Answer Sheet

Q1) Which of the following are default rules created with a network security group?

✅ DenyAllInBound
Explanation:-AllowVnetInBound,
AllowAzureLoadBalancerInBound,
DenyAllInBound,
AllowVnetOutBound,
AllowInternetOutBound,
DenyAllOutBound,
Are the default rules in all NSGs
✅ DenyAllOutBound
⚪ DenyVnetInBound
⚪ DenyVnetOutBound

Q2) You must minimise costs. What is the minimum license required to configure Azure AD MFA?

⚪ Azure AD Premium P1
⚪ Azure AD Premium P2
⚪ No license is required
⚪ Any Office 365 license
✅ No license is required, but the user must be an Azure AD Global Administrator
Explanation:-No license is required, but the user must be an Azure AD Global Administrator
MFA is free if you are a AAD global administrator - reduced functionality
You get MFA for all users with any O365 subscription - reduced functionality
You get full-featured MFA with AAD P1
You get full-featured MFA with AAD P2 (all AAD P1 features is included in AAD P2)
You can configure MFA for any user with no licenses and your subscription will be charged on a per-user consumption-based model
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing

---

Q3) When configuring AAD conditional access policies, which of the following are mandatory requirements?

✅ User/group
Explanation:-User / group,
Cloud Apps,
Access controls,
All the others are optional.
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/app-based-mfa
✅ Cloud Apps
Explanation:-User / group,
Cloud Apps,
Access controls,
All the others are optional.
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/app-based-mfa
⚪ Device state
⚪ Location
⚪ Client apps
✅ Access controls
Explanation:-User / group,
Cloud Apps,
Access controls,
All the others are optional.
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/app-based-mfa

---

Q4) Which option in the exhibit would you choose to configure endpoint security?

⚪ Networking
⚪ Security
✅ Extensions
Explanation:-You must install the Microsoft Antimalware extension to enable endpoint security on the VM
⚪ Configuration
⚪ Identity
⚪ Locks

Q5) 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
How should the next hop in Workload-SN be configured as?

⚪ FW Public IP
⚪ FW Name
✅ FW Internal IP
Explanation:-https://docs.microsoft.com/en-gb/azure/firewall/tutorial-firewall-deploy-portal
⚪ Blank

Q6) 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 address prefix should you configure in Workload-SN?

- ✅ 0.0.0.0/0
- 255.255.255.255/255
- Blank
- FW Internal IP

Q7) 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 should you configure on Test-FW01?

- Network rule
- Route Table
- ✅ Application rule

Explanation:-What should you configure on Test-FW01 [Application rule] (for www.google.com) https://docs.microsoft.com/en-gb/azure/firewall/tutorial-firewall-deploy-portal

- Nothing

Q8) 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 should you configure on Test-FW01 to ensure successful DNS resolution from Workload-SN?

- ✅ Network rule

Explanation:-What should you configure on Test-FW01 to ensure successful DNS resolution from Workload-SN? [Network rule] (for destination port 53) https://docs.microsoft.com/en-gb/azure/firewall/tutorial-firewall-deploy-portal

- Route Table
- Application rule
- Nothing

Q9) You are configuring AIP policies. You specify two labels:
Label1: matches "Word1"
Label2: matches "Word2"
You create a document in MS Word that contains both words, which label is applied?

- Label1
- ✅ Label2

Explanation:-Label 2 is applied. AIP labels are applied in the order they are listed in the policy with the last matching label (or sublable) winning. Only one label is applied to the document. Only Office documents are supported.
https://docs.microsoft.com/en-us/azure/information-protection/faqs-infoprotect#can-a-file-have-more-than-one-classification

- Label1 and Label2
- No label

Q10) What tools are available to you for changing the key scenario in AIP (from Microsoft managed to BYOK for example)?

- Azure portal
- O365 management portal
- Security and Compliance Centre
- ✅ Windows PowerShell

Explanation:-Windows PowerShell is currently the only option for key management in AIP.

- Azure CLI

Q11) You must minimise costs. What is the minimum license required to configure Azure AD Conditional Access?

