Comprehension:

Overview
Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

Existing Environment
The company hosts its entire server infrastructure in Azure.
Contoso has two Azure subscriptions named Sub1 and Sub2. Both subscriptions are associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

Azure AD
Contoso.com contains the users shown in the following table.

Name	City	Role
User1	Montreal	Global administrator
User2	MONTREAL	Security administrator
User3	London	Privileged role administrator
User4	Ontario	Application administrator
User5	Seattle	Cloud application administrator
User6	Seattle	User administrator
User7	Sydney	Reports reader
User8	Sydney	*None*
User9	Sydney	Owner

Contoso.com contains the security groups shown in the following table.

Name	Membership type	Dynamic membership rule
Group1	Dynamic user	`user.city –contains "ON"`
Group2	Dynamic user	`user.city –match "*on"`

Sub1
Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.
User9 creates the virtual networks shown in the following table.

Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.

Name	Set on	Lock type
Lock1	RG1	Delete
Lock2	RG2	Read-only
Lock3	RG3	Delete
Lock4	RG3	Read-only

Sub1 contains the Azure policies shown in the following table.

Policy definition	Resource type	Scope
Allowed resource types	networkSecurityGroups	RG4
Not allowed resource types	virtualNetworks/subnets	RG5
Not allowed resource types	networksSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6

Sub2

Sub2 contains the virtual networks shown in the following table.

Name	Subnet
VNetwork1	Subnet11, Subnet12, and Subnet13
VNetwork2	Subnet21

Sub2 contains the virtual machines shown in the following table.

Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet11
VM2	NIC2	ASG2	Subnet11
VM3	NIC3	*None*	Subnet12
VM4	NIC4	ASG1	Subnet13
VM5	NIC5	*None*	Subnet21

All virtual machines have public IP addresses and the Web Server (IIS) role installed. The firewalls for each virtual machine allow ping requests and web requests.
Sub2 contains the network security groups (NSGs) shown in the following table.

Name	Associated to
NSG1	NIC2
NSG2	Subnet11
NSG3	Subnet13
NSG4	Subnet21

NSG1 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow

65500	Any	Any	Any	Any	Deny

NSG2 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	80	TCP	Internet	VirtualNetwork	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG3 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	Any	TCP	ASG1	ASG1	Allow
150	Any	Any	ASG2	VirtualNetwork	Allow
200	Any	Any	Any	Any	Deny
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG4 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	Any	Any	Any	Any	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	Any	Internet	Allow
65500	Any	Any	Any	Any	Deny

Technical requirements

Contoso identifies the following technical requirements:
• Deploy Azure Firewall to VNetwork1 in Sub2.
• Register an application named App2 in contoso.com.
• Whenever possible, use the principle of least privilege.
• Enable Azure AD Privileged Identity Management (PIM) for contoso.com.

Q1)

"You need to ensure that User2 can implement PIM.

What should you do first?"

- Configure authentication methods for contoso.com.
- Configure the identity secure score for contoso.com.
- ✅ Assign User2 the Global administrator role.

Explanation:-"To start using PIM in your directory, you must first enable PIM. 1. Sign in to the Azure portal as a Global Administrator of your directory. You must be a Global Administrator with an organizational account (for example, @yourdomain.com), not a Microsoft account (for example, @outlook.com), to enable PIM for a directory. Scenario: Technical requirements include: Enable Azure AD Privileged Identity Management (PIM) for contoso.com"

- Enable multi-factor authentication (MFA) for User2.

Q2) In data classification, which of the following data ownership roles are given no permissions to use the data?

- ✅ Custodian

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

- Owner
- User
- ✅ Administrator

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

---

Q3) Which of the following are valid access control options for Storage Accounts?

- Service Key
- ✅ Shared Access Signature

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

- ✅ Role Based Access Control

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

- Shared Access Key
- ✅ Access Key

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

---

Q4)

It is considered best practice to add an additional layer of access control security to Azure SQL databases.

Which Azure features provides this capability?

- Network Security Appliance
- ✓ Azure SQL Database Firewall

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

- Azure Firewall
- Network Security Group
- Azure Active Directory Conditional Access
- Azure Information Protection

Q5) Which of the following are valid access control options for Azure Data Lake?

- Service Key
- Shared Access Key
- ✓ Access Key

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

- ✓ Shared Access Signature

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

- ✓ Role Based Access Control

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

---

Q6)

You have been requested to configure VM security in the form of encrypting IaaS VM disks.

You are planning to make use of PowerShell to encrypt the disks.

