Answer Sheet

Q1) Which of the following statements is correct for Azure Policy initiatives?

- A policy initiative is a policy definition
- A policy initiative is a policy assignment
- A policy initiative is a policy assignment scope
- A policy initiative is a policy parameter
- ✅ A policy initiative is a collection of policies

Explanation:-One can assign a built-in policy within a specific scope. Similarly, one can also define a custom policy for assignment. Policies can be parameterised to make them more generic. Lastly, one can define Policy Initiatives that are collections of policies that can be parameterised and assigned at the same time. See: https://docs.microsoft.com/en-us/azure/governance/policy/overview#initiative-definition

---

Q2) Which of the following is not a technology that can be used to visualise Azure Monitor data?

- All of these
- Azure Monitor Workbooks
- Power BI
- Azure Monitor Views
- ✅ None of these

Explanation:-All of the answers provided are valid ways to visualise Azure Monitor data. The question, however, asked which of the options can not be used to visualise Azure Monitor data. None of the answer option are therefore correct. It is doubtful that the official exam will use such double-negative tactics, but it is used here as a reminder to be aware of negative answers to negative questions. See: https://docs.microsoft.com/en-us/azure/azure-monitor/visualizations

- Azure Dashboards

Q3) You have configured VNet peering between 2 VNets in your "Production" resource group. You implement an Azure firewall and create a user defined route (UDR) that forces all traffic through the firewall. Will traffic destined to route over the VNet peering link be forced to route through the firewall?

- Correct
- ✅ Incorrect

Explanation:-This option is correct, even if there is a UDR defined for all traffic to route through the Azure firewall, traffic going over the VNet peering link will not go through the UDR (Azure firewall) and instead go directly over the peered link. https://docs.microsoft.com/en-us/azure/firewall/tutorial-hybrid-ps

---

Q4) What is the minimum Azure Active Directory built-in RBAC role required to manage Azure Key Vault?

- Security Admin
- Owner
- Key Vault Reader
- Key Vault Administrator
- Reader
- ✅ Key Vault Contributor

Explanation:-Key Vault Contributor is the built-in RBAC role required to manage Azure Key Vault. See: https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

---

Q5) What PowerShell cmdlet is used to initiate Azure Disk Encryption for a Linux-based VM on Azure?

- Disable-AzVMDiskEncryption
- Set-AzVMDiskEncryption
- ✅ Set-AzVMDiskEncryptionExtension

Explanation:-Set-AzVMDiskEncryptionExtension is the correct answer. The same cmdlet is used for both Windows and Linux VMs See https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-linux

- Set-AzVMDiskEncryptionWindows
- Get-AzVmDiskEncryptionStatus
- Set-AzVMDiskEncryptionLinux

Q6) You are the administrator for the Contoso financial group. You are responsible for all storage accounts in Azure. You have been tasked to share limited access to the Blob files in storage account "Company_function" with another company for a limited time. The other company should only be able to list and read the data in the blob storage. The other company's administrator is familiar with Azure Storage Explorer and want you to share secure access with him by using this tool. Which information should you configure and give the administrator?

- ✅ Create Shared Access Signature for "Company_function" and configure the following: start and expiry time, read and list permissions, service access to Blobs. Send the administrator the SAS URI to be used in Storage Explorer

Explanation:-You need to create a Shared Access Signature for "Company_function" and configure start and expiry time as this is part of the time limitation request, list and read permissions are the least intrusive and blob storage is correct. The administrator should be able to use the SAS URI to configure access in Storage Explorer in their side. Option 1 is incorrect as there is write permissions assigned. Option 3 is incorrect as there is no time limitation set. Option 4 is incorrect as sending a storage name and key will not provide limited access as required. https://docs.microsoft.com/en-us/azure/storage/common/storage-dotnet-shared-access-signature-part-1

- None of these
- Create Shared Access Signature for "Company_function" and configure the following: read and list permissions, service access to Blobs. Send the administrator the SAS URI to be used in Storage Explorer
- Provide the administrator with the storage name and key

Q7) What is the default retention period for Azure Monitor logs?

- 1 year
- 60 days
- 3 years
- ✅ 90 days

Explanation:-Azure monitor retains logs for 90 days before starting to purge the oldest logs. You can set up log archival to a storage account if a longer retention is required. See: https://docs.microsoft.com/en-us/azure/azure-monitor/learn/tutorial-archive-data

- Indefinite
- 30 days

Q8) When securing Azure Key Vault one has to secure the management plane and the data plane. Which of these options is relevant when securing the management plane?

- ✅ Set key vault access policies

Explanation:-Key vault management plane security operations covers administering the key vault itself; whereas the data plane covers the data (keys and secrets) inside the key vault. One would use built-in RBAC roles as part of assigning access control to the vault. One can create a custom RBAC role as part of this, but that would be performed in AAD and is not considered part of vault security operations. See: https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault#resource-endpoints

- ✅ Create, read, update, delete key vaults

Explanation:-Key vault management plane security operations covers administering the key vault itself; whereas the data plane covers the data (keys and secrets) inside the key vault. One would use built-in RBAC roles as part of assigning access control to the vault. One can create a custom RBAC role as part of this, but that would be performed in AAD and is not considered part of vault security operations. See: https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault#resource-endpoints

- Create key vault keys
- Create RBAC roles
- Set key vault secrets
- ✅ Set key vault tags

Explanation:-Key vault management plane security operations covers administering the key vault itself; whereas the data plane covers the data (keys and secrets) inside the key vault. One would use built-in RBAC roles as part of assigning access control to the vault. One can create a custom RBAC role as part of this, but that would be performed in AAD and is not considered part of vault security operations. See: https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault#resource-endpoints

---

Q9) correct or incorrect: You can move an API Management service from one subscription to another.

