Answer Sheet

Q1) You create an AAD conditional access policy that block the "Developers" group from accessing the Azure portal.

Another administrator configures an additional AAD conditional access policy that blocks the "Developers" group from accessing the Azure portal unless they supply MFA.

Correct/Incorrect: A user that is member of the "Developers" group attempts to access the Azure portal and is prompted for MFA before being allowed access.

✓ Incorrect
● Correct

Q2)

You are deploying VMs using JSON templates. You want to include enrolment into Azure Log Analytics as part of the deployment.

Which two parameters must you include in the JSON template?

● WorkspaceName
● WorkspaceURL
✓ WorkspaceID
Explanation:-WorkspaceID and WorkspaceKey must be included.
https://blogs.technet.microsoft.com/manageabilityguys/2015/11/19/enabling-the-microsoft-monitoring-agent-in-windows-json-templates/
● StarageAccountKey
✓ WorkspaceKey
Explanation:-WorkspaceID and WorkspaceKey must be included.
https://blogs.technet.microsoft.com/manageabilityguys/2015/11/19/enabling-the-microsoft-monitoring-agent-in-windows-json-templates/

Q3) Choose one correct answer to indicated the object for each of the listed RBAC assignment properties.

✓ Scope = Resource Group
Explanation:-Role Definition: [Owner]
Scope: [Resource group]
Security Principle: [Group]
● Role Definition = Domain Administrator
● Role Definition = Group
● Role Definition = Resource Group
✓ Role Definition = Owner
Explanation:-Role Definition: [Owner]
Scope: [Resource group]
Security Principle: [Group]
✓ Security Principle = Group
Explanation:-Role Definition: [Owner]
Scope: [Resource group]
Security Principle: [Group]

Q4)

You have a custom-written Web app and already-deployed Azure SQL Database. You are configuring security using Managed Service Identity (MSI).

Which of the following must you do? Each selection represents part of the solution.

● Create a client secret for the registered app
✓ Configure Active Directory admin in Azure SQL Database server
Explanation:-Create and configure Azure Key Vault - no, MSI doesn't use AKV.
Create a secret in AKV - no, MSI doesn't use AKV.
Create an app registration in Azure Active Directory - yes, you need to register the app in AAD in order to assign that identity to the SQL Database server.
Create a client secret for the registered app - no, they Web app code does not need the app registration secret; it uses the autentication library to get an access token.
Configure Active Directory admin in Azure SQL Database server - yes, this is where you assign the registered app (managed identity) access to the SQL Database server.
https://docs.microsoft.com/en-us/azure/app-service/app-service-web-tutorial-connect-msi
● Create and configure Azure Key Vault
● Create a secret in AKV
✓ Create an app registration in Azure Active Directory
Explanation:-Create and configure Azure Key Vault - no, MSI doesn't use AKV.
Create a secret in AKV - no, MSI doesn't use AKV.
Create an app registration in Azure Active Directory - yes, you need to register the app in AAD in order to assign that identity to the SQL Database server.
Create a client secret for the registered app - no, they Web app code does not need the app registration secret; it uses the autentication library to get an access token.
Configure Active Directory admin in Azure SQL Database server - yes, this is where you assign the registered app (managed identity) access to the SQL Database server.
https://docs.microsoft.com/en-us/azure/app-service/app-service-web-tutorial-connect-msi

Q5)

User1, User2 and User3 has the role of owner in a subscription.

You create an AAD PIM access review and specify the reviewers as "Members (self)".

For which users can User3 perform the access review?

● User1, User2 and User3
✓ User3 only
Explanation:-User3 only. The "Members (self)" reviewers asks members to only review their own access, not anyone else's.
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review?toc=%2fazure%2factive-directory%2fgovernance%2ftoc.json#create-one-or-more-access-reviews

---

Q6) Which of the following are valid Azure policy effects? (Choose 5)

