Answer Sheet

Q1) See the structure in the exhibit.
The following assignements are made:
Service principle / Scope / Role definition
- User1 / ITSub / Reader
- User1 / ITServersRg / Contributor
- User1 / DefaultMg1 / Reader
What is the effective role definition for User1 at the following scopes:

✓ MarketingServer1: Reader

Explanation:-Role assignments are inherited by the child objects of the scope.
Role assignments are cumulative on overlap.

● MarketingServer1: Contributor

● MarketingServer1: None

✓ ITKv1: Reader

Explanation:-Role assignments are inherited by the child objects of the scope.
Role assignments are cumulative on overlap.

✓ MarketingSub: Reader

Explanation:-Role assignments are inherited by the child objects of the scope.
Role assignments are cumulative on overlap.

✓ LabServer2: Contributor

Explanation:-Role assignments are inherited by the child objects of the scope.
Role assignments are cumulative on overlap.

Q2) Which two of the following options are not valid exclusion assignments when creating an Azure policy assignment?

● Resource group

● Resource

✓ Initiative

Explanation:-Policy scope exclusions allow Management group, Subscription, Resource group and Resource selection

● Subscription

✓ Tenant

Explanation:-Policy scope exclusions allow Management group, Subscription, Resource group and Resource selection

● Management group

Q3) Which of the following can be used to create a custom RBAC role in Azure?

● Azure CLI

● Azure Portal

● Azure PowerShell

● Azure Cloud Shell

● REST API

✓ All of these

Explanation:-You can create custom RBAC roles via Azure CLI, Powershell, Cloudshell and one feature that was added recently is that you can now create custom RBAC roles via the Azure portal.
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal

---

Q4) You have to ensure the principle of least privilege. Which Azure RBAC role is required to configure a lock on an Azure resource?

● Owner

● Contributor

✓ User Access Administrator

Explanation:-Only User Access Administrator and Owner has the RBAC permissions to create or delete resource locks. Lease privilege means you need to assign the fewest permissions to accomplish the task. Expect to see a focus on this principle throughout the exam. Know the difference between Azure AD roles and Azure resource (RBAC) roles. Azure AD roles allow you different permissions (AKA rights) to administer Azure identities. Azure resource roles allow you different permissions mainly for managing the configuration of Azure resources. There are roles with similar names in each category - User administrator (Azure AD) and User access administrator (Azure RBAC).
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources#who-can-create-or-delete-locks

● User Administrator

● Security Administrator

Q5) Which option in the exhibit would you choose to configure VM hardening?

● Networking

✓ Security

Explanation:-Security shows the VM hardening recommendations from Azure Security Center. VM hardening is not just one thing, but a collection of best practices as included in ASC policy. The security blade of a VM shows the ASC recommendations filtered for just the VM you are looking at.

● Extensions

● Configuration

● Identity

● Locks

Q6) When assigning an Azure policy, when is it necessary to assign a managed identity?

● When the policy is assigned to a management group and will have effect on multiple subscriptions

● For any security policy

✓ For any policy that includes the DeployIfNotExists policy action

Explanation:-Permission to deploy resources into the subscription must have a managed identity to deploy resources.

● For any policy that includes any policy action

● All policies require a managed identity assigned in order to assess (read) the Azure resources to be assessed

---

Q7) Which three of the following options are valid scope assignments when creating an Azure policy assignment?

✓ Resource group

Explanation:-Policies can be scoped to the management group, subscription and optionally the resource group level and will be applied to all resources within the scope.
You can perform a policy assignment or initiative assignment (multiple policies at the same time) at the selected scope.
You can also assign policies or initiatives to hierarchical management groups which are groups of subscriptions. The assignment is inherited by all child objects.

● Resource

● Initiative

✓ Subscription

Explanation:-Policies can be scoped to the management group, subscription and optionally the resource group level and will be applied to all resources within the scope.
You can perform a policy assignment or initiative assignment (multiple policies at the same time) at the selected scope.
You can also assign policies or initiatives to hierarchical management groups which are groups of subscriptions. The assignment is inherited by all child objects.

● Tenant

✓ Management group

Explanation:-Policies can be scoped to the management group, subscription and optionally the resource group level and will be applied to all resources within the scope.
You can perform a policy assignment or initiative assignment (multiple policies at the same time) at the selected scope.
You can also assign policies or initiatives to hierarchical management groups which are groups of subscriptions. The assignment is inherited by all child objects.

Q8) You create an Azure Policy assignment to a subscription. Which two of the following are valid scope exclusions?

✓ Resource group

Explanation:-Resource group and resource are valid exclusion scopes if the policy assignment scope is at the subscription level. If you had scoped the assignment to a management group, you could select individual subscriptions within that management group as exclusions, in addition to child resource groups and resources.

✓ Resource

Explanation:-Resource group and resource are valid exclusion scopes if the policy assignment scope is at the subscription level. If you had scoped the assignment to a management group, you could select individual subscriptions within that management group as exclusions, in addition to child resource groups and resources.

● Initiative

● Subscription

● Tenant

● Management group

Q9) You are creating a custom RBAC role and want to restrict all but a few allowable actions to the new role. What section of the role definition JSON file do you configure?