- ✅ Correct

Explanation:-This option is correct, you can move the API management service from one subscription to another. https://docs.microsoft.com/en-us/azure/api-management/api-management-faq

- Incorrect

Q10) Which of the following should be chosen as the trigger when creating an Azure Security Center playbook?

- Triggers when a Windows Defender ATP alert occurs
- When an event is created
- When a data driven alert is triggered
- ✅ When a response to an Azure Security Center alert is triggered

Explanation:-All of the options are valid triggers for Azure logic apps - the underlying technology used for ASC playbooks. When creating a playbook to be used with ASC, one must select When a response to an Azure Security Center alert is triggered as the trigger, else the playbook will not appear on the alert when View playbooks is selected. See: https://docs.microsoft.com/en-us/azure/security-center/security-center-playbooks

- When an incident is created

Q11) When Azure Information Protection classifies a document, how can the classification label applied to the document? Choose 3.

- ✅ Header and/or footer

Explanation:-AIP can use a header, footer, watermark and clear-text metadata to label a document as carrying a certain classification. The data can further be protected by encryption as well as the allowable actions (copy, print, etc) can be restricted. The metadata label added to the document header information must be clear-text so that DLP solutions can identify documents belonging to a certain classification, even if the document content (along with any visible labels) is encrypted and invisible to non-integrated DLP scanners. Document fingerprinting is used in O365 DLP, but is not part of AIP labeling. Digital text steganography is an advanced technique of invisibly watermarking documents, but is not used by AIP. https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-markings

- ✅ Watermark

Explanation:-AIP can use a header, footer, watermark and clear-text metadata to label a document as carrying a certain classification. The data can further be protected by encryption as well as the allowable actions (copy, print, etc) can be restricted. The metadata label added to the document header information must be clear-text so that DLP solutions can identify documents belonging to a certain classification, even if the document content (along with any visible labels) is encrypted and invisible to non-integrated DLP scanners. Document fingerprinting is used in O365 DLP, but is not part of AIP labeling. Digital text steganography is an advanced technique of invisibly watermarking documents, but is not used by AIP. https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-markings

- Encrypted metadata
- ✅ Clear-text metadata

Explanation:-AIP can use a header, footer, watermark and clear-text metadata to label a document as carrying a certain classification. The data can further be protected by encryption as well as the allowable actions (copy, print, etc) can be restricted. The metadata label added to the document header information must be clear-text so that DLP solutions can identify documents belonging to a certain classification, even if the document content (along with any visible labels) is encrypted and invisible to non-integrated DLP scanners. Document fingerprinting is used in O365 DLP, but is not part of AIP labeling. Digital text steganography is an advanced technique of invisibly watermarking documents, but is not used by AIP. https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-markings

- Document fingerprint

- Digital text steganography

Q12) Which of the following describe logging of control-plane actions on your Azure subscription?

- Metrics
- Diagnostic Log
- ✅ Activity Log

Explanation:-Monitoring data from Azure comes in three basic forms: Activity log - Azure subscription control-plane log; Metrics - near real-time monitoring information emitted by resources; Diagnostic log - traditional log information emitted by resources. See: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-sources

- Subscription Log
- Tenant Log
- Audit Log

Q13) What is the minimum required RBAC role required to view Azure Monitor logs?

- Security Admin
- Monitoring Contributor
- Monitoring Administrator
- ✅ Monitoring Reader

Explanation:-All the roles listed are valid built-in Azure roles, except for Monitoring Administrator that doesn't exist. The minimum role required to view Azure Monitor logs is Monitoring Reader. See: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/roles-permissions-security

- Security Reader

Q14) To configure Azure Monitor log collection and analysis on an Azure VM several configuration steps are required as listed in the answer options. Identify the step that is not required.

- Create a Log Analytics Workspace
- Enable a Log Analytics VM Extension
- Select logs and metrics to collect
- ✅ Provide the VM local administrator username and password

Explanation:-All of the options are required to enable Azure Monitor log collection and analytics on an Azure VM except for providing a local administrator username and password. See: https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-azurevm

Q15) In what two ways should applications (not users) be granted access to storage account resources?

- ✅ Access Key

Explanation:-Access keys were traditionally used to provide access to storage account resources for applications. Azure AD can also provide access control for application service principals using OAuth. https://docs.microsoft.com/en-us/azure/storage/common/storage-auth?toc=%2fazure%2fstorage%2fblobs%2ftoc.json

- Shared Access Key
- ✅ OAuth

Explanation:-Access keys were traditionally used to provide access to storage account resources for applications. Azure AD can also provide access control for application service principals using OAuth. https://docs.microsoft.com/en-us/azure/storage/common/storage-auth?toc=%2fazure%2fstorage%2fblobs%2ftoc.json

- Service Key
- Shared Access Signature

Q16) It is considered best practice to add an additional layer of access control security to Azure SQL databases. Which Azure features provides this capability?

