Answer Sheet

Q1) User1 is member of Group1

User2 is member of Group1 and Group2

An AAD Identity Protection user risk policy is configured to include Group1 and exclude Group2.

Is the policy applied to User2?

- [x] Yes

Explanation:-Yes - overlapping group membership defaults to applying the policy.

- [ ] No
- [ ] I don't know
- [ ] Maybe

Q2) What format is an OpenID Connect token?

- [x] JWT

Explanation:-JSON Web Token (JWT)

- [ ] SAML
- [ ] XML
- [ ] Java

Q3)

In Azure SQL Database AlwaysEncrypted, two types of column encryption is supported.

Match the requirement with the appropriate column encryption type.

Plaintext data values always produce the same cyphertext:

- [x] Deterministic
- [ ] Randomized

Q4)

In Azure SQL Database AlwaysEncrypted, two types of column encryption is supported.

Match the requirement with the appropriate column encryption type.

SQL Server can use the encrypted columns in joins and lookups:

- [x] Deterministic
- [ ] Randomized

Q5)

In Azure SQL Database AlwaysEncrypted, two types of column encryption is supported.

Match the requirement with the appropriate column encryption type.

Highest level of security:

- [ ] Deterministic
- [x] Randomized

Q6)

In Azure SQL Database AlwaysEncrypted, two types of column encryption is supported.

Match the requirement with the appropriate column encryption type.

Not suitable for columns containing boolean data:

- [x] Deterministic
- [ ] Randomized

Q7)

You create a new Azure Key Vault and want to ensure that malicious permanent deletions of key vault items can be recovered for 90 days.

What at a minimum would you have to enable on the Key Vault?

- [ ] Purge protection only
- [ ] Soft-delete and purge protection
- [x] Soft-delete only

Explanation:-Soft-delete will allow recovery of accidentally deleted key vault items (or the key vault itself) for 90 days. However a malicious user might purge soft-deleted items which will prevent their recovery despite soft-delete being enabled. To prevent purging of soft-deleted items you

should enable purge protection which in turn requires soft-delete to be enabled. The best answer is Soft-delete and purge protection.
https://docs.microsoft.com/en-za/azure/key-vault/key-vault-ovw-soft-delete

- Delete lock only
- Read-only lock only

Q8) You have a hybrid configuration of Azure Active Directory (Azure AD). You have an Azure HDInsight cluster on a virtual network. You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials. You need to configure the environment to support the planned authentication. Solution: You create a site-to-site VPN between the virtual network and the on-premises network. Does this meet the goal?

- Incorrect
- ✅ Correct

Explanation:-You can connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.
Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:
• Create Azure Virtual Network.
• Create a custom DNS server in the Azure Virtual Network.
• Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.
• Configure forwarding between the custom DN

Q9) As part of an Azure SQL Database AlwaysEncrypted configuration, where are the encryption keys stored?

- ✅ Column Master Key: AKV

Explanation:-https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine?view=sql-server-2017#how-it-works

- Column Master Key: SQL
- Column Master Key: Client
- Column Encryption Key: AKV
- ✅ Column Encryption Key: SQL

Explanation:-https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine?view=sql-server-2017#how-it-works

- Column Encryption Key: Client

Q10) You have an Azure HDInsights cluster on a Azure VNet. You need to secure communication between the cluster and your on-premises network, establish name resolution and use on-premises AD credentials to administer the cluster. You have to minimise costs. What do you deploy?

- Deploy an on-premises data gateway
- Deploy AD Connect
- ✅ Deploy a site-to-site VPN

Explanation:-Deploy an on-premises data gateway - no.
Deploy AD Connect - no, local AD credentials used with HDInsight does not need synchronisation with AAD.
Deploy a site-to-site VPN - yes, you need to establish network connectivity.
Deploy a custom DNS server on the Vnet - yes, you need to establish name resolution for the solution. On-premises DNS integration requires you to set up a custom DNS server for the VNet.
Deploy network security groups on the Vnet - yes, you need to secure the communication between the Vnet and the OPE network.
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

- ✅ Deploy a custom DNS server on the Vnet

Explanation:-Deploy an on-premises data gateway - no.
Deploy AD Connect - no, local AD credentials used with HDInsight does not need synchronisation with AAD.
Deploy a site-to-site VPN - yes, you need to establish network connectivity.
Deploy a custom DNS server on the Vnet - yes, you need to establish name resolution for the solution. On-premises DNS integration requires you to set up a custom DNS server for the VNet.
Deploy network security groups on the Vnet - yes, you need to secure the communication between the Vnet and the OPE network.
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