✓ Actions

Explanation:-You will configure the allowable actions in the Actions section of the file. Configuring items in allowable excludes everything not listed. Configuring items in NotActions only prevents the listed items.

● NotActions

● DataActions

● NotDataActions

● AssignableScopes

Q10) You want to ensure the use of trusted container images in your organisation. Which two of the following options should you choose?

● Docker hub

✓ Azure container registry

Explanation:-Azure container registry and Docker trusted registry are ways to ensure the use of trusted container images

✓ Docker trusted registry

Explanation:-Azure container registry and Docker trusted registry are ways to ensure the use of trusted container images

● Azure container instances

● Azure Kubernetes Service

● Azure Key Vault

Q11) You are configuring Azure Update Management. You onboarded several VMs that have been deployed to different resource groups and regions. You have configured the following update deployments:
- Item1: VM1, EastUS, RG1, Windows 2008R2
- Item2: VM2, WestUS, RG2, CentOS 6
You want to add additional VMs to the update deployments. Which of the following can you do?

✓ Add VM3, EastUS, RG2, Windows 2016 to Item1

Explanation:-A favourite trope of the exam - knowing the limitations of adding instances with different properties (region, resource group, OS, etc.)

to Azure services once you've already configured the service.

You can add any VM from and RG or Region to a Update Management deployment schedule as long as the new VM is also Windows or Linux respectively.

https://docs.microsoft.com/en-za/azure/automation/manage-update-multi#schedule-an-update-deployment

✓ Add VM4, WestEurope, RG1, Windows 2016 to Item1

Explanation:-A favourite trope of the exam - knowing the limitations of adding instances with different properties (region, resource group, OS, etc.) to Azure services once you've already configured the service.

You can add any VM from and RG or Region to a Update Management deployment schedule as long as the new VM is also Windows or Linux respectively.

https://docs.microsoft.com/en-za/azure/automation/manage-update-multi#schedule-an-update-deployment

● Add VM5, EastUS, RG1, CentOS 6 to Item1

✓ Add VM6, EastUS, RG2, CentOS 6 to Item2

Explanation:-A favourite trope of the exam - knowing the limitations of adding instances with different properties (region, resource group, OS, etc.) to Azure services once you've already configured the service.

You can add any VM from and RG or Region to a Update Management deployment schedule as long as the new VM is also Windows or Linux respectively.

https://docs.microsoft.com/en-za/azure/automation/manage-update-multi#schedule-an-update-deployment

---

Q12) You have the following resource groups containing the listed resources:
- RG1; VM1 (stopped)
- RG2; VM2 (stopped)
- RG3; VM3 (stopped)
You have locks configured as follows:
- Lock1; Read-only; RG1
- Lock2; Delete; RG1
- Lock3; Delete; RG2
- Lock4; Read-only; RG3
Which of the following actions can you perform?

● You can start VM1

✓ You can start VM2

Explanation:-You can start VM1 [No] Start is considered a change and is prevented by RO Lock1 inherited from RG1.

You can start VM2 [Yes] No-delete Lock3 inherited from RG2 does not prevent changes (including start/stop) to VM2.

You can delete VM1 [No] Delete is prevented by RO locks. RO Lock1 inherited from RG1 prevents delete. No-delete Lock2 inherited from RG1 also prevents delete.

You can delete VM2 [No] No-delete Lock3 inherited from RG2 prevents delete.

You can delete VM3 [No] Delete is prevented by RO locks. RO Lock4 inherited from RG3 prevents delete.

https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources

● You can delete VM1

● You can delete VM2

● You can delete VM3

Q13) You have an Azure container registry. You have users with these roles.
- User1: Contributor
- User2: Reader
- User3: AcrPush
- User4: AcrPull
Select what each user can do?

● User1 can sign an image

✓ User2 can pull an image

Explanation:-User1 can sign an image [No] Only AcrSign can do that, not even owner can.

User2 can pull an image [Yes]

User3 can pull an image [Yes] AcrPush can also pull.

User4 can pull an image [Yes] Obviously.

https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles

✓ User3 can pull an image

Explanation:-User1 can sign an image [No] Only AcrSign can do that, not even owner can.

User2 can pull an image [Yes]

User3 can pull an image [Yes] AcrPush can also pull.

User4 can pull an image [Yes] Obviously.

https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles

✓ User4 can pull an image

Explanation:-User1 can sign an image [No] Only AcrSign can do that, not even owner can.

User2 can pull an image [Yes]

User3 can pull an image [Yes] AcrPush can also pull.

User4 can pull an image [Yes] Obviously.

https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles

---

Q14) You have resources configured as in the exhibit.
You assign an Azure Policy to ITSub. Which of the following options are invalid for policy scope exclusions?

● LabServer1

✓ MarketingServer1

Explanation:-MarketingServer1, DefaultRg, ITSub, MarketingSub, DefaultMg1 are all invalid selections.

In this scenario you can only exclude LabServer1 and ITServersRg.

You can exclude any Management groups, subscriptions, resource groups or resources that are child objects of the selected scope object. You can not exclude the same object as the scope object and you cannot exclude any object that isn't a child object.

✓ DefaultRg

Explanation:-MarketingServer1, DefaultRg, ITSub, MarketingSub, DefaultMg1 are all invalid selections.