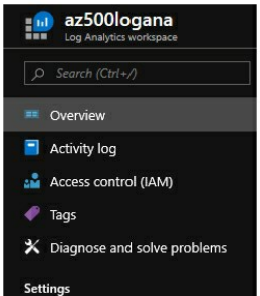
- Network Security Group
- Azure Firewall
- ✅ Azure SQL Database Firewall

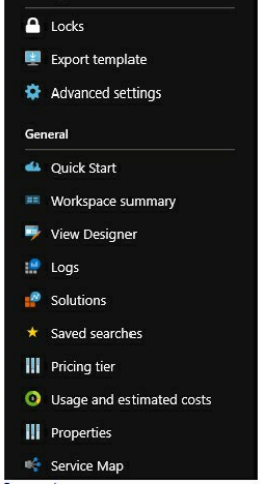
Explanation:-Azure SQL Database has a built-in firewall service commonly referred to as Azure SQL Database Firewall. A firewall rule is required for all sites and over-the-internet connections to the database. This is the best answer to the question. Network security groups, Azure Firewall and a 3rd party firewall appliance commonly referred to as a network security appliance can all also be configured as an additional layer of security - but this is not the best answer to the question. AAD conditional access and AIP is not directly involved in SQL database access control. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-security-overview

- Network Security Appliance
- Azure Active Directory Conditional Access
- Azure Information Protection

Q17)

Review the exhibit.





Which option would you choose to adjust the log data retention settings for this Azure Log Analytics Workspace?

- ✅ Usage and estimated costs

Explanation:-Usage and estimated costs, click Data Retention button.

- Pricing tier
- Logs
- Advanced Settings
- Properties

Q18) You are the administrator for the ACME banking group. You are responsible for managing the key vault in Azure. You need to create a new certificate in the ACMEvault with a key size of 2018 and that cannot be reused via an API call which should be called ACMEcertificate. Which statement below is correct?

- SET https://ACMEvault.vault.azure.net/certificates/ACMEcertificate/create?api-version=7.0
- ✅ POST https://ACMEvault.vault.azure.net/certificates/ACMEcertificate/create?api-version=7.0

Explanation:-POST {https://ACMEvault.vault.azure.net}/certificates/{ACMEcertificate}/create?api-version=7.0 is correct as this follows the correct way to create a new certificate. Here is the way the statement is used in general: POST {vaultBaseUrl}/certificates/{certificate-name}/create?api-version=7.0. It uses HTTPS by default, GET and SET are incorrect when creating a new certificate. https://docs.microsoft.com/en-us/rest/api/keyvault/createcertificate/createcertificate

- POST http://ACMEvault.vault.azure.net/certificates/ACMEcertificate/create?api-version=7.0
- GET https://ACMEvault.vault.azure.net/certificates/ACMEcertificate/create?api-version=7.0

Q19) Correct or Incorrect: Just-in-time VM access will automatically create the NSG rules, however you will need to manually remove the NSG rules afterwards.

- correct
- ✅ incorrect

Explanation:-This option is correct, JIT VM Access will automatically create the NSG rules to the user to connect securely to the VM and will also automatically remove the NSG rule it created after the configured time expired. https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time

---

Q20) You need to configure secure access to one of your production VMs. You are planning to enable secure remote access via Just-In-Time VM access. Which of the following settings can you configure? Select all that apply.

- ✅ Time range

Explanation:-Port number is correct as you can configure which ports are allowed to be requested to the VM. IP address and IP ranges are correct as you can either specify a specific IP or a range of IP's allowed to connect to the resource via JIT VM access. Time range is correct as you can specify how long a user can access the VM without having to request a new session via JIT VM access. Protocol type is correct as you need to specify TCP or UDP regarding the port ranges. Virtual network is incorrect as this option is not configurable via JIT VM access. https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time

- Virtual network
- ✅ Protocol type

Explanation:-Port number is correct as you can configure which ports are allowed to be requested to the VM. IP address and IP ranges are correct as you can either specify a specific IP or a range of IP's allowed to connect to the resource via JIT VM access. Time range is correct as you can specify how long a user can access the VM without having to request a new session via JIT VM access. Protocol type is correct as you need to specify TCP or UDP regarding the port ranges. Virtual network is incorrect as this option is not configurable via JIT VM access. https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time

- ✅ IP address

Explanation:-Port number is correct as you can configure which ports are allowed to be requested to the VM. IP address and IP ranges are correct as you can either specify a specific IP or a range of IP's allowed to connect to the resource via JIT VM access. Time range is correct as you can specify how long a user can access the VM without having to request a new session via JIT VM access. Protocol type is correct as you need to specify TCP or UDP regarding the port ranges. Virtual network is incorrect as this option is not configurable via JIT VM access. https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time

- ✅ IP range

Explanation:-Port number is correct as you can configure which ports are allowed to be requested to the VM. IP address and IP ranges are correct as you can either specify a specific IP or a range of IP's allowed to connect to the resource via JIT VM access. Time range is correct as you can specify how long a user can access the VM without having to request a new session via JIT VM access. Protocol type is correct as you need to specify TCP or UDP regarding the port ranges. Virtual network is incorrect as this option is not configurable via JIT VM access. https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time