- ✅ Deploy network security groups on the Vnet

Explanation:-Deploy an on-premises data gateway - no.
Deploy AD Connect - no, local AD credentials used with HDInsight does not need synchronisation with AAD.
Deploy a site-to-site VPN - yes, you need to establish network connectivity.
Deploy a custom DNS server on the Vnet - yes, you need to establish name resolution for the solution. On-premises DNS integration requires you to set up a custom DNS server for the VNet.
Deploy network security groups on the Vnet - yes, you need to secure the communication between the Vnet and the OPE network.
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

---

Q11) Check out the exhibit.
You have an Azure SQL database that you want to secure access to the database from your web application using a Managed Service Identity (MSI). You create an app registration for your application in AAD and now need to give permission to the app on the Azure SQL Database server. Which option do you choose?

- ✅ Active Directory admin

Explanation:-You will first assign an AAD user access as the SQL Server administrator. You also have to put the registered app in an AAD group and assign that group permissions in the SQL database (using SQL commands). Lastly you have to modify your app to use modern authentication when connecting to the DB.
https://docs.microsoft.com/en-us/azure/app-service/app-service-web-tutorial-connect-msi

- SQL databases
- Properties
- Locks
- Advanced Data Security

Q12) Which of the following options would you deploy and configure if you wanted to protect a Azure SQL Database against the OWASP-defined threat of SQL Injection?

- Azure Application Gateway with Web Application Firewall
- ✓ Azure SQL Server Advanced Threat Protection

Explanation:-Azure SQL Server Advanced Threat Protection protects agains SQL injection. If you wanted to secure a web app against SQL injection you would deploy Azure Application Gateway with Web Application Firewall.

- Azure Firewall
- Network Security Group
- Application Security Group
- Azure Security Center Standard

Q13) You are configuring BYOK for a storage account you manage. Which of the following are not prerequisites for the deployment.

- Azure Key Vault deployed in the same region
- ✓ Azure Key Vault deployed in the same resource group

Explanation:-AKV and storage account must be in the same region for BYOK, but need not be in the same RG or sub. AKV volume encryption access policy is for Azure Disk Encryption (BitLocker) and not used as part of BYOK storage.

- ✓ Azure Key Valut deployed in the same subscription

Explanation:-AKV and storage account must be in the same region for BYOK, but need not be in the same RG or sub. AKV volume encryption access policy is for Azure Disk Encryption (BitLocker) and not used as part of BYOK storage.

- ✓ Azure Key Vault access policy enabled for volume encryption

Explanation:-AKV and storage account must be in the same region for BYOK, but need not be in the same RG or sub. AKV volume encryption access policy is for Azure Disk Encryption (BitLocker) and not used as part of BYOK storage.

Q14) Correct/Incorrect: Azure SQL Database encrypts sensitive data using the column encryption key (CEK) in a AlwaysEncrypted deployment.

- correct
- ✓ incorrect

Explanation:-The Always Encrypted enabled client driver running on the client is responsible for encryption and decryption of data before it is sent to the database.
https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine?view=sql-server-2017#how-it-works

---

Q15) You are securing your web application by removing connection strings to Azure SQL Database from the web.config configuration file. What two options do you have in Azure to accomplish your goal?

- ✓ Azure Key Vault secret

Explanation:-https://docs.microsoft.com/en-us/azure/app-service/app-service-web-tutorial-connect-msi

- ✓ Azure Active Directory Managed Service Identity (MSI)

Explanation:-https://docs.microsoft.com/en-us/azure/app-service/app-service-web-tutorial-connect-msi

- Azure Active Directory Application Registration
- Azure SQL Database server Active Directory admin
- Azure SQL Database AlwaysEncrypted
- Azure SQL Database Transparent Data Encryption (TDE)

Q16) You're configuring AIP and want to help your users find more information about the information protection policies and classifications. What would you use to provide this information to users?

- Custom tooltip
- ✓ Custom URL

Explanation:-Custom URL for "tell me more"

- Custom label
- Custom policy

Q17) What are the three types of keys in AIP?

- ✓ Tenant Key

Explanation:-Tenant key: used as the root key to secure all other keys.
Content key: used to secure information.
User key: Used by the user to get access (and varying permissions) to content.

