs or a Log Analytics workspace, Storage is less expensive, and logs can be kept there indefinitely.

Create diagnostic settings

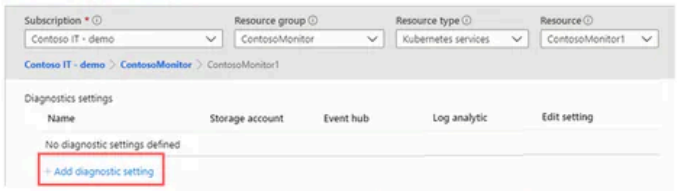
You can configure diagnostic settings in the Azure portal either from the Azure Monitor menu or from the menu for the resource.

Step 1: Select the Virtual Network VNET1.

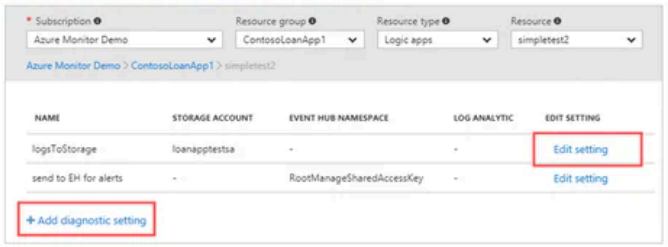
Step 2: Select Diagnostic settings under Monitoring on the resource's menu.



Step 3: If no settings exist on the resource you've selected, you're prompted to create a setting. Select Add diagnostic setting.

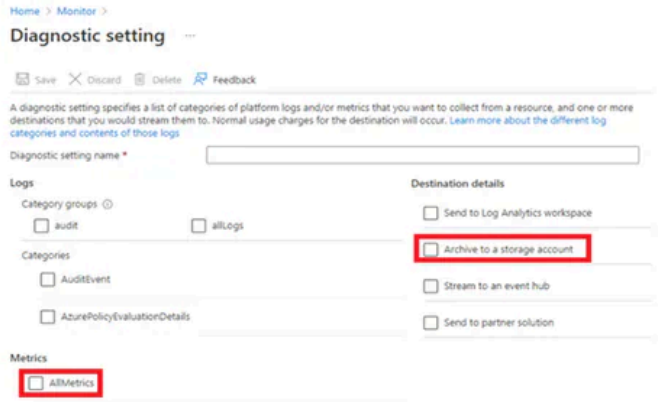


If there are existing settings on the resource, you see a list of settings already configured. Select Add diagnostic setting to add a new setting. Or select Edit setting to edit an existing one. Each setting can have no more than one of each of the destination types.



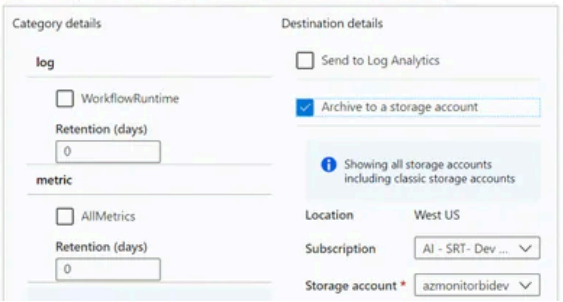
Step 4: Give your setting a name if it doesn't already have one.

Step 5: Logs and metrics to route: Select AllMetrics if you want to store metrics in Azure Monitor Logs too.



Step 6: Destination details. Select Archive to a storage account

Step 7: Storage: Select the Subscription, Storage account, and Retention policy.





Ozarsif Most Recent 1 year, 3 months ago

as of august, 2025, there is no labs anymore

upvoted 2 times

MCCC454 2 years, 3 months ago

Microsoft wont ask this question because its being deprecated 30 sept 2025. This question should be deleted from examtopics.

upvoted 2 times

HOzwei 2 years, 5 months 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 2 times

Question #43 *Topic 2*

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.

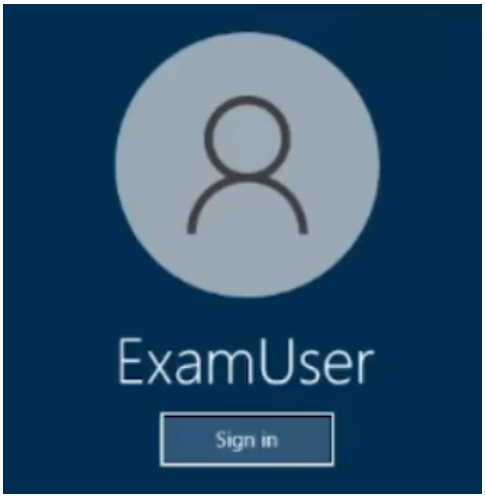
The following information is for technical support purposes only:

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.



Suggested Answer:

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

Ozarsif Most Recent 1 year, 3 months ago
as of august, 2025, there is no labs anymore
upvoted 2 times

Lazylinux 2 years, 4 months 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 4 times

bp_a_user 2 years, 7 months ago
key is here to use a ip-address prefix
upvoted 4 times

Techbiz 2 years, 7 months ago
The right solution involves provisioning a NAT gateway and integrating it with the subnet
upvoted 2 times

Shimi 3 years, 1 month ago
Shouldn't this be a standard load balancer?
upvoted 2 times

Shimi 3 years, 1 month ago

Shouldn't this be a standard load balancer?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 2 times

MrBlueSky Highly Voted 3 years, 1 month 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 9 times

Question #44 *Topic 2*

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.

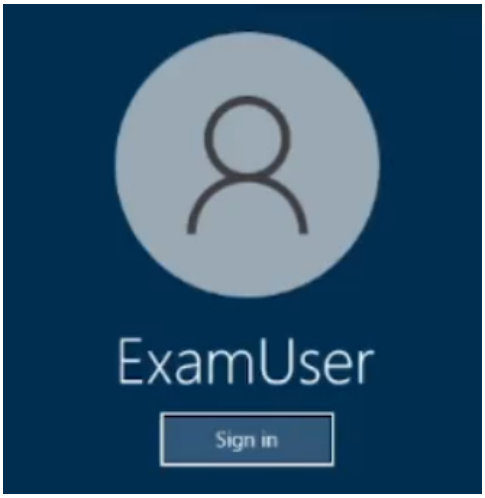
The following information is for technical support purposes only:

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.



Suggested Answer:

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*

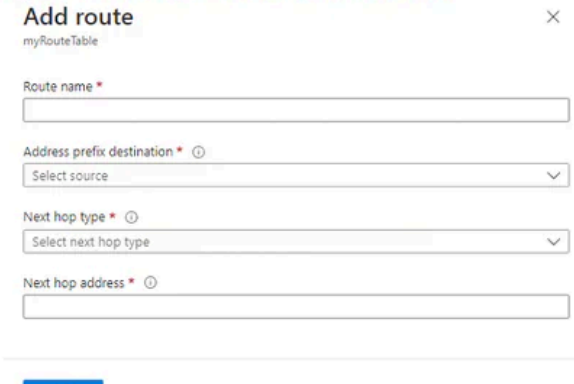
Step 5: Select Review + create and then Create to create your new route table.

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.



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.

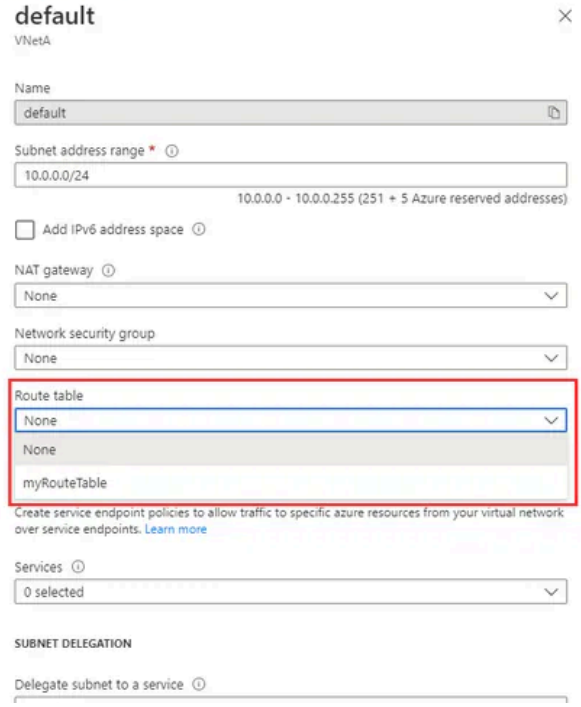
Stage 3: Associate a route table to a subnet

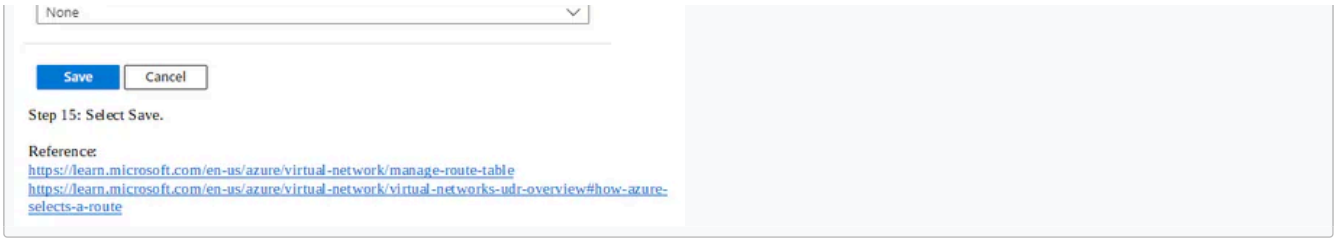
Step 11: In the virtual network list, choose the virtual network that contains the subnet you want to associate a route table to.

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.





khanda Highly Voted 3 years, 1 month ago

Next hop should not be internet if you want to send your internet traffic to an NVA. It should be "Virtual appliance"You are right. I have confirmed that when "Internet" is specified in the next hop type, the next hop address cannot be entered.you're right

upvoted 24 times

khanda Highly Voted 3 years, 1 month ago

Next hop should not be internet if you want to send your internet traffic to an NVA. It should be "Virtual appliance"

upvoted 24 times

trashbox 2 years, 6 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

occupatissimo 3 years ago

you're right

upvoted 2 times

Ozarsif Most Recent 1 year, 3 months ago

as of august, 2025, there is no labs anymore

upvoted 1 times

Lazylinux 2 years, 4 months 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 4 times

Question #45 *Topic 2*

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.

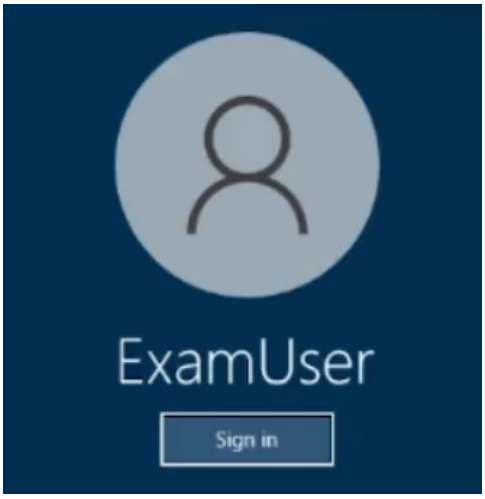
The following information is for technical support purposes only:

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.



Suggested 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.

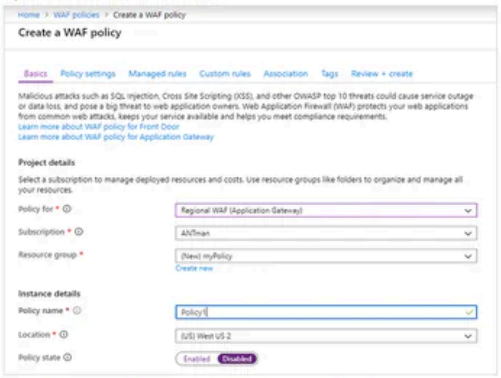
Step 1: On the upper left side of the portal, select Create a resource. Search for WAF, select Web Application Firewall, then select Create.

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.

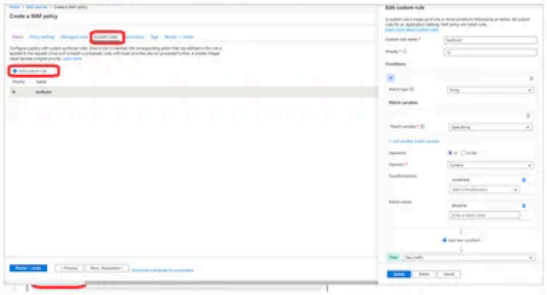
Step 4: Select Review + create, then select Create.



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.

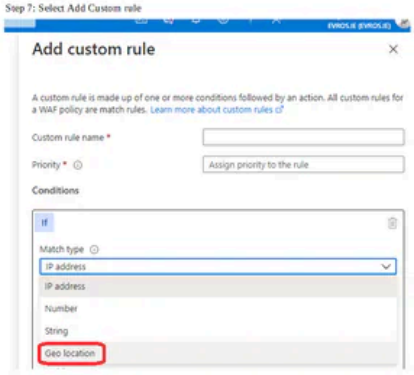
Custom rules

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



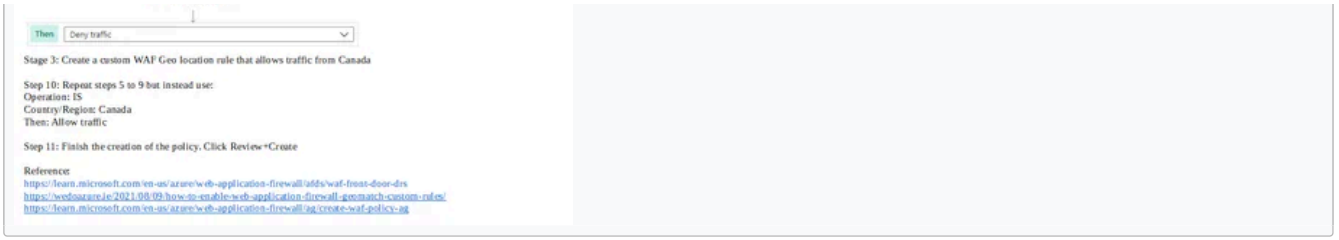
Step 8: Select Geo location

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.

Conditions





occupatissimo Highly Voted 3 years, 6 months ago

one rule blocking all that isn't from canada is enough

upvoted 15 times

Lazylinux Highly Voted 3 years 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 6 times

Ozarsif Most Recent 1 year, 3 months ago

as of august, 2025, there is no labs anymore

upvoted 1 times

thekhijir 2 years ago

Rule Priority Example Allow Canada IPs Rule: Priority: 100 (this rule will be evaluated first) Action: Allow requests from Canadian IP addresses. Block All Other Traffic Rule: Priority: 200 (this rule will be evaluated after the allow rule) Action: Block all other requests. Azure Portal View While I can't provide a direct screenshot, here's a textual representation of how it might look in the Azure portal: +----------+ | WAF Policy Rules | +----------+----------+ | Rule Name | Priority | +----------+----------+ | AllowCanadaIPs | 100 | | BlockAllOtherTraffic | 200 | +----------+----------+

upvoted 2 times

LieJ0n 2 years, 7 months ago

Creating an allow custom rule, omits all other rules and prevents the "protect from known web attack vectors" requirement. only create a block rule

upvoted 1 times

Question #46 *Topic 2*

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.

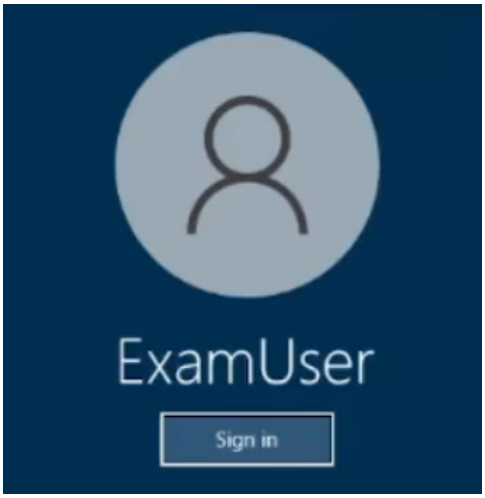
The following information is for technical support purposes only:

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.



Suggested 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.

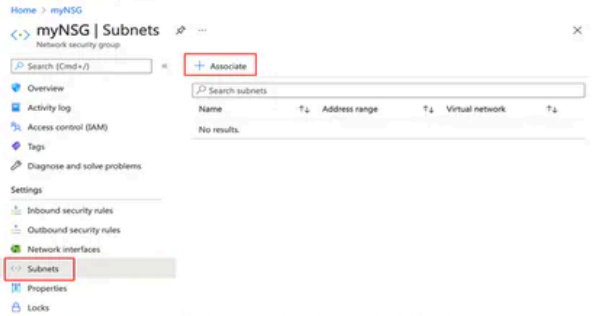
Step 5: Select Create.

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



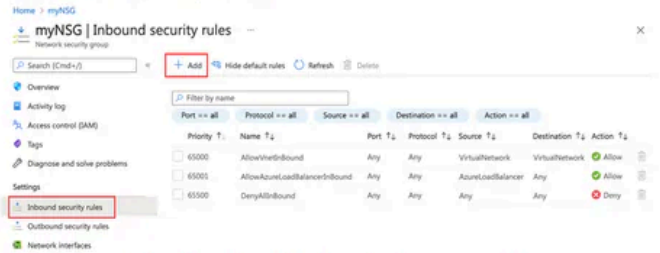
Step 9: Under Associate subnet, select myVNet (the virtual network that is available) for Virtual network.

Step 10: Select subnet1-2 for Subnet, and then select OK.

Stage 3: Create security rule

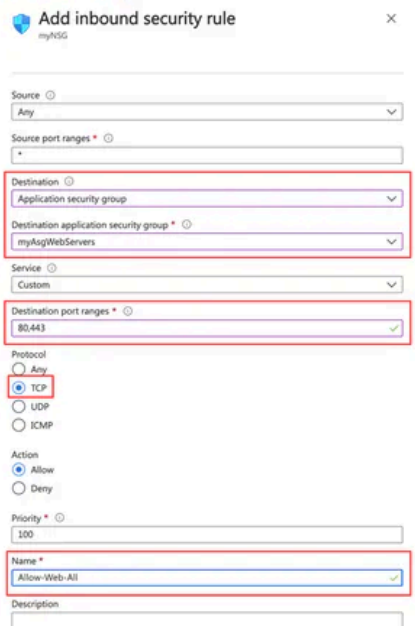
Step 11: Select Inbound security rules from the Settings section of myNSG.

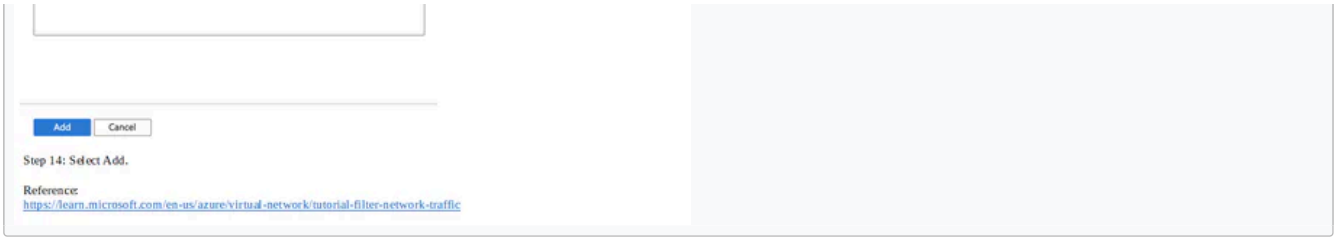
Step 12: In Inbound security rules page, select + Add:



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





ABIYGK Highly Voted 2 years, 11 months 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 SaveAllow 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.You need 2 rules, also allowing traffic inside the vnet, as @mabalon wrote.No need! There is a default rule “allowVnetInbound” to allow which permits communication between resources within the same virtual network (including the same subnet).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. By default, virtual machines in the same subnet can communicate based on a default NSG rule allowing intra-subnet traffic. 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

upvoted 15 times

trashbox Highly Voted 2 years, 6 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 7 times

volto 2 years, 7 months ago

You need 2 rules, also allowing traffic inside the vnet, as @mabalon wrote.No need! There is a default rule “allowVnetInbound” to allow which permits communication between resources within the same virtual network (including the same subnet).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. By default, virtual machines in the same subnet can communicate based on a default NSG rule allowing intra-subnet traffic. 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

upvoted 3 times

volto 2 years, 7 months ago

You need 2 rules, also allowing traffic inside the vnet, as @mabalon wrote.

upvoted 3 times

bobothewiseman 1 year, 10 months ago

No need! There is a default rule “allowVnetInbound” to allow which permits communication between resources within the same virtual network (including the same subnet).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. By default, virtual machines in the same subnet can communicate based on a default NSG rule allowing intra-subnet traffic. 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

upvoted 1 times

aki9892 1 year, 10 months ago

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. By default, virtual machines in the same subnet can communicate based on a default NSG rule allowing intra-subnet traffic. 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

upvoted 3 times

mabalon 2 years, 8 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 7 times

Ozarsif Most Recent 1 year, 3 months ago

as of august, 2025, there is no labs anymore

upvoted 1 times

bobothewiseman 1 year, 9 months ago

The best approach is: NSG Rule Configuration Property Value Priority 100 Name Deny_TCP_5585 Source Service Tag Source service tag VirtualNetwork Source Port Range * Destination IP range of subnet1-2 Destination Port Range 5585 Protocol TCP Action Deny

upvoted 1 times

Lazylinux 2 years, 6 months 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 4 times

Lazylinux 2 years, 6 months 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 afterWrong!! Only applies if u are applying NSG on a VM level.. Basic neetworkingI initially thought the same, but: https://learn.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works#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. By default, virtual machines in the same subnet can communicate based on a default NSG rule allowing intra-subnet traffic. 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.

upvoted 4 times

cerifyme85 2 years, 3 months ago

Wrong!! Only applies if u are applying NSG on a VM level.. Basic neetworking

upvoted 1 times

cerifyme85 2 years, 3 months ago

Wrong!! Only applies if u are applying NSG on a VM level.. Basic neetworkingI initially thought the same, but: https://learn.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works#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. By default, virtual machines in the same subnet can communicate based on a default NSG rule allowing intra-subnet traffic. 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.

upvoted 1 times

LieJ0n 2 years, 1 month ago

I initially thought the same, but: https://learn.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works#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. By default, virtual machines in the same subnet can communicate based on a default NSG rule allowing intra-subnet traffic. 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.

upvoted 2 times

njana94 2 years, 6 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 subet1-2 on port 5585 or a single deny policy (any to subnet1-2, port 5585) at priority 65200No need! There is a default rule “allowVnetInbound” to allow which permits communication between resources within the same virtual network (including the same subnet).

upvoted 5 times

njana94 2 years, 6 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 subet1-2 on port 5585

or a single deny policy (any to subnet1-2, port 5585) at priority 65200

upvoted 5 times

bobothewiseman 1 year, 10 months ago

No need! There is a default rule “allowVnetInbound” to allow which permits communication between resources within the same virtual network (including the same subnet).

upvoted 1 times

ABIYGK 2 years, 11 months 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

JohnAvlakiotis 2 years, 11 months ago

The "Add inbound rule" image is misleading. The text above for the rule is correct.

upvoted 2 times

Question #47 *Topic 2*

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
-

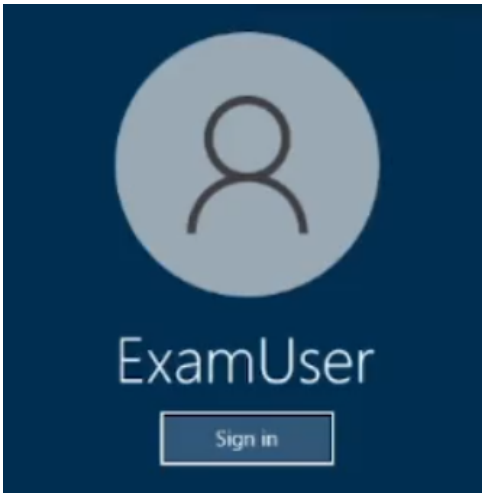
If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

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.



