Answer Sheet

Q1) Which of the following security concerns are relevant to container solutions? Select all that apply.

- Kernel Exploits
- Denial-of-service attacks
- Container breakouts
- Poisoned images
- ✅ All of these

Explanation:-All of these is correct. Kernel Exploits: Unlike in a VM, the kernel is shared among all containers and the host. This sharing magnifies the importance of any vulnerabilities in the kernel. DoS: All containers share kernel resources. If one container can monopolize access to certain resources—including memory and user IDs—it can starve out other containers on the host. The result is a denial of service (DoS), whereby legitimate users are unable to access part or all the system. Container breakouts: An attacker who gains access to a container should not be able to gain access to other containers or the host. By default, users are not included in the container namespace, so any process that breaks out of the container will have the same privileges on the host as it did in the container. If you were root in the container, you will be root on the host. You need to prepare for potential privilege escalation attacks—whereby a user gains elevated privileges such as those of the root user. Poisoned images: How do you know that the images you're using are safe, haven't been tampered with, and come from where they claim to come from? If an attacker can trick you into running an image, both the host and your data are at risk. Similarly, you want to be sure that the images you're running are up to date and don't contain versions of software with known vulnerabilities. https://azure.microsoft.com/mediahandler/files/resourcefiles/container-security-in-microsoft-azure/Open%20Container%20Security%20in%20Microsoft%20Azure.pdf

---

Q2) You need to delegate access to a system administrator to a specific VM labeled "LOB-VM" in the "Production" resource group. The system administrator should have full control over the VM but should not be able to grant additional users' access. The resource group is home to a combination of resources across different departments. You need to grant RBAC access with strict security in mind. Which is the correct RBAC configuration?

- Scope = "LOB-VM", Role = "Owner"
- Scope = "Production", Role = "Owner"
- Scope = "Production", Role = "Contributor"
- ✅ Scope = "LOB-VM", Role = "Contributor"

Explanation:-This option is correct as you need to granularly define the scope and role, the scope is at the VM level which is correct, you cannot set it at the resource group level because that user will then have permissions on all resources in that resource group which is incorrect in this scenario. The Contributor role is correct as this role grants the full permission for a person except adding additional users to the resource. https://docs.microsoft.com/en-us/azure/role-based-access-control/overview

---

Q3) You need to ensure that all current and future resources that are compliant are enrolled into Azure Security Center.
Solution: You configure an Azure policy on the subscription level.
Does this solution meet the goal?

- ✅ Correct

Explanation:-This option is correct as you can create an Azure policy to ensure all compliant resources are automatically enrolled into ASC. https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage

- Incorrect

Q4) You need to harden your Docker containers.
Solution: You enable AppArmor.
Does this solution meet the goal?

- ✅ Correct

Explanation:-This option is correct, you can use AppArmor, SELinux, GRSEC or another appropriate hardening system. https://docs.docker.com/engine/security/security/

- Incorrect

Q5) You have inherited an Azure environment which has plenty of resource groups. You have been tasked to manage access, policies and compliance for the subscriptions in an efficient manner.
Solution: You decide to make use of RBAC.
Does this solution meet the goal?

- Correct
- ✅ Incorrect

Explanation:-This option is correct, you cannot manage policies and compliance via RBAC, you should instead make use of Azure Management Groups. https://docs.microsoft.com/en-us/azure/governance/management-groups/index

---

Q6) You need to limit outbound HTTPS traffic to specific fully qualified domain names (FQDN). Which of the following technologies support this?

- Network Security Groups (NSG)
- Application Security Groups (ASG)
- ✅ Azure Firewall

Explanation:-Azure firewall is correct as this supports limiting outbound HTTPS traffic to a specified list of FQDN's including wildcards, this feature does not require SSL termination. NSG is incorrect as this does not have the ability to filter outbound traffic by FQDNs, rather by IP's or grouped IP's like the "Internet" tag. ASG is incorrect as this feature allows you to group VMs to make management easier for inbound and outbound traffic. JIT VM Access is incorrect as this is used to access Azure VMs remotely, JIT VM Access automatically creates NSG rules to allow temporary access to resources (VMs). https://docs.microsoft.com/en-us/azure/firewall/overview

- Just-in-time VM access (JIT VM Access)

Q7) You need to configure temporary access to an Azure VM on port 22, the solution should manage the inbound rules automatically in the back end and remove the rules when the time period expires. Which of the following technologies should you configure?