✅ Port numbers

Explanation:-Port number is correct as you can configure which ports are allowed to be requested to the VM. IP address and IP ranges are correct as you can either specify a specific IP or a range of IP's allowed to connect to the resource via JIT VM access. Time range is correct as you can specify how long a user can access the VM without having to request a new session via JIT VM access. Protocol type is correct as you need to specify TCP or UDP regarding the port ranges. Virtual network is incorrect as this option is not configurable via JIT VM access. https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time

---

Q21) You are the administrator for the ACME banking group. You are responsible for managing the key vault in Azure called ACMEvault. You have decommissioned a production server which has its password stored in the key vault labelled "FinanceAdmin". You need to remove the password from the vault by using an API call. Which API call is correct?

- ⚪ PURGE https://ACMEvault.vault.azure.net/secrets/FinanceAdmin?api-version=7.0
- ✅ DELETE https://ACMEvault.vault.azure.net/secrets/FinanceAdmin?api-version=7.0

Explanation:-DELETE is the correct operation name as it references the correct vault and secret name. REMOVE not a valid operation name. PURGE is used to remove the password irreversibly, almost the same as emptying the recycle bin on your desktop. RECOVER will not suffice as this is used to recover a deleted secret on soft-delete enabled vaults. https://docs.microsoft.com/en-us/rest/api/keyvault/deletesecret/deletesecret

- ⚪ RECOVER https://ACMEvault.vault.azure.net/secrets/FinanceAdmin?api-version=7.0
- ⚪ REMOVE https://ACMEvault.vault.azure.net/secrets/FinanceAdmin?api-version=7.0

Q22) You are the administrator for the Contoso financial group. You are responsible for managing the key vault in Azure. You need to update a certificate that has become stale in the CONTOSOvault which is called "WebsiteCertificate" via an API call to the Key Vault. Which statement below is correct?

- ⚪ POST https://CONTOSOvault.vault.azure.net/certificates/WebsiteCertificate/3d31d7b36c942ad83ef36fc?api-version=7.0
- ⚪ PATCH http://CONTOSOvault.vault.azure.net/certificates/WebsiteCertificate/3d31d7b36c942ad83ef36fc?api-version=7.0
- ⚪ POST http://CONTOSOvault.vault.azure.net/certificates/WebsiteCertificate/3d31d7b36c942ad83ef36fc?api-version=7.0
- ✅ PATCH https://CONTOSOvault.vault.azure.net/certificates/WebsiteCertificate/3d31d7b36c942ad83ef36fc?api-version=7.0

Explanation:-PATCH is correct https://CONTOSOvault.vault.azure.net/certificates/WebsiteCertificate/3d31d7b36c942ad83ef36fc?api-version=7.0 is correct as this follows the correct way to update a specific certificate in the Azure Key Vault via API call. Here is the way the statement is used in general: PATCH {vaultBaseUrl}/certificates/{certificate-name}/{certificate-version}?api-version=7.0. using HTTP will not suffice as the Key Vaults use HTTPS by default and POST is not the correct action. https://docs.microsoft.com/en-us/rest/api/keyvault/updatecertificate/updatecertificate

---

Q23) You are configuring security for data in transit for an Azure App Service. Which of the following security tasks should be performed? Choose all that apply, do not choose any that does not apply.

- ⚪ Upload SSL Certificate
- ⚪ Bind SSL Certificate
- ⚪ HTTPS enforced
- ⚪ Minimum TLS version enforced
- ⚪ Test HTTPS
- ✅ All of these

Explanation:-All the answer options should be configured for Azure App Service. See: https://docs.microsoft.com/en-us/azure/app-service/app-service-web-tutorial-custom-ssl

---

Q24) Which of the following Azure tools can help mature the security baseline specific to detecting malicious activity? Select all that apply.

- ⚪ Azure Key Vault
- ✅ Azure Monitor

Explanation:-Azure Security Center is correct as this tool allows you to mature the policies and processes in your Azure environment. Azure monitor is correct as this tool can also be used in maturing polices and processes regarding security baselines in Azure. The Azure portal, Key vault, Azure AD and Azure policy cannot be used as a tool regarding a security baseline when detecting malicious activity in your Azure environment. https://docs.microsoft.com/bs-latn-ba/azure/architecture/cloud-adoption/governance/security-baseline/toolchain

- ⚪ Azure policy
- ✅ Azure Security Center

Explanation:-Azure Security Center is correct as this tool allows you to mature the policies and processes in your Azure environment. Azure monitor is correct as this tool can also be used in maturing polices and processes regarding security baselines in Azure. The Azure portal, Key vault, Azure AD and Azure policy cannot be used as a tool regarding a security baseline when detecting malicious activity in your Azure environment. https://docs.microsoft.com/bs-latn-ba/azure/architecture/cloud-adoption/governance/security-baseline/toolchain

- ⚪ Azure portal
- ⚪ Azure AD

Q25) You have been requested to configure VM security in the form of encrypting IaaS VM disks. You are planning to make use of PowerShell to encrypt the disks. Complete the following PowerShell command: Set-1 -ResourceGroupName "MySecureRG" -VMName "MySecureVM" -2 "VaultID" -3 "VaultURL"