✓ AuditIfNotExists
Explanation:-Valid policy efects are:
Deny (prevent deployment).
Audit (log if present / create warning if applicable).
AuditIfNotExists (list if not present).
DeployIfNotExists (deploy is not present).
Append (add this property to a new deployment).
✓ Audit
Explanation:-Valid policy efects are:
Deny (prevent deployment).
Audit (log if present / create warning if applicable).
AuditIfNotExists (list if not present).
DeployIfNotExists (deploy is not present).
Append (add this property to a new deployment).
✓ Append
Explanation:-Valid policy efects are:
Deny (prevent deployment).
Audit (log if present / create warning if applicable).
AuditIfNotExists (list if not present).
DeployIfNotExists (deploy is not present).
Append (add this property to a new deployment).
✓ DeployIfNotExists
Explanation:-Valid policy efects are:
Deny (prevent deployment).
Audit (log if present / create warning if applicable).
AuditIfNotExists (list if not present).
DeployIfNotExists (deploy is not present).
Append (add this property to a new deployment).
● Scope
✓ Deny
Explanation:-Valid policy efects are:
Deny (prevent deployment).
Audit (log if present / create warning if applicable).
AuditIfNotExists (list if not present).
DeployIfNotExists (deploy is not present).
Append (add this property to a new deployment).

Q7)

You successfully created a new information protection label in AIP, but the new label is not available to the targeted user.

Which of the following would make the label available to the user?

✓ Create a new AIP policy
Explanation:-Create a new AIP policy is the correct answer. You must make a newly created label part of an existing or new policy applied to the target user for the label to become available to the user.
● Reinstall Azure Information Protection Client
● Get the user to log out and back in
● Get the user to close and reopen the document

Q8)

User1 is assigned a AAD identity protection user risk policy and enabled for "medium and above" risk.

The user signs in from an anonymous IP. Is the policy applied to the user?

● No
✓ Yes
Explanation:-Yes. Login from anonymous IP is considered medium risk and therefore the policy applies.
All risks are medium except for leaked credentials which is high and malware infected device which is low.
https://docs.microsoft.com/en-za/azure/active-directory/reports-monitoring/concept-risk-events#risk-level
● Maybe
● It depends

Q9) A user is configured for MFA in the Azure portal.

The user has not been assigned a Azure AD Premium license, or any other license and is not an administrator.

There are no unassigned Azure AD Premium licenses available in the tenant.

The user attempts to log in to myapps.microsoft.com.

Which of the following happens?

● The user is prompted for MFA without charge and the subscription owner is notified of the license issue

✓ The user is prompted for MFA and the subscription where Azure AD is configured is charged using per-user consumption-based billing

Explanation:-The user is prompted for MFA and the subscription where Azure AD is configured is charged using per-user consumption-based billing.
If an unassigned license is available, the MFA will go through without charge (no notification)
There is no blocking the user or grace logins

● The user cannot log in

● The user is permitted to log in using username and password without MFA

● The user is prompted for MFA without charge for 10 logins, after which the user is blocked

---

Q10) Which of the following Azure resources allows the configuration of a resource firewall? (Choose 3)

● Azure Virtual Network

✓ Azure SQL Server

Explanation:-Azure Storage Account,
Azure SQL Database,
Azure SQL Server,
allows the configuration of a resource firewall - these resources has built-in firewall configuration settings.

✓ Azure SQL Database

Explanation:-Azure Storage Account,
Azure SQL Database,
Azure SQL Server,
allows the configuration of a resource firewall - these resources has built-in firewall configuration settings.

✓ Azure Storage Account

Explanation:-Azure Storage Account,
Azure SQL Database,
Azure SQL Server,
allows the configuration of a resource firewall - these resources has built-in firewall configuration settings.

● Azure Virtual Machine

● Azure Resource Group

Q11) You have the following built-in Azure policies applied.

Policy1: RG1: AllowedResourcesTypes: virtualMachines

Policy2: RG2: NotAllowedResourceTypes: virtualMachines

Policy3: RG3: NotAllowedResourceTypes: virtualNetworks/subnets

Which of the following actions can you perform?