- Network Security Group (NSG)
- Application Security Groups (ASG)
- Azure Firewall
- ✅ Just-in-time VM access

Explanation:-Just-in-time VM access is correct as this allows you to connect to an Azure VM for a specific time period on specific ports- this is done automatically in the backend as this creates temporary NSG rules and removes them when the time expires. NSG is incorrect as this is a manual process and does not remove the rules after a specific time period. ASG is incorrect as this feature allows you to group VMs to make management easier for inbound and outbound traffic, however it cannot automatically create and remove NSG rules based on a time period. Azure firewall is incorrect as this is a stateful firewall and does not have the capability to automatically create rules for remote users to access VM's based on a specific time period. https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time

---

Q8) You create an Azure Information Protection classification policy that defines a number of classification levels. You configure labels for general, sensitive and confidential. You configure the visual marker for the confidential label as watermark. A few weeks later you change the policy by creating sub labels for the confidential class as Confidential \ All Employees and Confidential \ Recipients Only. You configure the visual marker for each of these as footer. When the Confidential \ All Employees classification is applied to the document, which of the following visual marking(s) is/are applied?

- None of these
- Footer and Watermark
- Watermark
- ✅ Footer

Explanation:-When you use sub-labels, don't configure visual markings, protection, and conditions at the primary label. When you use sub-levels, configure these settings on the sub-label only. If you configure these settings on the primary label and its sub-label, the settings at the sub-label take precedence. https://docs.microsoft.com/en-us/azure/information-protection/faqs-infoprotect#can-a-file-have-more-than-one-classification

---

Q9) What Azure feature ensures that data residency, sovereignty, compliance, and resiliency requirements are honored?

- ✅ Azure Geography

Explanation:-Azure geography ensures that data residency, sovereignty, compliance, and resiliency requirements are honored within geographical boundaries. https://azure.microsoft.com/en-us/global-infrastructure/geographies/

- Azure Region
- Azure Resource Group
- Azure Tenant
- Azure Trust Center

Q10) You are in the process of creating an Azure container registry via CLI in the "MyRG" resource group. Complete the following command to create the container registry labeled "MyContainer001".
Az (1) create –resource group MyRG –(2) MyContainer001 (3) –Basic

- ✅ 1=acr, 2=name, 3= sku

Explanation:-This option is correct as the correct Azure CLI code is as follows: az acr –resource group MyRG –name MyContainer001 –sku Basic. https://docs.microsoft.com/en-us/azure/container-registry/container-registry-get-started-azure-cli

- 1=akr, 2= id, 3= tier
- 1=docker, 2=name, 3=tier
- 1=acr, 2=id, 3=sku

Q11) You plan to secure remote access from your on-premises network to your AKS cluster which is deployed to an existing Azure VNet. The solution should have the lowest possible latency and very high network speeds.
Solution: You implement a Site-to-Site VPN solution.
Does this solution meet the goal?

- Correct
- ✅ Incorrect

Explanation:-This option is correct as you should rather make use of Express route. Express route enables you to connect from your on-premises network to Azure with high speeds and low latency. https://docs.microsoft.com/en-us/azure/aks/concepts-security#network-security

---

Q12) 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
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?

- ✅ 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

- Express route
- VNet peering
- VNet-to-VNet connection

Q13) 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
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

---

Q14) 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
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?

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

- VNet-to-VNet connection

Q15) 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
- "LOB VM" which is hosted on a Windows Server 2016 OS
***West US resource group which contains**
- Virtual network 4
“Japan Subscription” which has 1 resource group
*** Japan resource group which contains**
- Virtual network 5
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 Internet service tag and set the action to Deny
- ✅ Create outbound NSG rule with an Internet service tag and set the action to Deny

Explanation:-This option is correct. 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 ANY Destination and set the action to Deny
- Create outbound NSG rule with an ANY Destination and set the action to Deny

---

Q16) You need to manage inbound and outbound traffic rules at scale to specific VMs with minimum effort. You plan on creating separate inbound and outbound NSG rules with CIDR notation. Is this the easiest method to manage multiple VMs?

- Correct
- ✅ Incorrect

Explanation:-incorrect, you need to make use of Application Security Groups (ASG’s). ASG’s allows you to group VM’s to make management easier, for example you can group several VMs with an ASG and only make changes once to the ASG instead of manually adding/removing/editing NSG rules with CIDR notation. https://docs.microsoft.com/en-us/azure/virtual-network/security-overview#application-security-groups

---

Q17) You have a storage account named "BlobStore" and you have noticed that anyone can access this storage account over the internet. You need to secure this storage account so that only users from the Head Office with IP 197.145.42.202/32 can access this storage account, however you still require anonymous access over the internet to the storage metrics for this account. Which 2 options should you configure?

