SC-100$^{Q\&As}$

Microsoft Cybersecurity Architect

Pass Microsoft SC-100 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/sc-100.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

Your company has an on-premises network and an Azure subscription.

The company does NOT have a Site-to-Site VPN or an ExpressRoute connection to Azure.

You are designing the security standards for Azure App Service web apps. The web apps will access Microsoft SQL Server databases on the network.

You need to recommend security standards that will allow the web apps to access the databases. The solution must minimize the number of open internet-accessible endpoints to the on-premises network.

What should you include in the recommendation?

A. a private endpoint

B. hybrid connections

C. virtual network NAT gateway integration

D. virtual network integration

Correct Answer: B

Hybrid Connections can connect Azure App Service Web Apps to on-premises resources that use a static TCP port. Supported resources include Microsoft SQL Server, MySQL, HTTP Web APIs, Mobile Services, and most custom Web

Services.

Note: You can use an Azure App Service Hybrid Connections. To do this, you need to add and create Hybrid Connections in your app. You will download and install an agent (the Hybrid Connection Manager) in the database server or another

server which is in the same network as the on-premise database.

You configure a logical connection on your app service or web app.

A small agent, the Hybrid Connection Manager, is downloaded and installed on a Windows Server (2012 or later) running in the remote network (on-premises or anywhere) that you need to communicate with.

You log into your Azure subscription in the Hybrid Connection manager and select the logical connection in your app service.

The Hybrid Connection Manager will initiate a secure tunnel out (TCP 80/443) to your app service in Azure.

Your app service can now communicate with TCP-based services, on Windows or Linux, in the remote network via the Hybrid Connection Manager.

You could get more details on how to Connect Azure Web Apps To On-Premises.

Incorrect:

Not A: 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.

However, we need an inbound connection.

Not C: You can Azure web app service VNet integration with Azure VPN gateway to securely access the resource in an Azure VNet or on-premise network.

Note: 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. The virtual network integration feature behaves differently when it\\'s used

with virtual networks in the same region and with virtual networks in other regions. The virtual network integration feature has two variations:

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.

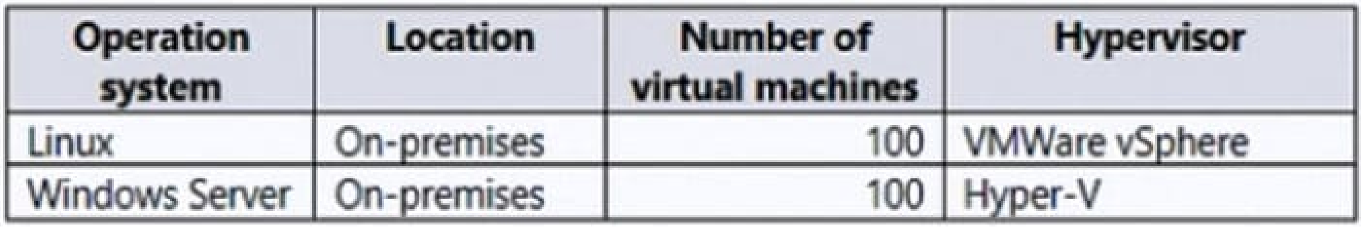
Gateway-required virtual network integration: When you connect directly to virtual networks in other regions or to a classic virtual network in the same region, you need an Azure Virtual Network gateway created in the target virtual network.

Reference: https://github.com/uglide/azure-content/blob/master/articles/app-service-web/web-sites-hybrid-connection-connect-on-premises-sql-server.md

https://docs.microsoft.com/en-us/answers/questions/701793/connecting-to-azure-app-to-onprem-datbase.html

QUESTION 2

Your company has the virtual machine infrastructure shown in the following table.



Operation system	Location	Number of virtual machines	Hypervisor
Linux	On-premises	100	VMWare vSphere
Windows Server	On-premises	100	Hyper-V

The company plans to use Microsoft Azure Backup Server (MABS) to back up the virtual machines to Azure.

You need to provide recommendations to increase the resiliency of the backup strategy to mitigate attacks such as ransomware.

What should you include in the recommendation?

A. Use geo-redundant storage (GRS).

B. Maintain multiple copies of the virtual machines.

C. Encrypt the backups by using customer-managed keys (CMKS).

D. Require PINs to disable backups.

Correct Answer: D

Azure Backup

Checks have been added to make sure only valid users can perform various operations. These include adding an extra layer of authentication. As part of adding an extra layer of authentication for critical operations, you\\'re prompted to enter a

security PIN before modifying online backups.

Authentication to perform critical operations

As part of adding an extra layer of authentication for critical operations, you\\'re prompted to enter a security PIN when you perform Stop Protection with Delete data and Change Passphrase operations.