● Add a subnet to RG3

✓ Add a VNet to RG3

Explanation:-Add a VM to RG1 [Yes] Allowed by Policy1.
Add a VNet to RG1 [No] Denied by Policy1. AllowedResourceTypes built-in policy denies deployment of all resources not selected in the Allowed Resource Types parameter.
Add a VM to RG2 [No] Denied by Policy2. NotAllowedResourceTypes allows any resource except those selected in the Not Allowed Resource Types parameter.
Add a VM to RG3 [Yes] VMs are not blocked by Policy3; only subnets are.
Add a VNet to RG3 [Yes] VNets aren't blocked by Policy3; only subnets are. The parent class of the subclass specified is not prevented by policy. In fact, part of a new VNet deployment is the deployment of a default subnet - this isn't blocked either... Go try it out - I'm telling you...
Add a subnet to RG3 [No] Denied by Policy3.
https://docs.microsoft.com/en-us/azure/governance/policy/samples/allowed-resource-types
https://docs.microsoft.com/en-us/azure/governance/policy/samples/not-allowed-resource-types

● Add a VM to RG2

✓ Add a VM to RG3

Explanation:-Add a VM to RG1 [Yes] Allowed by Policy1.
Add a VNet to RG1 [No] Denied by Policy1. AllowedResourceTypes built-in policy denies deployment of all resources not selected in the Allowed Resource Types parameter.
Add a VM to RG2 [No] Denied by Policy2. NotAllowedResourceTypes allows any resource except those selected in the Not Allowed Resource Types parameter.
Add a VM to RG3 [Yes] VMs are not blocked by Policy3; only subnets are.
Add a VNet to RG3 [Yes] VNets aren't blocked by Policy3; only subnets are. The parent class of the subclass specified is not prevented by policy. In fact, part of a new VNet deployment is the deployment of a default subnet - this isn't blocked either... Go try it out - I'm telling you...
Add a subnet to RG3 [No] Denied by Policy3.
https://docs.microsoft.com/en-us/azure/governance/policy/samples/allowed-resource-types
https://docs.microsoft.com/en-us/azure/governance/policy/samples/not-allowed-resource-types

● Add a VNet to RG1

✓ Add a VM to RG1

Explanation:-Add a VM to RG1 [Yes] Allowed by Policy1.
Add a VNet to RG1 [No] Denied by Policy1. AllowedResourceTypes built-in policy denies deployment of all resources not selected in the Allowed Resource Types parameter.
Add a VM to RG2 [No] Denied by Policy2. NotAllowedResourceTypes allows any resource except those selected in the Not Allowed Resource Types parameter.
Add a VM to RG3 [Yes] VMs are not blocked by Policy3; only subnets are.
Add a VNet to RG3 [Yes] VNets aren't blocked by Policy3; only subnets are. The parent class of the subclass specified is not prevented by policy. In fact, part of a new VNet deployment is the deployment of a default subnet - this isn't blocked either... Go try it out - I'm telling you...
Add a subnet to RG3 [No] Denied by Policy3.
https://docs.microsoft.com/en-us/azure/governance/policy/samples/allowed-resource-types
https://docs.microsoft.com/en-us/azure/governance/policy/samples/not-allowed-resource-types

Q12)

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

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

● Purge protection
● Soft-delete and purge protection
✓ Soft-delete
Explanation:-Soft-delete will allow recovery of accidentally deleted key vault items (or the key vault itself) for 90 days. However a malitious user might purge soft-deleted items which will prevent their recovery despite soft-delete being enabled.
https://docs.microsoft.com/en-za/azure/key-vault/key-vault-ovw-soft-delete
● Delete lock
● Read-only lock

Q13)

You have a legacy on-premises web application that isn't integrated with Azure AD. The on-premises environment is connected to the internet and your users want to use the application when they're away from the office.

You must ensure the identities of users of the application are secured using MFA. You have to minimise costs and administrative effort.

Each of the following options provide part of the solution and are not presented in order. Choose the best option in each of the listed items:

✓ Configuration: Configure Azure AD MFA
Explanation:-Migrate to IaaS or PaaS incurs additional costs (PaaS works with MFA).
Deploy on-premises MFA Server works with on-premises VPN solution. The application can also be integrated with this solution but would require application changes.
Azure Application Gateway (with WAF) is a good way to protect an Azure-deployed web application, but has nothing to do with MFA.
✓ Security: Don't deploy an on-premises security solution
Explanation:-Migrate to IaaS or PaaS incurs additional costs (PaaS works with MFA).
Deploy on-premises MFA Server works with on-premises VPN solution. The application can also be integrated with this solution but would require application changes.
Azure Application Gateway (with WAF) is a good way to protect an Azure-deployed web application, but has nothing to do with MFA.
✓ Connectivity: Deploy Azure AD Application Proxy
Explanation:-Migrate to IaaS or PaaS incurs additional costs (PaaS works with MFA).
Deploy on-premises MFA Server works with on-premises VPN solution. The application can also be integrated with this solution but would require application changes.
Azure Application Gateway (with WAF) is a good way to protect an Azure-deployed web application, but has nothing to do with MFA.
● Migration: Migrate the application to Azure IaaS
● Migration: Migrate the application to Azure PaaS
✓ Migration: Don't migrate the solution to Azure
Explanation:-Migrate to IaaS or PaaS incurs additional costs (PaaS works with MFA).
Deploy on-premises MFA Server works with on-premises VPN solution. The application can also be integrated with this solution but would require application changes.
Azure Application Gateway (with WAF) is a good way to protect an Azure-deployed web application, but has nothing to do with MFA.

Q14)

A user is registered with Azure AD MFA and have configured SMS text message as the authentication mode.

The user browses to myapps.microsoft.com and supplies his username and password.

What does the user have to do after the MFA message is received?

● Type the OTP and the user's MFA PIN into the browser page
● Reply to the text message with the user's MFA PIN
✓ Type the OTP into the browser page
Explanation:-Type the OTP into the browser page
Reply with # is used with phone call mode
Reply to text message with PIN is not a supported option
Type OTP and PIN into the browser is not a supported option
Reply with OTP (and optionally PIN) is supported with two-way SMS text mode but requires on-premises MFA server to be deployed
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods#text-message
● Reply to the text message with #

Q15)

You are configuring an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry.

You need to use the auto-generated service principal to authenticate to the Azure Container Registry.

What should you create?

● an Azure Active Directory (Azure AD) user
✓ an Azure Active Directory (Azure AD) role assignment
Explanation:-When you create an AKS cluster, Azure also creates a service principal to support cluster operability with other Azure resources. You can use this auto-generated service principal for authentication with an ACR registry. To do so, you need to create an Azure AD role assignment that grants the cluster's service principal access to the container registry.
● an Azure Active Directory (Azure AD) group
● a secret in Azure Key Vault

Q16)

You have an Azure virtual machine shown in the following table.

You create an Azure Log Analytics workspace named Analytics1 in RG1 in the East US region.

Which virtual machines can be enrolled in Analytics1?

✓ VM1 only
Explanation:-Create a workspace
In the Azure portal, click All services. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input. Select Log Analytics.
Click Create, and then select choices for the following items:
Provide a name for the new Log Analytics workspace, such as DefaultLAWorkspace. OMS workspaces are now referred to as Log Analytics workspaces.
Select a Subscription to link to by selecting from the drop-down list if the default selected is not appropriate.
For Resource Group, select an existing resource group that contains one or more Azure virtual machines.
Select the Location your VMs are deployed to. For additional information, see which regions Log Analytics is available in.
● VM1, VM2, and VM3 only
● VM1, VM2, VM3, and VM4
● VM1 and VM4 only

Q17)

You are testing an Azure Kubernetes Service (AKS) cluster. The cluster is configured as shown in the exhibit. (Click the Exhibit tab.)

You plan to deploy the cluster to production. You disable HTTP application routing.

You need to implement application routing that will provide reverse proxy and TLS termination for AKS services by using a single IP address.

What should you do?

● Install the container network interface (CNI) plug-in.
● Create an Azure Standard Load Balancer.
✓ Create an AKS Ingress controller.
Explanation:-An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services.
● Create an Azure Basic Load Balancer.

Q18)

You use Azure Security Center for the centralized policy management of three Azure subscriptions.

You use several policy definitions to manage the security of the subscriptions.

You need to deploy the policy definitions as a group to all three subscriptions.

Solution: You create a policy definition and assignments that are scoped to resource groups.

Does this meet the goal?

✓ Incorrect
● Correct

Q19)

You use Azure Security Center for the centralized policy management of three Azure subscriptions.