In this scenario you can only exclude LabServer1 and ITServersRg.

You can exclude any Management groups, subscriptions, resource groups or resources that are child objects of the selected scope object. You can not exclude the same object as the scope object and you cannot exclude any object that isn't a child object.

✓ ITSub

Explanation:-MarketingServer1, DefaultRg, ITSub, MarketingSub, DefaultMg1 are all invalid selections.

In this scenario you can only exclude LabServer1 and ITServersRg.

You can exclude any Management groups, subscriptions, resource groups or resources that are child objects of the selected scope object. You can not exclude the same object as the scope object and you cannot exclude any object that isn't a child object.

✓ MarketingSub

Explanation:-MarketingServer1, DefaultRg, ITSub, MarketingSub, DefaultMg1 are all invalid selections.

In this scenario you can only exclude LabServer1 and ITServersRg.

You can exclude any Management groups, subscriptions, resource groups or resources that are child objects of the selected scope object. You can not exclude the same object as the scope object and you cannot exclude any object that isn't a child object.

✓ DefaultMg1

Explanation:-MarketingServer1, DefaultRg, ITSub, MarketingSub, DefaultMg1 are all invalid selections.

In this scenario you can only exclude LabServer1 and ITServersRg.

You can exclude any Management groups, subscriptions, resource groups or resources that are child objects of the selected scope object. You can not exclude the same object as the scope object and you cannot exclude any object that isn't a child object.

Q15) When registering an app with Azure AD to use modern authentication, what three fields are configurable when first registering the app?

✓ Display name

Explanation:-Display name.

Supported account types (who can use this application - this AAD or others too).

Redirect URI (wat page to ask for after successful sign-in).

https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app

● App ID

● App Secret

✓ Supported account types

Explanation:-Display name.

Supported account types (who can use this application - this AAD or others too).

Redirect URI (wat page to ask for after successful sign-in).

https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app

✓ Redirect URI

Explanation:-Display name.

Supported account types (who can use this application - this AAD or others too).

Redirect URI (wat page to ask for after successful sign-in).

https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app

Q16) What are the four MFA modes?

✓ Phone call

Explanation:-Authentication modes, also known as authentication methods are all the second factors selectable in Azure MFA. There are more methods selectable when you use the on-premises Azure MFA server. Know the differences, especially the more obscure combinations when using on-premises MFA. Enabled, disabled and Enforced are the MFA states for each user - don't confuse terminology like modes and states like the question is trying to do.

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods

✓ SMS text message

Explanation:-Authentication modes, also known as authentication methods are all the second factors selectable in Azure MFA. There are more methods selectable when you use the on-premises Azure MFA server. Know the differences, especially the more obscure combinations when using on-premises MFA. Enabled, disabled and Enforced are the MFA states for each user - don't confuse terminology like modes and states like the question is trying to do.

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods

✓ MS Authenticator App

Explanation:-Authentication modes, also known as authentication methods are all the second factors selectable in Azure MFA. There are more methods selectable when you use the on-premises Azure MFA server. Know the differences, especially the more obscure combinations when using on-premises MFA. Enabled, disabled and Enforced are the MFA states for each user - don't confuse terminology like modes and states like the question is trying to do.

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods

● Google Authenticator App

✓ OATH token code

Explanation:-Authentication modes, also known as authentication methods are all the second factors selectable in Azure MFA. There are more methods selectable when you use the on-premises Azure MFA server. Know the differences, especially the more obscure combinations when using on-premises MFA. Enabled, disabled and Enforced are the MFA states for each user - don't confuse terminology like modes and states like the question is trying to do.

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods

● PKI Certificate

Q17) The exhibit shows the AAD conditional access configuration screen.
You're configuring conditional access that will require a user named Isabella to be required to undergo MFA by using the authenticator app only when accessing the Azure portal.

● Under Assignments select Users and Groups and select Global Administrator

✓ Under Assignments select Users and Groups and select Isabella

Explanation:-https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/app-based-mfa#create-your-conditional-access-policy

✓ Under Assignments select Cloud apps and select Microsoft Azure Management

Explanation:-https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/app-based-mfa#create-your-conditional-access-policy

✓ Under Access controls select Grant and check Require multi-factor authentication

Explanation:-https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/app-based-mfa#create-your-conditional-access-policy

● Under Access controls select Grant and check Notification through mobile app

● Under Access controls select Grant and check Text message to phone

Q18) A user is enrolled for MFA but loses his mobile device, but the company is not doing mobile device management. He gets a new mobile device with the same phone number. You must ensure that his lost device cannot be used to gain unwanted access to his account . Each option below represents part of the solution and are not in order. Select all options that you should perform:

● Revoke and reassign the user's AAD P2 license

● From MFA settings portal, choose service settings and disable "Allow users to remember multi-factor authentication on devices they trust"

● From MFA settings portal, choose user settings, enable "Require selected users to provide contact methods again"

✓ From MFA settings portal, choose user settings, enable "Delete all existing app passwords..."