- Configure Allow access from selected networks and specify 197.145.42.202/32
- Configure Allow access from all networks
- ✅ Configure IP ranges under the firewall section and specify 197.145.42.202/32

Explanation:-This option is correct as you need to specify the public IP address range you want to allow under the firewall section for the storage account. Option 5 is also correct as you need to allow only read access to storage metrics from any network. Option 1 is incorrect as you cannot specify the public IP address under the "selected networks" section as this is used to allow access from Virtual Networks in Azure to the storage account. Option 2 is incorrect as you should not configure "allow access from all networks" as you need to limit the access to specific public IPs as described in the scenario. Option 4 is incorrect as this will only allow Microsoft services access to the storage account and not the users from the Head Office. https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security

- Allow trusted Microsoft services to access this storage account
- ✅ Allow read access to storage metrics from any network

Explanation:-This option is correct as you need to specify the public IP address range you want to allow under the firewall section for the storage account. Option 5 is also correct as you need to allow only read access to storage metrics from any network. Option 1 is incorrect as you cannot specify the public IP address under the "selected networks" section as this is used to allow access from Virtual Networks in Azure to the storage account. Option 2 is incorrect as you should not configure "allow access from all networks" as you need to limit the access to specific public IPs as described in the scenario. Option 4 is incorrect as this will only allow Microsoft services access to the storage account and not the users from the Head Office. https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security

---

Q18) Which of the following elements are not associated with an Azure Region?

- Azure Virtual Machine
- Azure Resource Group
- Azure Managed Disk
- Storage Account
- ✅ None of these

Explanation:-All the listed Azure resources are associated with an Azure region. The region chosen for deployment of resources that holds data affects data sovereignty and residency.

- All of these

Q19) Which of the following lists of data classifications is arranged from highest to lowest level of sensitivity?

- ✅ 1. Confidential. 2. Internal only. 3. Public

Explanation:-Classification levels are usually defined from highest to lowest level of sensitivity, using various labeling strategies. Generally speaking the terminology is as follows: High, medium, low or Confidential, internal only, public or Restricted, sensitive, unrestricted or top-secret, secret, sensitive, unclassified. Each level of classification have a definition (or risk level if the data is lost or leaked), characteristics (what data are assigned to the level) and the protections applied (labeling, encryption and permissions). https://gallery.technet.microsoft.com/Data-Classification-for-51252f03/file/172083/1/Data%20Classification%20for%20Cloud%20Readiness%20(2017-04-11).pdf and https://docs.microsoft.com/en-us/azure/security/security-white-papers

- 1. Sensitive. 2. Restricted. 3. Unrestricted
- 1. Low. 2. Medium. 3. High
- 1. Secret. 2. Top-Secret. 3. Sensitive. 4. Unclassified

Q20) In data classification, which of the following data ownership roles are given no permissions to use the data? Choose 2

- Owner
- User
- ✅ Administrator

Explanation:-Using the data means having read and optionally modify and delete privileges for the data. Data users and owners (usually the user that created the data) are the only roles listed with these rights. Data custodians have delegate rights, meaning they can modify rights to the data for others (but not for themselves). Data administrators have only archive/restore rights. Owners have all rights to the data. https://gallery.technet.microsoft.com/Data-Classification-for-51252f03/file/172083/1/Data%20Classification%20for%20Cloud%20Readiness%20(2017-04-11).pdf and https://docs.microsoft.com/en-us/azure/security/security-white-papers

- ✅ Custodian

Explanation:-Using the data means having read and optionally modify and delete privileges for the data. Data users and owners (usually the user that created the data) are the only roles listed with these rights. Data custodians have delegate rights, meaning they can modify rights to the data for others (but not for themselves). Data administrators have only archive/restore rights. Owners have all rights to the data. https://gallery.technet.microsoft.com/Data-Classification-for-51252f03/file/172083/1/Data%20Classification%20for%20Cloud%20Readiness%20(2017-04-11).pdf and https://docs.microsoft.com/en-us/azure/security/security-white-papers

---

Q21) Which of the following elements are not included in a data retention policy?

- Data recovery rules
- Data disposal rules
- Regulatory requirements
- Corporate requirements
- Data retention periods per classification level
- ✅ Data security measures

Explanation:-All of the answers list an item typically included in a data retention policy, except for data security measures that is held in a data classification policy. https://gallery.technet.microsoft.com/Data-Classification-for-51252f03/file/172083/1/Data%20Classification%20for%20Cloud%20Readiness%20(2017-04-11).pdf and https://docs.microsoft.com/en-us/azure/security/security-white-papers

Q22) Which of the following are valid access control options for Storage Accounts? Choose 3

- ✅ Access Key

Explanation:-Access keys, Azure AD RBAC and Shared Access Signatures are all valid access control methods for storage accounts. Service key and shared access key are not valid names for storage account access controls. https://docs.microsoft.com/en-us/azure/storage/common/storage-security-guide?toc=%2fazure%2fstorage%2fblobs%2ftoc.json#data-plane-security

- Shared Access Key
- ✅ Role Based Access Control

Explanation:-Access keys, Azure AD RBAC and Shared Access Signatures are all valid access control methods for storage accounts. Service key and shared access key are not valid names for storage account access controls. https://docs.microsoft.com/en-us/azure/storage/common/storage-security-guide?toc=%2fazure%2fstorage%2fblobs%2ftoc.json#data-plane-security

- Service Key
- ✅ Shared Access Signature

Explanation:-Access keys, Azure AD RBAC and Shared Access Signatures are all valid access control methods for storage accounts. Service key and shared access key are not valid names for storage account access controls. https://docs.microsoft.com/en-us/azure/storage/common/storage-security-guide?toc=%2fazure%2fstorage%2fblobs%2ftoc.json#data-plane-security

---

Q23) What are the types of authentication supported as an access control measure to Azure SQL Database?