You use several policy definitions to manage the security of the subscriptions.

You need to deploy the policy definitions as a group to all three subscriptions.

Solution: You create a resource graph and an assignment that is scoped to a management group.

Does this meet the goal?

✓ Incorrect
● Correct

Q20)

You have an Azure Subscription. The subscription contains 50 virtual machines that run Windows Server 2012 R2 or Windows Server 2016.

You need to deploy Microsoft Antimalware to the virtual machines.

Solution: You add an extension to each virtual machine.

Does this meet the goal?

✓ Correct

Explanation:-You can use Visual Studio to enable and configure the Microsoft Antimalware service. This entails selecting Microsoft Antimalware extension from the dropdown list under Installed Extensions and click Add to configure with default antimalware configuration.

● Incorrect

Q21) You enable soft-delete and purge protection on your company's Azure Key Vault. A malicious user deletes your company's key vault thereby preventing decryption of most of your Azure data.

Correct or Incorrect: The malicious user - having the owner RBAC role at the subscription level removes the purge protection from the vault and purges (permanently deletes) the vault. You start looking for a new job...

● Correct

✓ Incorrect

Explanation:-Once purge protection is enabled for a vault, deleted items cannot be purged within 90 days of deletion regardless of RBAC role permissions.

https://docs.microsoft.com/en-za/azure/key-vault/key-vault-ovw-soft-delete#purge-protection

---

Q22) Correct or Incorrect: RBAC in Azure determines if a user is given access to a system when he/she provides his/her username and password.

● It depends

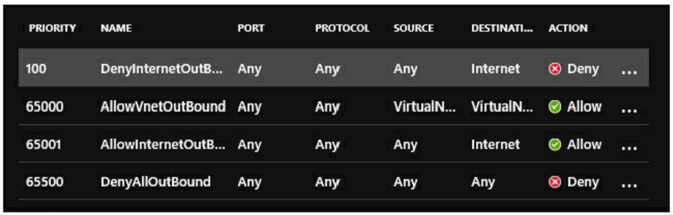
✓ Incorrect

Explanation:-RBAC is the authorisation (what can you access) model in Azure. Providing a username and password is part of authentication (prove who you are) model.

● Correct

Q23)

See the outbound NSG in the exhibit.



PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATI...	ACTION	
100	DenyInternetOutB...	Any	Any	Any	Internet	⊗ Deny	...
65000	AllowVnetOutBound	Any	Any	VirtualN...	VirtualN...	✓ Allow	...
65001	AllowInternetOutB...	Any	Any	Any	Internet	✓ Allow	...
65500	DenyAllOutBound	Any	Any	Any	Any	⊗ Deny	...

The NSG is assigned to a VM NIC.

Which of the following is true?

✓ The VM has connectivity to other VMs on the same Vnet

Explanation:-The VM has connectivity to the internet [No] Blocked by DenyInternetOutBound rule that has a higher (lower number) priority than AllowInternetOutBound default rule

The VM has connectivity to other VMs on the same subnet [Yes] Allowed by AllowVnetOutBound rule that has a higher priority (lower number) than DenyAllOutBound

The VM has connectivity to other VMs on the same Vnet [Yes] Allowed by AllowVnetOutBound rule that has a higher priority (lower number) than DenyAllOutBound

The VM can resolve DNS names [Yes] Allowed by AllowVnetOutBound rule that has a higher priority (lower number) than DenyAllOutBound Built-in DNS is hosted by the Vnet.

✓ The VM can resolve DNS names

Explanation:-The VM has connectivity to the internet [No] Blocked by DenyInternetOutBound rule that has a higher (lower number) priority than AllowInternetOutBound default rule

The VM has connectivity to other VMs on the same subnet [Yes] Allowed by AllowVnetOutBound rule that has a higher priority (lower number) than DenyAllOutBound

The VM has connectivity to other VMs on the same Vnet [Yes] Allowed by AllowVnetOutBound rule that has a higher priority (lower number) than DenyAllOutBound

The VM can resolve DNS names [Yes] Allowed by AllowVnetOutBound rule that has a higher priority (lower number) than DenyAllOutBound Built-in DNS is hosted by the Vnet.