Explanation:-Revoke and reassign the user's AAD P2 license
No - this will have no effect on the user's MFA settings or lost device
From MFA settings portal, choose service settings and disable "Allow users to remember multi-factor authentication on devices they trust"
No - this changes the setting for all users, you only want to change this for a specific user
From MFA settings portal, choose user settings, enable "Require selected users to provide contact methods again"
No - since the user has the same phone number, re-enrolment is not required
From MFA settings portal, choose user settings, enable "Delete all existing app passwords..."
Yes - this ensures that any apps on the user's mobile device that required an app password will no longer have access
From MFA settings portal, choose user settings, enable "Restore multi-factor authentication on all remembered devices"
Yes - this will revoke all remembered MFA on the user's devices, requiring MFA to be supplied again to get access
Disable and re-enable the user's user account
No - This will have no effect on the MFA settings for the user account
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted

✓ From MFA settings portal, choose user settings, enable "Restore multi-factor authentication on all remembered devices"

Explanation:-Revoke and reassign the user's AAD P2 license
No - this will have no effect on the user's MFA settings or lost device
From MFA settings portal, choose service settings and disable "Allow users to remember multi-factor authentication on devices they trust"
No - this changes the setting for all users, you only want to change this for a specific user
From MFA settings portal, choose user settings, enable "Require selected users to provide contact methods again"
No - since the user has the same phone number, re-enrolment is not required
From MFA settings portal, choose user settings, enable "Delete all existing app passwords..."
Yes - this ensures that any apps on the user's mobile device that required an app password will no longer have access
From MFA settings portal, choose user settings, enable "Restore multi-factor authentication on all remembered devices"
Yes - this will revoke all remembered MFA on the user's devices, requiring MFA to be supplied again to get access
Disable and re-enable the user's user account
No - This will have no effect on the MFA settings for the user account
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted

● Disable and re-enable the user's user account

Q19) When doing an app registration in Azure AD, which three of the following are options for application permission scopes (supported account types) can be assigned?

✓ Default Azure AD directory

Explanation:-https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app#register-a-new-application-using-the-azure-portal

✓ Any Azure AD directory

Explanation:-https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app#register-a-new-application-using-the-azure-portal

✓ Any Azure AD directory and Personal MS accounts

Explanation:-https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app#register-a-new-application-using-the-azure-portal

● Any Google account

● Any Facebook account

● Any federated B2B account

Q20) You have an existing dynamic group in AAD. You want the group to contain users and their devices. What should you configure?

● Create two membership rules that select the users and devices respectively

✓ Delete and recreate the group, manually add users and devices

Explanation:-This is a gotcha-question typical of recent MS exams... You must know the limitations of the features in Azure. Look out for less common usage scenarios.
You cannot have a dynamic group that contain both users and devices.
You cannot add dynamic groups to assigned groups.
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership

● Create a membership rule that selects the users. Manually add the devices to the group

● Create two dynamic groups, one for devices and one for users. Create an assigned group and add the two dynamic groups to it

● Create a membership rule that selects the devices. Manually add the users to the group

Q21) In OAuth 2.0 / OpenID Connect, what does the authentication provider return to the browser after a successful authentication?

● Certificate

✓ ID Token

Explanation:-ID Token in JSON Web Token (JWT) format

● Session Key

● Session Secret

● Azure Key Vault

Q22) Review the exhibit.
What option do you choose to configure MFA authentication methods?

● Overview

● Security

✓ Users

Explanation:-https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted#choose-verification-options

● Groups

● Identity Governance

● User settings

Q23) What VM extension is loaded when you connect a VM to Azure Log Analytics?

● Microsoft Antimalware

✓ Microsoft Monitoring Agent

● Microsoft Log Analytics Agent

● Microsoft Operations Management Suite (OMS)

Q24) What underlying resource does Azure Security Center use to enforce JIT VM Access?

● Azure Security Center Standard

● Azure Firewall

● Azure Active Directory

● Azure RBAC

✓ Network Security Group

Explanation:-Network Security Group associated with the VM NIC

● Application Security Group

Q25) What is the difference between OpenID Connect and OAuth 2.0?

● OAuth 2.0 is a protocol used for authentication

✓ OAuth 2.0 is a protocol used for authorisation

Explanation:-OAuth 2.0 is an industry-standard authorisation protocol. OpenID Connect is an authentication standard built on OAuth 2.0. The exam might sometimes explore the differences between authentication and authorisation by using the standard names instead of the terms.

● OAuth 2.0 is a protocol used for security assertion

✓ OpenID Connect is a protocol used for authentication

Explanation:-OAuth 2.0 is an industry-standard authorisation protocol. OpenID Connect is an authentication standard built on OAuth 2.0. The exam might sometimes explore the differences between authentication and authorisation by using the standard names instead of the terms.

● OAuth 2.0 is an extension of OpenID Connect

✓ OpenID Connect is an extension of OAuth 2.0

Explanation:-OAuth 2.0 is an industry-standard authorisation protocol. OpenID Connect is an authentication standard built on OAuth 2.0. The exam might sometimes explore the differences between authentication and authorisation by using the standard names instead of the terms.

Q26) When doing an app registration in Azure AD, what are two methods to ensure application security?