Suggested 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. 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.

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

aBAN Highly Voted 3 years, 4 months ago

The question says 'only hosts on VNET1' -> private endpoint. with service endpoint storage can be accessed access over the internet.private endpoints seem correct: https://learn.microsoft.com/en-us/azure/storage/common/storage-private-endpointsTotally 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-overviewSo, two issues with your response. While yes traffic does traverse the azure backbone via service endpoints traffic is still ingresses via the azure Paas service public interface. Using a private endpoint will re-write cname record for the azure storage instance to resolve to the fqdn of the private endpoint, which removes all access to the instance over the public interface. Second, without service endpoint policies in place. A service endpoint applies to traffic bound for all instances of an azure paas service and not just a singular instance.Incorrect! The task says "You need to ensure that only hosts on VNET1 can access the storage". This can be achieve only via Service Endpoint because Private Endpoint can allow you to configure further access to the storage from on-premises, and etc.Great!

upvoted 7 times

aBAN Highly Voted 3 years, 4 months ago

The question says 'only hosts on VNET1' -> private endpoint. with service endpoint storage can be accessed access over the internet.

upvoted 7 times

ubdubdoo 3 years, 4 months ago

private endpoints seem correct: https://learn.microsoft.com/en-us/azure/storage/common/storage-private-endpoints

upvoted 1 times

Lazylinux 3 years 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-overviewSo, two issues with your response. While yes traffic does traverse the azure backbone via service endpoints traffic is still ingresses via the azure Paas service public interface. Using a private endpoint will re-write cname record for the azure storage instance to resolve to the fqdn of the private endpoint, which removes all access to the instance over the public interface. Second, without service endpoint policies in place. A service endpoint applies to traffic bound for all instances of an azure paas service and not just a singular instance.

upvoted 5 times

Lazylinux 3 years 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 5 times

DC095 2 years ago

So, two issues with your response. While yes traffic does traverse the azure backbone via service endpoints traffic is still ingresses via the azure Paas service public interface. Using a private endpoint will re-write cname record for the azure storage instance to resolve to the fqdn of the private endpoint, which removes all access to the instance over the public interface. Second, without service endpoint policies in place. A service endpoint applies to traffic bound for all instances of an azure paas service and not just a singular instance.

upvoted 3 times

Sergovladi 1 year, 10 months ago

Incorrect! The task says "You need to ensure that only hosts on VNET1 can access the storage". This can be achieve only via Service Endpoint because Private Endpoint can allow you to configure further access to the storage from on-premises, and etc.

upvoted 1 times

RabbitB 2 years, 5 months ago

Great!

upvoted 1 times

MrIMG 3 years, 6 months 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 6 times

MrIMG 3 years, 6 months 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-overviewThe only condition is that the traffic stays in the backbone (not specifically in the vnet) so yeah service endpoint fits tooThis should be the only solution as it states that the access should happen over the Azure backbone. Service Endpoint is the correct option.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 6 times

Ben_88 3 years, 5 months ago

The only condition is that the traffic stays in the backbone (not specifically in the vnet) so yeah service endpoint fits too

upvoted 3 times

JohnAvlakiotis 3 years, 5 months 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 3 times

JohnAvlakiotis 3 years, 5 months 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.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 3 times

CristianM99 3 years, 3 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

Ozarsif Most Recent 1 year, 3 months ago

as of august, 2025, there is no labs anymore

upvoted 1 times

tc0369 1 year, 8 months ago

1.create storage service endpoint at vnet subnet; 2.from storage account, restrict access from selected vnet (security+networking -> networking)

upvoted 1 times

cda26aa 2 years, 6 months ago

I think in this case the answer is Private Endpoint because you want to restrict access to that specific storage instance

upvoted 2 times

SilverFox22 2 years, 7 months ago

I asked this to ChatGPT and it selected Private Endpoint. To summarize: With a service endpoint, you are allowing access from any subnet within your VNET or any virtual network that's been granted access. It doesn't restrict to a specific subnet or set of IPs within your VNET. Given your requirement to restrict access to only hosts on VNET1 and to ensure access over the Azure backbone network, a Private Endpoint is the correct choice.

upvoted 1 times

mjk666 2 years, 8 months ago

whenever we face a dilemma like this, I would go for the cheaper option, hence Service Endpoint

upvoted 1 times

Lazylinux 3 years 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-overviewFollowing 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 2 times

Lazylinux 3 years 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 3 years 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 years, 1 month ago

Can i use Storage Account Firewall to permit access only to VNET1?

upvoted 1 times

magnem66 3 years, 2 months ago

Wouldn't you need to use a Service Endpoint as Private Endpoints are applied to a subnet.

upvoted 2 times

Question #48 *Topic 2*

HOTSPOT

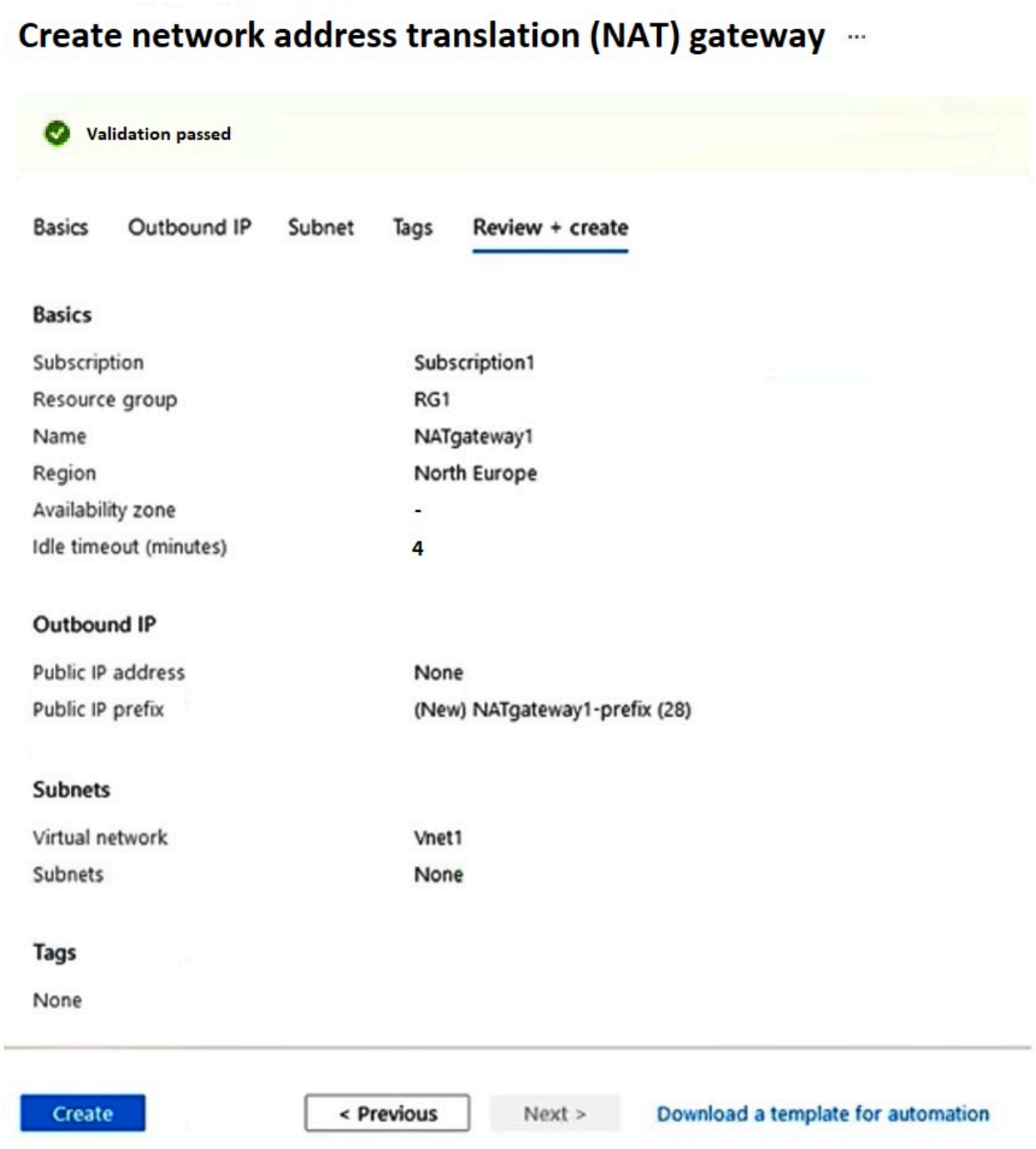
-

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.

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

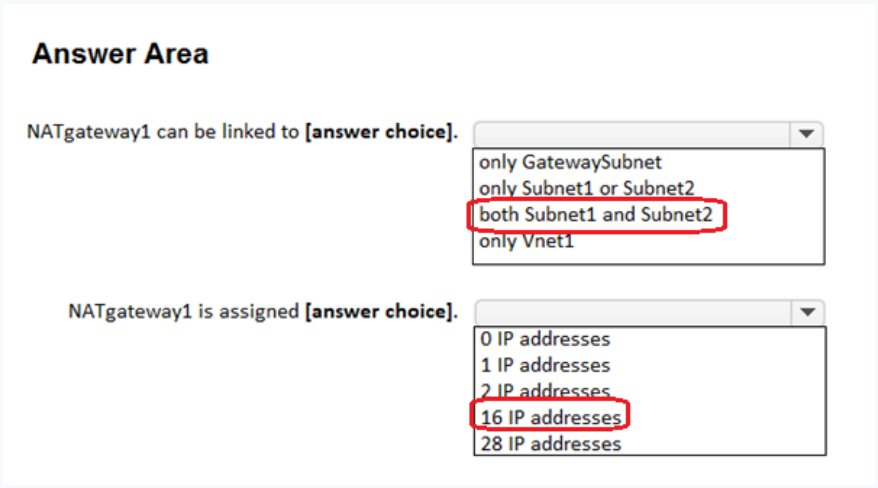
NATgateway1 can be linked to **[answer choice]**.

- 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

Suggested Answer:



MrBlueSky Highly Voted 3 years, 7 months 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 answerWhy not VNAT1? Technically Vnet1 has Subnet 1 & Subnet 2, so what might be the difference?Because of this: "NAT gateway can be associated to an Azure Firewall subnet in a hub virtual network and provide outbound connectivity from spoke virtual networks peered to the hub." - https://learn.microsoft.com/en-us/azure/nat-gateway/nat-overview

upvoted 11 times

MrBlueSky Highly Voted 3 years, 7 months 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 11 times

Lazylinux 3 years 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

thekhijir 2 years ago

Why not VNAT1? Technically Vnet1 has Subnet 1 & Subnet 2, so what might be the difference?

upvoted 1 times

khanda 3 years, 7 months ago

Answer is correct.

upvoted 3 times

ESAJRR 3 years, 7 months 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 3 times

sunsetblvdfightclub 3 years, 7 months ago

https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/faq#can-nat-gateway-be-attached-to-multiple-subnets

upvoted 4 times

thekhijir 2 years ago

Why not VNAT1?

Technically Vnet1 has Subnet 1 & Subnet 2, so what might be the difference?

upvoted 1 times

xRiot007 Most Recent 1 year, 7 months ago

Because of this: "NAT gateway can be associated to an Azure Firewall subnet in a hub virtual network and provide outbound connectivity from spoke virtual networks peered to the hub." - https://learn.microsoft.com/en-us/azure/nat-gateway/nat-overview

upvoted 1 times

Question #49 *Topic 2*

HOTSPOT

-

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

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.

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

Answer Area

Certificates: 1 2 3 4 5

Backend pool targets: 1 2 3 4

Suggested Answer:

Answer Area

Certificates: 1 2 3 4 5 — 1

Backend pool targets: 1 2 3 4 — 4

seth_saurabh84 Highly Voted 3 years, 7 months 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.AgreesThe questoin doesn't mention a Key Vault. Thats why the certificate needs to be installed on the individual VMs.it did not mention the traffic should apply end-to-end encryption. so you only need one certificate and upload it the to listener.

upvoted 35 times

seth_saurabh84 Highly Voted 3 years, 7 months 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 35 times

xRiot007 Most Recent 1 year, 7 months ago

Certificates: 1 - which will be added to the listener (https://learn.microsoft.com/en-us/azure/application-gateway/configuration-listeners#protocol)

Backend pools: 1 - a VMSS can be added as-is to a pool. More details: https://stackoverflow.com/questions/77320073/azure-issue-adding-vm-scale-set-flexible-orchestration-as-application-gateway

upvoted 1 times

_fvt 3 years, 7 months ago

Agrees

upvoted 6 times

_fvt 3 years, 7 months ago

AgreesThe questoin doesn't mention a Key Vault. Thats why the certificate needs to be installed on the individual VMs.it did not mention the traffic should apply end-to-end encryption. so you only need one certificate and upload it the to listener.

upvoted 6 times

thekhijir 1 year, 11 months ago

1 [VMSS] & 1 [Minimize the number of targets in the backend pool of AG1]]

upvoted 1 times

Tasli6 3 years, 4 months ago

The questoin doesn't mention a Key Vault. Thats why the certificate needs to be installed on the individual VMs.

upvoted 4 times

Tasli6 3 years, 4 months ago

The questoin doesn't mention a Key Vault. Thats why the certificate needs to be installed on the individual VMs.it did not mention the traffic should apply end-to-end encryption. so you only need one certificate and upload it the to listener.

upvoted 4 times

thekhijir 1 year, 11 months ago

So, 1 & 1? [Minimize the number of targets in the backend pool of AG1]

upvoted 1 times

rishabr019 2 years, 10 months ago

Correct answer is 1-1

upvoted 2 times

Lazylinux 3 years 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 4 times

RemmyT 2 years, 5 months ago

Tested the number of pool targets VMSS1 - Virtual machine scale set [2 VMs] VMSS1_0cd18cd5 10.20.2.5 VMSS1_b52baa23 10.20.2.4

IP address or FQDN : 10.20.2.4 IP address or FQDN : 10.20.2.5

Virtual machine : Vnet2-nic01-9395c435 (10.20.2.4) Virtual machine : Vnet2-nic01-d393ec3f (10.20.2.5)

Target type : VMSS Target : No available items

VMSS it's not possible to be added as a target in backend pool

The first test was with a VMSS of four VMs. I added VMSS1 as a target for backend pool of an AppWebGw (created during VMSS). I was surprised to see all 4 VMs listed as a target. I was exepected to see VMSS1. So I deleted the VMs and tried to add VMSS but was not possible: there was no VMSS listed.

So the most probable response is: we need 4 backend pool targets (all 4 VMs)

upvoted 1 times

RemmyT 2 years, 5 months ago

Tested the number of pool targets VMSS1 - Virtual machine scale set [2 VMs] VMSS1_0cd18cd5 10.20.2.5 VMSS1_b52baa23 10.20.2.4 IP address or FQDN : 10.20.2.4 IP address or FQDN : 10.20.2.5 Virtual machine : Vnet2-nic01-9395c435 (10.20.2.4) Virtual machine : Vnet2-nic01-d393ec3f (10.20.2.5) Target type : VMSS Target : No available items VMSS it's not possible to be added as a target in backend pool The first test was with a VMSS of four VMs. I added VMSS1 as a target for backend pool of an AppWebGw (created during VMSS). I was surprised to see all 4 VMs listed as a target. I was exepected to see VMSS1. So I deleted the VMs and tried to add VMSS but was not possible: there was no VMSS listed. So the most probable response is: we need 4 backend pool targets (all 4 VMs)I changed the Orchestration mode and succedeed to add VMSS as a target. I guess the number of backend pool targets depends by the Orchestration mode. Orchestration mode Flexible : no option for VMSS, add only VMs (4 targets) Uniform : no option for VMs, add only VMSS (1 target)So, 1 & 1? [Minimize the number of targets in the backend pool of AG1]

upvoted 1 times

RemmyT 2 years, 5 months ago

I changed the Orchestration mode and succedeed to add VMSS as a target. I guess the number of backend pool targets depends by the Orchestration mode.

Orchestration mode Flexible : no option for VMSS, add only VMs (4 targets) Uniform : no option for VMs, add only VMSS (1 target)

upvoted 2 times

RemmyT 2 years, 5 months ago

I changed the Orchestration mode and succedeed to add VMSS as a target. I guess the number of backend pool targets depends by the Orchestration mode. Orchestration mode Flexible : no option for VMSS, add only VMs (4 targets) Uniform : no option for VMs, add only VMSS (1 target)So, 1 & 1? [Minimize the number of targets in the backend pool of AG1]

upvoted 2 times

crypto700 3 years, 6 months ago

correct answer 1 & 1

upvoted 14 times

cloudselflearner 3 years, 7 months ago

Correct answer 1-1

upvoted 9 times

daemon101 3 years, 3 months ago

it did not mention the traffic should apply end-to-end encryption. so you only need one certificate and upload it the to listener.

upvoted 12 times

Question #50 *Topic 2*

HOTSPOT
-

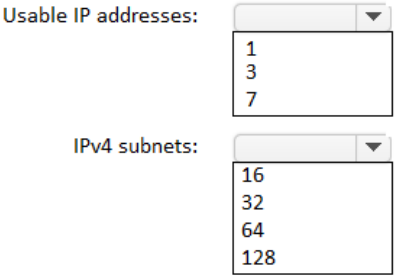
You have an Azure subscription that contains a virtual network named Vnet1. Vnet1 has a /24 IPv4 address space.

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.

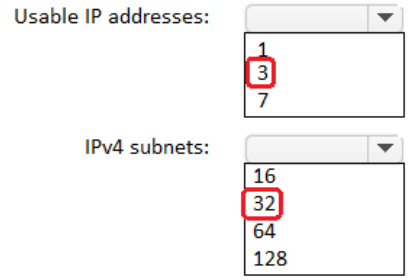
NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:

Answer Area



LieJ0n Most Recent 2 years, 1 month ago

Correct

For visualization (and doing some subnet planning) use tools like https://blog.pichuang.com.tw/azure-subnets.html and start dividing your /24 network into the smallest possible.

upvoted 2 times

Lazylinux Highly Voted 2 years, 9 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 7 times

bakamon 2 years, 11 months ago

Answer :

3

32

sidhi baat no bakwas

upvoted 3 times

Himank20 Highly Voted 3 years 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 26 times

twaller78 3 years, 1 month 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 3 years, 1 month 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 3 years, 1 month ago

Correct !

upvoted 1 times

seth_saurabh84 3 years, 1 month ago

Can someone explain the logic of the answer here?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 enought 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)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 3032 and 3Azure 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 1 times

seth_saurabh84 3 years, 1 month ago

Can someone explain the logic of the answer here?

upvoted 1 times

_fvt 3 years, 1 month 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 enought 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 3 years, 1 month 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 3 years, 1 month 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 3032 and 3

upvoted 1 times

Lapiduse 3 years, 1 month 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 3 years, 1 month 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 enought 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 3 years, 1 month ago

32 and 3

upvoted 3 times

HOTSPOT

-

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

The virtual network topology is shown in the following exhibit.

Firewall1 is configured as shown in following exhibit.