● The VM has connectivity to the internet

✓ The VM has connectivity to other VMs on the same subnet

Explanation:-The VM has connectivity to the internet [No] Blocked by DenyInternetOutBound rule that has a higher (lower number) priority than AllowInternetOutBound default rule

The VM has connectivity to other VMs on the same subnet [Yes] Allowed by AllowVnetOutBound rule that has a higher priority (lower number) than DenyAllOutBound

The VM has connectivity to other VMs on the same Vnet [Yes] Allowed by AllowVnetOutBound rule that has a higher priority (lower number) than DenyAllOutBound

The VM can resolve DNS names [Yes] Allowed by AllowVnetOutBound rule that has a higher priority (lower number) than DenyAllOutBound Built-in DNS is hosted by the Vnet.

Q24)

Your company has an Azure subscription named Sub1 that is associated to an Azure Active Directory Azure (Azure AD) tenant named contoso.com.

The company develops a mobile application named App1. App1 uses the OAuth 2 implicit grant type to acquire Azure AD access tokens.

You need to register App1 in Azure AD.

What information should you obtain from the developer to register the application?

● a reply URL
✓ a redirect URI
Explanation:-For Native Applications you need to provide a Redirect URI, which Azure AD will use to return token responses.
● a key
● an application ID

Q25)

From the Azure portal, you are configuring an Azure policy.

You plan to assign policies that use the DeployIfNotExist, AuditIfNotExist, Append, and Deny effects.

Which effect requires a managed identity for the assignment?

● Append
✓ DeployIfNotExist
Explanation:-When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity.
● AuditIfNotExist
● Deny

Q26)

You have an Azure subscription that contains an Azure key vault named Vault1.

In Vault1, you create a secret named Secret1.

An application developer registers an application in Azure Active Directory (Azure AD).

You need to ensure that the application can use Secret1.

What should you do?

● In Azure Key Vault, create a key.
● In Azure Key Vault, create an access policy.
✓ In Azure AD, create a role.
Explanation:-Azure Key Vault provides a way to securely store credentials and other keys and secrets, but your code needs to authenticate to Key Vault to retrieve them. Managed identities for Azure resources overview makes solving this problem simpler, by giving Azure services an automatically managed identity in Azure Active Directory (Azure AD). You can use this identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without having any credentials in your code.
● In Azure AD, enable Azure AD Application Proxy.

Q27)

You have an Azure SQL database.

You implement Always Encrypted.

You need to ensure that application developers can retrieve and decrypt data in the database.

Which two pieces of information should you provide to the developers?

● user credentials
✓ the column master key
Explanation:-Always Encrypted uses two types of keys: column encryption keys and column master keys. A column encryption key is used to encrypt data in an encrypted column. A column master key is a key-protecting key that encrypts one or more column encryption keys.
● a stored access policy
● a shared access signature (SAS)
✓ the column encryption key
Explanation:-Always Encrypted uses two types of keys: column encryption keys and column master keys. A column encryption key is used to encrypt data in an encrypted column. A column master key is a key-protecting key that encrypts one or more column encryption keys.

Q28)

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

All users have computers that run Windows 10 and are hybrid Azure AD joined.

You have an Azure SQL database that is configured to support Azure AD authentication.

Database developers must connect to the SQL database by using Microsoft SQL Server Management Studio (SSMS) and authenticate by using their on-premises Active Directory account.

You need to tell the developers which authentication method to use to connect to the SQL database from SSMS. The solution must minimize authentication prompts.

Which authentication method should you instruct the developers to use?

● Active Directory – Universal with MFA support
✓ Active Directory – Integrated
Explanation:-
Azure AD can be the initial Azure AD managed domain. Azure AD can also be an on-premises Active Directory Domain Services that is federated with the Azure AD.

Using an Azure AD identity to connect using SSMS or SSDT

The following procedures show you how to connect to a SQL database with an Azure AD identity using SQL Server Management Studio or SQL Server Database Tools.

Active Directory integrated authentication

Use this method if you are logged in to Windows using your Azure Active Directory credentials from a federated domain.

1. Start Management Studio or Data Tools and in the Connect to Server (or Connect to Database Engine) dialog box, in the Authentication box, select Active Directory - Integrated. No password is needed or can be entered because your existing credentials will be presented for the connection.