- Document Key
- Classification Key
- Label Key
- ✓ Content Key

Explanation:-Tenant key: used as the root key to secure all other keys.
Content key: used to secure information.
User key: Used by the user to get access (and varying permissions) to content.

- ✓ User Key

Explanation:-Tenant key: used as the root key to secure all other keys.
Content key: used to secure information.
User key: Used by the user to get access (and varying permissions) to content.

Q18) Check out the exhibit.
You have configured an AKV and have created a secret containing a SQL connection string for use by an application. You have

registered your application with AAD and need to give the application permissions to use the configured secret. Which option should you choose to accomplish your goal?

- Access control (IAM)
- Keys
- Secrets
- Certificates
- ✓ Access policies
- Firewalls and virtual networks

Q19) In Azure Information Protection, how many levels of sublabels are supported?

- ✓ 1

Explanation:-One sublevel under the main level.

- 2
- 3
- 4
- Unlimited

Q20) You have a hybrid Azure AD deployment and have just deployed an Azure SQL Database. You want selected users to use Azure AD credentials to access your Azure SQL Database. What steps do you perform to accomplish your goal?

- ✓ Create a Azure AD user account that will serve as the SQL server administrator and assign user privileges

Explanation:-https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure

- ✓ Provision the user account on the Active Directory Admin blade on SQL server

Explanation:-https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure

- ✓ Configure the client computers with ADALSQL.DLL

Explanation:-https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure

- Create a group (SQL Group) in Azure AD that contains the SQL server administrator account
- ✓ Create a group (SQL Group) in Azure AD that contains the users that will need to access SQL

Explanation:-https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure

- ✓ Connect to SQL using Azure Active Directory - Universal with MFA authentication

Explanation:-https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure

---

Q21) View the exhibit.
You have a regulatory requirement to manage your own encryption keys for data at rest for all SQL databases. What option do you select to enable the BYOK scenario?

- Active Directory admin
- SQL databases
- Locks
- Advanced Data Security
- ✓ Transparent data encryption

Q22) When creating a custom Azure Information Protection label condition, what format is used to configure the condition?

- XML
- JSON
- OAuth
- ✓ REGEX
- FIND

Q23) See the exhibit.
You have a corporate compliance requirement that mandates bring your own key for all SQL databases for data at rest encryption. Which area would you use to configure this?

- Properties
- Locks
- Advanced Data Security
- ✓ Transparent data encryption

Explanation:-Transparent data encryption allows for the configuration of BYOK scenarios through integration with Azure Key Vault. BYOK is enabled in TDE configuration of Azure SQL Server.

Q24) You have a preconfigured Key Vault which is configured for volume encryption. What is the next step to perform to apply ADE to a VM?

- Enable the key vault for virtual machines deployment
- Enable the key vault for volume encryption
- Use the New-AzKeyvault PowerShell commandlet
- Use the Get-AzKeyvault PowerShell commandlet
- ✓ Use the Set-AzVMDiskEncryptionExtension PowerShell commandlet

Explanation:-Use the Set-AzVMDiskEncryptionExtension PowerShell commandlet.
https://docs.microsoft.com/en-us/azure/security/azure-disk-encryption-windows-powershell-quickstart

---

Q25) Which of the following VM series is not supported for Azure Disk Encryption?

✅ B-Series - burstable

Explanation:-B-Series - burstable and smaller is not supported for ADE.
https://docs.microsoft.com/en-za/azure/security/azure-security-disk-encryption-prerequisites#supported-vm-sizes
https://azure.microsoft.com/en-gb/pricing/details/virtual-machines/series/

- D-Series - general purpose
- F-Series - compute optimised
- M-Series - memory optimised
- N-Series - GPU optimised

Q26) What are the three advanced data security capabilities of Azure SQL Database?

- Firewall
- ✅ Vulnerability assessment

Explanation:-https://docs.microsoft.com/en-za/azure/sql-database/sql-database-advanced-data-security#overview

- ✅ Data classification

Explanation:-https://docs.microsoft.com/en-za/azure/sql-database/sql-database-advanced-data-security#overview

- Anti-malware
- ✅ Advanced threat protection

Explanation:-https://docs.microsoft.com/en-za/azure/sql-database/sql-database-advanced-data-security#overview

- Identity and Access Management

Q27) Which of the following core features are available when you deploy Microsoft anti-malware for Azure applications?