- ⚪ 1 = DiskEncryptionKeyVaultUrl, 2 = DiskEncryptionKeyVaultId, 3 = AzVmDiskEncryptionExtension
- ✅ 1 = AzVmDiskEncryptionExtension, 2 = DiskEncryptionKeyVaultId, 3 = DiskEncryptionKeyVaultUrl

Explanation:-The correct command is as follows: Set-AzVmDiskEncryptionExtension -ResourceGroupName "MySecureRG" -VMName "MySecureVM" -DiskEncryptionKeyVaultId "VaultID" -DiskEncryptionKeyVaultUrl "VaultUrl". You need to use the AzVmDiskEncryption command first followed by the DiskEncryptionKeyVaultID and lastly the DiskEncryptionKeyVaultUrl command. https://docs.microsoft.com/en-us/azure/security/quick-encrypt-vm-powershell#bkmk_PrereqScript

- ⚪ 1 = AzVmDiskEncryptionExtension, 2 = DiskEncryptionKeyVaultUrl, 3 = DiskEncryptionKeyVaultId

---

Q26) When securing Azure Key Vault one has to secure the management plane and the data plane. Which of these options is relevant when securing the data plane?

- Set key vault tags
- Set key vault secrets

Explanation:-Key vault management plane security operations covers administering the key vault itself; whereas the data plane covers the data (keys and secrets) inside the key vault. One would use built-in RBAC roles as part of assigning access control to the vault. One can create a custom RBAC role as part of this, but that would be performed in AAD and is not considered part of vault security operations. See: https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault#resource-endpoints

- Create key vault keys

Explanation:-Key vault management plane security operations covers administering the key vault itself; whereas the data plane covers the data (keys and secrets) inside the key vault. One would use built-in RBAC roles as part of assigning access control to the vault. One can create a custom RBAC role as part of this, but that would be performed in AAD and is not considered part of vault security operations. See: https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault#resource-endpoints

- Create RBAC roles
- Create key vault
- Set key vault access policies

Q27) What are the three authentication mechanisms that an application can use when using Azure Key Vault for storing secrets, certificates and/or keys?

- Service principal with secret

Explanation:-The preferred method for applications to authenticate with an integrated Azure Key Vault is via Managed identities for Azure resources. Alternatively, applications can use service principal with secret or service principal with certificate. None of the other options exist - they are made-up. See: https://docs.microsoft.com/en-za/azure/key-vault/key-vault-whatis

- Container instance registry
- Azure app registry
- Managed identities for Azure resources

Explanation:-The preferred method for applications to authenticate with an integrated Azure Key Vault is via Managed identities for Azure resources. Alternatively, applications can use service principal with secret or service principal with certificate. None of the other options exist - they are made-up. See: https://docs.microsoft.com/en-za/azure/key-vault/key-vault-whatis

- Service principal with certificate

Explanation:-The preferred method for applications to authenticate with an integrated Azure Key Vault is via Managed identities for Azure resources. Alternatively, applications can use service principal with secret or service principal with certificate. None of the other options exist - they are made-up. See: https://docs.microsoft.com/en-za/azure/key-vault/key-vault-whatis

- Service principal with encrypted credential

Q28) You need to configure additional Network Security Group rules to allow the following types of traffic: • Remote Desktop Protocol • SSH • Secure web traffic Which three ports should you configure as part of the NSG rules?

- Port 80
- Port 23
- Port 22

Explanation:-Port 22 is correct as this is used for SSH, Port 443 is correct as this is used for secure web traffic (HTTPS), Port 3389 is correct as this is used for RDP. Port 23 is incorrect as this is used for Telnet. Port 80 is incorrect as this is used for insecure web traffic. Port 389 is incorrect as this is used with Lightweight Directory Access Protocol (LDAP). https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

- Port 3389

Explanation:-Port 22 is correct as this is used for SSH, Port 443 is correct as this is used for secure web traffic (HTTPS), Port 3389 is correct as this is used for RDP. Port 23 is incorrect as this is used for Telnet. Port 80 is incorrect as this is used for insecure web traffic. Port 389 is incorrect as this is used with Lightweight Directory Access Protocol (LDAP). https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

- Port 389
- Port 443

Explanation:-Port 22 is correct as this is used for SSH, Port 443 is correct as this is used for secure web traffic (HTTPS), Port 3389 is correct as this is used for RDP. Port 23 is incorrect as this is used for Telnet. Port 80 is incorrect as this is used for insecure web traffic. Port 389 is incorrect as this is used with Lightweight Directory Access Protocol (LDAP). https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

---

Q29) Select the most accurate description of the Always Encrypted feature of Azure SQL Database.

- Column-level encryption

Explanation:-Always Encrypted is applied on the data in the database at a column level. Unlike Transparent Data Encryption used by Azure SQL Database where the encryption/decryption key is known to the database management engine, Always Encrypted performs encryption/decryption on the endpoint application, out of band of the database engine. https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine?view=sql-server-2017

- User-level encryption
- Network-level encryption
- Table-level encryption
- Database-level encryption
- Row-level encryption

Q30) Correct or Incorrect: you can configure multiple domains to sync with ADConnect.