✓ Application Certificate

Explanation:-https://docs.microsoft.com/en-us/azure/healthcare-apis/register-confidential-azure-ad-client-app

● Application key

✓ Application secret

Explanation:-https://docs.microsoft.com/en-us/azure/healthcare-apis/register-confidential-azure-ad-client-app

● Azure Key Vault

● Azure Security Center

Q27) Correct/Incorrect: MFA can be implemented by requiring a primary "system access" username and password, and a secondary "application access" username and password.

● correct

✓ incorrect

Explanation:-MFA requires more than one factor of authentication at the same time
Something you know (password)
Something you have (token / device / certificate)
Something you are (biometrics)
Using two passwords is just using the same factor twice and is not considered correct MFA
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks

● Don't know

Q28) When a user is enabled for MFA in AAD, when would an app password be required?

● When the user doesn't have a license that enables MFA

● When the user is using an OS other than Windows

● When the user is using an Android-based mobile device

● When the user is using an IOS-based mobile device

● All of these

✓ None of these

Explanation:-A user will be required to have an app password for apps that don't support modern authentication like older versions of Office apps (Office 2010 or Office 2013) and native mail apps on mobile devices.
Modern Office apps for IOS and Android support modern authentication and don't need an app password.
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods#app-passwords

Q29) You create a dynmaic group with the following dynamic membership rule:
(user.surname -contains "SS") or (user.surname -match "*we")
Which of the following users will be in the dynamic group?

✓ Peter Bless

Explanation:-Peter Bless - yes, REGEX is not case sensitive and the surname contains "ss".
Simon BLESS - yes, REGEX is not case sensitive and the surname contains "SS".
Fargo Wells - no, the wildcard in "*we" must match at least one character.
Frank Lowe - yes, the surname ends with "we" and has preceeding characters.
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership#supported-values

✓ Simon BLESS

Explanation:-Peter Bless - yes, REGEX is not case sensitive and the surname contains "ss".
Simon BLESS - yes, REGEX is not case sensitive and the surname contains "SS".
Fargo Wells - no, the wildcard in "*we" must match at least one character.
Frank Lowe - yes, the surname ends with "we" and has preceeding characters.
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership#supported-values

● Fargo Wells

✓ Frank Lowe

Explanation:-Peter Bless - yes, REGEX is not case sensitive and the surname contains "ss".
Simon BLESS - yes, REGEX is not case sensitive and the surname contains "SS".
Fargo Wells - no, the wildcard in "*we" must match at least one character.
Frank Lowe - yes, the surname ends with "we" and has preceeding characters.
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership#supported-values

Q30) Which of these cannot be used to create AAD conditional access policies?

● Azure Portal

✓ Windows PowerShell

Explanation:-AAD conditional access policies can only be created using the Azure portal
https://feedback.azure.com/forums/169401-azure-active-directory/category/167259-conditional-access

✓ Azure Cloud Shell

Explanation:-AAD conditional access policies can only be created using the Azure portal
https://feedback.azure.com/forums/169401-azure-active-directory/category/167259-conditional-access

✓ PowerShell Core

Explanation:-AAD conditional access policies can only be created using the Azure portal
https://feedback.azure.com/forums/169401-azure-active-directory/category/167259-conditional-access

✓ Azure CLI

Explanation:-AAD conditional access policies can only be created using the Azure portal
https://feedback.azure.com/forums/169401-azure-active-directory/category/167259-conditional-access

✓ REST API

Explanation:-AAD conditional access policies can only be created using the Azure portal
https://feedback.azure.com/forums/169401-azure-active-directory/category/167259-conditional-access

Q31) What is the minimum license that is required to configure AAD Identity Protection?

● Azure AD Premium P1

✓ Azure AD Premium P2

Explanation:-Azure AD Premium P2
No other license option provides AAD Identity Protection
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview#license-requirements

● No license is required

● Any Office 365 license

● No license is required, but the user must be an Azure AD Global Administrator

Q32) You have to follow the principle of least privilege. What role do you need to enable PIM for your organisation?

✓ Global Administrator

Explanation:-Global administrator is required to opt-in to PIM for the first time.
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-getting-started

● User Administrator

● Security Administrator

● User Access Administrator

● Owner (Subscription)

Q33) You have assigned Azure AD P1 licenses and have enabled MFA for all your users. Your corporate security policy requires you to ensure that users get prompted for MFA when they access any Microsoft cloud app. How do you configure Azure AD conditional access to achieve your objective?

● Create a conditional access policy, choose all users, choose all cloud apps, choose grant access and require MFA, enable policy

✓ Don't create a conditional access policy

Explanation:-Don't create a conditional access policy

By default, when users are enabled for MFA they will get prompted to provide MFA whenever they log in to any cloud application that uses Azure AD for authentication.

Create a conditional access policy, choose all users, choose all cloud apps, choose grant access and require MFA, enable policy

This is also correct, but not required. You may want to do this if you want to exclude certain users from requiring MFA or would like to create an emergency-use "Bypass MFA" group.

You can select specific cloud apps as part of the policy, but there is no "Microsoft apps" selection.

You cannot alter a conditional access baseline policy, only enable or disable it.