Complete the following PowerShell command:

Set-1 -ResourceGroupName "MySecureRG" -VMName "MySecureVM" -2 "VaultID" -3 "VaultURL"

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

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

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

---

Q7)

You have an Azure subscription named Sub1.

In Azure Security Center, you have a security playbook named Play1. Play1 is configured to send an email message to a user named User1.

You need to modify Play1 to send email messages to a distribution group named Alerts.

What should you use to modify Play1?

- Azure DevOps
- Azure Application Insights
- Azure Monitor
- ✓ Azure Logic Apps Designer

Explanation:-You can change an existing playbook in Security Center to add an action, or conditions. To do that you just need to click on the name of the playbook that you want to change, in the Playbooks tab, and Logic App Designer opens up.

Q8)

You create a new Azure subscription.

You need to ensure that you can create custom alert rules in Azure Security Center.

Which two actions should you perform?

- Implement Azure Advisor recommendations.
- ✅ Create an Azure Log Analytics workspace.

Explanation:-You need write permission in the workspace that you select to store your custom alert.

- ✅ Create an Azure Storage account.

Explanation:-You need write permission in the workspace that you select to store your custom alert.

- Onboard Azure Active Directory (Azure AD) Identity Protection.
- Upgrade the pricing tier of Security Center to Standard.

Q9)

You have an Azure subscription named Sub1 that contains an Azure Log Analytics workspace named LAW1.

You have 100 on-premises servers that run Windows Server 2012 R2 and Windows Server 2016. The servers connect to LAW1. LAW1 is configured to collect security-related performance counters from the connected servers.

You need to configure alerts based on the data collected by LAW1. The solution must meet the following requirements:

Alert rules must support dimensions.
The time it takes to generate an alert must be minimized.
Alert notifications must be generated only once when the alert is generated and once when the alert is resolved.

Which signal type should you use when you create the alert rules?

- Log (Saved Query)
- ✅ Metric

Explanation:-Metric alerts in Azure Monitor provide a way to get notified when one of your metrics cross a threshold. Metric alerts work on a range of multi-dimensional platform metrics, custom metrics, Application Insights standard and custom metrics.

- Log
- Activity Log

Q10)

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

The company develops an application named App1. App1 is registered in Azure AD.

You need to ensure that App1 can access secrets in Azure Key Vault on behalf of the application users.

What should you configure?

- a delegated permission that requires admin consent
- ✅ a delegated permission without admin consent

Explanation:-Delegated permissions - Your client application needs to access the web API as the signed-in user, but with access limited by the selected permission. This type of permission can be granted by a user unless the permission requires administrator consent.

- an application permission without admin consent
- an application permission that requires admin consent

Q11)

You have a hybrid Azure AD deployment and have just deployed an Azure SQL Database.

You want selected users to use Azure AD credentials to access your Azure SQL Database.

What steps do you perform to accomplish your goal?

- ✅ Connect to SQL using Azure Active Directory - Universal with MFA authentication

Explanation:-https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure

- ✅ Create a contained database users specifying the user group created earlier in the database using CREATE USER [SQL Group] FROM EXTERNAL PROVIDER

Explanation:-https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure

- ✅ Create a group (SQL Group) in Azure AD that contains the users that will need to access SQL

Explanation:-https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure

- ✅ Configure the client computers with ADALSQL.DLL

Explanation:-https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure

- ✅ Provision the user account on the Active Directory Admin blade on SQL server

Explanation:-https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure

- ✅ Create a Azure AD user account that will serve as the SQL server administrator and assign user privileges

Explanation:-https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure

---

Q12)

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 Log Analytics Workspace
- ✅ Azure Logic Apps Designer

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

- Azure Monitor Action Group
- Azure Subscription

Q13)

You are the administrator for the Contoso financial group. You are responsible for managing the key vault in Azure.

You need to recover a certificate that has been deleted in the CONTOSOvault which is called "FinanceAdmin" via an API call to the Key Vault.

Which statement below is correct?

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

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

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

Q14)

When securing Azure Key Vault one has to secure the management plane and the data plane.

Which of these options is relevant when securing the data plane?

- Create RBAC roles
- ✅ Set key vault secrets

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

- Set key vault access policies
- ✅ Create key vault keys

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

- Set key vault tags
- Create key vault

Q15)

You need to configure additional Network Security Group rules to allow the following types of traffic:

• Remote Desktop Protocol

• SSH

• Secure web traffic

Which three ports should you configure as part of the NSG rules?

- Port 389
- ✅ Port 22

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

- Port 23
- ✅ Port 443
- Port 80
- ✅ Port 3389

Q16)

You are the administrator for the ACME banking group. You are responsible for managing the key vault in Azure called ACMEvault.