- ✅ Azure AD Premium P1

Explanation:-Azure AD Premium P1 is required to configure and use Conditional Access
Azure AD Premium P2 includes all the features of Azure Premium P1 (not minimum)
You cannot configure or use conditional access if you don't have at least AAD P1
Conditional access in not included in Azure AD for O365 - having an O365 license won't help
Being an Azure AD Global Administrator doesn't permit configuring AAD Conditional access, you must have an AAD P1 license at least.
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview#license-requirements

- Azure AD Premium P2
- No license is required
- Any Office 365 license
- No license is required, but the user must be an Azure AD Global Administrator

---

Q12) When configuring an privileged access review what are the three available settings when an assigned reviewer does not complete the review before the configured review ends?

- Do nothing
- ✅ Take recommendations

Explanation:-Do nothing - not an option
Take recommendations - use the PIM access review recommended action
Remove Access - revoke all access to the role
Approve Access - approve all existing access to the role
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review#upon-completion-settings

✅ Remove Access
Explanation:-Do nothing - not an option
Take recommendations - use the PIM access review recommended action
Remove Access - revoke all access to the role
Approve Access - approve all existing access to the role
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review#upon-completion-settings
✅ Approve Access
Explanation:-Do nothing - not an option
Take recommendations - use the PIM access review recommended action
Remove Access - revoke all access to the role
Approve Access - approve all existing access to the role
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review#upon-completion-settings
⚪ Prompt owner

Q13) When you configure Azure AD PIM for the first time, what are the three things you must do?

✅ Consent to PIM; verify your identity with MFA; sign-up PIM for AD roles
Explanation:-https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-discover-resources
⚪ Consent to PIM; verify your identity with MFA; discover AD roles; sign-up PIM for AD roles
⚪ Verify your identity with MFA; consent to PIM; discover AD roles; sign-up PIM for AD roles
⚪ Verify your identity with MFA; consent to PIM; sign-up PIM for AD roles

---

Q14) You deploy several VMs in Azure. You need to ensure that all the VMs have a consistent OS configuration including registry settings. Which of the following options would you configure?

⚪ ARM templates
✅ Desired State Configuration
Explanation:-Desired State Configuration (DSC) is used to ensure consistent VM deployment.
https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started
⚪ Application Security Groups
⚪ Device configuration policies

Q15) You're like the most awesome SQL DBA ever. You connect to your Azure SQL Database using SSMS and authenticate using the dialog as in the exhibit.
Which user account credentials do you supply?

⚪ Your Azure AD account credentials
✅ Your on-premises AD account credentials (your Windows workstation is joined to a different AD domain)
Explanation:-Your on-premises AD account credentials (your Windows workstation is joined to a different AD domain) - AD - Password. This is the correct answer.
Your Azure AD account credentials - Azure AD Universal.
The same user account you are signed-into your Windows workstation as - Windows Authentication.
Your on-premises AD account credentials (your Windows workstation is joined to the same AD domain) - AD - Integrated.
Your database user account - SQL Server Authentication.
https://docs.microsoft.com/en-us/sql/ssms/f1-help/connect-to-server-database-engine?view=sql-server-2017#options
⚪ The same user account you are signed-into your Windows workstation as
⚪ Your on-premises AD account credentials (your Windows workstation is joined to the same AD domain)
⚪ Your database user account

Q16) What are the three alert states in Azure Monitor?

✅ New
Explanation:-Alert states: New, Acknowledged, Closed are set by the user.
Alert conditions: Fired or Resolved (underlying condition that caused the alert has been resolved) are set by Azure Monitor.
Know the difference between alert states and alert conditions and who sets them (system or user).
⚪ Fired
⚪ Assigned
✅ Acknowledged
Explanation:-Alert states: New, Acknowledged, Closed are set by the user.
Alert conditions: Fired or Resolved (underlying condition that caused the alert has been resolved) are set by Azure Monitor.
Know the difference between alert states and alert conditions and who sets them (system or user).
⚪ Resolved
✅ Closed
Explanation:-Alert states: New, Acknowledged, Closed are set by the user.
Alert conditions: Fired or Resolved (underlying condition that caused the alert has been resolved) are set by Azure Monitor.
Know the difference between alert states and alert conditions and who sets them (system or user).

Q17) What are the four focus areas of Azure Security Center policy?

✅ Identity
Explanation:-VMs are included in Compute, Storage is included in data.
⚪ VMs
✅ Compute and apps
Explanation:-VMs are included in Compute, Storage is included in data.
⚪ Storage
✅ Data

Explanation:-VMs are included in Compute, Storage is included in data.