- Real-time protection
- Malware remediation
- Exclusions
- Anti-malware engine and platform updates
- ✅ All of these

Explanation:-All of these are correct. When deploying Microsoft antimalware for Azure applications, some of the features are: real-time protection, malware remediation, exclusion of files, processes and drives, and automatic updates to the antimalware engine and platform.
https://docs.microsoft.com/en-us/azure/security/azure-security-antimalware

---

Q28) When making use of resource locks, which of the following locking modes are valid? Select all that apply.

- Write only
- ✅ Do not delete

Explanation:-When creating a resource lock, you have the following options: Read only which means all resources can be viewed, however no changes are allowed. Do no delete is correct as you can modify resources however you are not allowed to remove/delete resources within that resource lock. Write-only is incorrect, there is no such option. https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking

- ✅ Read only

Explanation:-When creating a resource lock, you have the following options: Read only which means all resources can be viewed, however no changes are allowed. Do no delete is correct as you can modify resources however you are not allowed to remove/delete resources within that resource lock. https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking

---

Q29)

You need to provide RBAC access to a third party to manage a "LOB-VM".

The third party should be able to restart the VM, however not be able to shut down the VM.

When using Azure CLI, how should this be defined? Select all that apply.

- ✅ NotAction:Microsoft.compute/virtualmachines/shutdown/action

Explanation:-You need to define the allowed action as restart. You need to define the action which is not allowed, in this case it is shutdown.
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-cli https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations

- NotActions:Microsoft.compute/virtualmachines/start/action
- Action: Microsoft.compute/virtualmachines/start/action
- ✅ Action: Microsoft.compute/virtualmachines/restart/action

Explanation:-You need to define the allowed action as restart. You need to define the action which is not allowed, in this case it is shutdown.
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-cli https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations

---

Q30)

You are setting up AAD Connect. You must enforce the principle of least privilege.

What roles do you need to accomplish your goal?

- ✅ Enterprise Administrator on AD

Explanation:-https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions

- ✅ Global Administrator on AAD

Explanation:-https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions

- User Administrator on AAD
- Domain Administrator on AD

Q31)

You have a hybrid configuration of Azure Active Directory (Azure AD).

You have an Azure HDInsight cluster on a virtual network.

You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.

You need to configure the environment to support the planned authentication.

Solution: You create a site-to-site VPN between the virtual network and the on-premises network.

Does this meet the goal?

✅ Correct

Explanation:-You can connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.

⚪ Incorrect

Q32)

Your network contains an Active Directory forest named contoso.com. The forest contains a single domain.

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

You plan to deploy Azure AD Connect and to integrate Active Directory and the Azure AD tenant.

You need to recommend an integration solution that meets the following requirements:

Ensures that password policies and user logon restrictions apply to user accounts that are synced to the tenant
Minimizes the number of servers required for the solution.

Which authentication method should you include in the recommendation?

✅ password hash synchronization with seamless single sign-on (SSO)

Explanation:-PW Hash sync doesn't guarantee policy enforcement in real-time.

✅ pass-through authentication with seamless single sign-on (SSO)

Explanation:-

Pass Through Authentication. The reason being:

1. Ensures that password policies and user logon restrictions apply to user accounts that are synced to the tenant

>> Pass-Through Authentication enforce on-premises user account states, password policies, and sign-in hours.

2. Minimizes the number of servers required for the solution.

>> Pass-through needs a lightweight agent to be installed one (or more) on-premises servers.

>> PW Hash also require installing Azure AD Connect on your existing DC.

⚪ federated identity with Active Directory Federation Services (AD FS)

Q33)

Your network contains an on-premises Active Directory domain named corp.contoso.com.

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

You sync all on-premises identities to Azure AD.

You need to prevent users who have a givenName attribute that starts with TEST from being synced to Azure AD. The solution must minimize administrative effort.

What should you use?

⚪ Web Service Configuration Tool

⚪ the Azure AD Connect wizard

✅ Synchronization Rules Editor

Explanation:-Use the Synchronization Rules Editor and write attribute-based filtering rule.

⚪ Active Directory Users and Computers

Q34)

You are configuring AAD Identity Protection. You want to force a user to do a password change if the determined risk level is high.

Which of the following do you configure?

⚪ Conditional access policy

✅ User risk policy

Explanation:-AAD Identity protection allows only two types of policy to be configured: user risk and sign-in risk. both policies allow configuring block or allow access actions for the selected risk level. For the allow access action, the user risk policy allows you to require a password reset whereas the log-in risk policy allows you to require MFA with allow access.