- Simple (clear text) authentication
- Encrypted Challenge-response authentication
- ✅ Azure Active Directory authentication

Explanation:-AAD and SQL native authentication is supported by Azure SQL Database. The other answer options do not exist in the context of SQL Database. MFA is implemented by AAD but is not part of SQL Database. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-security-overview#authentication

- ✅ SQL authentication

Explanation:-AAD and SQL native authentication is supported by Azure SQL Database. The other answer options do not exist in the context of SQL Database. MFA is implemented by AAD but is not part of SQL Database. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-security-overview#authentication

- RADIUS authentication
- Multi-factor authentication

Q24) Which of the following is the correct actions for resetting the password for the SQL server admin login that is created as part of a new Azure SQL Database?

- ✅ Azure portal, SQL Servers, select server, reset password

Explanation:-The server admin login can be changed from the Azure portal by using the Reset password button for the selected SQL Server. If you use AAD-integrated login, changing the user password using AAD in the Azure portal would work, but the question asks for changing the SQL server admin, specifically. There is no reset password button on the selected SQL database (must be changed at server level). Using the SQL command ALTER LOGIN would also work, but that requires the SQL Query editor and is not the best answer for the question. CREATE LOGIN is used to create additional SQL logins. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-manage-logins#unrestricted-administrative-accounts

- Azure portal, SQL Databases, select database, reset password
- Azure portal, Azure Active Directory, select user, Reset password
- SQL Query editor, connect to Azure SQL Database, ALTER LOGIN command
- SQL Query editor, connect to Azure SQL Database, CREATE LOGIN command
- SQL Query editor, connect to Azure SQL Database, LOGIN command

---

Q25) What are the destinations available for Azure SQL Server audit logs? Choose 3.

- SQL Data Warehouse
- ✅ Storage

Explanation:-Storage (account), event hubs and log analytics are supported destinations for SQL Database (and/or SQL Server) audit logs. The other options are valid Azure services, but is not selectable as audit log destinations. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-auditing#subheading-2

- ✅ Event Hubs

Explanation:-Storage (account), event hubs and log analytics are supported destinations for SQL Database (and/or SQL Server) audit logs. The other options are valid Azure services, but is not selectable as audit log destinations. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-auditing#subheading-2

- SQL Database
- ✅ Log Analytics

Explanation:-Storage (account), event hubs and log analytics are supported destinations for SQL Database (and/or SQL Server) audit logs. The other options are valid Azure services, but is not selectable as audit log destinations. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-auditing#subheading-2

- Service Bus

Q26) You configure Azure SQL Database auditing. You select Storage as the audit log destination and don't change the retention period setting. What is the effect on audit log retention in this scenario?

- A retention period must be specified, in days up to a maximum of 3285 days
- ✅ Audit logs are kept indefinitely

Explanation:-The default retention period setting for Azure SQL Database audit logs is 0. This equates to keeping audit logs indefinitely. A retention period of up to a maximum of 3285 days can be specified. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-auditing#subheading-2

- Audit logs are kept for the default of 90 days
- Audit logs are kept for the default of 120 days

Q27) Describe the steps required to ensure that writing Azure SQL Database audit logs to a storage destination are uninterrupted by a storage access key refresh.

- Switch the storage destination to an alternative storage account; refresh the primary and secondary storage keys in the storage configuration of the original storage account; optionally switch the storage destination back to the original storage account
- Stop the Azure SQL Server associated with the Azure SQL Database; refresh the primary and secondary storage keys in the storage configuration; start the Azure SQL Server associated with the Azure SQL Database
- No action is required - storage keys are automatically updated for SQL Data audit logs when Storage access keys are refreshed
- ✅ Switch the storage access key in the audit configuration to secondary; refresh the primary storage key in the storage configuration; switch the storage access key in the audit configuration to primary; refresh the secondary storage access key in the storage configuration

Explanation:-Switching the storage configuration to secondary, refreshing the primary key, then switching the storage configuration back to primary before finally refreshing the secondary key is the recommended method to ensure uninterrupted audit logging in Azure SQL Database. You can not stop a SQL Server (unless you delete the server along with all databases on it). The storage configuration is not automatically updated. Switching the storage destination to an alternative storage account would work, but you will end up with two sources of audit log data which is not an ideal situation and not the best answer. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-auditing#storage-key-regeneration

---

Q28) What are the three headline capabilities of advanced data security in Azure SQL Database?