You have decommissioned a production server which has its password stored in the key vault labelled "FinanceAdmin".

You need to remove the password from the vault by using an API call.

Which API call is correct?

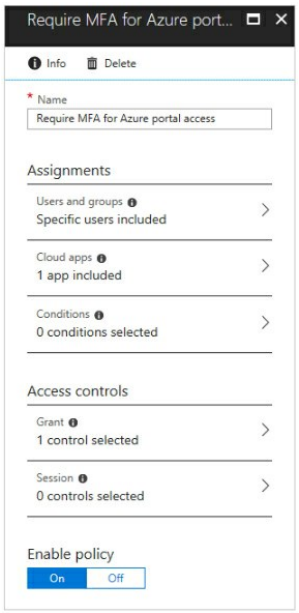
- 1. REMOVE https://ACMEvault.vault.azure.net/secrets/FinanceAdmin?api-version=7.0
- PURGE https://ACMEvault.vault.azure.net/secrets/FinanceAdmin?api-version=7.0
- ✅ DELETE https://ACMEvault.vault.azure.net/secrets/FinanceAdmin?api-version=7.0

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

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

Q17)

The exhibit shows the AAD conditional access configuration screen.



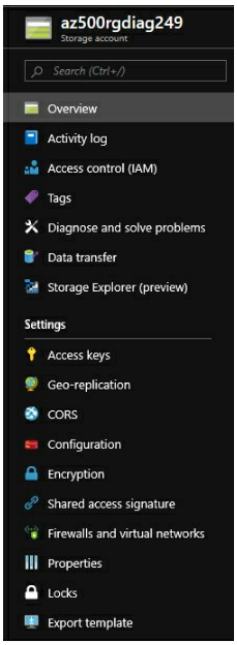
You're configuring conditional access that will require a user named Isabella to be required to undergo MFA by using the authenticator app only when accessing the Azure portal.

✅ Under 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 Assignments select Cloud apps and select Azure Portal
⚪ Under Assignments select Users and Groups and select the Azure Users group you created
✅ 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 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

---

Q18)

See the exhibit.



You have a corporate compliance requirement that mandates bring your own key for all storage accounts for data at rest encryption.

Which area would you use to configure this?

⚪ Data transfer
⚪ Access keys
✅ Encryption
Explanation:-You can use the Encryption configiuration option to configure BYOK for a storage account with integration with Azure Key Vault.
⚪ Access control (IAM)

Shared access signature

Q19) Which of the following cannot be used to create a custom RBAC role in Azure?

Azure PowerShell
Azure Portal
Explanation:-Azure portal cannot be used to create a custom RBAC role, you must use one of the command-line or scripting interfaces.
Azure CLI
Azure Cloud Shell
REST API

Q20)

You have to ensure the principle of least privilege.

Which Azure RBAC role is required to configure a lock on an Azure resource?

User Administrator
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
Contributor
Owner
Security Administrator

Q21)

In Azure Information Protection there are three types of key scenarios.

Match the key scenario with the technology used to create and maintain the keys. (Choose 3)

Hold your own key (HYOK): AD RMS
Explanation:-Azure Key Vault standard is a software-based HSM; Azure Key Vault Premium is a hardware-backed cloud HSM.
Bring your own key (BYOK): Key Vault
Explanation:-Azure Key Vault standard is a software-based HSM; Azure Key Vault Premium is a hardware-backed cloud HSM.
Key managed by Microsoft: HSM
Key managed by Microsoft: Key Vault
Key managed by Microsoft: AD RMS
Key managed by Microsoft: Microsoft
Explanation:-Azure Key Vault standard is a software-based HSM; Azure Key Vault Premium is a hardware-backed cloud HSM.

Q22)

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:

Disable and re-enable the user's user account
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
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

- Revoke and reassign the user's AAD P2 license

Q23)

You have an existing dynamic group in AAD. You want the group to contain users and their devices.

What should you configure?

- Create a membership rule that selects the devices. Manually add the users to the group
- 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
- ✅ Delete and recreate the group, manually add users and devices

Explanation:-
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 two membership rules that select the users and devices respectively

---

Q24)

You need to configure secure access to one of your production VMs. You are planning to enable secure remote access via Just-In-Time VM access.

Which of the following settings can you configure? Select all that apply.

- ✅ Time range

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

- Virtual network
- ✅ IP range

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

- ✅ IP address

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

- ✅ Port numbers

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

- ✅ Protocol type

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

---

Q25)

You have configured VNet peering between 2 VNets in your "Production" resource group.