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-configure-risk-policies

⚪ Sign-in risk policy

⚪ MFA policy

⚪ Password policy

Q35)

You deploy an Azure Kubernetes Cluster and need to configure a reverse proxy TLS termination.

What component do you deploy?

- Container Network Interface (CNI) plug-in
- Azure load balancer
- Azure Application Gateway
- ✅ AKS Ingress Controller

Explanation:-AKS Ingress Controller - yes.
Container Network Interface (CNI) plug-in - no, this is to connect Docker containers to the host-VM's VNet.
Azure load balancer - No, AKS handles the deployment of load balancing on your behalf. Azure Load Balancer does not provide TLS termination.
Azure Application Gateway - No, AKS handles the deployment of reverse proxy via the ingress controller.
https://docs.microsoft.com/en-us/azure/aks/ingress-tls

- AKS AppArmor
- AKS Container Registry

Comprehension:

Contoso Airways has adopted Azure as their cloud platform. Contoso has 2 offices: a head office in America and a secondary office in Japan. In Azure they have the following:

"US Subscription" which has 2 resource groups

* East US resource group which contains

  - Virtual network 1

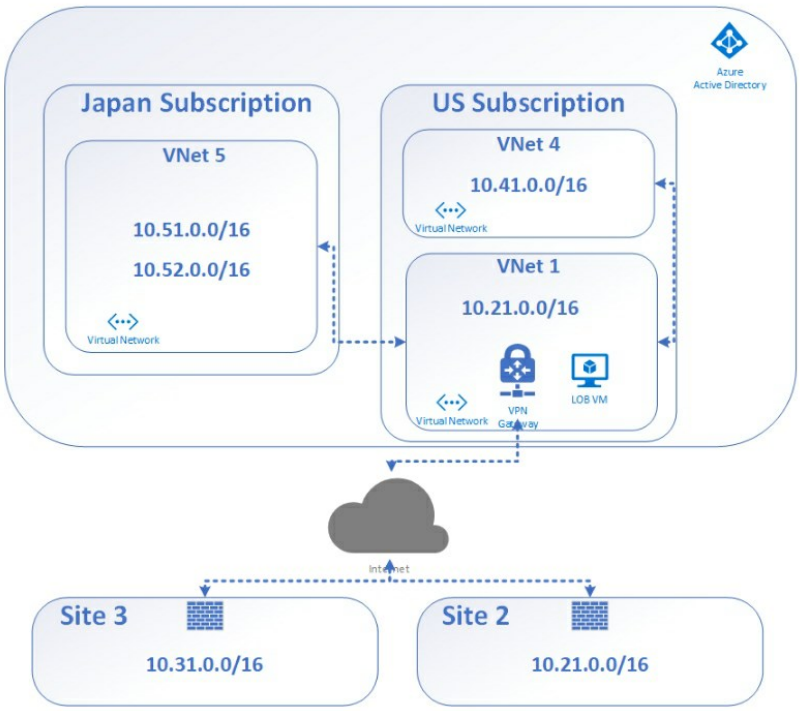
* West US resource group which contains

  - Virtual network 4

"Japan Subscription" which has 1 resource group

* Japan resource group which contains

  - Virtual network 5



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 once correct solution, while others might not have a correct solution.

Q36)

You need to connect resources from VNet1 to Site 2 and Site 3. The connectivity solution must be encrypted and cost-effective.

Which of the following should you configure?

- VNet peering
- Express route
- ✅ Site-to-Site VPN connection

Explanation:-Site-to-Site VPN is correct as this provides a connectivity solution between the required networks and uses IPsec encryption, this solution is also the most cost effective. Express route is incorrect as technically it can suffice as it is secure and can connect the required networks with each other, however the cost is considerably more than a VPN connection. VNet peering is incorrect as it can only be used to connect Azure virtual networks with each other and not on-premises to Azure networks. VNet-to-VNet connection is incorrect as this supports virtual networks in Azure and not on-premises workloads. https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal

- VNet-to-VNet connection

Comprehension:

Contoso Airways has adopted Azure as their cloud platform. Contoso has 2 offices: a head office in America and a secondary office in Japan. In Azure they have the following:

“US Subscription” which has 2 resource groups

* East US resource group which contains

- Virtual network 1

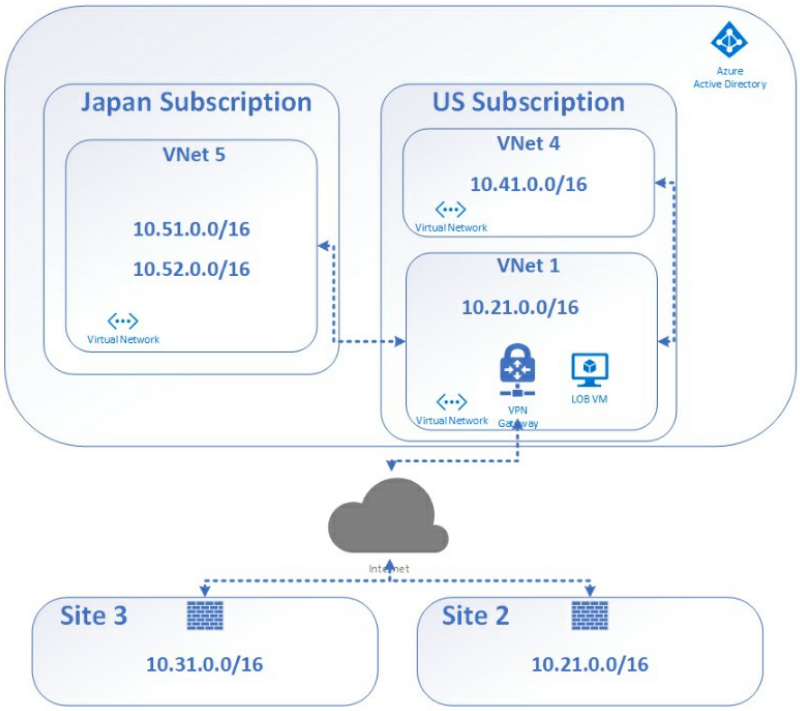
* West US resource group which contains

- Virtual network 4

“Japan Subscription” which has 1 resource group

* Japan resource group which contains

- Virtual network 5



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 once correct solution, while others might not have a correct solution.

Q37)

You need to connect resources from VNet1 to VNet 5. The connectivity solution must be encrypted and cost effective with the least amount of effort to configure and maintain.

Which of the following should you configure?

- Site-to-Site VPN connection
- Express route
- VNet peering
- ✅ VNet-to-VNet connection

Explanation:-VNet-to-VNet connection is correct as this provides a secure connectivity solution between the required networks, this connection also supports connectivity across different subscriptions and regions. Express route is incorrect as this is used to connect on-premises networks to Azure with low latency. VNet peering is incorrect as the traffic is not encrypted when traveling from one VNet to another VNet. Site-to-Site VPN is incorrect as this is method is used to connect on-premises networks to Azure networks, however both Site-to-Site and VNet-to-VNet connections makes use of a VPN gateway on each VNet. https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-faq

---

Comprehension:

Contoso Airways has adopted Azure as their cloud platform. Contoso has 2 offices: a head office in America and a secondary office in Japan. In Azure they have the following:

“US Subscription” which has 2 resource groups

* East US resource group which contains

- Virtual network 1

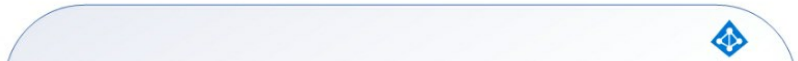
* West US resource group which contains

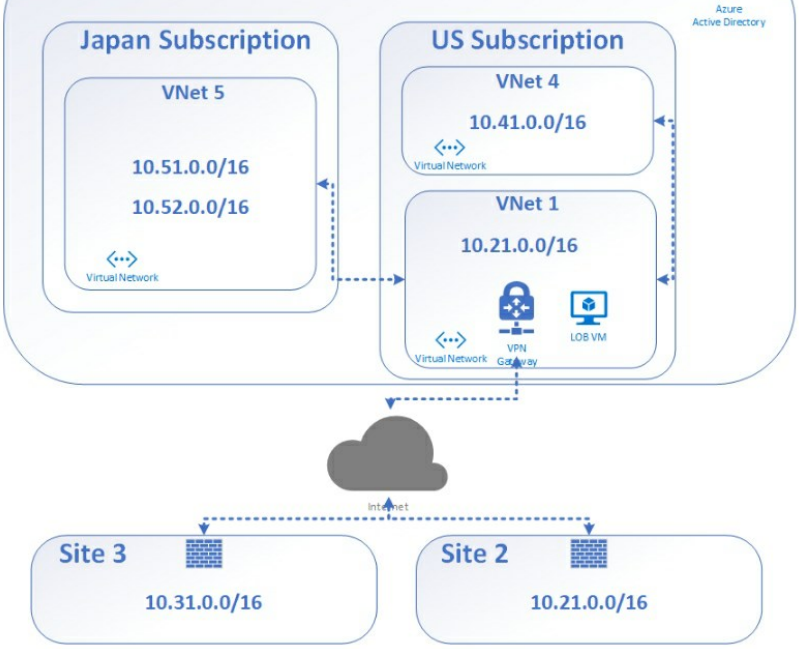
- Virtual network 4

“Japan Subscription” which has 1 resource group

* Japan resource group which contains

- Virtual network 5





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 once correct solution, while others might not have a correct solution.

Q38)

You need to connect resources from VNet1 to VNet 4. The connectivity solution must not route traffic over the public internet and the solution should be cost-effective with the least amount of effort to configure and maintain.

Which of the following should you configure?

- VNet-to-VNet connection
- ✅ VNet peering

Explanation:-VNet peering is correct as this is does not route traffic over the public internet, it routes traffic over the Microsoft backbone, however the data routed is not encrypted. Site-to-Site VPN is incorrect as this is method is used to connect on-premises networks to Azure networks and routes encrypted traffic over the public internet. Express route is incorrect as this is used to connect on-premises networks to Azure with low latency at a higher cost. VNet-to-VNet connection is incorrect as this routes encrypted traffic over the public internet and also is more expensive than VNet peering. https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview

- Express route
- Site-to-Site VPN connection

Comprehension:

Contoso Airways has adopted Azure as their cloud platform. Contoso has 2 offices: a head office in America and a secondary office in Japan. In Azure they have the following:

“US Subscription” which has 2 resource groups

* East US resource group which contains

  - Virtual network 1

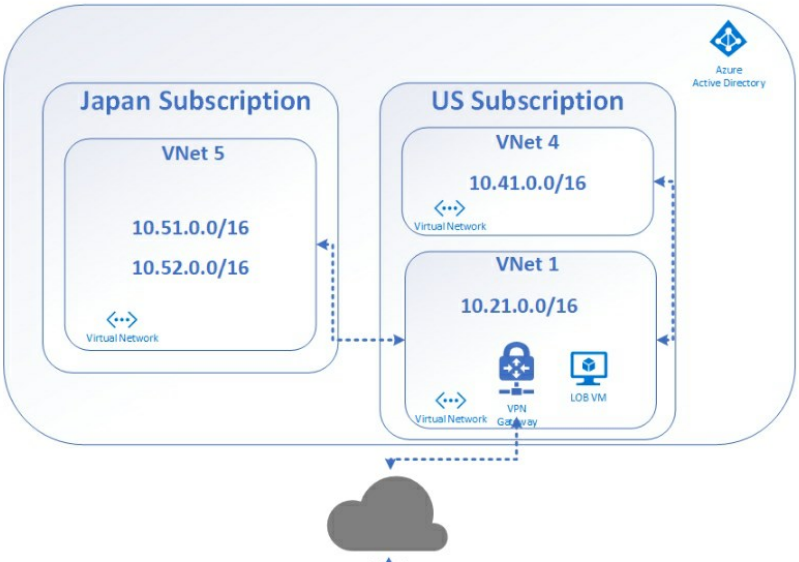
* West US resource group which contains

  - Virtual network 4

“Japan Subscription” which has 1 resource group

* Japan resource group which contains

  - Virtual network 5



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 once correct solution, while others might not have a correct solution.

Q39) You need to block the "LOB VM" from accessing the internet by using NSG rules, what is the easiest way to achieve this?

- Create inbound NSG rule with an ANY Destination and set the action to Deny
- ✅ Create outbound NSG rule with an Internet service tag and set the action to Deny

Explanation:-You need to create an OUTBOUND NSG rule with an “Internet” service tag as this will automatically block the VM from accessing the internet with the built-in service tag, the deny action is correct. https://docs.microsoft.com/en-us/azure/virtual-network/security-overview.

- Create inbound NSG rule with an Internet service tag and set the action to Deny
- Create outbound NSG rule with an ANY Destination and set the action to Deny