- SQL Server Firewall
- ✅ Data discovery and classification

Explanation:-The advanced data security capability of Azure SQL Database provides data discovery and classification; vulnerability assessment and advanced threat protection. ADS is integrated with ASC where alerts and incidents are surfaced and managed. SQL Database firewall and dynamic data masking are valid SQL Database features, but they are not part of advanced data security. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-advanced-data-security#overview

- ✅ Vulnerability assessment

Explanation:-The advanced data security capability of Azure SQL Database provides data discovery and classification; vulnerability assessment and advanced threat protection. ADS is integrated with ASC where alerts and incidents are surfaced and managed. SQL Database firewall and dynamic data masking are valid SQL Database features, but they are not part of advanced data security. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-advanced-data-security#overview

- Azure security center
- ✅ Advanced threat protection

Explanation:-The advanced data security capability of Azure SQL Database provides data discovery and classification; vulnerability assessment and advanced threat protection. ADS is integrated with ASC where alerts and incidents are surfaced and managed. SQL Database firewall and dynamic data masking are valid SQL Database features, but they are not part of advanced data security. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-advanced-data-security#overview

- Dynamic data masking

Q29) Which of the following authentication mechanisms is used by Azure HDInsight?

- ✅ Kerberos

Explanation:-Azure HDInsight uses Kerberos authentication provided through integration with Azure Active Directory Domain Services. The other authentication standards are not supported. https://docs.microsoft.com/en-us/azure/hdinsight/domain-joined/apache-domain-joined-architecture

- OAuth
- SAML
- Azure Active Directory
- OpenID

Q30) Multiple layers of security is recommended for Azure HDInsight. Which of the following is not considered a protection layer?

- Perimeter security
- Authorisation security
- Authentication security
- Data security
- ✅ Cluster security

Explanation:-Perimeter, authentication, authorisation and data layer security is recommended. Cluster security is not considered part of deploying Azure HDInsight security. https://docs.microsoft.com/en-us/azure/hdinsight/domain-joined/apache-domain-joined-introduction

---

Q31) Which component is used to manage role-based access control in Azure HDInsight?

- Azure Active Directory
- Azure Active Directory Domain Services
- ✅ Apache Ranger

Explanation:-Apache Ranger is used to create RBAC policies in Azure HDInsight. HDInsight is integrated with Azure AD DS for Kerberos authentication services, but RBAC is handled in the HDInsight cluster itself using Apache Ranger. https://docs.microsoft.com/en-us/azure/hdinsight/domain-joined/apache-domain-joined-introduction#authorization

- Apache Hive Server
- Apache Spark

Q32) How does HDInsight provide protection for data at rest?

- Apache Hive Server Encryption
- ✅ Azure Storage Service Encryption

Explanation:-HDInsight integrates with Azure Blob storage and Azure Data Lake Storage as the underlying storage infrastructure which is automatically encrypted by Azure Storage Service Encryption. SSE uses AES 256-bit, but this is not the best answer for the question. The Apache components is not responsible for encryption. https://docs.microsoft.com/en-us/azure/hdinsight/domain-joined/apache-domain-joined-introduction#encryption

- Apache HBase Encryption
- Apache Ranger Encryption
- AES 256-bit Encryption

Q33) It is considered best practice to add an additional layer of access control security to Azure Cosmos DB. Which Azure features provides this capability?

- Network Security Group
- Azure Firewall
- ✅ Cosmos DB Firewall

Explanation:-Azure Cosmos DB has a built-in firewall service. Similar to any other 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 Cosmos DB access control. https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-configure-firewall#configure-ip-policy

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

Q34) Azure Cosmos DB uses two types of keys to authenticate users and provide access to its data and resources. Select them from the answer options.

- Access Key
- Shared Access Key
- Role Based Access Control
- ✅ Resource Token

Explanation:-Cosmos DB uses a Master Key for administrative resources: database accounts, databases, users, and permissions. It also uses a Resource Token for application resources: containers, documents, attachments, stored procedures, triggers, etc. https://docs.microsoft.com/en-us/azure/cosmos-db/database-security#how-does-azure-cosmos-db-secure-my-database

- Shared Access Signature
- ✅ Master Key

Explanation:-Cosmos DB uses a Master Key for administrative resources: database accounts, databases, users, and permissions. It also uses a Resource Token for application resources: containers, documents, attachments, stored procedures, triggers, etc. https://docs.microsoft.com/en-us/azure/cosmos-db/database-security#how-does-azure-cosmos-db-secure-my-database

---

Q35) How does Cosmos DB provide protection for data at rest?