You implement an Azure firewall and create a user defined route (UDR) that forces all traffic through the firewall.

Will traffic destined to route over the VNet peering link be forced to route through the firewall?

- Correct
- ✅ Incorrect

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

---

Q26)

You are the administrator of all resources in Azure. You need to enforce all new resources created to a specific region.

Solution: You create an Azure policy

Does this meet the requirements?

✅ Correct

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

⚪ Incorrect

Q27)

Azure Policy allows the assignment of a policy to a management group.

What level of scope is provided by management groups?

⚪ Resource group

✅ Subscription

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

⚪ Tenant

⚪ Resource

⚪ All of the options

Q28)

Your organization is planning on synchronizing their on premises identities to Azure via the AD Connect tool.

You need to ensure that all domain user identities are properly formatted before they are synchronized as to not cause synchronization errors.

What should you do?

⚪ Run synchronization service manager

✅ Run the IdFix tool

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

⚪ Re-run the AD Connect application

⚪ Run synchronization rules editor

Q29) Which of the following statements is true for Azure Policy initiatives?

⚪ A policy initiative is a policy assignment scope

⚪ A policy initiative is a policy assignment

✅ A policy initiative is a collection of policies

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

⚪ A policy initiative is a policy parameter

⚪ A policy initiative is a policy definition

Q30)

When securing Azure Key Vault one has to secure the management plane and the data plane.

Which of these options is relevant when securing the management plane?

✅ Set key vault tags

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

⚪ Create RBAC roles

⚪ Set key vault secrets

✅ Set key vault access policies

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

✅ Create, read, update, delete key vaults

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

⚪ Create key vault keys

Comprehension:

Overview
Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.

Existing Environment
Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.

Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.

Name	Type	Description
Group1	Security group	A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources.
Group2	Security group	A group that has the Dynamic User membership type and contains the Chicago IT team

The Azure subscription contains the objects shown in the following table.

Name	Type	Description
VNet1	Virtual network	VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet.
VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
VM1	Virtual machine	VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subent0.
SQLDB1	Azure SQL Database	SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.
WebApp1	Web app	WebApp1 is an Azure web app that is accessible by using https://litwareinc.com and http://www.litwareinc.com.
Resource Group1	Resource group	Resource Group1 is a resource group that contains VNet1, VM0, and VM1.
Resource Group2	Resource group	Resource Group2 is a resource group that contains shared IT resources.

Azure Security Center is set to the Free tier.

Planned changes
Litware plans to deploy the Azure resources shown in the following table.

Name	Type	Description
Firewall1	Azure Firewall	An Azure firewall on VNet1.
RT1	Route table	A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0.
AKS1	Azure Kubernetes Service (AKS)	A managed AKS cluster

Litware identifies the following identity and access requirements:
• All San Francisco users and their devices must be members of Group1.
• The members of Group2 must be assigned the Contributor role to Resource Group2 by using a permanent eligible assignment.
• Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the users' behalf.

Platform Protection Requirements
Litware identifies the following platform protection requirements:
• Microsoft Antimalware must be installed on the virtual machines in Resource Group1.
• The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.
• Azure AD users must be to authenticate to AKS1 by using their Azure AD credentials.
• Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.
• A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.

Security Operations Requirements
Litware must be able to customize the operating system security configurations in Azure Security Center.

Data and Application Requirements
Litware identifies the following data and applications requirements:
• The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials
• WebApp1 must enforce mutual authentication

General Requirements
Litware identifies the following general requirements:
• Whenever possible, administrative effort must be minimized
• Whenever possible, use of automation must be minimized

Q31) "You need to ensure that users can access VM0. The solution must meet the platform protection requirements.What should you do?"

- Assign RT1 to AzureFirewallSubnet.
- On Firewall, configure a network traffic filtering rule.
- ✔ Move VM0 to Subnet1.
- On Firewall, configure a DNAT rule.

Comprehension:

Overview
Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.

Existing Environment
Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.

Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.

Name	Type	Description
Group1	Security group	A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources.
Group2	Security group	A group that has the Dynamic User membership type and contains the Chicago IT team

The Azure subscription contains the objects shown in the following table.

Name	Type	Description
VNet1	Virtual network	VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet.
VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
VM1	Virtual machine	VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subent0.
SQLDB1	Azure SQL Database	SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.
WebApp1	Web app	WebApp1 is an Azure web app that is accessible by using https://litwareinc.com and http://www.litwareinc.com.
Resource Group1	Resource group	Resource Group1 is a resource group that contains VNet1, VM0, and VM1.
Resource Group2	Resource group	Resource Group2 is a resource group that contains shared IT resources.