2. Select the Options button, and on the Connection Properties page, in the Connect to database box, type the name of the user database you want to connect to. (The AD domain name or tenant ID" option is only supported for Universal with MFA connection options, otherwise it is greyed out.)

● Active Directory – Password
● SQL Login

Q29)

You have an Azure SQL Database server named SQL1.

You plan to turn on Advanced Threat Protection for SQL1 to detect all threat detection types.

Which action will Advanced Threat Protection detect as a threat?

● A user deletes more than 100 records from the same table.
● A user is added to the db_owner database role.
✓ A user attempts to sign as select * from table1.
Explanation:-Advanced Threat Protection can detect potential SQL injections: This alert is triggered when an active exploit happens against an identified application vulnerability to SQL injection. This means the attacker is trying to inject malicious SQL statements using the vulnerable application code or stored procedures.
● A user updates more than 50 percent of the records in a table.

Q30)

Your company uses Azure DevOps.

You need to recommend a method to validate whether the code meets the company's quality standards and code review standards.

What should you recommend implementing in Azure DevOps?

● branch permissions
✓ branch policies
Explanation:-Branch policies help teams protect their important branches of development. Policies enforce your team's code quality and change management standards.
● branch folders
● branch locking

Q31)

You have an Azure subscription that contains a virtual machine named VM1.

You create an Azure key vault that has the following configurations:

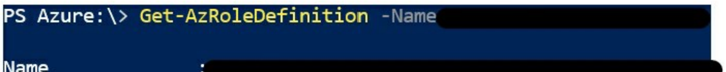
Name: Vault5
Region: West US
Resource group: RG1

You need to use Vault5 to enable Azure Disk Encryption on VM1. The solution must support backing up VM1 by using Azure Backup.
Which key vault settings should you configure?

● Keys
● Secrets
✓ Access policies
● Locks

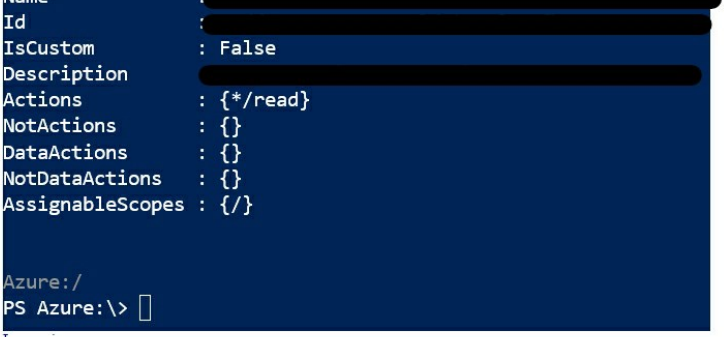
Q32)

See the PowerShell output in the exhibit



```
PS Azure:\> Get-AzRoleDefinition -Name [redacted]

Name             : [redacted]
```



```
Id               : [redacted]
IsCustom         : False
Description      [redacted]
Actions          : {*/read}
NotActions       : {}
DataActions      : {}
NotDataActions   : {}
AssignableScopes : {/}


Azure:/
PS Azure:\> 
```

What RBAC role is being represented here?

● Security Reader
● Owner
✓ Reader
Explanation:-This is the built-in reader role. You could create a custom role with the same permissions as Reader, but this is not the best answer for this simple question. Know the basic RBAC roles and their permission outputs from Get-AzRoleDefinition powershell.
● Contributor
● Read-only
● Custom role with read-only permissions

Q33)

You create a new Azure subscription and deploy a Windows VM. You want to query the event logs of the Azure VM using Azure Monitor.

Which of the following do you have to do. Each option represents part of the solution and is not in order.