FirewallPolicy1 contains the following rules:

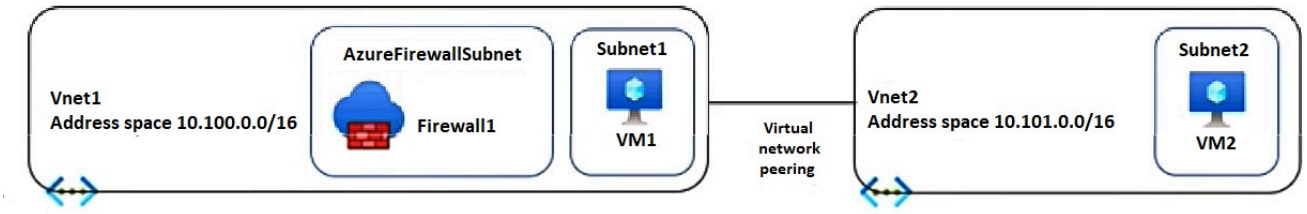
• Allow outbound traffic from Vnet1 and Vnet2 to the internet.
• Allow any traffic between Vnet1 and Vnet2.

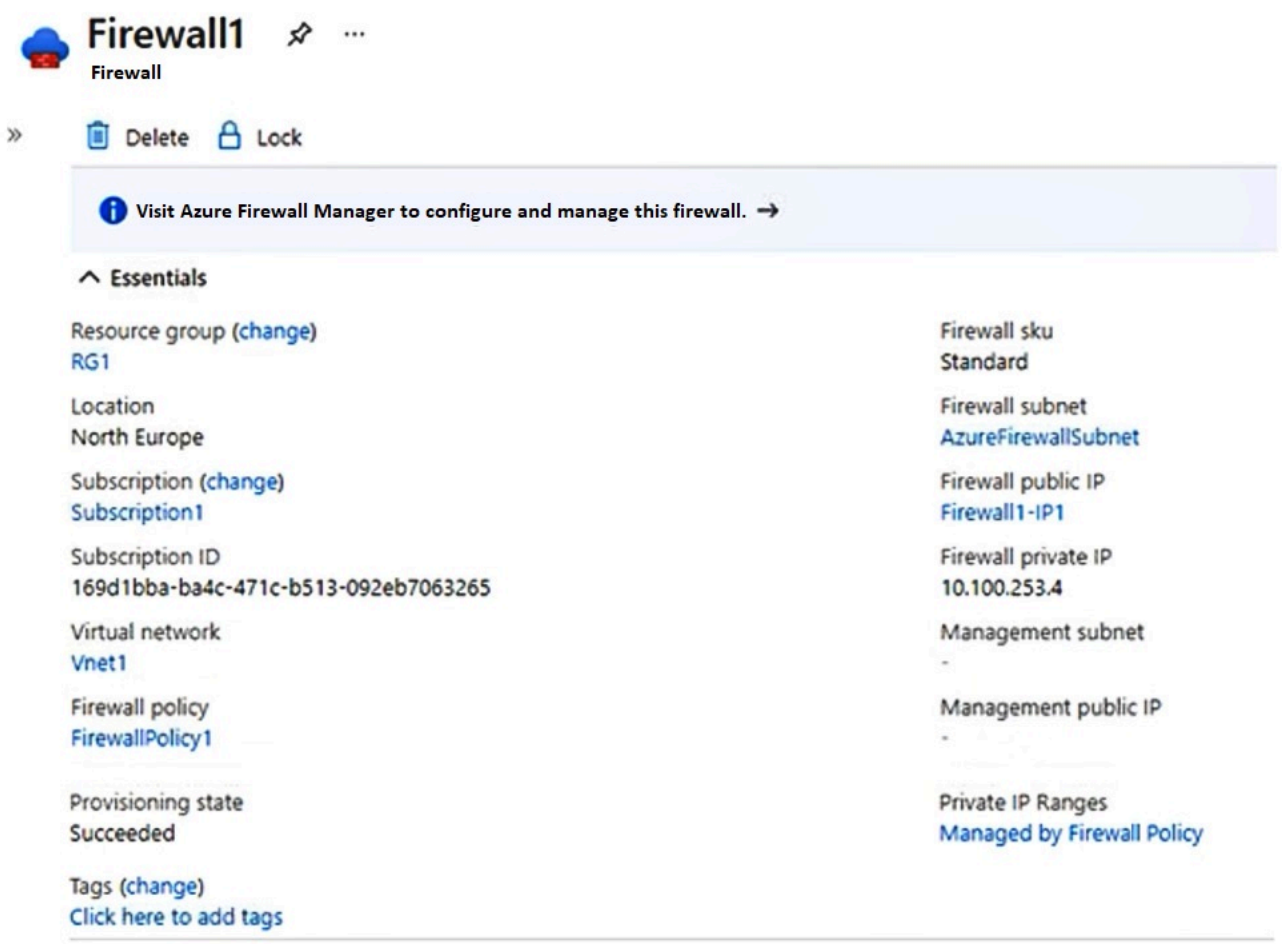
No custom private endpoints, service endpoints, routing tables, or network security groups (NSGs) were created.

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

NOTE: Each correct selection is worth one point.

Name	Type
Vnet1	Virtual network
Vnet2	Virtual network
Firewall1	Azure Firewall
Subnet1	Virtual subnet
Subnet2	Virtual subnet
VM1	Virtual machine
VM2	Virtual machine





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.	○	○
The enable remote gateway setting must be enabled on the virtual net peering to provide VM2 Internet access by using Firewall1.	○	○
Firewall1 can be configured to limit access to websites by categories.	○	○

Suggested Answer:

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.	○	○
The enable remote gateway setting must be enabled on the virtual net peering to provide VM2 Internet access by using Firewall1.	○	○
Firewall1 can be configured to limit access to websites by categories.	○	○

toto74500 Most Recent 2 years, 4 months ago

YNY

1- Yes because the route priority for the same adress 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 3 times

KyleHodg Highly Voted 2 years, 11 months ago

The Firewall SKU states standard. Wouldn't Premium be required for filtering by category? Meaning YNN?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-skuTo filter Web categories standard is enough.

upvoted 8 times

KyleHodg 2 years, 11 months ago

The Firewall SKU states standard. Wouldn't Premium be required for filtering by category? Meaning YNN?

upvoted 8 times

GBAU 2 years, 6 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

volto 2 years, 7 months ago

You need a Routing Table or Azure Route Server to add UDR.

upvoted 3 times

Lazylinux 2 years, 9 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 6 times

ConanBarb 2 years, 7 months 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-skuYou need a Routing Table or Azure Route Server to add UDR.

upvoted 1 times

ConanBarb 2 years, 7 months 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

daemon101 2 years, 10 months 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 2 times

TheBigMan 2 years, 11 months ago

Think it should be NNN 1) Question is about gateway nor UDR 3) Firewall is standard, only premium has categories

upvoted 1 times

TheBigMan 2 years, 11 months ago

Think it should be NNN 1) Question is about gateway nor UDR 3) Firewall is standard, only premium has categories3) Standard has categories https://learn.microsoft.com/en-us/azure/firewall/choose-firewall-skuThe 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

makkelijkzat 2 years, 10 months ago

3) Standard has categories https://learn.microsoft.com/en-us/azure/firewall/choose-firewall-sku

upvoted 3 times

makkelijkzat 2 years, 10 months ago

3) Standard has categories https://learn.microsoft.com/en-us/azure/firewall/choose-firewall-skuThe 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 3 times

Azused 2 years, 8 months ago

To filter Web categories standard is enough.

upvoted 3 times

Apptech 2 years, 11 months 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 7 times

occupatissimo 2 years, 11 months ago

question ask for a routing table, not for a udr, be aware ....NNY

upvoted 3 times

khanda 3 years, 1 month ago

Answer should be YNY, see @_fvt comment.

upvoted 2 times

ckyap 3 years, 1 month 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

ckyap 3 years, 1 month 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)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 1 times

Tasli6 2 years, 10 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 3 years, 1 month ago

it should be YNY

upvoted 3 times

_fvt Highly Voted 3 years, 1 month 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 49 times

Question #52 *Topic 2*

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

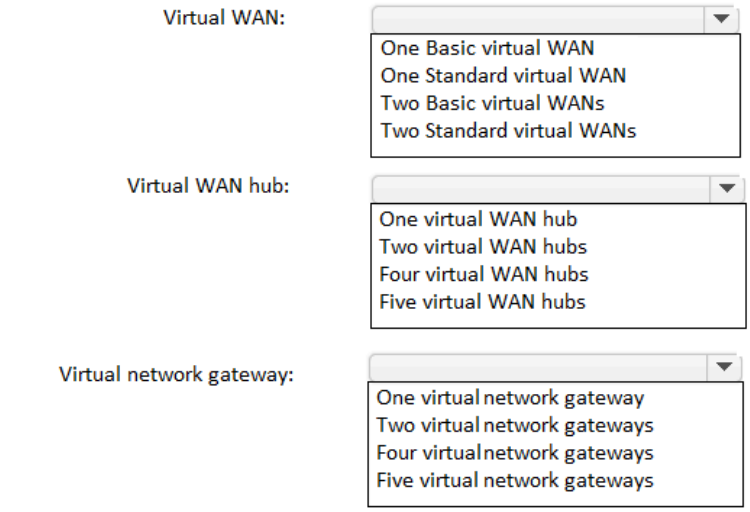
You need to implement Azure Virtual WAN. The solution must meet the following requirements:

- 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.

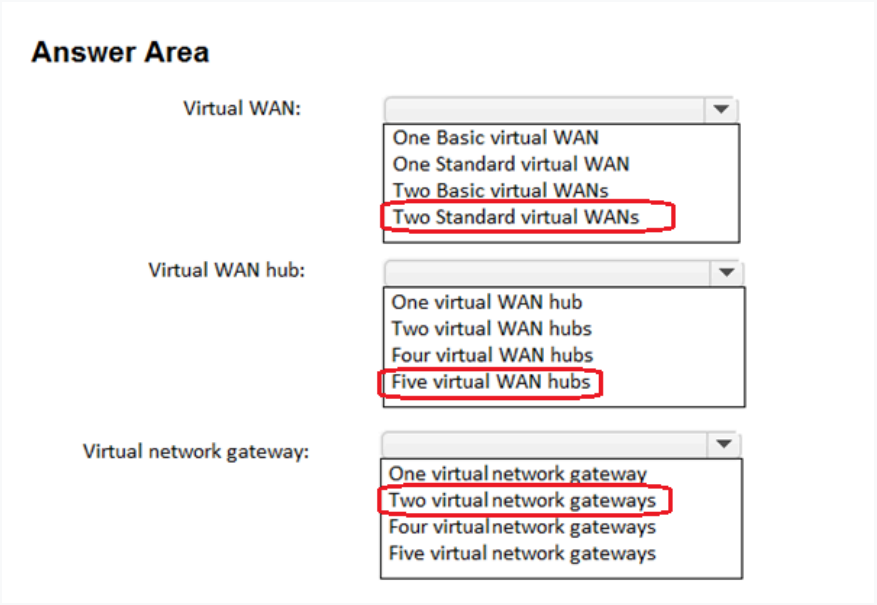
What is the minimum number of Virtual WAN resources required? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:



bobothewiseman Most Recent 1 year, 9 months ago

• Virtual WAN: One Standard Virtual WAN

• Virtual WAN hub: Two Virtual WAN hubs

• Virtual Network Gateway: Four Virtual Network Gateways

Since there are two Virtual WAN hubs, and each requires two Virtual Network Gateways, the total number of virtual network gateways needed is four.

upvoted 2 times

stack120566 Highly Voted 3 years, 7 months 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 13 times

manny72 2 years, 2 months ago

Correction, 4 GWs. 2 Gateways (ER and VPN) can coexist on the same subnet but the question is about gateways.

upvoted 2 times

galahad 2 years, 9 months ago

The answer is 1 Standard VWAN, 2 VHUBs, and 2 VPNGW. The reason why I say 2 VPNGW is because the question is looking for how many VPNGW is needed. VPNGW can only handle S2S connectivity whereas Express Route Gateway will handle Express Route traffic which is a private none encrypted traffic.

upvoted 2 times

manny72 2 years, 3 months ago

1 Standard VWAN 2 VHUBS connected to the single VWAN2 Vnet GWs - ER and S2S gateway can coexist in the same vnet gateway. To note that a virtual network gateway is not just for VPN. Express route gateway is also a vnet gateway of a different type. So the question is how many for all connections and the key point, like others have pointed out, is that co-existence is possible. https://learn.microsoft.com/en-us/azure/expressroute/expressroute-howto-coexist-resource-manager Said that, Microsoft questions are not well exposed as usual. There are limitations and different case scenarios to use co-existence, and here there are no details to help. But it's generally possible.Correction, 4 GWs. 2 Gateways (ER and VPN) can coexist on the same subnet but the question is about gateways.

upvoted 1 times

manny72 2 years, 3 months ago

1 Standard VWAN 2 VHUBS connected to the single VWAN

upvoted 1 times

manny72 2 years, 3 months ago

2 Vnet GWs - ER and S2S gateway can coexist in the same vnet gateway. To note that a virtual network gateway is not just for VPN. Express route gateway is also a vnet gateway of a different type. So the question is how many for all connections and the key point, like others have pointed out, is that co-existence is possible. https://learn.microsoft.com/en-us/azure/expressroute/expressroute-howto-coexist-resource-manager Said that, Microsoft questions are not well exposed as usual. There are limitations and different case scenarios to use co-existence, and here there are no details to help. But it's generally possible.Correction, 4 GWs. 2 Gateways (ER and VPN) can coexist on the same subnet but the question is about gateways.

upvoted 1 times

manny72 2 years, 3 months ago

2 Vnet GWs - ER and S2S gateway can coexist in the same vnet gateway. To note that a virtual network gateway is not just for VPN. Express route gateway is also a vnet gateway of a different type. So the question is how many for all connections and the key point, like others have pointed out, is that co-existence is possible. https://learn.microsoft.com/en-us/azure/expressroute/expressroute-howto-coexist-resource-manager

Said that, Microsoft questions are not well exposed as usual. There are limitations and different case scenarios to use co-existence, and here there are no details to help. But it's generally possible.

upvoted 1 times

y0eri 2 years, 10 months 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 2 years, 11 months 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 3 years, 3 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 7 times

Webesciaki 2 years, 10 months 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 ?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 3 times

Webesciaki 2 years, 10 months 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 3 times

bakamon 3 years, 5 months ago

: One standard virtual WAN

: 2 hubs

: 4 gateways

upvoted 3 times

Qunlay 3 years, 6 months ago

1 Standard VWAN, 2 VHubs, 5 VPNGWs

upvoted 2 times

MrBlueSky Highly Voted 3 years, 7 months 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 59 times

Chief_D11 3 years, 7 months 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 3 years, 7 months 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 3 years, 7 months 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 7 times

silvarohit 3 years, 7 months ago

Standard Virtual WAN - 1

Hub - 2

VPN GW - 4

upvoted 4 times

MrBlueSky 3 years, 7 months 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

stack120566 3 years, 7 months 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 13 times

BenyIR 3 years, 7 months 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 8 times

_fvt 3 years, 7 months ago

Yes I agree

upvoted 1 times

Question #53 *Topic 2*

DRAG DROP

-

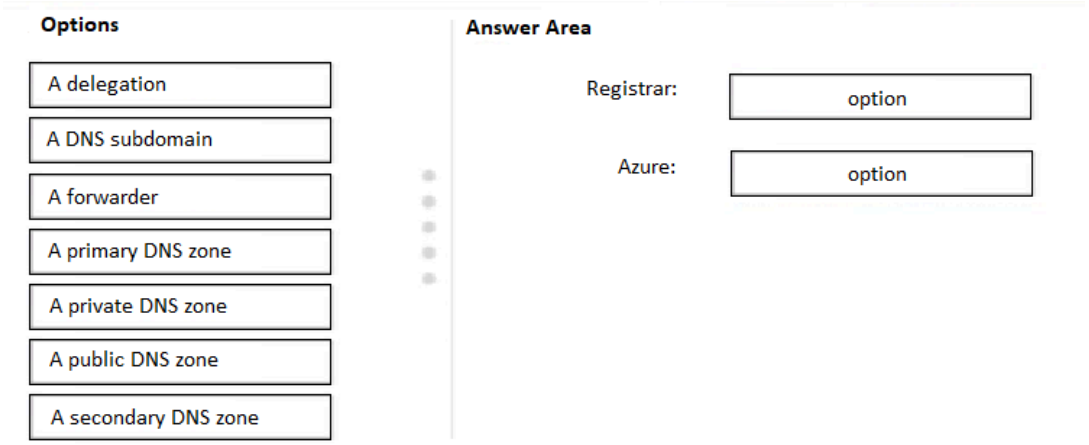
You have a DNS domain named contoso.com that is hosted by a third-party domain name registrar.

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.



Suggested Answer:



CarlosLeite Highly Voted 2 years, 2 months ago

This question was present in the exam of 2024/08/22

upvoted 5 times

TheBlob 2 years, 3 months ago

If you ask me the question is wrong because a delegation is meant for sub-DNS zones.

upvoted 1 times

Lazylinux Highly Voted 3 years, 3 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 Registar 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 9 times

vigklk 3 years, 6 months ago

is it correct?Yes. Delegate, create zone and then modify NS records

upvoted 2 times

vigklk 3 years, 6 months ago

is it correct?

upvoted 2 times

khksoma 3 years, 6 months ago

Yes. Delegate, create zone and then modify NS records

upvoted 4 times

Question #54 *Topic 2*

HOTSPOT
-

You have an on-premises network.

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

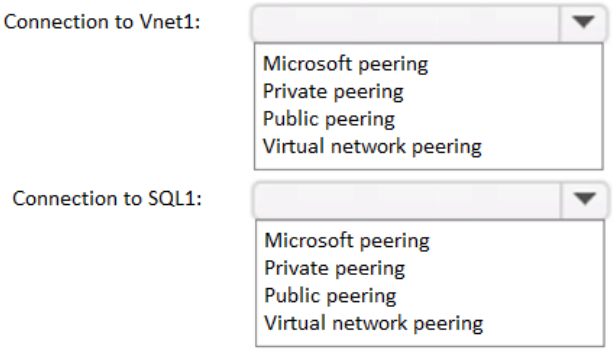
You need to implement an ExpressRoute circuit to access the resources in the subscription. The solution must ensure that the on-premises network connects to the Azure resources by using the ExpressRoute circuit.

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.

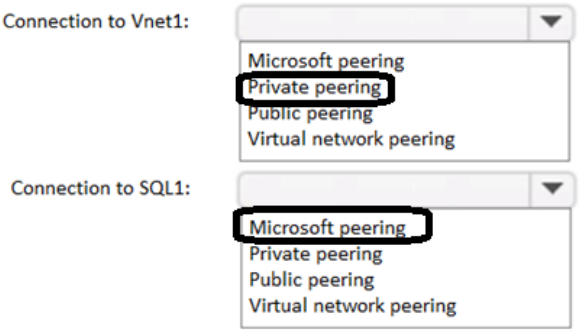
Name	Type	Description
Vnet1	Virtual network	*None*
VM1	Virtual machine	Connect to Vnet1
VM2	Virtual machine	Connect to Vnet1
SQL1	Azure SQL Database	Internet accessible

Answer Area



Suggested Answer:

Answer Area



Feliphus Most Recent 1 year, 12 months ago

I want to think "Microsoft peering" is the Azure Peering Service

https://learn.microsoft.com/en-us/azure/peering-service/about

upvoted 1 times

Lazylinux 3 years, 3 months ago

Yep given answer is correct

upvoted 3 times

UR Highly Voted 3 years, 6 months ago

The answer is correct!

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

upvoted 15 times

Question #55 *Topic 2*

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

Suggested Answer: *B*

Community vote distribution

B (100%)

amitnahmias Highly Voted 2 years, 3 months ago

Selected Answer: B

this question better be on the exam

upvoted 8 times

amitnahmias Highly Voted 2 years, 3 months ago

this question better be on the exam:') clicked on discussion for this comment

upvoted 8 times

LieJ0n Most Recent 2 years, 1 month ago

:') clicked on discussion for this comment

upvoted 1 times

trashbox 2 years, 6 months ago

Selected Answer: B

The answer is correct.

upvoted 2 times

sibishrewd 2 years, 10 months ago

answer is correct

upvoted 2 times

UR 3 years ago

The answer is correct.

B

upvoted 5 times

Question #56 *Topic 2*

You have the on-premises networks shown in the following table.

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?