Azure Security Center is set to the Free tier.

Planned changes
Litware plans to deploy the Azure resources shown in the following table.

Name	Type	Description
Firewall1	Azure Firewall	An Azure firewall on VNet1.
RT1	Route table	A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0.
AKS1	Azure Kubernetes Service (AKS)	A managed AKS cluster

Litware identifies the following identity and access requirements:
• All San Francisco users and their devices must be members of Group1.
• The members of Group2 must be assigned the Contributor role to Resource Group2 by using a permanent eligible assignment.
• Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the users' behalf.

Platform Protection Requirements
Litware identifies the following platform protection requirements:
• Microsoft Antimalware must be installed on the virtual machines in Resource Group1.
• The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.
• Azure AD users must be to authenticate to AKS1 by using their Azure AD credentials.
• Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.
• A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.

Security Operations Requirements
Litware must be able to customize the operating system security configurations in Azure Security Center.

Data and Application Requirements
Litware identifies the following data and applications requirements:
• The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials
• WebApp1 must enforce mutual authentication

General Requirements
Litware identifies the following general requirements:
• Whenever possible, administrative effort must be minimized
• Whenever possible, use of automation must be minimized

Q32) "You need to ensure that you can meet the security operations requirements.What should you do first?"

- Integrate Security Center and Microsoft Cloud App Security.
- ✅ Upgrade the pricing tier of Security Center to Standard.

Explanation:-"The Standard tier extends the capabilities of the Free tier to workloads running in private and other public clouds, providing unified security management and threat protection across your hybrid cloud workloads. The Standard tier also adds advanced threat detection capabilities, which uses built-in behavioral analytics and machine learning to identify attacks and zero-day exploits, access and application controls to reduce exposure to network attacks and malware, and more. Scenario: Security Operations Requirements Litware must be able to customize the operating system security configurations in Azure Security Center."

- Turn on Auto Provisioning in Security Center.
- Modify the Security Center workspace configuration.

Comprehension:

Overview
Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.

Existing Environment
Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.

Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.

Name	Type	Description
Group1	Security group	A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources.
Group2	Security group	A group that has the Dynamic User membership type and contains the Chicago IT team

The Azure subscription contains the objects shown in the following table.

Name	Type	Description
VNet1	Virtual network	VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet.
VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
VM1	Virtual machine	VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subent0.
SQLDB1	Azure SQL Database	SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.
WebApp1	Web app	WebApp1 is an Azure web app that is accessible by using https://litwareinc.com and http://www.litwareinc.com.
Resource Group1	Resource group	Resource Group1 is a resource group that contains VNet1, VM0, and VM1.
Resource Group2	Resource group	Resource Group2 is a resource group that contains shared IT resources.

Azure Security Center is set to the Free tier.

Planned changes
Litware plans to deploy the Azure resources shown in the following table.

Name	Type	Description
Firewall1	Azure Firewall	An Azure firewall on VNet1.
RT1	Route table	A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0.
AKS1	Azure Kubernetes Service (AKS)	A managed AKS cluster

Litware identifies the following identity and access requirements:
• All San Francisco users and their devices must be members of Group1.
• The members of Group2 must be assigned the Contributor role to Resource Group2 by using a permanent eligible assignment.
• Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the users' behalf.

Platform Protection Requirements
Litware identifies the following platform protection requirements:
• Microsoft Antimalware must be installed on the virtual machines in Resource Group1.
• The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.
• Azure AD users must be to authenticate to AKS1 by using their Azure AD credentials.
• Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.
• A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.

Security Operations Requirements
Litware must be able to customize the operating system security configurations in Azure Security Center.

Data and Application Requirements
Litware identifies the following data and applications requirements:
• The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials
• WebApp1 must enforce mutual authentication

General Requirements
Litware identifies the following general requirements:
• Whenever possible, administrative effort must be minimized
• Whenever possible, use of automation must be minimized

Q33) "You need to configure WebApp1 to meet the data and application requirements.Which two actions should you perform?"

- Turn on the HTTPS Only protocol setting.
- ✅ Set the Minimum TLS Version protocol setting to 1.2.

Explanation:-Over time, multiple versions of TLS have been released to mitigate different vulnerabilities. TLS 1.2 is the most current version available for apps running on Azure App Service.

- ✅ Upload a public certificate.

Explanation:-To configure Certificates for use in Azure Websites Applications you need to upload a public Certificate.

- Change the pricing tier of the App Service plan.