✅ Network

Explanation:-VMs are included in Compute, Storage is included in data.

Q18) What are the two Azure Monitor alert conditions?

- New
- ✅ Fired

Explanation:-Alert states: New, Acknowledged, Closed are set by the user
Alert conditions: Fired or Resolved (underlying condition that caused the alert has been resolved) are set by Azure Monitor

- Assigned
- Acknowledged
- ✅ Resolved

Explanation:-Alert states: New, Acknowledged, Closed are set by the user
Alert conditions: Fired or Resolved (underlying condition that caused the alert has been resolved) are set by Azure Monitor

- Closed

Q19) From what interface can you launch a previously-configured security playbook?

- Azure Security Center
- ✅ Security Alert

Explanation:-Playbooks can be launched from the investigation screen of a security alert or security incident in Azure Security Center

- Azure Monitor
- Azure Logic App

Q20) You are investigating and responding to incidents in Azure Security Center. You routinely use a playbook as part of the response procedure that sends an email to the security operations manager. The company has recently appointed an assistant security operations manager and she needs to be included as an email recipient when the playbook is fired. What tool would you use to make the change?

- Azure Monitor Action Group
- ✅ Azure Logic Apps Designer

Explanation:-https://docs.microsoft.com/en-us/azure/security-center/security-center-playbooks

- Azure Log Analytics Workspace
- Azure Subscription

Q21) What VM extension is loaded when you connect a VM Azure Security Center?

- Microsoft Antimalware
- ✅ Microsoft Monitoring Agent
- Microsoft Log Analytics Agent
- Microsoft Operations Management Suite (OMS)

Q22) What are the two fundamental types of data used by Azure Monitor?

- Azure audit data
- O365 audit data
- ✅ Metrics

Explanation:-Metrics and logs are the fundamental types of data used by Azure Monitor. These are generated by various Azure resources. correct story... :p

- Telemetry
- Subscription analytics
- ✅ Logs

Explanation:-Metrics and logs are the fundamental types of data used by Azure Monitor. These are generated by various Azure resources. correct story... :p

---

Q23) Which of the following will generate an alert from SQL ATP?

- A user updates more than half of the content of a table in a single procedure
- ✅ password' OR 1=1 entered into a password field

Explanation:-password' OR 1=1 entered into a password field is an attempt at SQL injection and SQL ATP will detect and alert on this. The following will also generate alerts:
Login from an unusual location or Azure region.
Login by an unfamiliar principle.
Access from a potentially harmful application.
Brute force attempt on SQL Authentication.
https://docs.microsoft.com/en-us/azure/sql-database/sql-database-threat-detection-overview#advanced-threat-protection-alerts

- A user is added to the db_owner database role
- A user deletes more than 50% of the content of a table in a single procedure

---

Q24) You need to ensure that data is secured in transit for a web application on your Azure subscription. Which of the following is required? Each answer is part of the solution and you have to minimise costs. Choose 4.

- ✅ Upload a certificate to Azure Key Vault

Explanation:-Upload a certificate to Azure Key Vault - yes, use key vault to store and secure the private key.
Obtain a custom domain name - yes, this is a prerequisite for obtaining a public certificate.