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*

A. the VPN connection to Branch1

B. the VPN connection to Branch2

C. the ExpressRoute connection to Branch2

D. the ExpressRoute connection to Branch3

Suggested Answer: *B*

Community vote distribution

D (97%) (3

crypto700 Highly Voted 3 years, 6 months 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 23 times

crypto700 Highly Voted 3 years, 6 months ago

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 preferreddon't agree: ANSWER should be C. the ExpressRoute connection to Branch2 Explanation: Since the virtual hub routing preference for VWAN1 is based on AS Path, and Branch2's ExpressRoute connection has the shortest AS path length compared to Branch1 (VPN) and Branch3 (ExpressRoute), traffic will prefer the connection with the shortest AS path.How did you come up with the idea that branch 2 has the shortest AS path? It says in the description for branch 2 that the local AS is listed 3 times indicating it's doing as-path prepending. As far as we know, branch 3 is not doing any prepending....so Answer is D, Branch 3.By default, VWAN prefers ExpressRoute connections over VPN connections for routing traffic. This is because ExpressRoute typically offers more reliable and higher bandwidth connections compared to VPN. Also, for BGP, /24 is always preferred over /16 as it's the longest match.

upvoted 23 times

stormtraining 2 years ago

don't agree: ANSWER should be C. the ExpressRoute connection to Branch2

Explanation: Since the virtual hub routing preference for VWAN1 is based on AS Path, and Branch2's ExpressRoute connection has the shortest AS path length compared to Branch1 (VPN) and Branch3 (ExpressRoute), traffic will prefer the connection with the shortest AS path.

upvoted 1 times

stormtraining 2 years ago

don't agree: ANSWER should be C. the ExpressRoute connection to Branch2 Explanation: Since the virtual hub routing preference for VWAN1 is based on AS Path, and Branch2's ExpressRoute connection has the shortest AS path length compared to Branch1 (VPN) and Branch3 (ExpressRoute), traffic will prefer the connection with the shortest AS path.How did you come up with the idea that branch 2 has the shortest AS path? It says in the description for branch 2 that the local AS is listed 3 times indicating it's doing as-path prepending. As far as we know, branch 3 is not doing any prepending....so Answer is D, Branch 3.By default, VWAN prefers ExpressRoute connections over VPN connections for routing traffic. This is because ExpressRoute typically offers more reliable and higher bandwidth connections compared to VPN. Also, for BGP, /24 is always preferred over /16 as it's the longest match.

upvoted 1 times

billgoldberg14 1 year, 9 months ago

How did you come up with the idea that branch 2 has the shortest AS path? It says in the description for branch 2 that the local AS is listed 3 times indicating it's doing as-path prepending. As far as we know, branch 3 is not doing any prepending....so Answer is D, Branch 3.

upvoted 1 times

thekhijir 2 years ago

By default, VWAN prefers ExpressRoute connections over VPN connections for routing traffic. This is because ExpressRoute typically offers more reliable and higher bandwidth connections compared to VPN. Also, for BGP, /24 is always preferred over /16 as it's the longest match.

upvoted 2 times

de3ca78 Most Recent 8 months, 3 weeks ago

Compare AS Path lengths Branch1 VPN → AS path length = 1 Branch2 ExpressRoute → AS path length = 3 -> worse Branch3 ExpressRoute → AS path length = 1 Branch2 VPN → also length = 3 -> worse Best candidates: Branch1 VPN or Branch3 ExpressRoute Tie-breaker rule: VPN preferred over ExpressRoute in Virtual WAN when AS Path is equal So between: Branch1 VPN (AS path = 1) & Branch3 ExpressRoute (AS path = 1) the correct answer is A !

upvoted 1 times

thekhijir 2 years ago

By default, VWAN prefers ExpressRoute connections over VPN connections for routing traffic. This is because ExpressRoute typically offers more reliable and higher bandwidth connections compared to VPN. Also, for BGP, /24 is always preferred over /16 as it's the longest match.we are routing to 10.61.1.5 which matches the /16 not /24. Your answer is wrong.

upvoted 2 times

kewokil120 1 year, 2 months ago

we are routing to 10.61.1.5 which matches the /16 not /24. Your answer is wrong.

upvoted 1 times

620b351 2 years, 2 months ago

Crypto 700 is correct. In basic BGP, one of the most common tiebreakers (and in this example as well) is the AS path. If the AS path is bigger, it has less preference. What is done here is called an AS prepend, where the AS path is influenced, so branch 2 is totally out.

upvoted 1 times

cda26aa 2 years, 6 months ago

Answer should A. AS Path Prefer routes with the shortest BGP AS-Path length irrespective of the source of the route advertisements. Note: In vWANs with multiple remote virtual hubs, if there's a tie between remote ExpressRoute routes and remote site-to-site VPN routes, remote site-to-site VPN routes will be preferred. Prefer routes from local virtual hub connections over routes learned from remote virtual hub. If there are routes from both ExpressRoute and Site-to-site VPN connections: If all the routes are local to the virtual hub, the routes from ExpressRoute connections will be chosen. If all the routes are through remote virtual hubs, the routes from Site-to-site VPN connections will be chosen. https://learn.microsoft.com/en-us/azure/virtual-wan/about-virtual-hub-routing-preference#routing-scenarios

upvoted 2 times

LieJ0n 2 years, 7 months ago

D - Branch 3 See the example at https://learn.microsoft.com/en-us/azure/virtual-wan/about-virtual-hub-routing-preference#routing-scenarios

upvoted 2 times

ronin201 3 years, 1 month ago

Pls carefully see ASN!!! ER uses standard ASN 12076 not mentioned in BGP AS

upvoted 1 times

CiscoTerminator 3 years, 3 months 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 3 years, 3 months ago

D Crypto700 explanation is right.

upvoted 1 times

Lazylinux 3 years, 3 months ago

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 3 years, 5 months 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.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 Branch3all 3 branch has the 10.61.0.0/16 range

upvoted 2 times

roshingrg 3 years, 5 months 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 3 years, 5 months 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 Branch3all 3 branch has the 10.61.0.0/16 range

upvoted 3 times

roshingrg 3 years, 5 months 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 years, 1 month ago

all 3 branch has the 10.61.0.0/16 range

upvoted 4 times

Kipper_2022 3 years, 6 months ago

Agree with crypto700

upvoted 1 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.

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.

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.

Zone1.contoso.com has the virtual network links shown in the following table.

Other Azure Resources
-

The Azure subscription contains additional resources as shown in the following table.

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.

• 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.

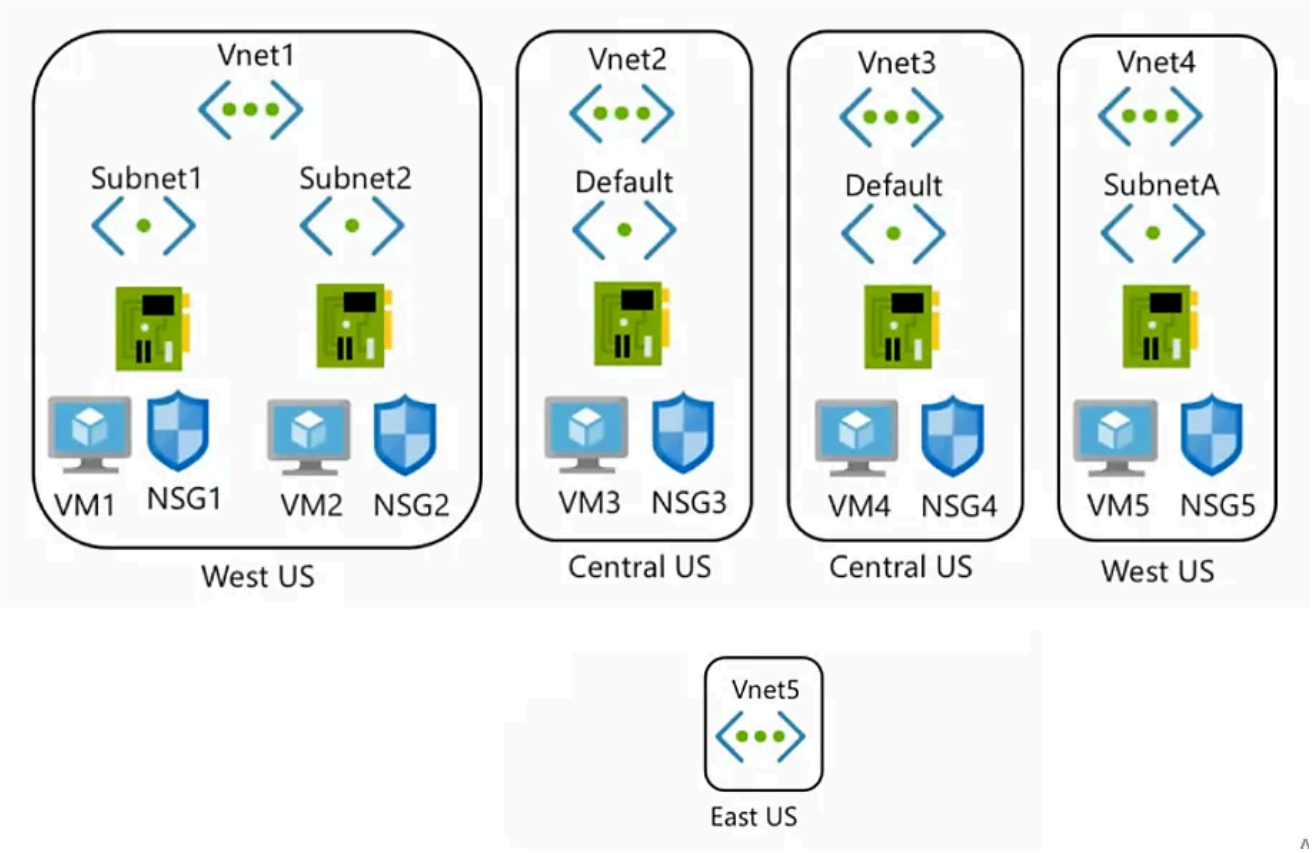
You are implementing the virtual network requirements for Vnet6.

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.

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**

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



Name	Location
zone1.contoso.com	Central US
zone2.contoso.com	West US

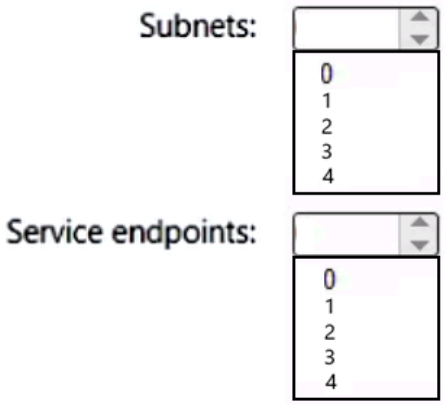
Name	Virtual Network	Auto registration
Link1	Vnet2	No
Link2	Vnet3	Yes

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

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

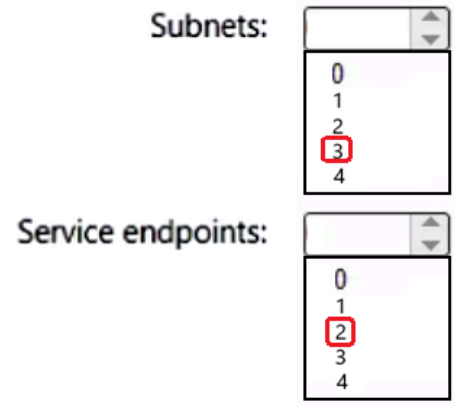
Priority	Port	Protocol	Source	Destination	Action
200	3389	TCP	10.1.0.0/16	VirtualNetwork	Deny

Answer Area



Suggested Answer:

Answer Area



ironbornson Highly Voted 3 years, 3 months 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 conection can use peering

upvoted 18 times

ironbornson Highly Voted 3 years, 3 months 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 conection can use peeringagreed, container need dedicated subnet.the same with gateway for vpn.this appeared in the 4th Juy 2026 examThinks should be 2 subnets not 3 since subnet2 is on vnet1

upvoted 19 times

AlfKay Most Recent 4 months, 2 weeks ago

agreed, container need dedicated subnet.the same with gateway for vpn.this appeared in the 4th Juy 2026 exam

upvoted 1 times

rga91 3 years, 2 months 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 13 times

c2e9cb4 2 years, 10 months ago

Thinks should be 2 subnets not 3 since subnet2 is on vnet1

upvoted 4 times

rga91 3 years, 2 months 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 DB1You do not need a dedicated subnet for DB1, because DB1 is not part of the VNet.I agree the Container Group Instance will need its own Subnet.What is a "Container Group" ? If it means Azure Container Instance (ACI), it has to run in its own subnet, then you need two subnets for the "Container Group". Then, the answer for first question is 4Correction: 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 ith a storage account): https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview

upvoted 13 times

galahad 2 years, 9 months ago

I agree the Container Group Instance will need its own Subnet.

upvoted 1 times

xRiot007 1 year, 7 months ago

You do not need a dedicated subnet for DB1, because DB1 is not part of the VNet.

upvoted 1 times

galahad 2 years, 9 months ago

I agree the Container Group Instance will need its own Subnet.What is a "Container Group" ? If it means Azure Container Instance (ACI), it has to run in its own subnet, then you need two subnets for the "Container Group". Then, the answer for first question is 4

upvoted 1 times

Feliphus 2 years ago

What is a "Container Group" ? If it means Azure Container Instance (ACI), it has to run in its own subnet, then you need two subnets for the "Container Group". Then, the answer for first question is 4

upvoted 1 times

rga91 3 years, 2 months 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 ith a storage account): https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview

upvoted 11 times

bobothewiseman 1 year, 9 months ago

Its 4 subnets and 2 SE 1. Gateway Subnet: 2. Container Instances 3. VM 4. DB1

upvoted 1 times

bobothewiseman 1 year, 9 months ago

Its 4 subnets and 2 SE 1. Gateway Subnet: 2. Container Instances 3. VM 4. DB1I was wrong! 3 subnets and 2 SE Vnet integration is not in use. The ACI subnet is not required

upvoted 1 times

bewavos102 1 year, 11 months ago

Answer is correct.

For Vnet6, you need a minimum of 3 subnets: - One for the container groups - One for the virtual machines - One for a GatewaySubnet for the VPN gateway to establish VPN connections. Container groups and VMs can't share a subnet due to networking conflicts since Azure Container Instances (ACI) requires its own subnet.

Then, you need a minimum of 2 private endpoints: - One for KeyVault1 - One for DB1

Not sure why people are mentioning subnet2, is on a completely different virtual network (vnet1).

Not sure why people are mentioning DB1 as in Vnet6 that requires a subnet. Is outside Vnet6, otherwise what would be the purpose for a private endpoint.

upvoted 3 times

bobothewiseman 1 year, 9 months ago

I was wrong! 3 subnets and 2 SE Vnet integration is not in use. The ACI subnet is not required

upvoted 1 times

bewavos102 1 year, 11 months ago

Answer is correct. For Vnet6, you need a minimum of 3 subnets: - One for the container groups - One for the virtual machines - One for a GatewaySubnet for the VPN gateway to establish VPN connections. Container groups and VMs can't share a subnet due to networking conflicts since Azure Container Instances (ACI) requires its own subnet. Then, you need a minimum of 2 private endpoints: - One for KeyVault1 - One for DB1 Not sure why people are mentioning subnet2, is on a completely different virtual network (vnet1). Not sure why people are mentioning DB1 as in Vnet6 that requires a subnet. Is outside Vnet6, otherwise what would be the purpose for a private endpoint.Thanks Bewavos102. Container groups and VMs can't share a subnet due to networking conflicts since Azure Container Instances (ACI) requires its own subnet. Ref: https://learn.microsoft.com/en-us/azure/container-instances/container-instances-virtual-network-concepts#:~:text=Subnet%20(delegated),the%20operation%20fails. Also, you can use one Subnet for both Container Groups as confirmed in the following diagram: Ref: https://learn.microsoft.com/en-us/azure/container-instances/container-instances-virtual-network-concepts#:~:text=The%20following%20diagram%20depicts%20several%20container%20groups%20deployed%20to%20a%20subnet%20delegated%20to%20Azure%20Container%20Instances.%20Once%20you%20deploy%20one%20container%20group%20to%20a%20subnet%2C%20you%20can%20deploy%20more%20container%20groups%20to%20it%20by%20specifying%20the%20same%20network%20profile. So, 3 subnets

upvoted 3 times

bp_a_user 3 years, 1 month ago

I would say 0 service endpoints: private endpoints could be used for both, key vault and azure sql db

upvoted 3 times

Knight_Of_Peace 1 year, 10 months ago

Thanks Bewavos102. Container groups and VMs can't share a subnet due to networking conflicts since Azure Container Instances (ACI) requires its own subnet. Ref: https://learn.microsoft.com/en-us/azure/container-instances/container-instances-virtual-network-concepts#:~:text=Subnet%20(delegated),the%20operation%20fails. Also, you can use one Subnet for both Container Groups as confirmed in the following diagram: Ref: https://learn.microsoft.com/en-us/azure/container-instances/container-instances-virtual-network-concepts#:~:text=The%20following%20diagram%20depicts%20several%20container%20groups%20deployed%20to%20a%20subnet%20delegated%20to%20Azure%20Container%20Instances.%20Once%20you%20deploy%20one%20container%20group%20to%20a%20subnet%2C%20you%20can%20deploy%20more%20container%20groups%20to%20it%20by%20specifying%20the%20same%20network%20profile. So, 3 subnets

upvoted 1 times

bp_a_user 3 years, 1 month ago

I would say 0 service endpoints: private endpoints could be used for both, key vault and azure sql dbCould be, but not in this context. Here we have to use service endpoints. One for DB and one for KW

upvoted 3 times

xRiot007 1 year, 7 months ago

Could be, but not in this context. Here we have to use service endpoints. One for DB and one for KW

upvoted 1 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

Suggested Answer: *C*

Community vote distribution

C (100%)

Lazylinux Most Recent 2 years ago

Selected Answer: C

I C is correct :)

upvoted 3 times

Acaer 2 years, 2 months 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 4 times

Question #59 *Topic 2*

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.

You have the subnets shown in the following table.

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

NOTE: Each correct selection is worth one point.

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

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

Answer Area

Statements	Yes	No
You can deploy Azure Bastion to Subnet1-1.	○	○
You can deploy 100 additional virtual machines to Subnet2-1.	○	○
You can change the IP address range of Subnet3-1 to 10.3.1.0/16.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
You can deploy Azure Bastion to Subnet1-1.	○	●
You can deploy 100 additional virtual machines to Subnet2-1.	●	○
You can change the IP address range of Subnet3-1 to 10.3.1.0/16.	○	●

Acaer Highly Voted 3 years, 2 months 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 10.3.0.0/16correctAlso 10.3.1.0/16 doesn't exist. it should be 10.3.0.0/16.

upvoted 27 times

Acaer Highly Voted 3 years, 2 months 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 27 times

Aydin 2 years, 7 months ago

N - Az Bastion service require a dedicated subnet for deploying

Y - in /25 has 128 ip address, and azure use 5 ip address for its purpose and you can create additional VMs

N - Because CIDR range of VNet is 10.3.0.0/16 , firstly you should remove VNet Cidr space

N

upvoted 1 times

Lazylinux 3 years ago

NYN

1-N as per https://learn.microsoft.com/en-us/azure/bastion/configuration-settings

2-Y 2/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 2 times

Yodao 3 years, 2 months ago

what's the correct answer?

upvoted 1 times

KeenOnTech 3 years, 2 months 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 3 times

KeenOnTech 3 years, 2 months 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.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.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 3 times

sam881989 2 years, 10 months 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

JackeD 3 years, 1 month 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.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 6 times

JackeD 3 years, 1 month 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 6 times

CheMetto Most Recent 1 year, 1 month ago

Also 10.3.1.0/16 doesn't exist. it should be 10.3.0.0/16.

upvoted 1 times

goooru 3 years, 2 months ago

correct

upvoted 1 times

Question #60 *Topic 2*

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

Suggested Answer: *B*

Community vote distribution

B (100%)

MCCC454 Highly Voted 2 years, 3 months ago

Why is this question here again and again?

upvoted 5 times

MCCC454 Highly Voted 2 years, 3 months ago

Why is this question here again and again?I got it correct every time :)

upvoted 5 times

AusInIndy Most Recent 1 year, 5 months ago

I got it correct every time :)

upvoted 2 times

kay000001 2 years, 6 months ago

Awfully repeatitive question...

upvoted 2 times

trashbox 2 years, 6 months ago

Selected Answer: B

The answer is correct.

upvoted 2 times

Question #61 *Topic 2*

You have the Azure virtual networks shown in the following table.

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?

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

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

Suggested Answer: *B*

Community vote distribution

B (100%)

Acaer Highly Voted 2 years, 8 months 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 Subnet2-1https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal#create-a-default-route

upvoted 5 times

Acaer 2 years, 8 months ago

https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal#create-a-default-route

upvoted 3 times

Acaer 2 years, 8 months 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 4 times

barxan1 Most Recent 2 years, 2 months ago

Is correct

upvoted 2 times

Lazylinux 2 years, 6 months ago

B is Honey - use RT to point to FW as next hope with CIDR 0.0.0.0/0

upvoted 2 times

Question #62 *Topic 2*

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

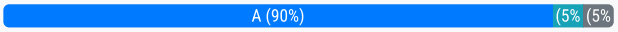
B. /120

C. /48

D. /24

Suggested Answer: *D*

Community vote distribution



efayed 2 years, 3 months ago

Given the requirements, the best recommendation for the subnet mask size would be: B. /120 Here's the reasoning: IPv6 addressing: IPv6 has a much larger address space than IPv4, allowing for more granular subnetting. Subnet size: Each subnet needs to host up to 200 load-balanced virtual machines. /120 subnet mask: In IPv6, a /120 subnet provides 2^8 = 256 addresses. This is more than enough to accommodate 200 virtual machines per subnet while leaving some room for network infrastructure addresses (e.g., gateway). A /120 subnet mask offers the necessary address space while conserving address allocations for other potential subnets or uses within your Azure virtual network.Chat GPT's "reasoning" is garbage. IPv6 subnets can have ONLY one mask: /64. No exceptions

upvoted 2 times

efayed 2 years, 3 months ago

Given the requirements, the best recommendation for the subnet mask size would be:

B. /120

Here's the reasoning:

IPv6 addressing: IPv6 has a much larger address space than IPv4, allowing for more granular subnetting. Subnet size: Each subnet needs to host up to 200 load-balanced virtual machines. /120 subnet mask: In IPv6, a /120 subnet provides 2^8 = 256 addresses. This is more than enough to accommodate 200 virtual machines per subnet while leaving some room for network infrastructure addresses (e.g., gateway). A /120 subnet mask offers the necessary address space while conserving address allocations for other potential subnets or uses within your Azure virtual network.

upvoted 2 times

xRiot007 Most Recent 1 year, 7 months ago

Chat GPT's "reasoning" is garbage. IPv6 subnets can have ONLY one mask: /64. No exceptions

upvoted 4 times

orionduo 2 years, 8 months ago

Selected Answer: A

A /64 subnet mask provides an enormous address space of 2^64 addresses, which is far more than enough to accommodate the required number of virtual machines in each subnet (up to 200).