- incorrect
- correct

Explanation:-This option is correct, you can configure multiple domains to sync with Azure AD via AD Connect. https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-multiple-domains

---

Q31) You are the administrator for the Contoso financial group. You are responsible for managing the key vault in Azure. You need to recover a certificate that has been deleted in the CONTOSOvault which is called “FinanceAdmin” via an API call to the Key Vault. Which statement below is correct?

- GET https://CONTOSOvault.vault.azure.net/deletedsecrets/FinanceAdmin/recover?api-version=7.0
- GET http://CONTOSOvault.vault.azure.net/deletedsecrets/FinanceAdmin/recover?api-version=7.0
- ✅ POST https://CONTOSOvault.vault.azure.net/deletedsecrets/FinanceAdmin/recover?api-version=7.0

Explanation:-POST https://CONTOSOvault.vault.azure.net/deletedsecrets/FinanceAdmin/recover?api-version=7.0 is correct as this follows the correct way to recover a deleted certificate in the Azure Key Vault via API call. Here is the way the statement is used in general: POST {vaultBaseUrl}/deletedsecrets/{secret-name}/recover?api-version=7.0. It uses HTTPS by default, GET is incorrect when recovering a deleted certificate. https://docs.microsoft.com/en-us/rest/api/keyvault/restorecertificate/restorecertificate

- POST http://CONTOSOvault.vault.azure.net/deletedsecrets/FinanceAdmin/recover?api-version=7.0

Q32) Which of the following is not a configuration step required to create an Azure Monitor Alert?

- Define alert details
- Define alert condition
- Define action group
- ✅ Define notification action

Explanation:-Creating an Azure Monitor Alert required defining alert conditions, alert details and the action group. Although specifying the alert action is part of defining the action group, there is no define notification action step. See: https://docs.microsoft.com/en-us/azure/azure-monitor/learn/tutorial-response

---

Q33) Which of the following are valid access control options for Azure Data Lake? Choose 3

- ✅ Role Based Access Control

Explanation:-Access keys, Azure AD RBAC and Shared Access Signatures are all valid access control methods for storage accounts - the underlying technology for Data Lake. Service key and shared access key are not valid names for storage account access controls. https://docs.microsoft.com/en-za/azure/storage/blobs/data-lake-storage-access-control

- Shared Access Key
- Service Key
- ✅ Access Key

Explanation:-Access keys, Azure AD RBAC and Shared Access Signatures are all valid access control methods for storage accounts - the underlying technology for Data Lake. Service key and shared access key are not valid names for storage account access controls. https://docs.microsoft.com/en-za/azure/storage/blobs/data-lake-storage-access-control

- ✅ Shared Access Signature

Explanation:-Access keys, Azure AD RBAC and Shared Access Signatures are all valid access control methods for storage accounts - the underlying technology for Data Lake. Service key and shared access key are not valid names for storage account access controls. https://docs.microsoft.com/en-za/azure/storage/blobs/data-lake-storage-access-control

---

Q34) Which of the following Azure features provide the capability to define and enforce security settings when new Azure resources are created?

- Azure Resource Manager
- ✅ Azure Policy

Explanation:-Azure Policy can be used to enforce security settings when new Azure resources are created. Security policies is visible in Azure Security Center, but the capability is provided by Azure Policy. Azure Resource Manager is the service used to provision resources in Azure - it will respect assigned policies, but doesn't provide the ability to define security policies. RBAC can be used to prevent certain users from creating resources, but doesn't enforce what security settings that must be applied when RBAC allows the creation of resources. ATP detects and can be configured to respond to breaches in security, but doesn't allow the definition and enforcement of security settings to be applied when new resources are created. See: https://docs.microsoft.com/en-us/azure/security-center/tutorial-security-policy

- Azure Security Center
- Role-Based Access Control
- Azure Advanced Threat Protection

Q35) Azure Policy allows the assignment of a policy to a management group. What level of scope is provided by management groups?

- ✅ Subscription

Explanation:-An Azure management group provides a level of scope at the subscription level. One can assign a policy to a management group which is made up of a defined set of subscriptions. All subscriptions in the management group inherits the policy. A root management group is created that contains all other management groups. See: https://docs.microsoft.com/en-za/azure/governance/management-groups/index and https://docs.microsoft.com/en-us/azure/security-center/tutorial-security-policy#management-groups

- All of the options
- Tenant
- Resource group
- Resource

Q36) Which of the following Azure tools can help mature the security baseline specific to securing virtual networks? Select all that apply.

- ✅ Azure portal

Explanation:-Azure portal is correct as you can use the portal to mature network policies and processes. Azure policy is also correct as you can enforce policies that supports security baselines. Key Vault, Azure AD, Azure Security Center and Azure Monitor does not contribute to the security baseline for securing virtual networks. https://docs.microsoft.com/bs-latn-ba/azure/architecture/cloud-adoption/governance/security-baseline/toolchain

- Azure AD
- ✅ Azure policy

Explanation:-Azure portal is correct as you can use the portal to mature network policies and processes. Azure policy is also correct as you can enforce policies that supports security baselines. Key Vault, Azure AD, Azure Security Center and Azure Monitor does not contribute to the security baseline for securing virtual networks. https://docs.microsoft.com/bs-latn-ba/azure/architecture/cloud-adoption/governance/security-

baseline/toolchain

- Azure Key Vault
- Azure Monitor
- Azure Security Center

Q37) You have an existing AD Connect implementation. You have to prevent users from a certain department to be synchronised to AAD. What tool do you use?