- Hash-based Message Authentication Code (HMAC)
- ✅ Azure Storage Service Encryption

Explanation:-Azure storage encryption is used to encrypt data at rest for Cosmos DB. HMAC is used in Cosmos DB authorisation, but not for data encryption. Applications can make use of Cosmos DB by storing the access tokens in Azure Key Vault instead of with the application. SSL/TLS is used by the system to ensure data protection (encryption) in transit. https://docs.microsoft.com/en-us/azure/cosmos-db/database-encryption-at-rest

- Azure Key Vault
- SSL/TLS 1.2
- AES 256-bit Encryption

Q36) Which of the following core features are available when you deploy Microsoft anti-malware for Azure applications. Select all that apply.

- 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

---

Q37) Which of the following is supported to create custom RBAC roles? Select all that apply.

- ✅ Azure PowerShell

Explanation:-Azure PowerShell, CLI and Rest API is correct and can be used to create custom RBAC roles in Azure. CMD is incorrect as this is not supported. https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles

- ✅ Azure CLI

Explanation:-Azure PowerShell, CLI and Rest API is correct and can be used to create custom RBAC roles in Azure. CMD is incorrect as this is not supported. https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles

- ✅ Rest API

Explanation:-Azure PowerShell, CLI and Rest API is correct and can be used to create custom RBAC roles in Azure. CMD is incorrect as this is not supported. https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles

- CMD

Q38) 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.

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

Explanation:-This option is correct as you need to define the allowed action as restart. Option 4 is correct as you need to define the action which is

not allowed, in this case it is shutdown. Option 2 is incorrect as you do not want the third party to start the VM as this is not a requirement. Option 3 is incorrect as you should make use of the shutdown parameter instead of start as you want to prohibit the shutdown of the VM, not the starting of the VM. 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

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

Explanation:-This option is correct as you need to define the allowed action as restart. Option 4 is correct as you need to define the action which is not allowed, in this case it is shutdown. Option 2 is incorrect as you do not want the third party to start the VM as this is not a requirement. Option 3 is incorrect as you should make use of the shutdown parameter instead of start as you want to prohibit the shutdown of the VM, not the starting of the VM. 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

---

Q39) Which of the following can be associated to a Network Security Group (NSG) ? Select all that apply.

- ✅ Subnet

Explanation:-Subnet and Network Interface cards (NIC's) are correct, you cannot associate a VNet or resource group to a Network Security Group (NSG). https://docs.microsoft.com/en-us/azure/virtual-network/security-overview

- ✅ Network Interface Card (NIC)

Explanation:-Subnet and Network Interface cards (NIC's) are correct, you cannot associate a VNet or resource group to a Network Security Group (NSG). https://docs.microsoft.com/en-us/azure/virtual-network/security-overview

- Virtual Network (VNet)

Q40) correct or incorrect: when there are 2 NSG's associated to the same subnet, when one NSG denies traffic on port 80 inbound and another allows traffic on port 80 inbound to the same VM, the traffic will automatically be blocked due to the one NSG rule that denies the traffic.

- ✅ Correct

Explanation:-This option is correct, whenever a VM/subnet is associated to 2 or more NSG's and there are conflicting rules on each NSG (i.e. one NSG has allow and one NSG deny) the NSG which has the deny rule will take preference and traffic will not pass through. https://docs.microsoft.com/en-us/azure/virtual-network/security-overview

- Incorrect

Q41) correct or incorrect: you can create custom service tags when making use of Network Security Groups?

- Correct
- ✅ Incorrect

Explanation:-This option is correct, you cannot create your own service tag or specify which IP's are included within a tag.https://docs.microsoft.com/en-us/azure/virtual-network/security-overview#service-tags

---

Q42) How does Azure Data Lake provide protection for data at rest?

- BitLocker
- ✅ Azure Storage Service Encryption

Explanation:-Azure Data Lake is built on Azure Storage, just like Blobs, Tables and Queues. It uses the same underlying encryption for data at rest - Storage Service Encryption. SSE uses AES 256-bit as the underlying encryption algorithm, but this is not the best answer for the question. SSL/TLS is encryption for data in transit, not data at rest. Azure Key Vault can be used for SSE in a Bring Your Own Key scenario, but does not perform encryption itself. Bitlocker is Microsoft's encryption technology used on the endpoint, not relevant for SSE. https://docs.microsoft.com/en-za/azure/storage/common/storage-service-encryption?toc=%2fazure%2fstorage%2fblobs%2ftoc.json#view-encryption-settings-in-the-azure-portal

- Azure Key Vault
- SSL/TLS 1.2
- AES 256-bit Encryption

Q43) What are two types of data store used by Azure Monitor?