Using a /64 subnet mask aligns with standard IPv6 practices and ensures compatibility with various IPv6 features and functionalities.

upvoted 2 times

kghosh4 2 years, 11 months ago

Selected Answer: A

Definately A

upvoted 1 times

Lazylinux 3 years 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 2 times

Lazylinux 3 years ago

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.more info here https://docs.netgate.com/pfsense/en/latest/network/ipv6/subnets.htmlThis is wrong, a /120 can host 2^8 (256) ipsmy bad -->not accepted below /64 so response 1 /64

upvoted 2 times

c2e9cb4 2 years, 10 months ago

This is wrong, a /120 can host 2^8 (256) ips

upvoted 1 times

c2e9cb4 2 years, 10 months ago

This is wrong, a /120 can host 2^8 (256) ipsmy bad -->not accepted below /64 so response 1 /64

upvoted 1 times

c2e9cb4 2 years, 10 months ago

my bad -->not accepted below /64

so response 1 /64

upvoted 1 times

Lazylinux 3 years ago

more info here

https://docs.netgate.com/pfsense/en/latest/network/ipv6/subnets.html

upvoted 1 times

voldemort123 3 years, 1 month 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 3 times

Abra_2021 3 years, 2 months 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

MrAmaeg Highly Voted 3 years, 1 month 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 9 times

Abra_2021 3 years, 2 months 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

Yodao 3 years, 2 months 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

Yodao 3 years, 2 months ago

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.and this is why I don't use chatGPT ;)

upvoted 1 times

Lazylinux 3 years ago

Totally wrong your mindset is WIRED to IPv4, this is about IPv6, read my explanation

upvoted 3 times

PandaTuga 2 years, 11 months ago

and this is why I don't use chatGPT ;)

upvoted 2 times

tomasek88 3 years, 2 months ago

Selected Answer: A

IPv6 does NOT have /24 --> D is correct --> /64

upvoted 4 times

Acaer 3 years, 2 months 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 4 times

tomasek88 3 years, 2 months ago

Selected Answer: A

IPv6 does NOT have /24 --> D is correct --> /64

upvoted 4 times

Bigfatdavey 3 years, 2 months ago

should be /64

upvoted 2 times

Bigfatdavey 3 years, 2 months ago

should be /64What is your explaining Bigfatdavye?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."Could you explain ?

upvoted 2 times

Lazylinux 3 years ago

U Mean A

upvoted 1 times

Thulas 3 years, 2 months ago

What is your explaining Bigfatdavye?

upvoted 1 times

Thulas 3 years, 2 months ago

What is your explaining Bigfatdavye?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 3 years, 2 months ago

Could you explain ?

upvoted 1 times

ConanBarb 3 years, 1 month 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

Question #63 *Topic 2*

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: Route solution

On-premises datacenters: Route solution

Suggested Answer:

Answer Area

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

Acaer Highly Voted 2 years, 8 months 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 11 times

Acaer Highly Voted 2 years, 8 months 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 + 4IMHO its wrong VNET1 and VNET2 supposed to talk to each other that means it is not met with given answer.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 thoughI guess VNET3 and VENT 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 missleading question if you ask me. From your link: "I think the question is a bit missleading. 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 11 times

Webesciaki 2 years, 4 months ago

IMHO its wrong VNET1 and VNET2 supposed to talk to each other that means it is not met with given answer.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

Webesciaki 2 years, 4 months 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

CiscoExam Most Recent 2 years, 3 months 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 2 years, 4 months 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 5 times

y0eri 2 years, 4 months 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: Defaultyou 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 6 times

y0eri 2 years, 4 months 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 6 times

Webesciaki 2 years, 4 months 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 2 times

ironbornson 2 years, 7 months ago

I guess VNET3 and VENT 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 missleading question if you ask me.

From your link: "I think the question is a bit missleading. 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

Question #64 *Topic 2*

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

Suggested Answer: *C*

bewavos102 Highly Voted 1 year, 12 months ago

You better not get this wrong, fellas. It makes up 10% of the exam according to ExamTopics.

upvoted 14 times

Kanoniermalri Highly Voted 3 years ago

This question comes up for the 4th or 5th time in this course

upvoted 9 times

Question #65 *Topic 2*

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

Suggested Answer:

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**

Lazylinux Highly Voted 2 years, 6 months 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 25 times

Lazylinux 2 years, 6 months 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 paragraphAdding 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 serviceand 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 25 times

Zorro2003 Most Recent 1 year, 2 months ago

DNS records: A CNAME record and a TXT record

Import the certificate to: Vault1

Why:

Front Door requires a CNAME from app1.contoso.com to the Front Door endpoint and a TXT record for domain verification.

When bringing your own SSL certificate for Front Door, it must be stored in Azure Key Vault, so you import the third-party CA cert into Vault1.

upvoted 1 times

Lazylinux 2 years, 6 months 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 23 times

Lazylinux 2 years, 6 months 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 serviceand 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 23 times

Lazylinux Highly Voted 2 years, 6 months 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 35 times

seedati 2 years, 6 months ago

CorrectCould you explain it?Read Lazylinux previous comment ;)U WRONG, read my comments

upvoted 1 times

seedati 2 years, 6 months ago

Correct

upvoted 1 times

MattM70 2 years, 6 months 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 7 times

jorgesoma 2 years, 6 months ago

Could you explain it?

upvoted 1 times

jorgesoma 2 years, 6 months ago

Could you explain it?Read Lazylinux previous comment ;)

upvoted 1 times

Lazylinux 2 years, 6 months ago

U WRONG, read my comments

upvoted 3 times

itsmenida1 2 years, 5 months ago

Read Lazylinux previous comment ;)

upvoted 4 times

Question #66 *Topic 2*

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

Suggested Answer: *C*

Community vote distribution

C (100%)

Lazylinux Highly Voted 3 years ago

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"C" is correct, but you are likely to get the error during deployment if you try to assign /28 subnet to AG as /26 is recommended for AGv1 which may have up to 32 instances.

upvoted 6 times

Lazylinux Highly Voted 3 years 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 6 times

MarkMac Most Recent 11 months ago

Selected Answer: C

Makes sense. One for private IP, plus ten for max backends. Is says "assignable" so Azure reserved IPs aren't counted.

upvoted 1 times

tictaclu 1 year, 11 months ago

C is correct,

When you use a public endpoint for Azure Application Gateway, the public IP is allocated from the Azure public IP address pool, not from the subnet's IP address range.

Thus, the public endpoint does not consume an IP address from the Application Gateway subnet.

Calculation

Given the above:

Reserved by Azure: 5 IPs.

Private frontend IP: 1 IP.

Instances: 10 IPs (maximum).

5 (reserved)+1 (private IP)+10(instances)=16 IP addresses required

To meet this requirement, the smallest subnet that supports at least 16 assignable IPs is a /28

opt E 20 is because you count 1 IP for public endpoint which is not required.

upvoted 1 times

fraym 2 years, 1 month ago

Without even looking at the specifics of the question we know that 5 IPs are used per subnet, and the size of a subnet is a power of 2. Therefore the only possible solution is C: add 5 to any other answer and you don't get a power of 2 :)

upvoted 4 times

OrangeSG 3 years 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 2 times

Sergovladi 1 year, 10 months ago

"C" is correct, but you are likely to get the error during deployment if you try to assign /28 subnet to AG as /26 is recommended for AGv1 which may have up to 32 instances.

upvoted 2 times

Discussions22 3 years ago

Why not 12?Max 10 + 1 Private = 11 Public is not used from that scope.. it has a public IP

upvoted 1 times

Discussions22 3 years ago

Why not 12?

upvoted 1 times

ExamTopics2_EIS 3 years ago

Max 10 + 1 Private = 11

Public is not used from that scope.. it has a public IP

upvoted 6 times

Question #67 *Topic 2*

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.

The on-premises network connects to Vnet1 by using a Site-to-Site VPN.

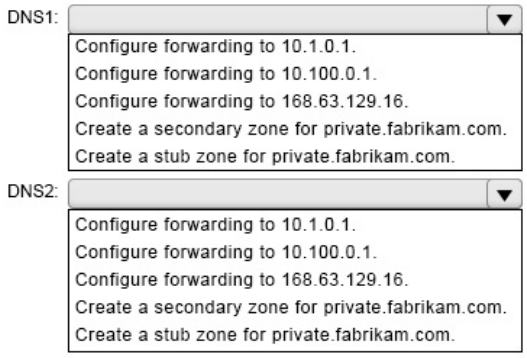
You need to ensure that the computers on the on-premises network can resolve the IP address for sql1.private.fabrikam.com.

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.

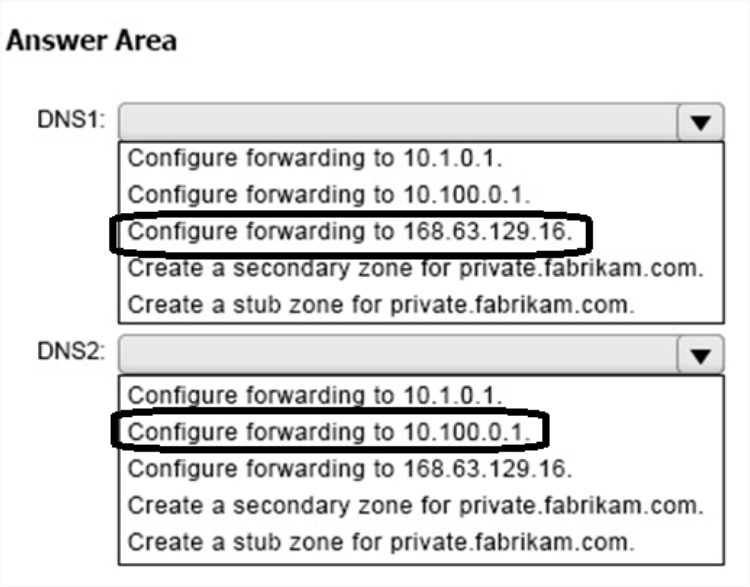
NOTE: Each correct selection is worth one point.

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

Answer Area



Suggested Answer:



Lazylinux Highly Voted 2 years 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 20 times

Lazylinux Highly Voted 2 years 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-168-63-129-16Correct. However, it's up to you to decide whether to use Private DNS resolver or forwarders depending on the complexity.

upvoted 20 times

40a4d4c Most Recent 7 months, 2 weeks ago

Answer is correct:

Client → DNS1 → DNS2 → Azure DNS (168.63.129.16) → Private DNS zone

Azure built-in DNS IP:

• 168.63.129.16

upvoted 1 times

getafix 1 year, 8 months ago

The answer is incorrect. The address 168.63.129.16 is an Azure internal address and it is not routable outside Azure. You cannot advertise this address out of Azure and it is not even visible to you to modify. Your on-prem DNS1 cannot directly communicate with this address.

Your on-prem dns1 will communicate with the dns2 in Azure. The DNS2 in Azure will communicate with the 168.63.129.16 address which in turn will resolve the DNS record

upvoted 1 times

aminiasin 1 year, 11 months 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 15 times

Sergovladi 1 year, 10 months ago

Correct. However, it's up to you to decide whether to use Private DNS resolver or forwarders depending on the complexity.

upvoted 1 times

Discussions22 2 years ago

What is correct if we have no?

upvoted 1 times

ExamTopics2_EIS 2 years ago

Clearly this is not correct. DNS2 is creating a forwarding to it's own IP address?

upvoted 5 times

Dungeon_Master 2 years ago

DNS1: Configure COnditional forwarding to DNS2 DNS2: Configure COnditional forwarding to 168.x.x.xI think it's correct. DNS1 (On-Prem): Forward to DNS2 (VM on Azure) DNS2 (Azure): Forward to 168.x.x.x (Azure DNS)

upvoted 6 times

Dungeon_Master 2 years ago

DNS1: Configure COnditional forwarding to DNS2 DNS2: Configure COnditional forwarding to 168.x.x.x

upvoted 6 times

jorgesoma 2 years 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 5 times

jorgesoma 2 years ago

Is it correct?

upvoted 1 times

Question #68 *Topic 2*

DRAG DROP

-

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

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.

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

Actions

- 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

Suggested Answer:

Answer Area

- Disassociate PIP1 from NIC1.
- Change the PIP1 SKU to Standard.
- Associate PIP1 to NIC1.

SilverFox22 Highly Voted 2 years, 7 months ago

Using the steps found in https://learn.microsoft.com/en-us/azure/nat-gateway/tutorial-migrate-ilip-nat The given answers are incomplete. It should be: Disassociate PIP1 from NIC1 Change the PIP1 SKU to Standard Associate PIP1 with Gateway1I think the point of this question is to reinforce that a NAT gateway can't be associated with a subnet that has recourses using public IPs with Basic sku'sThis makes sense. However, there is no option that states associating the NAT GW to the subnet, so Internet connection for that VM will go bye bye.

upvoted 7 times

SilverFox22 Highly Voted 2 years, 7 months ago

Using the steps found in https://learn.microsoft.com/en-us/azure/nat-gateway/tutorial-migrate-ilip-nat

The given answers are incomplete. It should be: Disassociate PIP1 from NIC1 Change the PIP1 SKU to Standard Associate PIP1 with Gateway1

upvoted 7 times

bobothewiseman 1 year, 9 months ago

Disassociate PIP1 from NIC1 Change the PIP1 SKU to Standard Associate PIP1 with Gateway1

upvoted 2 times

Sergovladi 1 year, 10 months ago

nothing to guess here: NAT gateway cannot be associated with a subnet containing a resource with Basic SKU IP

upvoted 1 times

fraym 2 years, 1 month ago

Again we have to guess from the choices given to us that the NAT gateway is supposed to use PIP1, this should be part of the instructions...

upvoted 4 times

fraym 2 years, 1 month ago

Again we have to guess from the choices given to us that the NAT gateway is supposed to use PIP1, this should be part of the instructions...nothing to guess here: NAT gateway cannot be associated with a subnet containing a resource with Basic SKU IP

upvoted 4 times

MarkMac Most Recent 11 months ago

This makes sense. However, there is no option that states associating the NAT GW to the subnet, so Internet connection for that VM will go bye bye.

upvoted 1 times

DC095 2 years ago

I think the point of this question is to reinforce that a NAT gateway can't be associated with a subnet that has recourses using public IPs with Basic sku's

upvoted 2 times

shako 2 years, 8 months ago

The 3rd step should be Associate PIP1 with the NAT Gateway

upvoted 1 times

mjk666 2 years, 8 months ago

why would we associate the PIP to NIC again ? we want to use Nat GW not a direct PIP.

upvoted 1 times

mjk666 2 years, 8 months ago

why would we associate the PIP to NIC again ? we want to use Nat GW not a direct PIP.Given answer is right.Nat Gateway doesn't accept private IPs with Basic SKU. Hence, need to upgrade it to Standard

upvoted 1 times

mb0812 2 years, 6 months ago

Given answer is right.Nat Gateway doesn't accept private IPs with Basic SKU. Hence, need to upgrade it to Standard

upvoted 3 times

CiscoExam 2 years, 9 months ago

https://learn.microsoft.com/en-us/azure/nat-gateway/tutorial-migrate-ilip-nat

upvoted 3 times

CiscoExam 2 years, 9 months ago

This is correct

upvoted 2 times

HOTSPOT

-

Your on-premises network contains the subnets shown in the following table.

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.

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.

Name	IPv4 network address
Subnet1	192.168.10.0/24
Subnet2	192.168.20.0/24

Name	Type	Description
VNet1	Virtual network	Uses an address space of 10.1.0.0/16
GW1	Virtual network gateway	• 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*

Answer Area

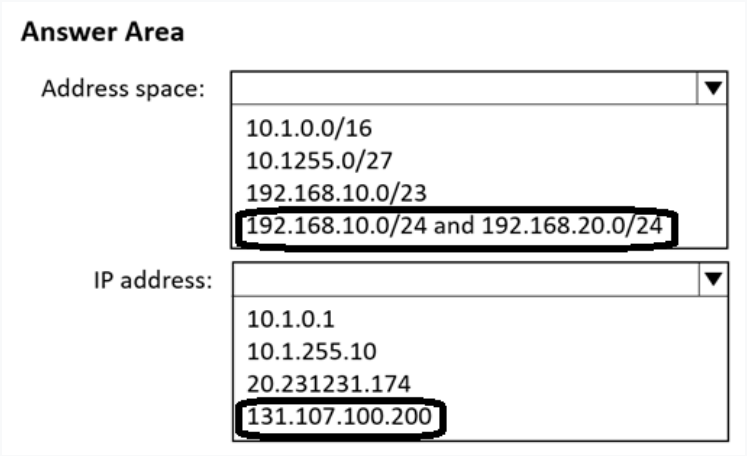
Address space:

- 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

Suggested Answer:



jom3az Most Recent 2 years, 4 months ago

Correct Answers

upvoted 2 times

galahad 2 years, 9 months ago

Answer seems to be correct.

upvoted 2 times

SJHCI 2 years, 10 months ago

Correct Answer!

upvoted 2 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.

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.

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.

Zone1.contoso.com has the virtual network links shown in the following table.

Other Azure Resources
-

The Azure subscription contains additional resources as shown in the following table.

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.

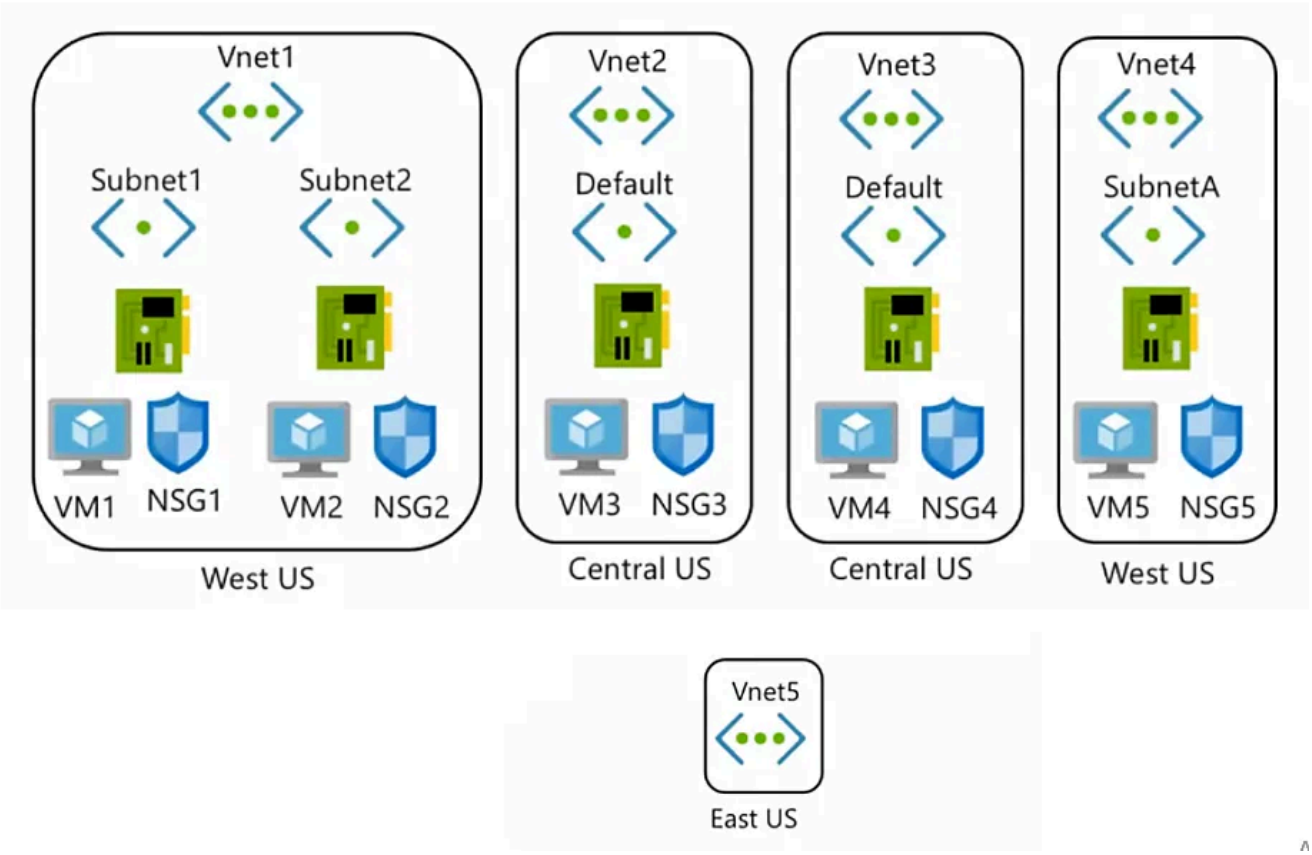
• Create an NSG named NSG11 that will be associated to Vnet1/Subnet2 and will have the custom outbound security rules shown in the following table.

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.