- AAD Connect wizard on the AD Connect server
- ✅ Synchronization Rules Editor on the AD Connect server

Explanation:-Synchronization Rules Editor on the AD Connect server is used to change the users to be synced. https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration

- AAD Connect in the Azure portal
- AD Users and Computers on the local DC

Q38) Which two of the following are objects you can configure to apply AAD PIM to?

- Access Reviews
- ✅ AAD Roles

Explanation:-AAD Roles and Azure resources https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure#who-can-do-what-in-pim

- ADD Groups
- ✅ Azure Resources

Explanation:-AAD Roles and Azure resources https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure#who-can-do-what-in-pim

- AAD Dynamic Groups

Q39) 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:

- ✅ Deterministic
- Randomized

Q40) 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:

- ✅ Deterministic
- Randomized

Q41) 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
- ✅ Randomized

Q42) 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:

- ✅ Deterministic
- Randomized

Q43) You are deploying Azure Firewall as in the exhibit.
You want to ensure all traffic from Workload-SN going to www.google.com is routed through the Azure Firewall
What do you have to create in Workload-SN in to ensure that Test-FW01 will inspect outgoing traffic?

- NSG
- ✅ Route Table

Explanation:-https://docs.microsoft.com/en-gb/azure/firewall/tutorial-firewall-deploy-portal

- Firewall Rule

Q44) 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?

- Soft-delete only
- Purge protection only
- ✅ Soft-delete and purge protection

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

Q45) Review the exhibit.
Which option would you choose to adjust the log data retention settings for this Azure Log Analytics Workspace?

- Advanced Settings
- Logs
- Pricing tier
- ✅ Usage and estimated costs

Explanation:-Usage and estimated costs, click Data Retention button.

- Properties

Q46) Your organization is planning on synchronizing their on premises identities to Azure via the AD Connect tool. You need to ensure that all domain user identities are properly formatted before they are synchronized as to not cause synchronization errors. What should you do?

- ✅ Run the IdFix tool

Explanation:-IdFix tool is correct as this free tool is used to isolate and remediate common errors reported by the AD Connect tool like formatting issues with domain user names. Re-running the AD Connect application will not resolve any sync issues. Running the synchronization service manager is incorrect as this tool is used to configure more advanced aspects of AD Connect like connectors and synchronization schedule. Running the synchronization rules editor is incorrect as this can only be run post-deployment of directory synchronization, this tool is used to customize user and group attributes synched between on-prem and Azure. https://docs.microsoft.com/en-us/office365/enterprise/install-and-run-idfix

- Run synchronization service manager
- Run synchronization rules editor
- Re-run the AD Connect application

Q47) Azure backup can be configured to backup on-premises VMs. What is used to ensure data is encrypted at rest?

- Transparent Data Encryption
- Azure Storage Service Encryption
- Azure Recovery Vault
- ✅ Passphrase

Explanation:-When using Azure backup to backup on-premises VMs a passphrase is used along with AES256 to encrypt the backup. See: https://docs.microsoft.com/en-us/azure/backup/backup-azure-backup-faq#encryption

- Azure Recovery Services

Q48) Azure backup can be configured to Azure VMs. What is used to ensure data is encrypted at rest?

- Transparent Data Encryption
- Azure Recovery Services
- Azure Recovery Vault
- Passphrase
- ✅ Azure Storage Service Encryption

Explanation:-When using Azure backup to backup Azure VMs, Azure Storage Service encryption is used to encrypt the backup. See: https://docs.microsoft.com/en-us/azure/backup/backup-azure-backup-faq#encryption

---

Q49) You notice a recommendation in the Azure Security Center to add a vulnerability assessment solution to your Azure virtual machines. Which of the following options are Azure Security Center-integrated solutions to the recommendation. Select two.

- ✅ Rapid7

Explanation:-Azure Security Center supports Qualys and Rapid7 as integrated vulnerability assessment solutions. Nessus is not currently integrated with Azure Security Center. Azure Log Analytics, Azure Monitor and Microsoft ATA are not vulnerability assessment solutions related to this ASC recommendation. See: https://docs.microsoft.com/en-us/azure/security-center/security-center-vulnerability-assessment-recommendations

- Azure Log Analytics
- ✅ Qualys

Explanation:-Azure Security Center supports Qualys and Rapid7 as integrated vulnerability assessment solutions. Nessus is not currently integrated with Azure Security Center. Azure Log Analytics, Azure Monitor and Microsoft ATA are not vulnerability assessment solutions related to this ASC recommendation. See: https://docs.microsoft.com/en-us/azure/security-center/security-center-vulnerability-assessment-recommendations

- Nessus
- Azure Monitor
- Microsoft Advanced Threat Analytics

Q50) correct or Incorrect: Azure firewall supports inbound and outbound filtering.

- incorrect
- ✅ correct

Explanation:-This option is correct as the Azure firewall supports inbound and outbound filtering, however inbound filtering is for non HTTP/S protocols i.e. RDP, SSH and FTP protocols are supported. https://docs.microsoft.com/en-us/azure/firewall/firewall-faq

---

Q51) Correct or Incorrect: you can configure multiple AD Connect connectors for the same Active Directory domain.