✓ In the Log Analytics Workspace, connect the VM
Explanation:-Create a Log Analytics Workspace - yes
In the Log Analytics Workspace, connect the VM - yes
In Log Analytics Workspace, advanced settings, add Windows event logs - yes, select all the logs you want to transfer to the log analytics workspace
In Azure Monitor, Logs, run query - yes
In the VM, add the Log Analytics agent extension - no, this is done automatically when you connect the VM in Log Analytics Workspace
In Azure Monitor, connect the VM - no, this is not done in Azure Monitor for logs.
● In Azure Monitor, connect the VM
● In the VM, add the Log Analytics agent extension
✓ In Azure Monitor, Logs, run query
Explanation:-Create a Log Analytics Workspace - yes
In the Log Analytics Workspace, connect the VM - yes
In Log Analytics Workspace, advanced settings, add Windows event logs - yes, select all the logs you want to transfer to the log analytics workspace
In Azure Monitor, Logs, run query - yes
In the VM, add the Log Analytics agent extension - no, this is done automatically when you connect the VM in Log Analytics Workspace
In Azure Monitor, connect the VM - no, this is not done in Azure Monitor for logs.
✓ Create a Log Analytics Workspace
Explanation:-Create a Log Analytics Workspace - yes
In the Log Analytics Workspace, connect the VM - yes
In Log Analytics Workspace, advanced settings, add Windows event logs - yes, select all the logs you want to transfer to the log analytics workspace
In Azure Monitor, Logs, run query - yes
In the VM, add the Log Analytics agent extension - no, this is done automatically when you connect the VM in Log Analytics Workspace
In Azure Monitor, connect the VM - no, this is not done in Azure Monitor for logs.
✓ In Log Analytics Workspace, advanced settings, add Windows event logs
Explanation:-Create a Log Analytics Workspace - yes
In the Log Analytics Workspace, connect the VM - yes
In Log Analytics Workspace, advanced settings, add Windows event logs - yes, select all the logs you want to transfer to the log analytics workspace
In Azure Monitor, Logs, run query - yes
In the VM, add the Log Analytics agent extension - no, this is done automatically when you connect the VM in Log Analytics Workspace
In Azure Monitor, connect the VM - no, this is not done in Azure Monitor for logs.

Q34)

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?

● Audit logs are kept for the default of 90 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
● A retention period must be specified, in days up to a maximum of 3285 days
● Audit logs are kept for the default of 120 days

Q35)

You are planning on rolling out Privilege Identity Management (PIM) to the IT and Dev department.

Which of the following licenses should be assigned to your directory to enable this functionality? Select all that apply.

✓ Microsoft 365 M5

Explanation:-When you want to make use of PIM, you need one of the following trail or paid licenses assigned to your tenant: Azure AD P2, EMS E5 and Microsoft 365 M5. Azure AD P1 and EMS E3 does not support PIM functionality. https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/subscription-requirements

● EMS E3

✓ EMS E5

Explanation:-When you want to make use of PIM, you need one of the following trail or paid licenses assigned to your tenant: Azure AD P2, EMS E5 and Microsoft 365 M5. Azure AD P1 and EMS E3 does not support PIM functionality. https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/subscription-requirements

● Azure AD P1

✓ Azure AD P2

Explanation:-When you want to make use of PIM, you need one of the following trail or paid licenses assigned to your tenant: Azure AD P2, EMS E5 and Microsoft 365 M5. Azure AD P1 and EMS E3 does not support PIM functionality. https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/subscription-requirements

Q36) Correct or Incorrect: "When you use External Identities features to collaborate with guest users, you'll be automatically billed using the MAU model."

● Incorrect

✓ Correct

Explanation:-We can use use External Identities features to collaborate with guest users, you'll be automatically billed using the MAU model. Refer: https://docs.microsoft.com/en-us/azure/active-directory/external-identities/external-identities-pricing

Q37) Which of the following statements are true when transferring the subscription ownership to another user? Select all that apply.

● When transferring a subscription to another administrator will cause downtime

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

Explanation:-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 a new Azure AD tenant, all RBAC assignments are permanently deleted from the source tenant and not migrated to the target tenant

Explanation:-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

● The offer type can be changed during the transferring a subscription

Q38) Correct or Incorrect: The API management gateway IP address is constant and can be used in firewall rules as a static IP.

✓ Correct

Explanation:-True is correct, in all tiers of API management the public IP address of the API management tenant is static of the lifetime of the tenant, however there are some exceptions like if the service is deleted and re-created. https://docs.microsoft.com/en-us/azure/api-management/api-management-faq

● Incorrect