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**

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



Name	Location
zone1.contoso.com	Central US
zone2.contoso.com	West US

Name	Virtual Network	Auto registration
Link1	Vnet2	No
Link2	Vnet3	Yes

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

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

Priority	Port	Protocol	Source	Destination	Action
200	3389	TCP	10.1.0.0/16	VirtualNetwork	Deny

Answer Area

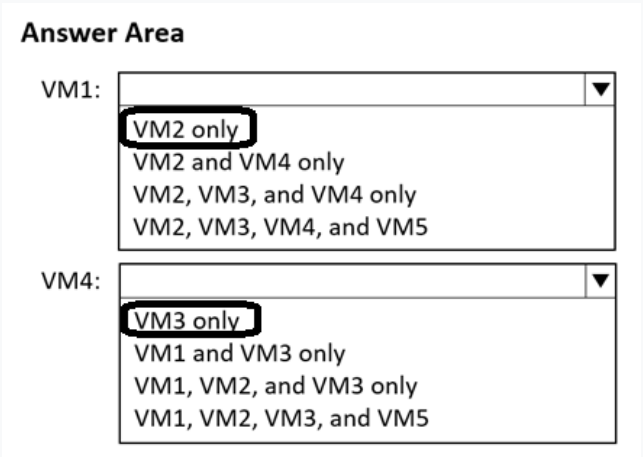
VM1:

- 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

Suggested Answer:



SJHCI Highly Voted 2 years, 4 months ago

For me as peering description:

- Vm 2,3,4 - VM 1,2,3

upvoted 46 times

SJHCI Highly Voted 2 years, 4 months ago

For me as peering description: - Vm 2,3,4 - VM 1,2,3Correct. First of all, VMs can access each other from the subnets within a VNET by default. Then we also need to look for mutual peering between VNETs

upvoted 46 times

Sergovladi 1 year, 10 months ago

Correct. First of all, VMs can access each other from the subnets within a VNET by default. Then we also need to look for mutual peering between VNETs

upvoted 1 times

samir111 2 years, 4 months 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 16 times

samir111 2 years, 4 months 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.Samir111 i agree with you on this now that you mentioned peering between VNET1 peered with VNET2/VNET3 which I overlooked on this question glad we have many pairs of eyes here to cover each other.

upvoted 16 times

galahad 2 years, 3 months ago

Samir111 i agree with you on this now that you mentioned peering between VNET1 peered with VNET2/VNET3 which I overlooked on this question glad we have many pairs of eyes here to cover each other.

upvoted 1 times

getafix Most Recent 1 year, 7 months ago

VNET1 has peering with VNET2 and VNET3 -> VM1 can ping VM2(same VNET as VM1), VM3(VNET2) and VM4(VNET3) VNET3 is peered with VNET1 and VNET2 -> VM4(VNET3) can ping VM1, VM2(both in VNET1) and VM3(VNET2) Only RDP allow custom rule is added, all other rules are still there by default. Those rules allow VNET to VNET communication hence allowing the ICMP response

upvoted 2 times

4d1c008 1 year, 7 months ago

I looked over this like five times to try and find the Peering everyone was talking about. I am blind out it is in one of the tables in case anyone else missed it.

upvoted 2 times

floanimation 1 year, 11 months ago

with peering : VM1 <> VM 2/3/4 (VNET 1 <> VNET2 + VNET1 <> VNET3) VM4 <> VM 1/2/3 (VNET 3 <> VNET1 + VNET3 <> VNET2) ICMP Is allowed Before NSG 10 - 11

upvoted 3 times

rAyLeE29 2 years, 3 months ago

"before NSG10 and NSG11 are created" is the keyword?

upvoted 4 times

rishabr019 2 years, 4 months ago

Correct answer. Vm 2,3,4 and vm3 onlu

upvoted 10 times

Question #71 *Topic 2*

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.

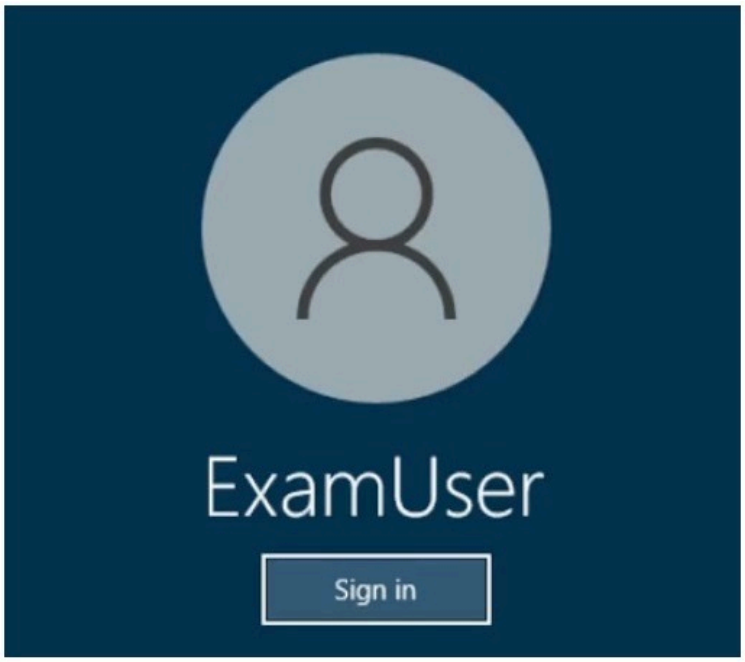
The following information is for technical support purposes only:

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.



Suggested 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

MarkMac Most Recent 11 months ago
The subnet name name must be "GatewaySubnet" and now you must specify the purpose of the subnet when you create it.
upvoted 1 times

Omniglass 2 years ago
Both types of gateways are able to exist in the same subnet, as long as the size is larter than /27
upvoted 2 times

Omniglass 2 years ago
Both types of gateways are able to exist in the same subnet, as long as the size is larter than /27The Gateway Subnet must be /27 or a shorter prefix (such as /26 or /25).
upvoted 2 times

Sergovladi 1 year, 10 months ago
The Gateway Subnet must be /27 or a shorter prefix (such as /26 or /25).
upvoted 1 times

jayek 2 years, 8 months ago
https://learn.microsoft.com/en-us/azure/expressroute/how-to-configure-coexisting-gateway-portal#to-configure-coexisting-connections-for-an-already-existing-vnet
upvoted 4 times

Question #72 *Topic 2*

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.

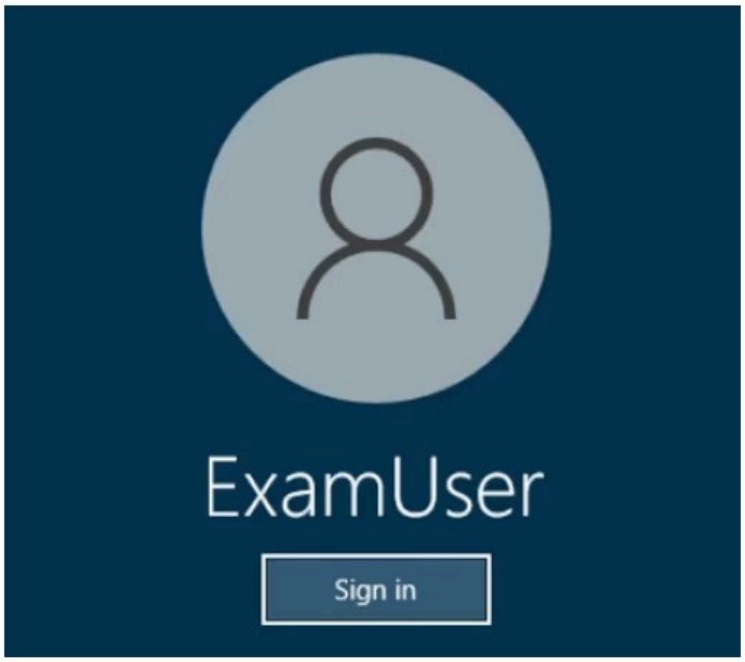
The following information is for technical support purposes only:

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.



Suggested 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

windowsmodulesinstallerworker Most Recent 1 year, 5 months ago

correct

upvoted 1 times

Question #73 *Topic 2*

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.

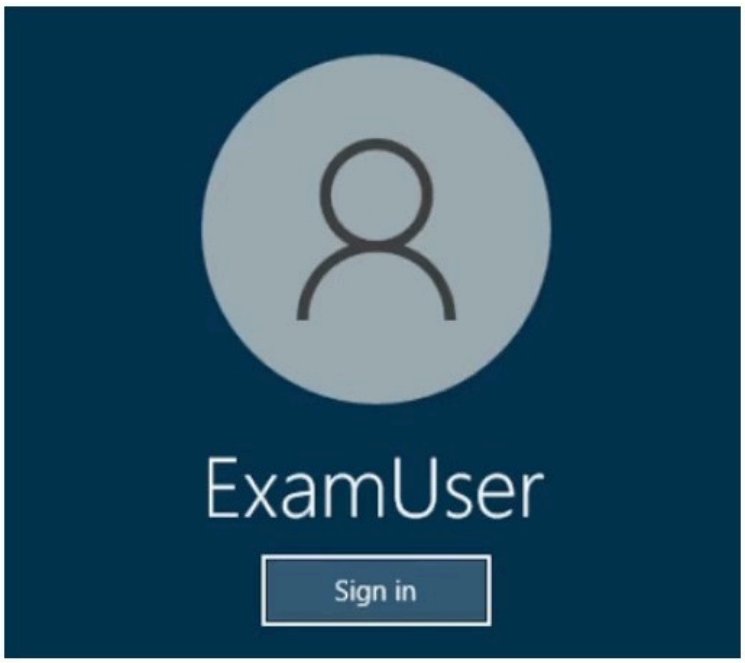
The following information is for technical support purposes only:

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.



Suggested 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.

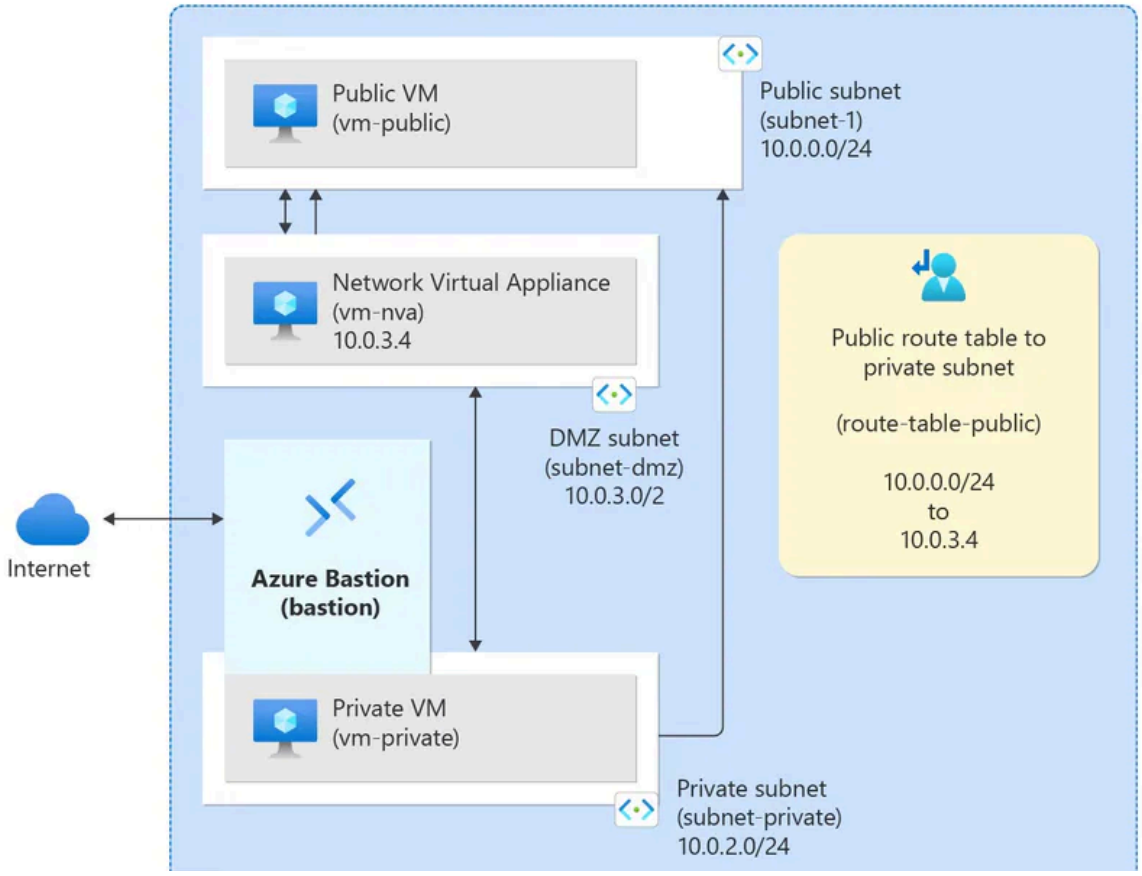
Step 8: Select + Associate.

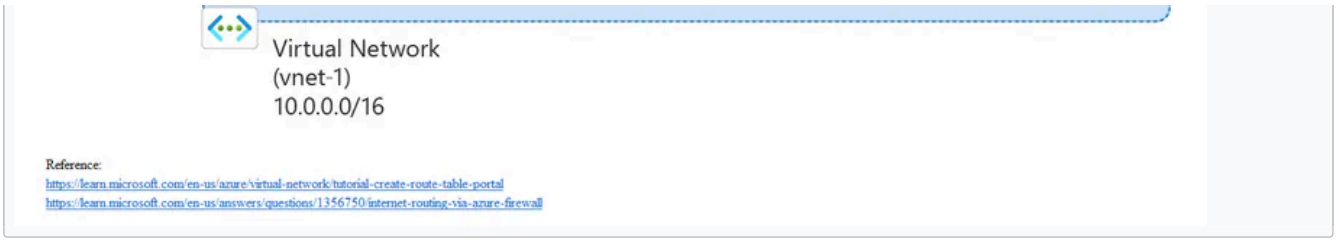
Step 9: Enter or select the following information in Associate subnet:

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).





cerifyme85 Highly Voted 2 years, 8 months ago

This is wrong. U route all traffic using UDRs to "Virtual Network Gateway" as this gateway connects to firewallYes, you need to configure UDR for 0.0.0.0/0 (all traffic) with next hop to VPN Gatewaythe picture with the adduced answer has nothing to do with the actual questionThe choice between using Virtual Appliance or Virtual Network Gateway (VNG) as the next hop in the User-Defined Route (UDR) depends on your requirements, architecture, and administrative preferences. What if VNG does not exist? Are you going to create one?

upvoted 5 times

cerifyme85 Highly Voted 2 years, 8 months ago

This is wrong. U route all traffic using UDRs to "Virtual Network Gateway" as this gateway connects to firewall

upvoted 5 times

Sergovladi 1 year, 10 months ago

Yes, you need to configure UDR for 0.0.0.0/0 (all traffic) with next hop to VPN Gatewaythe picture with the adduced answer has nothing to do with the actual question

upvoted 1 times

Sergovladi 1 year, 10 months ago

Yes, you need to configure UDR for 0.0.0.0/0 (all traffic) with next hop to VPN Gateway

upvoted 1 times

Sergovladi 1 year, 10 months ago

the picture with the adduced answer has nothing to do with the actual question

upvoted 2 times

bobothewiseman 1 year, 10 months ago

The choice between using Virtual Appliance or Virtual Network Gateway (VNG) as the next hop in the User-Defined Route (UDR) depends on your requirements, architecture, and administrative preferences. What if VNG does not exist? Are you going to create one?

upvoted 1 times

MarkMac Most Recent 11 months ago

Agree that this is wrong. The given answer works when the NVA in in a vNet, not on-prem. Besides the question doesn't even give the IP address of the FW.

upvoted 1 times

LearnICC 1 year, 8 months ago

This is correct (assuming the used Firewall IP is the internal one) But given network diagram in answer has nothing to do with it!

upvoted 1 times

bobothewiseman 1 year, 9 months ago

Both VNG and Virtual Appliance would work on this scenario. But I would prefer VNG

upvoted 1 times

Omniglass 2 years ago

Configure forced tunneling by assigning a Default Site to the virtual network gateway. Requires powershell command to set.

upvoted 3 times

Question #74 *Topic 2*

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.

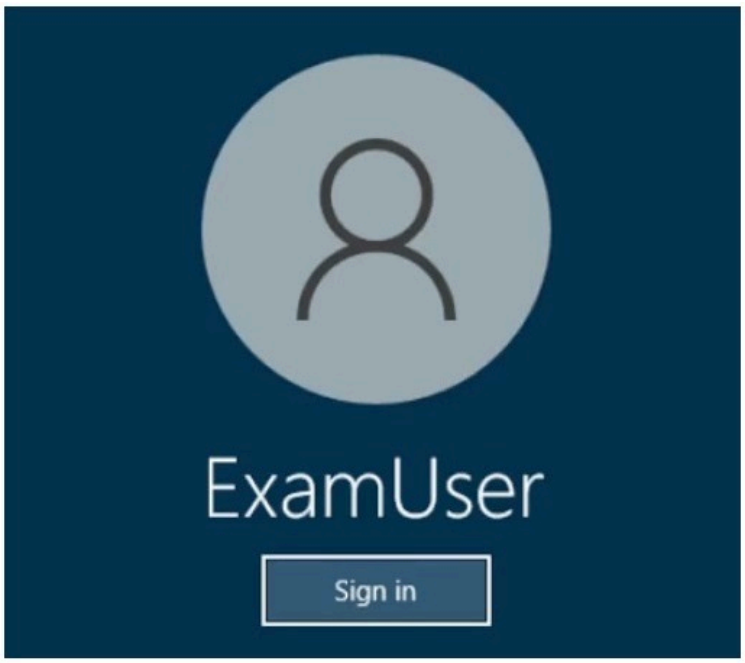
The following information is for technical support purposes only:

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.



Suggested 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.

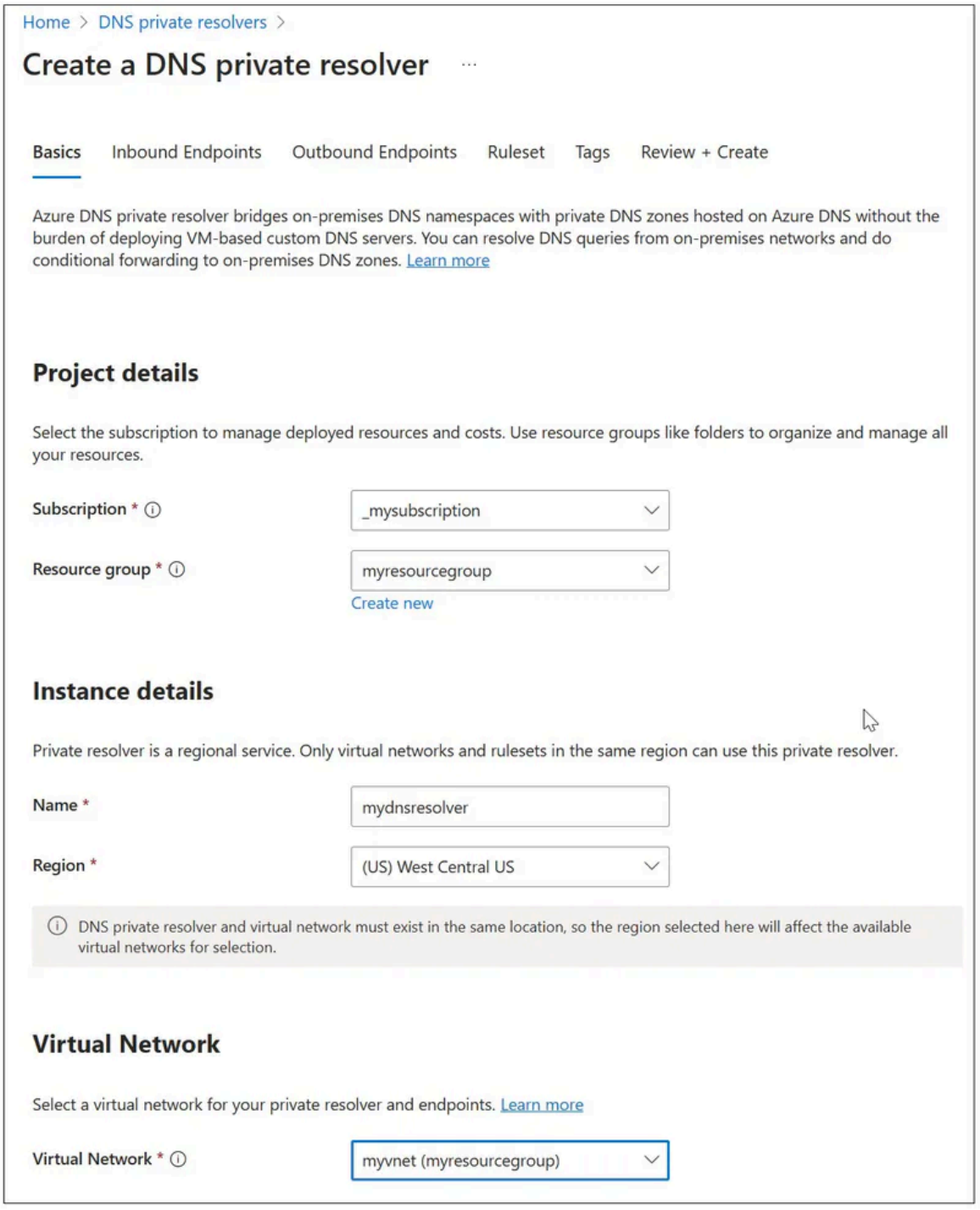
Create a DNS resolver inside the virtual network

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.



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 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 10.2.1.5, and then select Add.