Purchase an app service certificate - yes, this is required to enable TLS for the app service.
Purchase a certificate from a CA - no, TLS certificates for Azure app service can be bought from the Azure portal.
Create a self-signed certificate - no, this is not supported with app service.
Create SSL bindings - yes, to ensure the all browser comms are encrypted to the web app.
Deploy Azure Application Gateway - no, this is not required to enable TLS, but you might want to deploy it to provide additional layer of security.
✅ Obtain a custom domain name
Explanation:-Upload a certificate to Azure Key Vault - yes, use key vault to store and secure the private key.
Obtain a custom domain name - yes, this is a prerequisite for obtaining a public certificate.
Purchase an app service certificate - yes, this is required to enable TLS for the app service.
Purchase a certificate from a CA - no, TLS certificates for Azure app service can be bought from the Azure portal.
Create a self-signed certificate - no, this is not supported with app service.
Create SSL bindings - yes, to ensure the all browser comms are encrypted to the web app.
Deploy Azure Application Gateway - no, this is not required to enable TLS, but you might want to deploy it to provide additional layer of security.
✅ Purchase an app service certificate
Explanation:-Upload a certificate to Azure Key Vault - yes, use key vault to store and secure the private key.
Obtain a custom domain name - yes, this is a prerequisite for obtaining a public certificate.
Purchase an app service certificate - yes, this is required to enable TLS for the app service.
Purchase a certificate from a CA - no, TLS certificates for Azure app service can be bought from the Azure portal.
Create a self-signed certificate - no, this is not supported with app service.
Create SSL bindings - yes, to ensure the all browser comms are encrypted to the web app.
Deploy Azure Application Gateway - no, this is not required to enable TLS, but you might want to deploy it to provide additional layer of security.
⚪ Create a self-signed certificate
✅ Create SSL bindings
Explanation:-Upload a certificate to Azure Key Vault - yes, use key vault to store and secure the private key.
Obtain a custom domain name - yes, this is a prerequisite for obtaining a public certificate.
Purchase an app service certificate - yes, this is required to enable TLS for the app service.
Purchase a certificate from a CA - no, TLS certificates for Azure app service can be bought from the Azure portal.
Create a self-signed certificate - no, this is not supported with app service.
Create SSL bindings - yes, to ensure the all browser comms are encrypted to the web app.
Deploy Azure Application Gateway - no, this is not required to enable TLS, but you might want to deploy it to provide additional layer of security.
⚪ Deploy Azure Application Gateway

Q25) Your organisation has a new regulatory requirement that all cloud VM deployments must meet the Center for Internet Security Hardened Benchmarks. How can you ensure that this requirement is met while minimising costs, downtime and administrative effort? Each option represents part of the solution and is not listed in order. Select each of the options that you should do.

⚪ Assign a built-in Azure Policy
✅ Choose a CIS VM image when creating new VMs
Explanation:-Assign a built-in Azure Policy - no.
Choose a CIS VM image when creating new VMs - yes.
Download CIS-compliant VM images from www.cisecurity.org - no, they're avaialble from the Azure marketplace directly.
Assign a custom Azure Policy - yes, there are ones on GitHub.
Review compliance against Azure Policy - yes, newly created VMs will only pass validation if the correct image is chosen; existing VMs will be reported on as being non-compliant.
Redeploy non-compliant VMs - yes, to meet the regulatory requirement you will have to redeploy non-compliant VMs over time.
Create a separate compliance Resource Group - no, not needed for the solution. The policy can be assigned at the management group, subscription or resource group scope level.
Create an application security group - no, not relevant to this solution.
✅ Assign a custom Azure Policy
Explanation:-Assign a built-in Azure Policy - no.
Choose a CIS VM image when creating new VMs - yes.
Download CIS-compliant VM images from www.cisecurity.org - no, they're avaialble from the Azure marketplace directly.
Assign a custom Azure Policy - yes, there are ones on GitHub.
Review compliance against Azure Policy - yes, newly created VMs will only pass validation if the correct image is chosen; existing VMs will be reported on as being non-compliant.
Redeploy non-compliant VMs - yes, to meet the regulatory requirement you will have to redeploy non-compliant VMs over time.
Create a separate compliance Resource Group - no, not needed for the solution. The policy can be assigned at the management group, subscription or resource group scope level.
Create an application security group - no, not relevant to this solution.
✅ Review compliance against Azure Policy
Explanation:-Assign a built-in Azure Policy - no.
Choose a CIS VM image when creating new VMs - yes.
Download CIS-compliant VM images from www.cisecurity.org - no, they're avaialble from the Azure marketplace directly.
Assign a custom Azure Policy - yes, there are ones on GitHub.
Review compliance against Azure Policy - yes, newly created VMs will only pass validation if the correct image is chosen; existing VMs will be reported on as being non-compliant.
Redeploy non-compliant VMs - yes, to meet the regulatory requirement you will have to redeploy non-compliant VMs over time.
Create a separate compliance Resource Group - no, not needed for the solution. The policy can be assigned at the management group, subscription or resource group scope level.
Create an application security group - no, not relevant to this solution.
✅ Redeploy non-compliant VMs
Explanation:-Assign a built-in Azure Policy - no.
Choose a CIS VM image when creating new VMs - yes.
Download CIS-compliant VM images from www.cisecurity.org - no, they're avaialble from the Azure marketplace directly.
Assign a custom Azure Policy - yes, there are ones on GitHub.
Review compliance against Azure Policy - yes, newly created VMs will only pass validation if the correct image is chosen; existing VMs will be reported on as being non-compliant.
Redeploy non-compliant VMs - yes, to meet the regulatory requirement you will have to redeploy non-compliant VMs over time.
Create a separate compliance Resource Group - no, not needed for the solution. The policy can be assigned at the management group, subscription

or resource group scope level.
Create an application security group - no, not relevant to this solution.
- Create a separate compliance Resource Group

Q26) You create an Azure Policy assignment as in the exhibit.
For each of the following, select all the statements which are correct.