- ✅ Logs

Explanation:-Azure monitor stores data in Logs and Metrics data stores. The other answers are examples of Azure storage products. See: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-platform

- ✅ Metrics

Explanation:-Azure monitor stores data in Logs and Metrics data stores. The other answers are examples of Azure storage products. See: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-platform

- Event Hubs
- Blobs
- Queues

Q44) Which of the following are not characteristics of Azure Monitor Metrics?

- ✅ Text or numeric data

Explanation:-All the options are correct for Azure Monitor Metrics except for Text or numeric data. Metrics are only numeric data. Azure Monitor Logs can also contain Text data. See: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-platform#compare-azure-monitor-metrics-and-logs

- Collected at regular intervals
- Lightweight
- Sourced from Application Insights
- Sourced from Azure resources

Q45) Which of the following are valid Azure Monitor data sources?

- Application Insights
- Log Analytics Agent
- Azure Resource Diagnostic Log
- Azure Subscription
- Azure Tenant Audit Log
- ✅ All of these

Explanation:-All of the options are valid sources for Azure Monitor. Custom sources (via Data Collector API), Guest Operating Systems and Application Insights are supported for on-premises or other clouds deployments. See: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-sources

---

Q46) Which of the following access control options would you use to provide temporary anonymous access to a Storage Account?

- Access Key
- Shared Access Key
- Role Based Access Control
- Service Key
- ✅ Shared Access Signature

Explanation:-One would use a shared access signature to allow temporary (timed) access control for anonymous access to a storage account via a URI. https://docs.microsoft.com/en-us/azure/storage/common/storage-security-guide?toc=%2fazure%2fstorage%2fblobs%2ftoc.json#data-plane-security

---

Q47) You are reviewing the security policies assigned to your subscription in Azure Security Center. In addition to the ASC Default policy that is already assigned, you need to assign the built-in policy initiative named Enable Data Protection Suite that contains a policy named Deploy Threat Detection on SQL servers. Choose the correct list of steps to accomplish your goals.

- Azure Security Center, Security Policy, Assign Initiative, Select Enable Data Protection, Click Assign
- ✅ Azure Policy, Assignments, Assign Initiative, Select Enable Data Protection, Click Assign

Explanation:-Adding policies to Azure security center is performed through Azure Policy. There is no Assign Initiative option on the ASC security policy blade. From the resource group, clicking on the policies item redirects to Azure Policy - this option will work, but the assignment is performed on the RG level where the question refers to the subscription level. One can configure Advanced Data Security on the SQL database, but this will have to be repeated for all SQL servers - the policy applies the security measure to all SQL servers in the subscription. See: https://docs.microsoft.com/en-us/azure/security-center/tutorial-security-policy

- SQL Databases, Advanced Data Security, Assign Policy/Initiative, Select Enable Data Protection, Click Assign
- Resource Group, Policies, Assign Initiative, Select Enable Data Protection, Click Assign

---

Q48) Which of the following is correct for an Azure Security Center incident?

- A single alert detected by more than one ASC detection mechanism
- ✅ An aggregation of alerts that align with kill chain patterns

Explanation:-An aggregation of alerts that align with kill chain patterns is listed in ASC as a security incident. Incidents are listed with the other ASC alerts. They are almost always listed with a high severity and are very likely to be a correct positive. Alerts are sometimes detected by multiple detection measures including ATP, but the defining factor for identifying an incident is multiple alerts that together alight to a known kill chain pattern. See: https://docs.microsoft.com/en-us/azure/security-center/security-center-incident-response

- A single alert with a high probability of being a correct positive
- Any high-severity alert (not low-severity or medium-severity alerts)
- An alert detected by Azure Advanced Threat Protection

Q49) You are the security administrator for your Azure subscription and are reviewing the security alerts as listed in Azure Security Center. You select one of the high-severity alerts and select the resource identified by the alert as being attacked. What response options are available to you? Choose 3.

- Click remediate from the alert details pane
- Click isolate from the alert details pane
- Select one or more of the recommended remediation steps and click Remediate
- ✅ Manually execute the remediation steps recommended

Explanation:-Generally speaking you would manually act on the remediation steps listed on the alert details pane. The investigate button will launch the investigation interface of ASC. You can also run predefined playbooks (Azure Logic Apps) to automatically execute action steps for common alerts. See: https://docs.microsoft.com/en-us/azure/security-center/security-center-investigation and https://docs.microsoft.com/en-us/azure/security-center/security-center-playbooks and https://docs.microsoft.com/en-us/azure/security-center/security-center-incident-response