● Create a conditional access policy, choose all users, select all Microsoft apps, choose grant access and require MFA, enable policy

● Choose the end-user protection baseline policy, choose all cloud apps, choose grant access and require MFA, enable policy

---

Q34) You are configuring AAD conditional access and want to ensure that you don't lock out everyone in your organisation. You notice an empty group named "MFA bypass" with a description "Place users into this group temporarily if they need to bypass MFA". Which of the following do you need to do to ensure that users that are placed in that group effectively bypasses MFA.

● Nothing; the MFA bypass group is a built-in MFA lock-out failsafe

● Create a AAD conditional access policy that grants access to the "MFA bypass" group for all applications

✓ Add the "MFA bypass" group to the exclude section of the users and groups assignment

Explanation:-MFA bypass is not a built-in group.

Creating a grant policy won't work since the most restrictive policy applies when policies overlap.

Adding the Global Administrator's account to the group in not the best answer.

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/best-practices#how-should-you-deploy-a-new-policy

● Add the AAD Global administrator's account to the "MFA bypass" group

● There is no way to bypass an AAD conditional access policy

Q35) When doing an app registration in Azure AD, what option in the exhibit allows configuration of the services the application has access to?

● Authentication

● Certificates & secrets

✓ API permissions

● Expose an API

● Roles and administrators

Q36) You can create custom RBAC roles for which of the following?

● Azure AD permissions

✓ Azure Resource permissions

Explanation:-https://docs.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles?context=azure/active-directory/users-groups-roles/context/ugr-context

---

Q37) User1 is member of Group1
User2 is member of Group1 and Group2
An AAD Identity Protection user risk policy is configured to include Group1 and exclude Group2.
Is the policy applied to User2?

✓ correct

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

● incorrect

Q38) In OAuth 2.0 / OpenID Connect, what action does the browser take after receiving a successful ID token?

✓ Redirects to sign-in URI

Explanation:-Redirects to the app sign-in URI as configured on the app registration.

● Returns to the previous page

● Launches the application

● Connects to the database

Q39) Which of the following tools do you use to conduct an identity access review on Azure Active Directory roles or Azure Resource roles?

● Azure AD Identity Protection

✓ Azure AD Privileged Identity Management

Explanation:-Azure AD Privileged Identity Management

AAD Identity Protection allows you to detect and set policies around sign-in and user risk, but not do access reviews

Azure AD Connect synchronises OPE AD and Azure AD, but does not have the ability to conduct access reviews

Azure AD Premium P2 is the license that is required to implement and use Azure AD PIM, but is not the tool itself

https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

● Azure AD Connect

● Azure AD Premium P2

Q40) How can you choose when a user will be prompted for MFA?

● By configuring users with enforced for MFA to be prompted for MFA at every login

✓ By configuring Azure AD conditional access

Explanation:-By configuring Azure AD conditional access

Without conditional access settings, a user enrolled in MFA will be prompted for MFA with every login attempt.

● By deploying Microsoft Intune

● By deploying Microsoft Cloud App Security

Q41) Where can you buy an Azure AD Premium P2 subscription?

● Azure marketplace

● Azure portal

● Retail outlet

✓ M365 admin portal

Explanation:-M365 admin portal is used to buy a subscription to AAD

Azure marketplace has 3rd party resources you can add to your Azure subscription

Azure portal can be used to add a trial subscription, but not buy a subscription

aad.portal.azure.com is a AAD-focussed version of the normal Azure portal where you can add a trial subscription, but not buy a subscription

● aad.portal.azure.com

Q42) What is the OpenID Connect authentication provider in Azure?

● Azure Log Analytics Workspace

● Azure Security Center

● Azure Monitor

✓ Azure Active Directory

Q43) Which two of these offer a limited set of MFA functionality?

✓ MFA for Office 365

Explanation:-MFA for Office 365 and MFA for Azure AD Admins have limited functionality.

Azure MFA is a feature of AAD Premium P1 and P2.

Full MFA functionality is included with AAD Premium P1.

All features of AAD Premium P1 is included in AAD Premium P2.

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing#available-versions-of-azure-multi-factor-authentication

● Azure MFA

✓ MFA for Azure AD Admins

Explanation:-MFA for Office 365 and MFA for Azure AD Admins have limited functionality.

Azure MFA is a feature of AAD Premium P1 and P2.

Full MFA functionality is included with AAD Premium P1.

All features of AAD Premium P1 is included in AAD Premium P2.

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing#available-versions-of-azure-multi-factor-authentication

● Azure AD Premium P1

● Azure AD Premium P2

Q44) You are setting up AAD Connect. You must enforce the principle of least privilege. What roles do you need to accomplish your goal?

✓ Global Administrator on AAD

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

✓ Enterprise Administrator on AD

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

● User Administrator on AAD

● Domain Administrator on AD

Q45) Organise the following built-in RBAC roles into Azure AD and Azure Resource (RBAC) roles by selecting only the Azure Resource (RBAC) roles.

✓ User Access Administrator

Explanation:-https://docs.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles?context=azure/active-directory/users-groups-roles/context/ugr-context

✓ Owner

Explanation:-https://docs.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles?context=azure/active-directory/users-groups-roles/context/ugr-context

● Global Administrator

● Billing Administrator

✓ Contributor

Explanation:-https://docs.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles?context=azure/active-directory/users-groups-roles/context/ugr-context

✓ Reader

Explanation:-https://docs.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles?context=azure/active-directory/users-groups-roles/context/ugr-context

Q46) You are configuring AAD Identity Protection. You want to force a user to do a password change if the determined risk level is high. Which of the following do you configure?