- correct
- ✅ incorrect

Explanation:-This option is correct, multiple connectors for the same AD domain are not supported. You can however configure a secondary connector in staging mode for DR purposes. https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-faq

---

Q52) Select all the answers that specify the technology and Azure resource prerequisites for Azure Disk Encryption.

- ✅ BitLocker

Explanation:-Azure Disk Encryption uses BitLocker for Windows-based VMs and DM-Crypt for supported Linux-based VMs in Azure. It also requires Azure Key Vault to provide secure access to the encryption/decryption keys. https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-overview

- SSL/TLS 1.2
- ✅ DM-Crypt

Explanation:-Azure Disk Encryption uses BitLocker for Windows-based VMs and DM-Crypt for supported Linux-based VMs in Azure. It also requires Azure Key Vault to provide secure access to the encryption/decryption keys. https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-overview

- ✅ Azure Key Vault

Explanation:-Azure Disk Encryption uses BitLocker for Windows-based VMs and DM-Crypt for supported Linux-based VMs in Azure. It also requires Azure Key Vault to provide secure access to the encryption/decryption keys. https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-overview

- Azure Storage Service Encryption
- Transparent Data Encryption

Q53) Which of the following roles can make use of Azure Identity Protection in the portal?

- ✅ Security reader

Explanation:-The following roles can make use of Identity Protection: Security reader, security admin and global admin. Contributor and owner roles are both incorrect as these are related to https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/faqs

- Owner role
- Contributor role
- ✅ Security Administrator

Explanation:-The following roles can make use of Identity Protection: Security reader, security admin and global admin. Contributor and owner roles are both incorrect as these are related to https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/faqs

- ✅ Global administrator

Explanation:-The following roles can make use of Identity Protection: Security reader, security admin and global admin. Contributor and owner roles are both incorrect as these are related to https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/faqs

---

Q54) You have synchronized your IT departments on-premises identities with Azure AD via the AD Connect tool. You need to onboard the rest of the on-premises users with the least amount of effort. What should you do?

- Restart the ADConnect VM
- ✅ Re-run the ADConnect tool

Explanation:-Re-run ADConnect tool is correct, this will allow you to customize the synchronization properties to add additional Object Unit filtering. Uninstall and re-install ADConnect is incorrect as this will take more effort than to re-run the ADConnect tool. Stopping the synchronization service is incorrect as this will stop all configured identities from synching. Restarting the ADConnect VM is incorrect as this will not enable you to onboard the additional users. https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-installation-wizard

- Uninstall and re-install the ADConnect tool
- Stop the synchronization service

Q55) How does Azure SQL Database provide protection for data at rest?

- BitLocker
- AES Encryption
- ✅ Transparent Data Encryption

Explanation:-Azure SQL Database has a built-in data at rest encryption capability called Transparent Data Encryption. The encryption key is managed by Microsoft, but it is possible to bring your own key through the TDE integration with Azure Key Vault - Key Vault is not the best answer here though. SSL/TLS is used for securing data in transit. Bitlocker is used for endpoint encryption, not for SQL Database encryption. By default TDE uses the AES encryption algorithm, but this is also not the best answer for the question. TDE is used for database encryption and is very similar to the Azure Storage counterpart called Storage Service Encryption. https://docs.microsoft.com/en-us/azure/sql-database/transparent-data-encryption-azure-sql

- Azure Storage Service Encryption
- Azure Key Vault
- SSL/TLS 1.2

Q56) You are the administrator of all resources in Azure. You need to enforce all new resources created to a specific region. Solution: You create an Azure policy Does this meet the requirements?

- incorrect
- ✅ correct

Explanation:-This option is correct, you can create an Azure Policy to enforce a specific region when new resources are created. https://docs.microsoft.com/en-us/azure/governance/policy/samples/allowed-locations

---

Q57) What PowerShell cmdlet is used to initiate Azure Disk Encryption for a Windows-based VM on Azure?

- Set-AzVMDiskEncryptionWindows
- ✅ Set-AzVMDiskEncryptionExtension

Explanation:-Set-AzVMDiskEncryptionExtension is the correct answer. The same cmdlet is used for both Windows and Linux VMs See https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-windows

- Set-AzVMDiskEncryption
- Get-AzVmDiskEncryptionStatus
- Disable-AzVMDiskEncryption
- Set-AzVMDiskEncryptionLinux

Q58) Which single Azure SQL Database feature provides data security for data at rest, data in transit and data in use?

- SSL/TLS 1.2
- ✅ Always Encrypted

Explanation:-Always Encrypted is a data encryption technology in Azure SQL Database and SQL Server that helps protect sensitive data at rest on the server, during movement between client and server, and while the data is in use, ensuring that sensitive data never appears as plain text inside the database system. The encryption is performed on the endpoint application before writing the data to the database. The encryption keys are not revealed to the database management system. The encrypted data is also not readable by other privileged users like database administrators.
https://docs.microsoft.com/en-us/azure/sql-database/sql-database-always-encrypted-azure-key-vault

- Transparent Data Encryption
- AES Encryption
- Azure Storage Service Encryption
- Azure Key Vault