- ✅ Creating new non-compliant resources are blocked

Explanation:-Creating new non-compliant resources are blocked - correct (fails validation).
Creating new non-compliant resources are allowed but generates a validation warning - incorrect (blocked by failing validation).
Creating new non-compliant resources are allowed but requires Owner RBAC role on the resource containter (resource group) - incorrect (policy block cannot be overridden during resource creatin regardless of RBAC role).
Non-compliant resources are reported on the Azure Policy compliance blade - correct.
Non-compliant resources are stopped - incorrect.
Non-compliant resources are deleted - incorrect.

- Creating new non-compliant resources are allowed but generates a validation warning
- Creating new non-compliant resources are allowed but requires Owner RBAC role on the resource containter (resource group)
- ✅ Non-compliant resources are reported on the Azure Policy compliance blade

Explanation:-Creating new non-compliant resources are blocked - correct (fails validation).
Creating new non-compliant resources are allowed but generates a validation warning - incorrect (blocked by failing validation).
Creating new non-compliant resources are allowed but requires Owner RBAC role on the resource containter (resource group) - incorrect (policy block cannot be overridden during resource creatin regardless of RBAC role).
Non-compliant resources are reported on the Azure Policy compliance blade - correct.
Non-compliant resources are stopped - incorrect.
Non-compliant resources are deleted - incorrect.

- Non-compliant resources are stopped
- Non-compliant resources are deleted

Q27) What standard is used for 3rd-party MFA hardware token authentication?

- ✅ OATH

Explanation:-OATH is the supported standard for Azure MFA authentication tokens
OAuth is the authorisation protocol used by AAD
AD Connect is the synchronisation tool used between AD and AAD
OpenID Connect is the standard built on top of OAuth for authentication
JSON WebToken (JWT) is the standard used by OpenID Connect to exchange authentication information
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods#oath-hardware-tokens-public-preview

- OAuth
- AD Connect
- OpenID Connect
- JSON Web Token (JWT)

Q28) 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.

- correct
- ✅ incorrect

Explanation:-incorrect! The user is blocked. The most restrictive policy applies when overlapping policies are put in place.
Block unless MFA is supplied is actually called Grant access, but require MFA in the configuration.
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/best-practices#what-happens-if-i-have-multiple-policies-for-the-same-user-configured

---

Q29) 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?

- 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/

- 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/

Q30) Choose one correct answer to indicated the object for each of the listed RBAC assignment properties.

- Role Definition = Resource Group
- ✅ Role Definition = Owner

Explanation:-Role Definition: [Owner]
Scope: [Resource group]
Security Principle: [Group]

- ✅ Scope = Resource Group

Explanation:-Role Definition: [Owner]

Scope: [Resource group]
Security Principle: [Group]
- Security Principle = Owner
- ✅ Security Principle = Group

Explanation:-Role Definition: [Owner]
Scope: [Resource group]
Security Principle: [Group]
- Security Principle = Subscription

Q31) 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 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

- 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

---

Q32) Having which two of these roles will allow you to create a custom RBAC role?

- ✅ Owner

Explanation:-Owner,
User Access Administrator,
is required to create custom RBAC roles
Security Admin only has "Microsoft.Authorization/*/read" and needs "Microsoft.Authorization/*"
Contributor has "Microsoft.Authorization/*/Write" as one of the NotActions, so cannot create custom RBAC roles
User Administrator is not an RBAC role, but rather an AAD role that is not relevant to Azure resource RBAC

- Contributor
- ✅ User Access Administrator

Explanation:-Owner,
User Access Administrator,
is required to create custom RBAC roles
Security Admin only has "Microsoft.Authorization/*/read" and needs "Microsoft.Authorization/*"
Contributor has "Microsoft.Authorization/*/Write" as one of the NotActions, so cannot create custom RBAC roles
User Administrator is not an RBAC role, but rather an AAD role that is not relevant to Azure resource RBAC

- Security Admin
- User Administrator

Q33) Which of the following describes credential stuffing?