● Sign-in risk policy

✓ User risk policy

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

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

● Conditional access policy

● MFA policy

● Password policy

Q47) What two components must be configured by the application developer for the application that have been registered with AAD for modern user authentication?

✓ Tenant ID

Explanation:-After doing app registration in Azure AD.

- Supply the Azure AD tenant ID or URL.

- Supply the Client ID (this is the app ID).

Both are GUID supplied after successful app registration.

Redirect URL does not need to be configured in the applicaiton, it is sent back to the browser by AAD after successful authentication.

The App Secret is only needed if the applicaiton itself must authenticate with AAD in order to perform some action.

https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-v2-aspnet-core-webapp#step-3-configure-your-visual-studio-project

✓ Client ID

Explanation:-After doing app registration in Azure AD.

- Supply the Azure AD tenant ID or URL.

- Supply the Client ID (this is the app ID).

Both are GUID supplied after successful app registration.

Redirect URL does not need to be configured in the applicaiton, it is sent back to the browser by AAD after successful authentication.

The App Secret is only needed if the applicaiton itself must authenticate with AAD in order to perform some action.

https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-v2-aspnet-core-webapp#step-3-configure-your-visual-studio-project

● Redirect URL

● App Secret

Q48) What is used to secure access to resource groups?

● Azure Active Directory

✓ Azure Role Based Access Control

● Azure Security Center

● Azure Policy

Q49) See the exhibit.
Which of the following is the correct route in the route table associated with Web Subnet?

● Prefix: 10.0.1.4/24; Next Hop: 0.0.0.0

● Prefix: 10.0.2.0/24; Next Hop: 10.0.1.4

● Prefix: 10.0.1.0/24; Next Hop: 192.168.1.1

✓ Prefix: 0.0.0.0/0; Next Hop: 10.0.1.4

Explanation:-Prefix: 0.0.0.0/0; Next Hop: 10.0.1.4

Routes associated with the workload subnets must be a prefix of "default gateway" (0.0.0.0/0) and point to the private IP of the firewall (10.0.1.4).

You could also make the prefix 192.168.1.0/24 if you only want traffic destined for the Office network to go via the firewall, but then traffic towards the Internet won't go via the firewall.

You should also create a route associated with GatewaySubnet with prefix 10.0.0.0/8 and next hop of 10.0.1.4 to force all traffic destined for both Azure VNets via the FW.

https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal#create-a-default-route

---

Q50) You deploy a VM on a VNet and plan to use it to host Docker containers. You have service endpoints on the VNet for Azure PaaS resources. You want the Docker containers to have access to the PaaS resources, what must you deploy?

● Azure Firewall

● Network Security Groups

✓ Azure Virtual Network container network interface (CNI) plug-in

Explanation:-Azure Virtual Network container network interface (CNI) plug-in assigns VNet IP addresses to the containers on the VM. This allows the contrainers connectivity to everything else on the VNet, NSGs permitting.

https://docs.microsoft.com/en-us/azure/virtual-network/container-networking-overview

● Azure container registry

● AppArmor

Q51) Which of the following will you create and configure if you want to connect an individual workstation directly to an Azure VNET? Each option represents part of the solution.

✓ Virtual Network Gateway

Explanation:-Virtual Network Gateway, Gateway Subnet, Self-signed certificate, Client configuration package, are required for a P2S VPN.

Virtual Network Gateway, Gateway Subnet, Local Network Gateway, VPN connection, are required for a S2S VPN.

✓ Gateway Subnet

Explanation:-Virtual Network Gateway, Gateway Subnet, Self-signed certificate, Client configuration package, are required for a P2S VPN.

Virtual Network Gateway, Gateway Subnet, Local Network Gateway, VPN connection, are required for a S2S VPN.

✓ Self-signed certificate

Explanation:-Virtual Network Gateway, Gateway Subnet, Self-signed certificate, Client configuration package, are required for a P2S VPN.

Virtual Network Gateway, Gateway Subnet, Local Network Gateway, VPN connection, are required for a S2S VPN.

● Local Network Gateway

✓ Client configuration package

Explanation:-Virtual Network Gateway, Gateway Subnet, Self-signed certificate, Client configuration package, are required for a P2S VPN. Virtual Network Gateway, Gateway Subnet, Local Network Gateway, VPN connection, are required for a S2S VPN.

● VPN connection

Q52) See the exhibit.
Which of the following do you configure to ensure that internet-connected browsers can access the web application (www.contoso.com) on Web Subnet via HTTPS?

● Route: Prefix: 0.0.0.0/0; Next Hop: 10.1.1.1
● Network rule; Protocol: TCP; Source: *; Destination: 10.1.1.1
✓ DNAT rule; Protocol: TCP; Source: *; Translated Addr: 10.1.1.1

Explanation:-DNAT rule; Protocol: TCP; Source: *; Translated Addr: 10.1.1.1
You use DNAT to do reverse proxy for traffic incoming from the Internet.
https://docs.microsoft.com/en-za/azure/firewall/rule-processing#nat-rules
https://docs.microsoft.com/en-za/azure/firewall/tutorial-firewall-dnat#configure-a-nat-rule

● Application rule; Source: *; Target: www.contoso.com

Q53) Which of the following would you implement to comply with restrictive geo-location compliance requirements in your Azure subscription?