- ✅ Click investigate on the alert details pane

Explanation:-Generally speaking you would manually act on the remediation steps listed on the alert details pane. The investigate button will launch the investigation interface of ASC. You can also run predefined playbooks (Azure Logic Apps) to automatically execute action steps for common alerts. See: https://docs.microsoft.com/en-us/azure/security-center/security-center-investigation and https://docs.microsoft.com/en-us/azure/security-center/security-center-playbooks and https://docs.microsoft.com/en-us/azure/security-center/security-center-incident-response

- ✅ Click run playbooks on the alert details pane

Explanation:-Generally speaking you would manually act on the remediation steps listed on the alert details pane. The investigate button will launch the investigation interface of ASC. You can also run predefined playbooks (Azure Logic Apps) to automatically execute action steps for common alerts. See: https://docs.microsoft.com/en-us/azure/security-center/security-center-investigation and https://docs.microsoft.com/en-us/azure/security-center/security-center-playbooks and https://docs.microsoft.com/en-us/azure/security-center/security-center-incident-response

---

Q50) What Azure resource is created when an Azure Security Center playbook is created?

- ✅ Azure Logic App

Explanation:-The underlying technology used when ASC playbooks are created is an Azure Logic App. It does not require a Log Analytics

workspace. MS Flow uses the same underlying technology, but you cannot create ASC alert triggers in Flow. Azure Playbook or Runbook are generic terms and do not identify the Azure resource being created. https://docs.microsoft.com/en-us/azure/security-center/security-center-playbooks

- Azure Function
- Microsoft Flow
- Azure Log Analytics Workspace
- Azure Playbook
- Azure Runbook

Q51) correct or incorrect: a guest user in Azure AD can make use of the paid Azure AD features without having a member account in Azure AD.

- ✅ Correct

Explanation:-This option is correct as you can invite external "guest" users to use your paid Azure AD services, for each paid Azure AD license you can invite up to five guest users. https://docs.microsoft.com/en-us/azure/active-directory/b2b/licensing-guidance

- Incorrect

Q52) Which of the following statements are correct when transferring the subscription ownership to another user? Select all that apply.

- ✅ When transferring a subscription to a new Azure AD tenant, all RBAC assignments are permanently deleted from the source tenant and not migrated to the target tenant

Explanation:-This option is correct, when transferring a subscription to a new Azure AD tenant, all existing RBAC roles linked to the subscription will be permanently deleted and not migrated to the new tenant. Option 2 is correct as the self-serve option is only available for selected offers. Option 3 is incorrect as there will be no downtime when transferring ownership to another user/administrator. Option 4 is incorrect as you cannot change the offer type while transferring the subscription, the offer must remain the same. https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer

- ✅ Self-serve subscription transfer is only available for selected offers

Explanation:-This option is correct, when transferring a subscription to a new Azure AD tenant, all existing RBAC roles linked to the subscription will be permanently deleted and not migrated to the new tenant. Option 2 is correct as the self-serve option is only available for selected offers. Option 3 is incorrect as there will be no downtime when transferring ownership to another user/administrator. Option 4 is incorrect as you cannot change the offer type while transferring the subscription, the offer must remain the same. https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer

- When transferring a subscription to another administrator will cause downtime
- The offer type can be changed during the transferring a subscription

---

Q53) Which of the following roles are required to manage assignments for other administrators in Privilege Identity Management (PIM) for Azure AD roles?

- Global administrators
- Security administrators
- Security readers
- ✅ Privilege role administrator

Explanation:-Privilege role administrator is correct as this is the only role that can manage other administrators in PIM for Azure AD roles. Global administrator, Security administrator and security readers can only view assignments to Azure AD roles in PIM. https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

---

Q54) Which of the following roles are required to manage assignments for other administrators in PIM for Azure Resource roles?

- ✅ Subscription administrator

Explanation:-Only the following roles can manage assignments for other administrators in PIM for Azure resource roles: Subscription admin, resource owner and resource user access admin. Security admin and security reader do not by default have access to view assignments to Azure resource roles in PIM. https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

- ✅ Resource owner

Explanation:-Only the following roles can manage assignments for other administrators in PIM for Azure resource roles: Subscription admin, resource owner and resource user access admin. Security admin and security reader do not by default have access to view assignments to Azure resource roles in PIM. https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

- ✅ Resource User Access Administrator

Explanation:-Only the following roles can manage assignments for other administrators in PIM for Azure resource roles: Subscription admin, resource owner and resource user access admin. Security admin and security reader do not by default have access to view assignments to Azure resource roles in PIM. https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

- Security administrator
- Security reader

Q55) One of the developers needs API access to the "Dev" resource group. Which of the following roles do you need to assign to the developer?

- Owner role
- Contributor role
- ✅ API management contributor role

Explanation:-API management contributor role is correct, this also needs to be assigned on the resource group level. The developer should now be able to sign in via PowerShell. https://docs.microsoft.com/en-us/azure/api-management/api-management-faq

- Reader role