Reference:
https://learn.microsoft.com/en-us/azure/dns/dns-private-resolver-get-started-portal

matanzpl Highly Voted 2 years, 8 months ago

think you should change DNS servers on the given VNET to 10.2.1.4 and 10.2.1.5

why create DNS resolver if you already have DNS servers as VMs?!

upvoted 9 times

matanzpl Highly Voted 2 years, 8 months ago

think you should change DNS servers on the given VNET to 10.2.1.4 and 10.2.1.5 why create DNS resolver if you already have DNS servers as VMs?!I don't agree! DNS Private Resolver is the better solution if you add custom DNS to vnet2 then ALL DNS resolution will run over 10.2.1.4 + 10.2.1.5 and you have to ensure, that these DNS servers have a DNS forwarding back to Azure (for Azure resources) on 168.63.129.16 which leads to more (DNS) traffic With DNS private resolver, you only resolve the on-prem domain fabrikam.com over 10.2.1.4 + 10.2.1.5 - it's some kind of "conditional DNS forwarder"dont forget that private resolver requires an outbound endpoint in a dedicated subnet that has IP visibility to your custom dns serversAgreed!I think the same Add DNS Servers Custom on VNET2

upvoted 9 times

LearnICC 1 year, 8 months ago

I don't agree! DNS Private Resolver is the better solution if you add custom DNS to vnet2 then ALL DNS resolution will run over 10.2.1.4 + 10.2.1.5 and you have to ensure, that these DNS servers have a DNS forwarding back to Azure (for Azure resources) on 168.63.129.16 which leads to more (DNS) traffic With DNS private resolver, you only resolve the on-prem domain fabrikam.com over 10.2.1.4 + 10.2.1.5 - it's some kind of "conditional DNS forwarder"dont forget that private resolver requires an outbound endpoint in a dedicated subnet that has IP visibility to your custom dns servers

upvoted 2 times

LearnICC 1 year, 8 months ago

I don't agree! DNS Private Resolver is the better solution if you add custom DNS to vnet2 then ALL DNS resolution will run over 10.2.1.4 + 10.2.1.5 and you have to ensure, that these DNS servers have a DNS forwarding back to Azure (for Azure resources) on 168.63.129.16 which leads to more (DNS) traffic With DNS private resolver, you only resolve the on-prem domain fabrikam.com over 10.2.1.4 + 10.2.1.5 - it's some kind of "conditional DNS forwarder"

upvoted 2 times

windowsmodulesinstallerworker 1 year, 6 months ago

dont forget that private resolver requires an outbound endpoint in a dedicated subnet that has IP visibility to your custom dns servers

upvoted 2 times

LieJ0n 2 years, 7 months ago

Agreed!

upvoted 1 times

floanimation 2 years, 5 months ago

I think the same Add DNS Servers Custom on VNET2

upvoted 3 times

MarkMac Most Recent 11 months ago

Given the requirements, adding custom DNS servers to the vNet is the easiest. Private resolver is a superior solution if the VMs (Azure and on-prem) need to access Azure resources in Azure Private DNS.

upvoted 1 times

Feliphus 1 year, 12 months ago

I think in that case you will change the DNS por all the queries and not only the queries to fabrikan.com domain Maybe others Azure resources will stop working when these can not resolve Azure internal domainsIt's better to follow the proposal solution with the Azure service DNS private resolver. You have to select vnet2 on the basic tabs for the virtual network, create two new Outbound endpoints (10.2.1.4 and 10.2.1.5) and set two new rules to resolve frabrikam.com DNS queries. If the statement would indicate one subnet to resolver or another not to resolve, you can set them at Inbound endpointsthis is not entirely correct. an outbound enpoint is just used for the private resolver to be able to communicate with your custom DNS servers. the endpoint also requires a minimum /28 dedicated subnet in the VNET where the private resolver is linked. You then specify your custom dns server ip addresses in the ruleset that specifies what dns requests should go to your custom servers.small correction: the outbound endpoint does not need to be necesarrily in the vnet where the private resovler is linked, it just needs to be in a vnet that has IP visibility to your custom DNS server. This is becose the client is communicating with azure DNS and azure DNS is doing the query on behalf of the client through its outbound IP address

upvoted 1 times

Feliphus 1 year, 12 months ago

I think in that case you will change the DNS por all the queries and not only the queries to fabrikan.com domain Maybe others Azure resources will stop working when these can not resolve Azure internal domains

upvoted 1 times

Feliphus 1 year, 12 months ago

It's better to follow the proposal solution with the Azure service DNS private resolver. You have to select vnet2 on the basic tabs for the virtual network, create two new Outbound endpoints (10.2.1.4 and 10.2.1.5) and set two new rules to resolve frabrikam.com DNS queries. If the statement would indicate one subnet to resolver or another not to resolve, you can set them at Inbound endpoints

upvoted 1 times

Feliphus 1 year, 12 months ago

It's better to follow the proposal solution with the Azure service DNS private resolver. You have to select vnet2 on the basic tabs for the virtual network, create two new Outbound endpoints (10.2.1.4 and 10.2.1.5) and set two new rules to resolve frabrikam.com DNS queries. If the statement would indicate one subnet to resolver or another not to resolve, you can set them at Inbound endpointsthis is not entirely correct. an outbound enpoint is just used for the private resolver to be able to communicate with your custom DNS servers. the endpoint also requires a minimum /28 dedicated subnet in the VNET where the private resolver is linked. You then specify your custom dns server ip addresses in the ruleset that specifies what dns requests should go to your custom servers.small correction: the outbound endpoint does not need to be necesarrily in the vnet where the private resovler is linked, it just needs to be in a vnet that has IP visibility to your custom DNS server. This is becose the client is communicating with azure DNS and azure DNS is doing the query on behalf of the client through its outbound IP address

upvoted 1 times

windowsmodulesinstallerworker 1 year, 6 months ago

this is not entirely correct. an outbound enpoint is just used for the private resolver to be able to communicate with your custom DNS servers. the endpoint also requires a minimum /28 dedicated subnet in the VNET where the private resolver is linked. You then specify your custom dns server ip addresses in the ruleset that specifies what dns requests should go to your custom servers.small correction: the outbound endpoint does not need to be necesarrily in the vnet where the private resovler is linked, it just needs to be in a vnet that has IP visibility to your custom DNS server. This is becose the client is communicating with azure DNS and azure DNS is doing the query on behalf of the client through its outbound IP address

upvoted 1 times

windowsmodulesinstallerworker 1 year, 6 months ago

this is not entirely correct. an outbound enpoint is just used for the private resolver to be able to communicate with your custom DNS servers. the endpoint also requires a minimum /28 dedicated subnet in the VNET where the private resolver is linked. You then specify your custom dns server ip addresses in the ruleset that specifies what dns requests should go to your custom servers.

upvoted 1 times

windowsmodulesinstallerworker 1 year, 6 months ago

small correction: the outbound endpoint does not need to be necesarrily in the vnet where the private resovler is linked, it just needs to be in a vnet that has IP visibility to your custom DNS server. This is becose the client is communicating with azure DNS and azure DNS is doing the query on behalf of the client through its outbound IP address

upvoted 1 times

Question #75 *Topic 2*

HOTSPOT

-

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

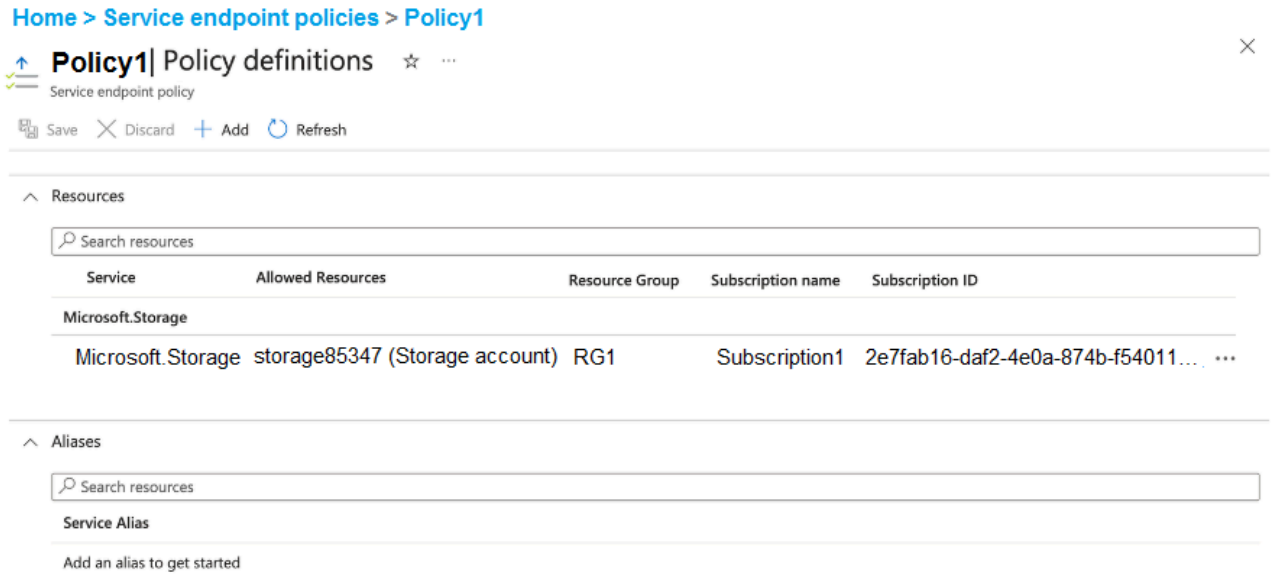
You create a service endpoint policy as shown in the Policy exhibit. (Click the Policy tab.)

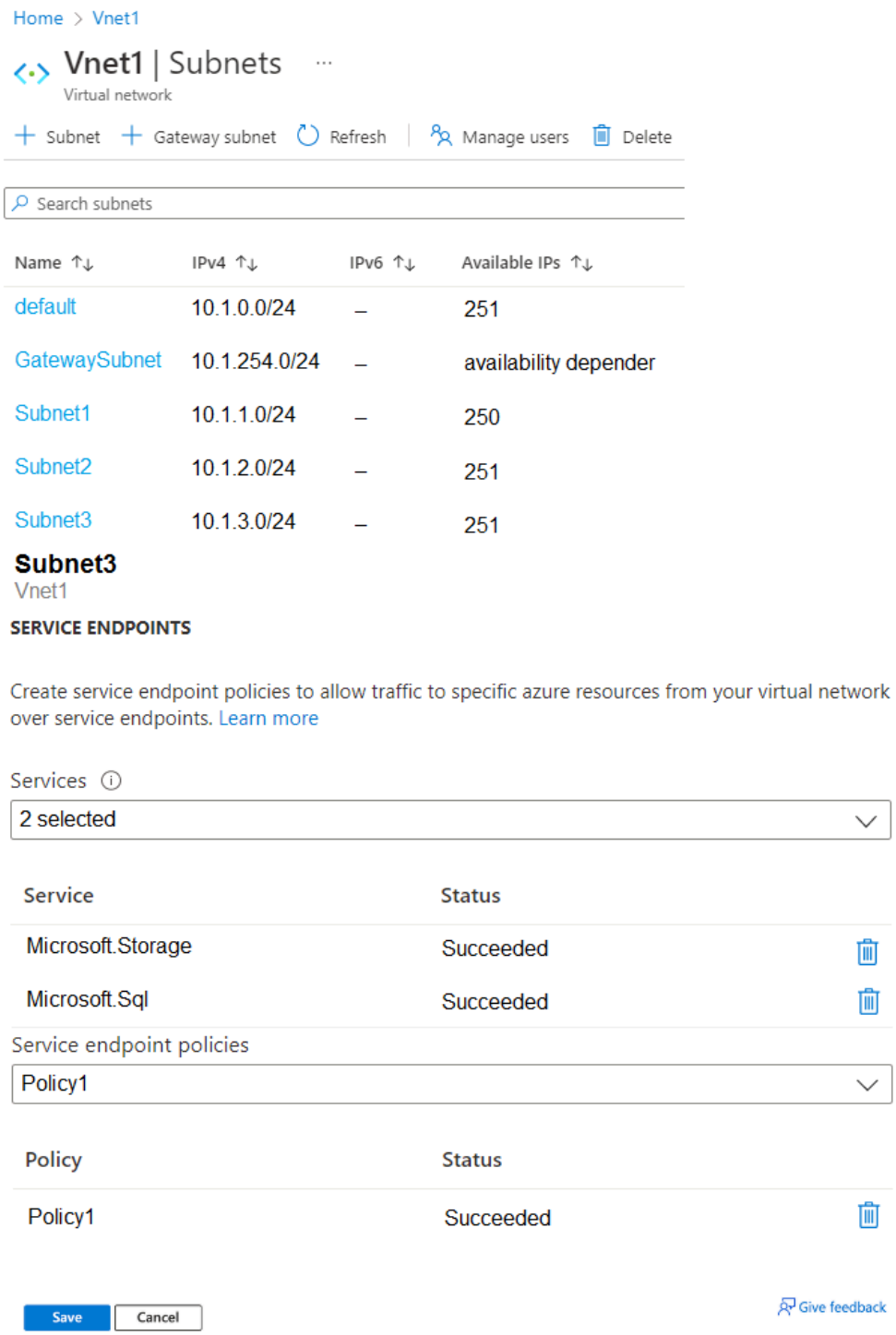
You configure the Service Endpoints settings for Subnet3 as shown in the Subnets exhibit. (Click the Subnets tab.)

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

NOTE: Each correct selection is worth one point.

Name	Description
storage85347	Storage account
storage85348	Storage account
DB1	Azure SQL database
VNet1	Virtual network
Subnet1	Subnet on VNet1
Subnet2	Subnet on VNet1
Subnet3	Subnet on VNet1

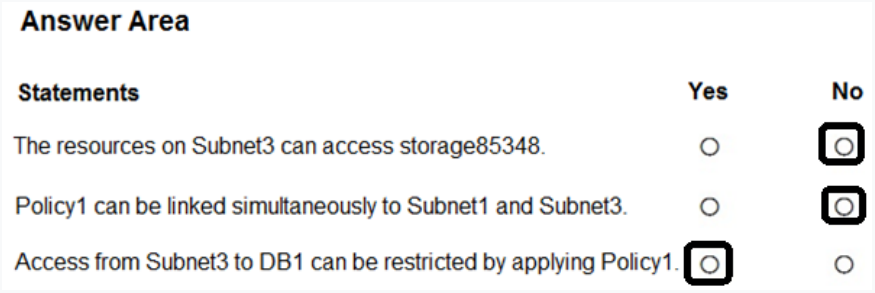




Answer Area

Statements	Yes	No
The resources on Subnet3 can access storage85348.	○	○
Policy1 can be linked simultaneously to Subnet1 and Subnet3.	○	○
Access from Subnet3 to DB1 can be restricted by applying Policy1.	○	○

Suggested Answer:



bobothewiseman Highly Voted 1 year, 10 months ago

1. No 2. Yes 3. No Policy1 is a service endpoint policy configured for Microsoft.Storage, which controls access to Azure Storage accounts only. • DB1 is an Azure SQL Database, and access to Azure SQL resources is governed by firewall rules or network security rules, not by service endpoint policies created for Microsoft.Storage.

upvoted 10 times

bobothewiseman Highly Voted 1 year, 10 months ago

1. No 2. Yes 3. No Policy1 is a service endpoint policy configured for Microsoft.Storage, which controls access to Azure Storage accounts only. • DB1 is an Azure SQL Database, and access to Azure SQL resources is governed by firewall rules or network security rules, not by service endpoint policies created for Microsoft.Storage.this is the correct answer

upvoted 12 times

CheMetto Most Recent 1 year, 1 month ago

I mean, maybe the second one is No because it's missing service endpoints? What is the way to think about those question?

I know that i can apply the same SE Policy to multiple vnet, but i also know that a SE is required. I'll go with NNN.

upvoted 1 times

manhattan 1 year, 10 months ago

Selected Answer: C

1) NO the only accessible storage is storage85347 because once the service endpoint policy is assigned it allows ONLY the resources listed in the policy, look here: https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoint-policies?tabs=portal#apply-policy-to-allow-access-to-valid-storage-account "Ensure that all the resources accessed from the subnet are added to the policy definition before associating the policy to the given subnet. Once the policy is associated, only access to the allow listed resources will be allowed over service endpoints. 2) YES, you can assign the policy to multiple subnets as long as you enable the microsoft.storage service endpoint in advance for all of them. (tested in lab) 3) YES, of course for the same reason mentioned above, the policy (once applied) can restrict the access to the resources add into the policy list only. so to me, is NO, YES, YES

upvoted 10 times

windowsmodulesinstallerworker 1 year, 5 months ago

this is the correct answer

upvoted 2 times

manhattan 1 year, 10 months ago

Selected Answer: C

1) NO the only accessible storage is storage85347 because once the service endpoint policy is assigned it allows ONLY the resources listed in the policy, look here:

https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoint-policies?tabs=portal#apply-policy-to-allow-access-to-valid-storage-account

"Ensure that all the resources accessed from the subnet are added to the policy definition before associating the policy to the given subnet. Once the policy is associated, only access to the allow listed resources will be allowed over service endpoints.

2) YES, you can assign the policy to multiple subnets as long as you enable the microsoft.storage service endpoint in advance for all of them. (tested in lab)

3) YES, of course for the same reason mentioned above, the policy (once applied) can restrict the access to the resources add into the policy list only.

so to me, is NO, YES, YES

upvoted 10 times

windowsmodulesinstallerworker 1 year, 5 months ago

the last one is no. the policy is configured for the storage provider

upvoted 4 times

Question #76 *Topic 2*

You have an on-premises DNS server named Server that hosts a primary DNS zone named fabrikam.com.

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

Users on the on-premises network access resources on all the virtual networks by using a Site-to-Site (S2S) VPN.

You need to deploy an Azure DNS Private Resolver solution that meets the following requirements:

• Resources connected to the virtual networks must be able to resolve DNS names for fabrikam.com.
• Server1 must be able to resolve the DNS names of the resources in contoso.com.
• The solution must minimize costs and administrative effort.

What is the minimum number of resolvers you should deploy?

Name	Type	Description
VNet1	Virtual network	In the US West Azure region
VNet2	Virtual network	In the US West Azure region
VNet3	Virtual network	In the West Europe Azure region
VNet4	Virtual network	In the West Europe Azure region
contoso.com	Azure Private DNS zone	In the West Europe Azure region and linked to VNet1, VNet2, VNet3, and VNet4

A. 1

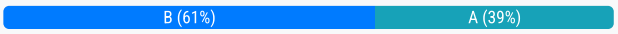
B. 2

C. 3

D. 4

Suggested Answer: *B*

Community vote distribution



Gambito11 Highly Voted 1 year, 11 months ago

Azure Dns private resolver is a regional service. "A DNS resolver can only refer to a virtual network that's in the same region as the DNS resolver" https://learn.microsoft.com/en-us/azure/architecture/networking/architecture/azure-dns-private-resolver

upvoted 12 times

Mo_Aly Most Recent 5 months, 3 weeks ago

DNS resolver AND the ruleset are regional. On-premises to VNet via inbound endpoint can be across regions, however the other way round (VNet to On-premises) is regional

upvoted 1 times

TheCloudGuruu 6 months, 3 weeks ago

The key: DNS forwarding rulesets can be linked to VNets across regions. Even though VNet1/VNet2 are in US West and VNet3/VNet4 are in West Europe, a single ruleset from one outbound endpoint can serve all of them. The resolver is regional, but its ruleset links are not. Deploy the resolver in any one of the four VNets (ideally one connected via S2S VPN for the inbound path), and both requirements are covered.

upvoted 1 times

Patel777 1 year, 4 months ago

A single Azure DNS Private Resolver can handle both inbound and outbound DNS queries for multiple VNets, as long as you peer the VNets and/or link them to the resolver's VNet.

upvoted 1 times

Patel777 1 year, 4 months ago

There is no peering or connectivity mentioned in the question from US West VNets to West Europe VNets.

upvoted 1 times

goos5 1 year, 4 months ago

Since the on-premises network can access all Azure resources via S2S, it is given that all vnets are peered. One resolver, in the hub, can reached all other peered vnets. The same Resolver can be reached from on-premises.

upvoted 1 times

xRiot007 1 year, 7 months ago

https://learn.microsoft.com/en-us/azure/architecture/networking/architecture/azure-dns-private-resolver An Azure DNS Private Resolver has REGIONAL AVAILABILITY, so no, it will not work across multiple regions. Without VNet peering or vWAN, this resolver is bound to its VNet.

upvoted 1 times

bobothewiseman 1 year, 10 months ago

Selected Answer: A

I go for A! You can deploy the resolver in the US West region (e.g., VNet1 or VNet2) because it can handle DNS queries for all Azure VNets connected via VPN or peering.

upvoted 1 times

bobothewiseman 1 year, 10 months ago

I go for A! You can deploy the resolver in the US West region (e.g., VNet1 or VNet2) because it can handle DNS queries for all Azure VNets connected via VPN or peering.Microsoft test though... if it isn't mentioned it doesn't exist. With the way the questions is worded I would go with B. Yeah there are better ways but that's Microsoft for you.Forwarding rulesets cannot be applied to VNETS in a separate region from the Private DNS Resolver instance. Peering is irrelevant. Even with global peerings a VNET in one region cannot forward DNS request to a private DNS resolver in another.

upvoted 1 times

4d1c008 1 year, 7 months ago

Microsoft test though... if it isn't mentioned it doesn't exist. With the way the questions is worded I would go with B. Yeah there are better ways but that's Microsoft for you.

upvoted 1 times

DC095 11 months, 2 weeks ago

Forwarding rulesets cannot be applied to VNETS in a separate region from the Private DNS Resolver instance. Peering is irrelevant. Even with global peerings a VNET in one region cannot forward DNS request to a private DNS resolver in another.

upvoted 1 times

prekair0 1 year, 11 months ago

Private DNS zone is global. private DNS resolver is restricted to the location of the VNET, but it can lookup any address in the private DNS zone as long as it's linked. So 1 private DNS resolver should be sufficient.

upvoted 4 times

maciek8131 1 year, 11 months ago

I think that is should be A. Only One

upvoted 3 times

niau 1 year, 11 months ago

Azure Dns private resolver is a regional service. "A DNS resolver can only refer to a virtual network that's in the same region as the DNS resolver" https://learn.microsoft.com/en-us/azure/architecture/networking/architecture/azure-dns-private-resolver

upvoted 2 times

Question #77 *Topic 2*

HOTSPOT
-

You have an Azure subscription that contains a dual-stack virtual network named VNet1. VNet1 has the following IP address spaces:

• IPv4: 192.168.0.0/24
• IPv6: fd00:db8:deca:deed:/48

You plan to deploy an Azure VPN gateway and multiple virtual machines to VNet1.

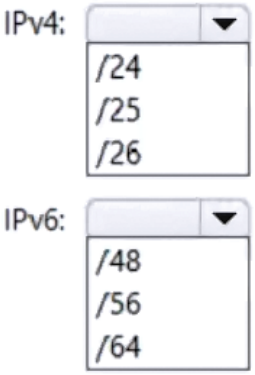
You need to configure the subnet masks for VNet1. The solution must meet the following requirements:

• Maximize the number of usable IP addresses.
• Support the deployment of the VPN gateway and the virtual machines.