✓ Azure Policy

Explanation:-The "Allowed Locations" Azure Policy is used to restrict the geo-location of resources deployed in the subscription (or whatever policy scope)

● Microsoft Compliance Manager
● Azure Subscription
● Azure Active Directory
● Azure Security Center

Q54) You have an NSG as in the exhibit and it is the only NSG configured in the environment.
Correct/Incorrect: The virtual machines in the AZ-500-rg resource group are blocked from communicating outbound to the internet.

● correct
✓ incorrect

Explanation:-incorrect. The NSG is not associated with any subnets or network interfaces and will therefore have no effect. It must be associated with the VMs or subnets in order to take effect. Had it been associated, it would have blocked outbound internet communication due to the DenyInternetOutBound rule having a higher (lower number) priority than the AllowInternetOutBound rule.

Q55) Infrastructure
- VM1 is part of RG1 and is in a stopped state.
- VM2 is part of RG2 and is in a stopped state.
- VM3 is part of RG3 and is in a stopped state.
Policies
-RG1 has a not allowed virtual machines policy applied.
-RG2 has an allowed virtual machines policy applied.
Locks
-VM1 has a read-only lock applied.
-RG2 has a read-only lock applied.
-RG3 has a delete-lock applied.
Superfluous information
You've got to love combining policies and locks; inheritance and permissions.
Select all the actions that can be performed.

● You can start VM1
● You can start VM2
● You can create a new VM in RG1
● You can create a new VM in RG2
✓ You can start VM3

Explanation:-You can start VM1 [No] VM1 has read-only lock that prevents starting.
You can start VM2 [No] VM2 has inherited RG2 read-only lock preventing starting.
You can create a new VM in RG1 [No] RG1 has no-VM policy applied.
You can create a new VM in RG2 [No] RG2 has read-only lock applied.
No-delete locks don't prevent change like start/stop.
Locks override policy allowances and RBAC permissions.
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources

Q56) Which Azure resource should you use to safeguard container access?

● Azure Active Directory
● Azure RBAC
✓ Azure Key Vault

Explanation:-You should be using Azure Key Vault to safeguard container access secrets, certificates and credentials.
https://docs.microsoft.com/en-us/azure/container-instances/container-instances-image-security

● Azure Security Center

Q57) You have a VNet named VNet1 containing a subnet named Sn1 containing a VM named VM1. You have another subnet in VNet1 named AzureFirewallSubnet containing an Azure Firewall. In order to ensure that all network traffic from Sn1 is routed through the Azure Firewall, what must you configure?

● NSG associated with Sn1 containing a outgoing rule allowing any source to any destination

✓ Route Table associated with Sn1 containing a route with address prefix of 0.0.0.0/0 and next hop with the private IP of the Azure Firewall

Explanation:-https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal#create-a-default-route

● NSG associated with AzureFirewallSubnet containing a outgoing rule allowing any source to any destination

● Route Table associated with AzureFirewallSubnet containing a route with address prefix of 0.0.0.0/0 and next hop with the private IP of the Azure Firewall

---

Q58) You deploy an Azure Kubernetes Cluster and need to configure a reverse proxy TLS termination. What component do you deploy?

✓ AKS Ingress Controller

Explanation:-AKS Ingress Controller - yes.

Container Network Interface (CNI) plug-in - no, this is to connect Docker containers to the host-VM's VNet.

Azure load balancer - No, AKS handles the deployment of load balancing on your behalf. Azure Load Balancer does not provide TLS termination.

Azure Application Gateway - No, AKS handles the deployment of reverse proxy via the ingress controller.

The other options don't exist. Or do they...? :p

https://docs.microsoft.com/en-us/azure/aks/ingress-tls

● Container Network Interface (CNI) plug-in

● Azure load balancer

● Azure Application Gateway

● AKS AppArmor

● AKS Container Registry

Q59) See the exhibit.
Which of the following is the correct route in the route table associated with GatewaySubnet?

● Prefix: 10.0.1.4/24; Next Hop: 0.0.0.0

● Prefix: 10.0.2.0/24; Next Hop: 10.0.1.4

● Prefix: 10.0.1.0/24; Next Hop: 192.168.1.1

● Prefix: 0.0.0.0/0; Next Hop: 10.0.1.4

✓ Prefix: 10.0.0.0/8; Next Hop: 10.0.1.4

Explanation:-Routes associated with the workload subnets must be a prefix of "default gatway" (0.0.0.0/0) and point to the private IP of the firewall (10.0.1.4).

You could also make the prefix 192.168.1.0/24 if you only want traffic destined for the Office network to go via the firewall, but then traffic towards the Internet won't go via the firewall.

You should also create a route associated with GatewaySubnet with prefix 10.0.0.0/8 and next hop of 10.0.1.4 to force all traffic destined for both Azure VNets via the FW.

https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal#create-a-default-route

---