Reference: https://docs.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware

https://docs.microsoft.com/en-us/azure/backup/backup-azure-security-feature#prevent-attacks

QUESTION 3

You have an Azure AD tenant that syncs with an Active Directory Domain Services (AD DS) domain.

You are designing an Azure DevOps solution to deploy applications to an Azure subscription by using continuous integration and continuous deployment (CI/CD) pipelines.

You need to recommend which types of identities to use for the deployment credentials of the service connection. The solution must follow DevSecOps best practices from the Microsoft Cloud Adoption Framework for Azure.

What should you recommend?

A. a managed identity in Azure

B. an Azure AD user account that has role assignments in Azure AD Privileged Identity Management (PIM)

C. a group managed service account (gMSA)

D. an Azure AD user account that has a password stored in Azure Key Vault

Correct Answer: D

QUESTION 4

Your company plans to provision blob storage by using an Azure Storage account. The blob storage will be accessible from 20 application servers on the internet.

You need to recommend a solution to ensure that only the application servers can access the storage account.

What should you recommend using to secure the blob storage?

A. managed rule sets in Azure Web Application Firewall (WAF) policies

B. inbound rules in network security groups (NSGs)

C. firewall rules for the storage account

D. inbound rules in Azure Firewall

E. service tags in network security groups (NSGs)

Correct Answer: C

Configure Azure Storage firewalls and virtual networks.

To secure your storage account, you should first configure a rule to deny access to traffic from all networks (including internet traffic) on the public endpoint, by default. Then, you should configure rules that grant access to traffic from specific

VNets. You can also configure rules to grant access to traffic from selected public internet IP address ranges, enabling connections from specific internet or on-premises clients. This configuration enables you to build a secure network

boundary for your applications.

Storage firewall rules apply to the public endpoint of a storage account. You don\\'t need any firewall access rules to allow traffic for private endpoints of a storage account. The process of approving the creation of a private endpoint grants

implicit access to traffic from the subnet that hosts the private endpoint.

Incorrect:

Not B: You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound

network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

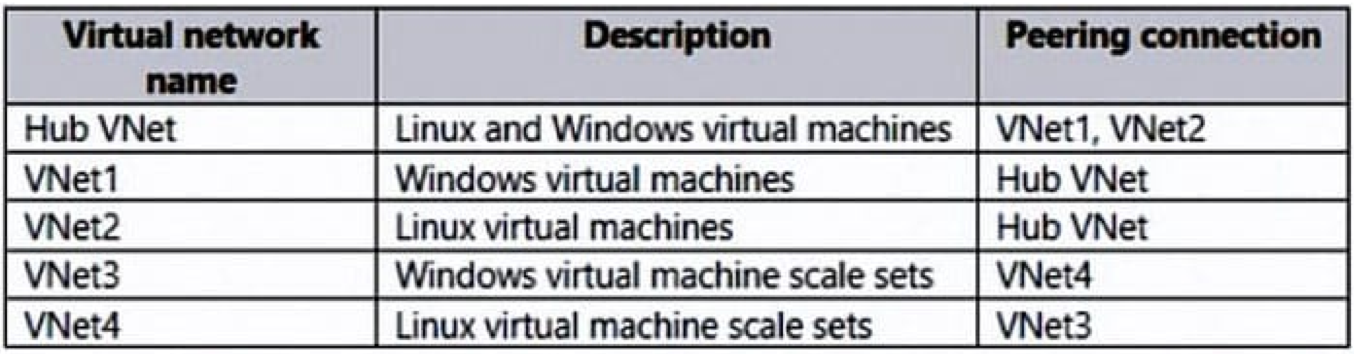
Not E: A service tag represents a group of IP address prefixes from a given Azure service. Microsoft manages the address prefixes encompassed by the service tag and automatically updates the service tag as addresses change, minimizing

the complexity of frequent updates to network security rules.

Reference: https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security

QUESTION 5

Your company plans to move all on-premises virtual machines to Azure. A network engineer proposes the Azure virtual network design shown in the following table.



Virtual network name	Description	Peering connection
Hub VNet	Linux and Windows virtual machines	VNet1, VNet2
VNet1	Windows virtual machines	Hub VNet
VNet2	Linux virtual machines	Hub VNet
VNet3	Windows virtual machine scale sets	VNet4
VNet4	Linux virtual machine scale sets	VNet3

You need to recommend an Azure Bastion deployment to provide secure remote access to all the virtual machines. Based on the virtual network design, how many Azure Bastion subnets are required?

A. 1

B. 2

C. 3

D. 4

E. 5

Correct Answer: B

https://docs.microsoft.com/en-us/azure/bastion/vnet-peering https://docs.microsoft.com/en-us/learn/modules/connect-vm-with-azure-bastion/2-what-is-azure-bastion