Which subnet mask should you use for each address space? To answer, select the appropriate options in the answer area.

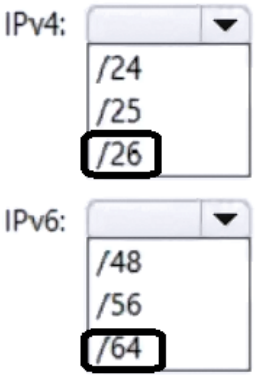
NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:

Answer Area



40a4d4c Most Recent 7 months, 1 week ago

/24 /64.....gives the maximum usable IPv4 addresses (256) from the 192.168.0.0/24 space, and /64 is the standard maximally-sized IPv6 subnet (providing 2^{64} addresses per subnet) supported by Azure for VPN gateway deployments.

upvoted 2 times

black2jm 9 months ago

The wording of this is terrible. If talking about VNET Address space, the space assigned is the largest. If dealing with subnet size, then /25 (due to GatewaySubnet) for IPv4 and /64 for IPv6

upvoted 3 times

Silverpro29 1 year, 6 months ago

Why is the answer A? There is no radius option A, B, C, or D. This is a drop option for the Answer Area. It's confusing.

Address Space Correct Subnet Mask Why?

IPv4 /24 Maximizes number of IPv4 addresses. /24 = 256 addresses

IPv6 /64 Azure requires subnets to be /64 for IPv6. /48 and /56 are too large.

Quick numbers:

IPv4 /24 gives 256 IPs minus Azure reserved IPs (5 reserved), so 251 usable.

IPv6 /64 is standard — extremely large — Azure won't allow smaller subnet masks than /64 for IPv6.

upvoted 1 times

Henk_2025 1 year, 8 months ago

**** Answer /25 and /64****

Vpn gw need a dedicated subnet. So two or more subnets are at least needed. You can split /24 into more subnets of /25 and /26. With the use of 2 times a /25 you have maximized the the usable IP addresses , if you use /26 subnets you have less usable IP adresses in totall

Example > 251 with /24 , 246 with /25 , 236 with /26

upvoted 2 times

Henk_2025 1 year, 8 months ago

**** Answer /25 and /64**** Vpn gw need a dedicated subnet. So two or more subnets are at least needed. You can split /24 into more subnets of /25 and /26. With the use of 2 times a /25 you have maximized the the usable IP addresses , if you use /26 subnets you have less usable IP adresses in totall Example > 251 with /24 , 246 with /25 , 236 with /26

upvoted 2 times

Henk_2025 1 year, 8 months ago

Correction > Example > 252 with /24 , 248 with /25 , 240 with /26

upvoted 1 times

Henk_2025 1 year, 8 months ago

Correction > Example > 252 with /24 , 248 with /25 , 240 with /26

upvoted 1 times

DC095 11 months, 2 weeks ago

This is wildly incorrect subnetting. Outside of Azure a /25 prefix length translates to 126 usable addresses. In Azure it would be 123 addresses. The formula for determining the number of addresses is (2^Host bits)-2. With a /25 network you have 7 host bits. 2^7 is 128. Subtract 2 is 126. In azure you would subtract 5(network, broadcast, and reserved addresses)

upvoted 1 times

manhattan 1 year, 10 months ago

Selected Answer: A

to be honest this seems a weird question, at first it asks for "You need to configure the subnet masks for VNet1" and then it says "Which subnet mask should you use for each address space?" which subnet is it speaking of? Gateway, VMs or the whole Vnet one? to maximize the whole Vnet you should use /24 for IPv4 and /64 for IPv6 but for vpn gateway subnet a /26 is enough and you should subnetting the whole /24 assigned.. any ideas? Maybe I'm missing something...

upvoted 3 times

Knight_Of_Peace Highly Voted 1 year, 9 months ago

Suggested answer is: /25 and /64

The question is asking maximize the number of usable IP addresses, which means all the subnets apart from the Gateway subnet because it can be used only from the Gateway deployment.

Sine the address space for the entire VNet is /24, that will give 256 IP address which needs to be used to cover the Gateway subnet and the VMs subnets.

Can't used /24 for the VMs subnets because that will take the entire IP range to the VMs subnet and then the Gateway subnet will not be able to be implemented in the VNet. So /24 is not an option.

The minimum subnet can be assigned for the Gateway is /29 which will give 8 IP addresses.

This will give 248 IP address which can be used for VMs subnets. To use these IP addresses (248), it needs to be created in multiple subnets starting with /25, /26, /27, /28, & /29.

So the biggest subnet with usable IP addresses is /25.

upvoted 6 times

Sergovladi 1 year, 10 months ago

should be /24 and /64 because asked for maximum

upvoted 1 times

Sergovladi 1 year, 10 months ago

should be /24 and /64 because asked for maximumYou need a subnet for gateway, so /25

upvoted 1 times

manhattan 1 year, 10 months ago

Selected Answer: A

to be honest this seems a weird question, at first it asks for "You need to configure the subnet masks for VNet1" and then it says "Which subnet mask should you use for each address space?"

which subnet is it speaking of? Gateway, VMs or the whole Vnet one?

to maximize the whole Vnet you should use /24 for IPv4 and /64 for IPv6 but for vpn gateway subnet a /26 is enough and you should subnetting the whole /24 assigned..

any ideas? Maybe I'm missing something...

upvoted 3 times

khengoolman 1 year, 5 months ago

You need a subnet for gateway, so /25

upvoted 2 times

Question #78 *Topic 2*

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

You need to implement a solution for the traffic originating from VNet1. The solution must meet the following requirements:

• Perform transparent proxying to external web servers.
• Inspect all outbound TLS traffic.
• Minimize costs.

Which resource should you include in the solution?

Name	Type	Description
AG1	Azure Application Gateway configured with Azure Web Application Firewall (WAF)	Connected to VNet1
FD1	Azure Front Door configured with Azure Web Application Firewall (WAF)	*None*
FW1	Azure Firewall Premium	Deployed to VNet1
FW2	Azure Firewall Standard	Deployed to VNet1

A. FW2

B. AG1

C. FD1

D. FW1

Suggested Answer: *D*

Community vote distribution

D (100%)

manhattan Highly Voted 1 year, 11 months ago

it should be the FW1 Azure Firewall operates in a transparent proxy mode by default. In this mode, traffic is sent to the firewall using a user defined route (UDR) configuration. The firewall intercepts that traffic inline and passes it to the destination. https://learn.microsoft.com/en-us/azure/firewall/explicit-proxy the KEY element here is the TLS feature that seems included in the premium only "advanced threat protection https://learn.microsoft.com/en-us/azure/firewall/choose-firewall-sku

upvoted 6 times

Gambito11 1 year, 11 months ago

Correct https://learn.microsoft.com/es-es/azure/firewall/choose-firewall-sku

upvoted 2 times

Question #79 *Topic 2*

HOTSPOT

-

You have an on-premises network.

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

You need to ensure that on-premises devices can communicate with Azure resources that are connected to Subnet4.

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

NOTE: Each correct selection is worth one point.

Name	Type	Description
Subnet1	On-premises subnet	Assigned an IP address of 10.1.1.0/24
Subnet2	On-premises subnet	Assigned an IP address of 10.1.2.0/24
Subnet3	Azure virtual subnet	Assigned an IP address of 10.1.3.0/24
Subnet4	Azure virtual subnet	Assigned an IP address of 10.1.1.0/24
VNet1	Azure virtual network	Contains Subnet3 and Subnet4
Server1	Windows Server 2022	On-premises server that is connected to Subnet1 and Subnet2.
VM2	Windows Server 2022	Azure virtual machine that is connected to Subnet3 and Subnet4
S2SVPN1	Site-to-Site (S2S) VPN	Connects the on-premises network to VNet1

Answer Area

Server1:
- Configure an Azure Network Adapter.
- Deploy the Network Controller role.
- Deploy the On-Premises Extended-Network Gateway appliance.
- Deploy the Web Application Proxy role service.

VM2:
- Configure an Azure Network Adapter.
- Deploy the Routing and Remote Access server.
- Deploy the Azure Extended-Network Gateway appliance.
- Deploy the On-Premises Extended-Network Gateway appliance.

Suggested Answer:

Answer Area

Server1:
- Configure an Azure Network Adapter.
- Deploy the Network Controller role.
- Deploy the On-Premises Extended-Network Gateway appliance.
- Deploy the Web Application Proxy role service.

VM2:
- Configure an Azure Network Adapter.
- Deploy the Routing and Remote Access server.
- Deploy the Azure Extended-Network Gateway appliance.
- Deploy the On-Premises Extended-Network Gateway appliance.

Patel777 Most Recent 1 year, 3 months ago

Server1: Deploy the On-Premises Extended-Network Gateway appliance

VM2: Configure an Azure Network Adapter

This setup uses Azure Network Adapter (ANA) on VM2 to securely connect to on-premises, but not the other way around. You only expose Subnet4, because VM2 is the only resource being connected back to on-prem. You are not creating full VNet-to-VNet peering or VPN tunnels, just targeted hybrid access from Azure VM2 to Server1, via on-premises gateway appliance.

This design limits exposure, requires minimal configuration, and is Microsoft-supported.

upvoted 1 times

manhattan 1 year, 10 months ago

Selected Answer: A

it should be correct, deploy the On-prem extended network GW appliance

Deploy the Azure extended network GW appliance

https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/azure/azure-extended-network

upvoted 2 times

Question #80 *Topic 2*

DRAG DROP

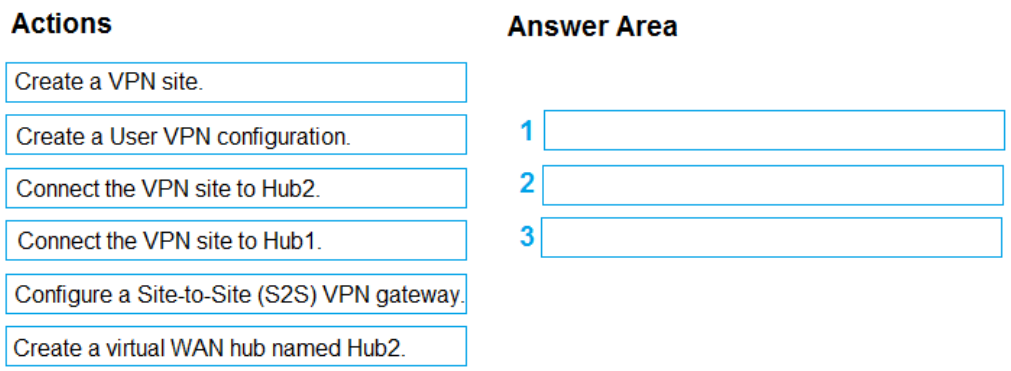
-

You have an on-premises network.

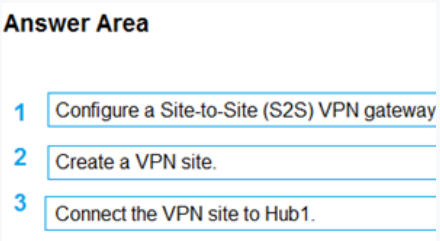
You have an Azure subscription that contains a virtual network named VNet1. VNet1 is connected to an Azure Virtual WAN hub named Hub1.

You need to enable connectivity between the on-premises network and VNet1 by using Hub1.

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.



Suggested Answer:



Bl4d3 Most Recent 1 year ago

Create a VPN site

This defines your on-premises network in Azure Virtual WAN.

You'll specify the public IP of your on-prem VPN device and the address space (e.g., 10.1.0.0/24).

Connect the VPN site to Hub1

This links your defined VPN site to the existing Virtual WAN hub (Hub1).

It establishes the Site-to-Site VPN tunnel between your on-premises gateway and Azure.

Configure a Site-to-Site (S2S) VPN gateway

This step is done on your on-premises VPN device.

You configure it to connect to Azure using the parameters provided when you connected the VPN site to Hub1 (e.g., IP, shared key, tunnel settings).

upvoted 2 times

Zorro2003 1 year, 2 months ago

Do these in order:

Configure a Site-to-Site (S2S) VPN gateway (on Hub1).

Create a VPN site (representing the on-premises gateway).

Connect the VPN site to Hub1.

This is the normal vWAN flow: enable the hub's VPN gateway, define the on-prem site, then create the site-to-hub connection (VNet1 is already attached to Hub1).

upvoted 2 times

Raheal 1 year, 3 months ago

Configure site-to-site VPN gateway

Create a site

Connect a site to a virtual hub

upvoted 1 times

marcin1999 1 year, 7 months ago

I guess it could be Create a site

Configure site-to-site VPN gateway settings

Connect a site to a virtual hub

upvoted 2 times

marcin1999 1 year, 7 months ago

I guess it could be Create a site Configure site-to-site VPN gateway settings Connect a site to a virtual hubis it really correct ?

upvoted 2 times

szp87 1 year, 3 months ago

is it really correct ?

upvoted 1 times

xRiot007 1 year, 7 months ago

You don't "Create a user VPN config" you download it.

Also Hub2 does not exist, so you can ignore all options related to it.

Given that, the correct answers should be:

1. Create a VPN site

2. Connect the site to Hub1

3. Download VPN config

Ref: https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-site-to-site-portal

upvoted 1 times

manhattan Highly Voted 1 year, 10 months ago

Selected Answer: A

It looks correct, it starts at the 3rd step of this procedure

Create a virtual WAN

Configure virtual hub Basic settings

Configure site-to-site VPN gateway settings

Create a site

Connect a site to a virtual hub

Connect a VPN site to a virtual hub

Connect a VNet to a virtual hub

Download a configuration file

View or edit your VPN gateway

https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-site-to-site-portal

upvoted 9 times

Question #81 *Topic 2*

You have an Azure subscription. The subscription contains a locally-redundant storage (LRS) account named storage1 that is deployed to the US East Azure region and has a Microsoft.Storage service endpoint.

You set Redundancy for storage1 to Read-access geo-redundant storage (RA-GRS).

You need to ensure that the contents of storage1 will be accessible by using a service endpoint in a paired region. The solution must minimize administrative effort.

What should you do first?

A. Create an object replication rule for storage.

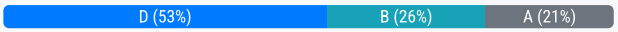
B. Delete the existing service endpoint.

C. From storage1, select Secure transfer required.

D. Create a service endpoint policy.

Suggested Answer: *D*

Community vote distribution



Patel777 Most Recent 1 year, 4 months ago

Selected Answer: A

first set up object replication from storage1 to a storage account in the paired region.

Only then can a service endpoint in that paired region provide access.

upvoted 1 times

xRiot007 1 year, 7 months ago

D - set a policy to control to what can the VNet have access when using the service point.

Ref: https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoint-policies-overview

upvoted 1 times

a250fb0 1 year, 9 months ago

Selected Answer: B

When you switch the redundancy of a storage account from Locally Redundant Storage (LRS) to Read-Access Geo-Redundant Storage (RA-GRS), the storage account gains a secondary endpoint in the paired region. However, existing service endpoints are tied to the primary region only, and they do not automatically support access to the secondary endpoint in the paired region. D. Create a service endpoint policy: Service endpoint policies are used to restrict which storage accounts can be accessed via a service endpoint, but they do not enable access to paired regions.

upvoted 4 times

a250fb0 1 year, 9 months ago

When you switch the redundancy of a storage account from Locally Redundant Storage (LRS) to Read-Access Geo-Redundant Storage (RA-GRS), the storage account gains a secondary endpoint in the paired region. However, existing service endpoints are tied to the primary region only, and they do not automatically support access to the secondary endpoint in the paired region. D. Create a service endpoint policy: Service endpoint policies are used to restrict which storage accounts can be accessed via a service endpoint, but they do not enable access to paired regions.When you create a secondary RA-GRS, both primary and secondary are automatically available and can be used. You don't need to delete anything. You need to set a policy to control which VNets have access to what storage account.

upvoted 4 times

xRiot007 1 year, 7 months ago

When you create a secondary RA-GRS, both primary and secondary are automatically available and can be used. You don't need to delete anything. You need to set a policy to control which VNets have access to what storage account.

upvoted 1 times

bobothewiseman 1 year, 9 months ago

Selected Answer: D

My final answer is D. Create a service endpoint policy.

upvoted 2 times

bobothewiseman 1 year, 10 months ago

Selected Answer: B

I will go with B! When you enable Read-access geo-redundant storage (RA-GRS) for your storage account, the data is replicated to a secondary region (the paired region) to provide read access in case of a regional outage. However, service endpoints are tied to the original region where they were created and do not automatically update to include access from the paired region

upvoted 1 times

bobothewiseman 1 year, 10 months ago

I will go with B! When you enable Read-access geo-redundant storage (RA-GRS) for your storage account, the data is replicated to a secondary region (the paired region) to provide read access in case of a regional outage. However, service endpoints are tied to the original region where they were created and do not automatically update to include access from the paired regionMy final answer is D. Create a service endpoint policy.

upvoted 1 times

alexastein 1 year, 11 months ago

Selected Answer: D

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

upvoted 2 times

NK203 Highly Voted 1 year, 11 months ago

Selected Answer: D

When Service Endpoint policies are applied on a subnet, the Azure Storage Service Endpoint scope gets upgraded from regional to global. This process means that all the traffic to Azure Storage is secured over service endpoint thereafter. The Service endpoint policies are also applicable globally. Any storage accounts that aren't explicitly allowed are denied access.

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

upvoted 6 times

sismer 1 year, 11 months ago

Selected Answer: A

To ensure that the contents of your storage account (storage1) will be accessible by using a service endpoint in a paired region with minimal administrative effort, you should:

A. Create an object replication rule for storage.

This will allow you to replicate the contents of storage1 to another storage account in the paired region, ensuring accessibility through a service endpoint in that region.

upvoted 3 times

Question #82 *Topic 2*

HOTSPOT
-

You have two Azure subscriptions.

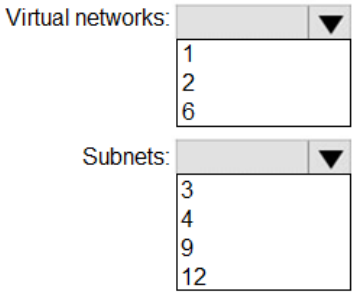
You need to perform the following actions in the East US Azure region of each subscription:

• Deploy 50 virtual machines to availability zone 1.
• Deploy 50 virtual machines to availability zone 2.
• Deploy 50 virtual machines to availability zone 3.

What is the minimum number of virtual networks and /25 subnets you should create? To answer, select the appropriate options in the answer area.

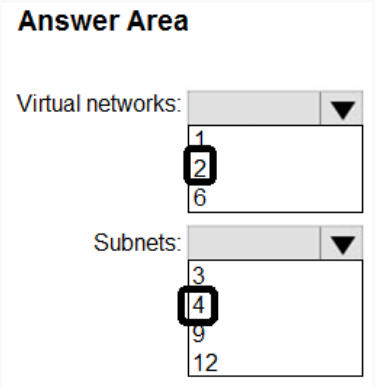
NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:

Answer Area



40a4d4c Most Recent 7 months, 1 week ago

2 VNET

6 Subnet

----2 subscriptions >>>>>2 VNET>>>Each VENT 3 Subnet(3 AZ)

upvoted 2 times

easy_t Highly Voted 1 year, 10 months ago

Given Answer is Correct.

Normally, you just need to create a /24 Virtual Network with minimum of 2 different zones /25 subnets.

/25 Subnet = (128 - 5) IPs : 123 available IPs

=> 50 VMs in zone A, 50 VMs in zone B

/25 Subnet = (128 - 5) IPs: 123 available IPs

=> 50 VMs in zone C

But,

the questions mentioned that 2 subscriptions. (Highlighted the "each subscription").

So, the minimum requirements should be:

1 of /24 Vnets for each subscriptions => 2 Vnets

2 of /25 subnets for each subscriptions => 4 subnets

Answer: 2 Vnets with 4 subnets for 2 subscriptions

upvoted 6 times

manhattan 1 year, 11 months ago

Selected Answer: A

Modified the HTML to add a comment..... Virtual networks and availability zones 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. https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview#virtual-networks-and-availability-zones so in my opinion answers are correct, 2 Virtual network and 2 subnets. 1 Vnet and 2 /25 subnets per subscription, you have (128-5) +(128-5) IPS in each sub to accommodate the 150VMs

upvoted 3 times

manhattan 1 year, 11 months ago

Modified the HTML to add a comment..... Virtual networks and availability zones 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. https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview#virtual-networks-and-availability-zones so in my opinion answers are correct, 2 Virtual network and 2 subnets. 1 Vnet and 2 /25 subnets per subscription, you have (128-5) +(128-5) IPS in each sub to accommodate the 150VMsSon 2 Suscripciones de Azure, entonces es 1 vnet y 2 subnet por cada suscripcion, entonces la respuesta es 2 vnet y 4 subnetsyes exactly, as wrote above 1 Vnet and 2 /25 subnets per subscription Total 2 Vnets Total 4 subnets

upvoted 3 times

Gambito11 1 year, 10 months ago

Son 2 Suscripciones de Azure, entonces es 1 vnet y 2 subnet por cada suscripcion, entonces la respuesta es 2 vnet y 4 subnetsyes exactly, as wrote above 1 Vnet and 2 /25 subnets per subscription Total 2 Vnets Total 4 subnets

upvoted 3 times

Gambito11 1 year, 10 months ago

Son 2 Suscripciones de Azure, entonces es 1 vnet y 2 subnet por cada suscripcion, entonces la respuesta es 2 vnet y 4 subnets

upvoted 3 times