- An attacker attempts to crack a password using every possible character combination
- An attacker uses a database of pre-calculated password hashes against a security accounts database
- An attacker attempts to replay intercepted authentication traffic
- ✅ An attacker uses a database of breached credentials against public web services

Explanation:-Credential stuffing is when an attacker uses a database of breached credentials (usernames with passwords) against public web services in an attempt to access confidential information.
An attacker attempts to crack a password using every possible character combination. This is called brute force.
An attacker uses a database of pre-calculated password hashes against a security accounts database. This is called a rainbow-table attack.
An attacker attempts to replay intercepted authentication traffic. This is called pass-the-hash attack.
Credential stuffing is one of the attacks that is detected by AAD identity protection.
https://docs.microsoft.com/en-za/azure/active-directory/reports-monitoring/concept-risk-events#leaked-credentials

---

Q34) 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

Q35) Which of the following is possible if a user has been granted the Contributor role for a specific virtual machine in Azure?

- ✅ Delete the virtual machine

Explanation:-RDP to the virtual machine is not part of the privileges assigned as part of RBAC. You need the local Administrator username and password or if the VM is part of an ADDS domain, you need a user account that has been given remote access privileges like AD Global Domain Administrator. You must be owner or user access administrator to manipulate VM locks.

- ✅ Stop the virtual machine

Explanation:-RDP to the virtual machine is not part of the privileges assigned as part of RBAC. You need the local Administrator username and password or if the VM is part of an ADDS domain, you need a user account that has been given remote access privileges like AD Global Domain Administrator. You must be owner or user access administrator to manipulate VM locks.

- ✅ Change the virtual machine size

Explanation:-RDP to the virtual machine is not part of the privileges assigned as part of RBAC. You need the local Administrator username and password or if the VM is part of an ADDS domain, you need a user account that has been given remote access privileges like AD Global Domain Administrator. You must be owner or user access administrator to manipulate VM locks.

- RDP to the virtual machine
- Create a lock on the virtual machine

Q36) A certain user is in scope for the global information protection policy in AIP as well as for a number of other policies. These policies have conflicting settings. Which settings are effectively applied to the user?

- The most restrictive policy
- The least restrictive policy
- ✅ The last policy on the list

Explanation:-Policies are applied sequentially starting with the global policy and then in order of how they appear on AIP. The last policy on the list is the effective policy.

- The first policy on the list

Q37) You have Azure Key Vault deployed and want to delegate administrative access. What should you do ?

- ✅ Set key vault policy: RBAC

Explanation:-https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault

- Set key vault policy: Key Vault access policy
- Add and delete certificates: RBAC
- ✅ Add and delete certificates: Key Vault access policy

Explanation:-https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault

Q38) Using a connection string containing the access key in an application configuration filr to access an Azure storage account is considered insecure. Microsoft recommends to use Azure Key vault to store the connection string for use with the applicaiton. How does Azure Key vault ensure that only authorised accounts get to access the connection string? Each answer is part of the solution.

- Built-in firewall
- ✅ Azure AD App registration

Explanation:-Azure AD App registration and Azure RBAC is used by Key Vault to only provide the secured connection string to a registered and authorised app in Azure AD via Azure RBAC assignment to the secret.

- ✅ Azure RBAC

Explanation:-Azure AD App registration and Azure RBAC is used by Key Vault to only provide the secured connection string to a registered and authorised app in Azure AD via Azure RBAC assignment to the secret.

- Network Security Group
- Azure Application Gateway with Web Application Firewall

Q39) By default, Azure storage accounts are exposed to the internet and allow access to anyone with the storage account key, a shared access signature or the appropriate Azure RBAC permissions.
You want to remove this default internet access and only allow trusted Microsoft services to access the storage account. Which option on the Exhibit would you choose to accomplish your task?

- Access control (IAM)
- Access keys
- Configuration
- Shared access signature
- ✅ Firewalls and virtual networks

Explanation:-https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?toc=%2fazure%2fstorage%2fblobs%2ftoc.json#grant-access-from-a-virtual-network

- Locks

Q40) Which of the following are valid Azure policy effects? Choose 5.

- ✅ 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).

- ✅ 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).
✅ 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).
✅ 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).
⚪ DeleteIfNotComply
✅ 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).

Q41) What users or groups does the AIP global policy apply to?

⚪ Azure AD Global Admins
⚪ Azure RBAC Owners
✅ Everyone in the organisation
⚪ All users and/or groups configured in the AIP global policy

---

Q42) 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?

⚪ Reinstall Azure Information Protection Client
⚪ Get the user to log out and back in
⚪ Get the user to close and reopen the document
✅ 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.

Q43) 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?

✅ 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
⚪ No
⚪ Maybe
⚪ It depends

**Q44) 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 cannot log in
⚪ The user is permitted to log in using username and password without MFA
✅ 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 is prompted for MFA without charge and the subscription owner is notified of the license issue
⚪ The user is prompted for MFA without charge for 10 logins, after which the user is blocked

---

Q45) Which of the following Azure resources allows the configuration of a resource firewall? Choose 3.

⚪ Azure Virtual Machine
✅ 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 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 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 Virtual Network
- Azure Resource Group

Q46) 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 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

- Add a VNet to RG1
- 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 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 subnet to RG3

Q47) 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?

✅ 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

- Purge protection
- Soft-delete and purge protection
- Delete lock
- Read-only lock

Q48) Where would you configure a custom condition in AIP?

✅ Azure Information Protection Label

Explanation:-Conditions are configured as part of the Label configuration, but must be made part of an existing or new policy to become available to

users.
- Azure Information Protection Policy
- Azure Information Protection Client
- Azure Active Directory

Q49) How long is metrics data stored for?

- 90 days
- ✅ 93 days

Explanation:-https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-platform-metrics#retention-of-metrics

- 60 days
- 120 days
- 30 days

Q50) 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?

- Reply to the text message with #
- 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

- Type the OTP and the user's MFA PIN into the browser page

Q51) Which three of the following features are not included in MFA for O365 license?

- Phone call as second factor
- ✅ On-premises MFA server

Explanation:-PIN mode, fraud alert and OPE MFA are not provided with the reduced functionality of MFA in O365
Full-featured MFA is available as part of AAD P1
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing#feature-comparison-of-versions

- ✅ PIN mode

Explanation:-PIN mode, fraud alert and OPE MFA are not provided with the reduced functionality of MFA in O365
Full-featured MFA is available as part of AAD P1
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing#feature-comparison-of-versions

- ✅ Fraud alert

Explanation:-PIN mode, fraud alert and OPE MFA are not provided with the reduced functionality of MFA in O365
Full-featured MFA is available as part of AAD P1
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing#feature-comparison-of-versions

- Mobile app as second factor
- SMS as second factor

Q52) You are configuring Azure Policy. Which one of the following policy effects requires you to assign a managed identity for the assignment?

- Append
- Audit
- AuditIfNotExists
- Deny
- ✅ DeployIfNotExists

Explanation:-DeployIfNotExists requires a managed identity to be provided to deploy resources on behalf of the policy. The policy assignment will automatically create the managed identity and assign the appropriate RBAC roles.
https://docs.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources#how-remediation-security-works

- Disabled

Q53) 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/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:-incorrect. 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

---

Q54) How many keys are required as part of an Azure SQL Database AlwaysEncrypted architecture?

- 1
- ✅ 2

Explanation:-2 keys are involved. The Column Master Key (CMK) and the Column Encryption Key (CEK).
https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine?view=sql-server-2017#how-it-

works
- 3
- 4
- Unlimited

Q55) Correct/Incorrect: RBAC in Azure determines if a user is given access to a system when he/she provides his/her username and password.

- correct
- ✅ incorrect

Explanation:-incorrect
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.

- It depends

Q56) See the outbound NSG in the exhibit.
The NSG is assigned to a VM NIC.
Which of the following is correct?

- 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.

- ✅ 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 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.

Q57) See the PowerShell output in the exhibit.
What RBAC role is being represented here?

- Contributor
- ✅ 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.

- Owner
- Security Reader
- Read-only
- Custom role with read-only permissions

Q58) 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 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.

- ✅ 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 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.

- In the VM, add the Log Analytics agent extension
- ✅ 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