Answer Sheet

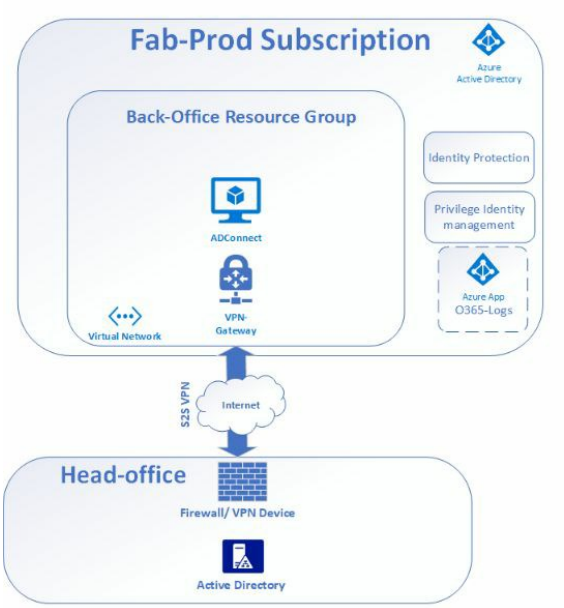
Comprehension:

Fabrikam Inc. has adopted Azure as their cloud platform. Fabrikam currently has a hybrid identity model which is supported by ADConnect. Within the Azure environment, there is 1 subscription labeled **"Fab-Prod"** which has a resource group labeled **"Back-Office"**. The "Back-Office" resource group has the following resources:

1. **"ADConnect"** VM is running on a standard A2M spec VM

2. **"VPN-Gateway"** is the VPN gateway which is configured for Site-to-Site VPN (Azure to on-premises)

There are 250 Azure Active Directory user accounts which has the Office E5 licenses assigned to each user individually. The Azure tenant is configured for Privilege Identity Management and has 3 global administrator accounts (Admin01, Admin02 and Admin03) enrolled which is used to manage the environment, these administrator accounts have EMS E5 license associated to each account. Admin01 is the subscription owner for the "Fab-Prod" subscription and permissions are handled via Privilege Identity Management (PIM).



Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than once correct solution, while others might not have a correct solution.

Q1)

You create an additional administrator account labeled "Admin04" as a normal Azure AD user. This account should be eligible for "Global Administrator" access via Privilege Identity Management for safekeeping and auditing purposes.

Solution: You enroll "Admin04" as an Azure AD role member with the global admin permission.

Does this solution meet the goal?

Incorrect

Correct

Explanation:-"Admin04" needs to be added as an "Azure AD roles" member as this is used for identities in Azure/Office 365. The user "Admin04" should not be configured under the "Azure resources" member as this is used to grant access to resources in Azure i.e. Owner role for a subscription. https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-add-role-to-user

---

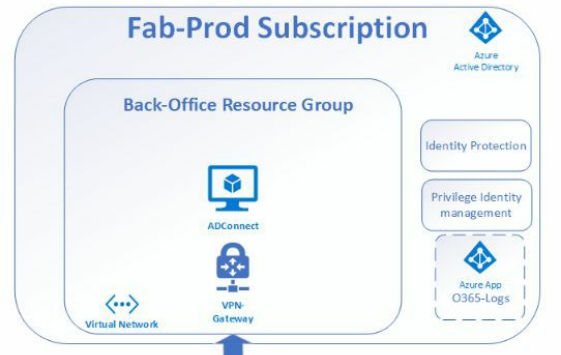
Comprehension:

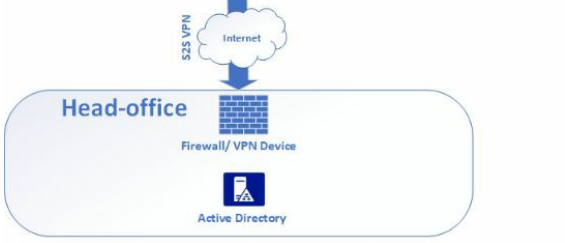
Fabrikam Inc. has adopted Azure as their cloud platform. Fabrikam currently has a hybrid identity model which is supported by ADConnect. Within the Azure environment, there is 1 subscription labeled **"Fab-Prod"** which has a resource group labeled **"Back-Office"**. The "Back-Office" resource group has the following resources:

1. **"ADConnect"** VM is running on a standard A2M spec VM

2. **"VPN-Gateway"** is the VPN gateway which is configured for Site-to-Site VPN (Azure to on-premises)

There are 250 Azure Active Directory user accounts which has the Office E5 licenses assigned to each user individually. The Azure tenant is configured for Privilege Identity Management and has 3 global administrator accounts (Admin01, Admin02 and Admin03) enrolled which is used to manage the environment, these administrator accounts have EMS E5 license associated to each account. Admin01 is the subscription owner for the "Fab-Prod" subscription and permissions are handled via Privilege Identity Management (PIM).





Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than once correct solution, while others might not have a correct solution.

Q2)

You need to enroll "Admin02" into PIM so that the administrator is eligible to manage resources in the "Fab-Prod" subscription for a maximum of 8-hour time period. Admin02 requires full access to all resources within the subscription however he should not be able to add additional role assignments to the subscription.

Which role should you assign to Admin02?

- Reader role
- ✅ Contributor role

Explanation:-Contributor role is correct as this lets you manage all resources in the "Fab-Prod" subscription except access to resources. Owner role is incorrect as this allows full control on the subscription. Reader role is incorrect as this only allows you to view resources but not make any changes. Security Admin role is incorrect as this is role is used to manage Azure Security Center specifically and not all resources within the subscription. https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

- Owner role
- Security administrator role

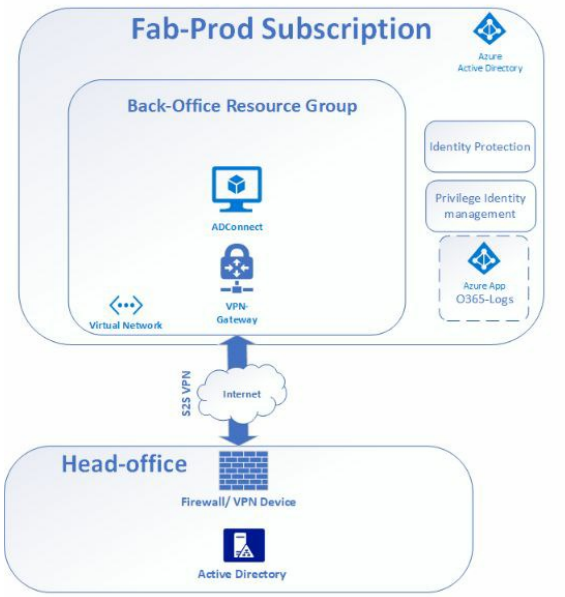
Comprehension:

Fabrikam Inc. has adopted Azure as their cloud platform. Fabrikam currently has a hybrid identity model which is supported by ADConnect. Within the Azure environment, there is 1 subscription labeled **"Fab-Prod"** which has a resource group labeled **"Back-Office"**. The "Back-Office" resource group has the following resources:

1. **"ADConnect"** VM is running on a standard A2M spec VM

2. **"VPN-Gateway"** is the VPN gateway which is configured for Site-to-Site VPN (Azure to on-premises)

There are 250 Azure Active Directory user accounts which has the Office E5 licenses assigned to each user individually. The Azure tenant is configured for Privilege Identity Management and has 3 global administrator accounts (Admin01, Admin02 and Admin03) enrolled which is used to manage the environment, these administrator accounts have EMS E5 license associated to each account. Admin01 is the subscription owner for the "Fab-Prod" subscription and permissions are handled via Privilege Identity Management (PIM).



Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than once correct solution, while others might not have a correct solution.

Q3)

"You plan on rolling out Microsoft Intune to a control group of 20 random users. You need to assign EMS E3 licenses for all users which are part of the control group, this process should be scalable going forward and make license management for In tune users as easy as possible.

Solution: Create a new security group with an assigned membership type and configure group-based licensing.

Does this solution meet the goal?"

- Incorrect
- ✅ Correct

Explanation:-The easiest way to manage licenses going forward for users is to create a new security group and configure group-based licensing, this will ensure whenever a new user is assigned to the group it will automatically assign a EMS E3 license to support Intune, it will also revoke an

EMS E3 license whenever a user is removed from the group (i.e. when a user leaves the company). You need to configure an “Assigned” membership type as specific users are targeted and requires to be selected manually. https://docs.microsoft.com/en-us/microsoft-365/enterprise/identity-self-service-group-management

---

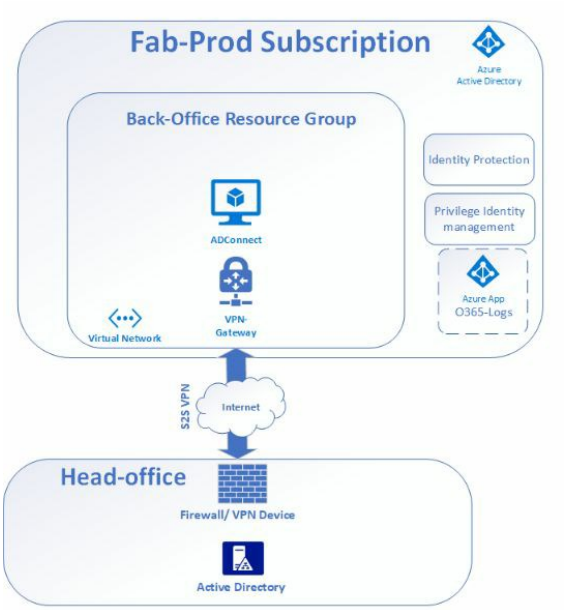
Comprehension:

Fabrikam Inc. has adopted Azure as their cloud platform. Fabrikam currently has a hybrid identity model which is supported by ADConnect. Within the Azure environment, there is 1 subscription labeled **“Fab-Prod”** which has a resource group labeled **“Back-Office”**. The “Back-Office” resource group has the following resources:

1. **“ADConnect”** VM is running on a standard A2M spec VM

2. **“VPN-Gateway”** is the VPN gateway which is configured for Site-to-Site VPN (Azure to on-premises)

There are 250 Azure Active Directory user accounts which has the Office E5 licenses assigned to each user individually. The Azure tenant is configured for Privilege Identity Management and has 3 global administrator accounts (Admin01, Admin02 and Admin03) enrolled which is used to manage the environment, these administrator accounts have EMS E5 license associated to each account. Admin01 is the subscription owner for the “Fab-Prod” subscription and permissions are handled via Privilege Identity Management (PIM).



Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than once correct solution, while others might not have a correct solution.

Q4)

You have been tasked to better manage all user accounts per department in the Azure AD tenant. You plan to group all user accounts automatically by using a dynamic group membership called “Dynamic-Guests”.

Which of the following criteria is the best to identify these accounts as the below information has been set for all users?

✅ Department

Explanation:-Job title is correct as you can configure the dynamic rule to select “contains” “Job Title” i.e. (“Contains” “Marketing” will add accounts for Marketing director, marketing assistant etc.). Department is also correct as this can be used as part of the dynamic rule configuration i.e. (“Match” “Department” will add accounts per the department tag i.e. “Finance”). Location is incorrect as this is not a good parameter to use when filtering per department as there usually are several departments per location/region. Manager is incorrect as this not a good parameter to use as there might be some people reporting into a specific person that is not part of a specific department per sè i.e. several departments will report into the General Manager). https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership

⚫ Location

⚫ Manager

✅ Job title

Explanation:-Job title is correct as you can configure the dynamic rule to select “contains” “Job Title” i.e. (“Contains” “Marketing” will add accounts for Marketing director, marketing assistant etc.). Department is also correct as this can be used as part of the dynamic rule configuration i.e. (“Match” “Department” will add accounts per the department tag i.e. “Finance”). Location is incorrect as this is not a good parameter to use when filtering per department as there usually are several departments per location/region. Manager is incorrect as this not a good parameter to use as there might be some people reporting into a specific person that is not part of a specific department per sè i.e. several departments will report into the General Manager). https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership

---

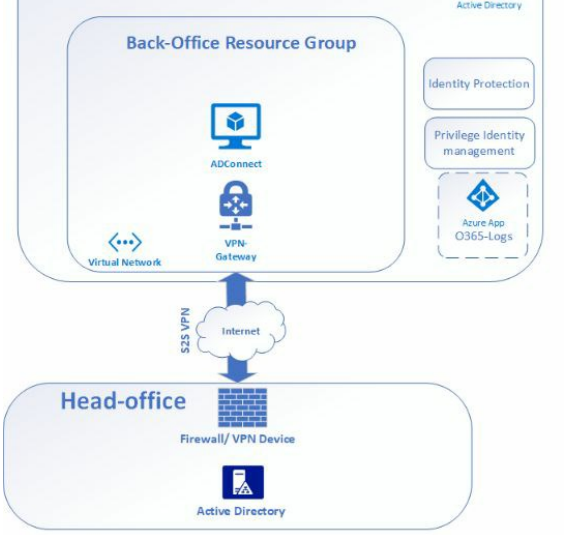
Comprehension:

Fabrikam Inc. has adopted Azure as their cloud platform. Fabrikam currently has a hybrid identity model which is supported by ADConnect. Within the Azure environment, there is 1 subscription labeled **“Fab-Prod”** which has a resource group labeled **“Back-Office”**. The “Back-Office” resource group has the following resources:

1. **“ADConnect”** VM is running on a standard A2M spec VM

2. **“VPN-Gateway”** is the VPN gateway which is configured for Site-to-Site VPN (Azure to on-premises)

There are 250 Azure Active Directory user accounts which has the Office E5 licenses assigned to each user individually. The Azure tenant is configured for Privilege Identity Management and has 3 global administrator accounts (Admin01, Admin02 and Admin03) enrolled which is used to manage the environment, these administrator accounts have EMS E5 license associated to each account. Admin01 is the subscription owner for the “Fab-Prod” subscription and permissions are handled via Privilege Identity Management (PIM).



Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than once correct solution, while others might not have a correct solution.

Q5)

You are tasked to secure all guest user identities by only allowing logging into Microsoft Teams via Windows and blocking sign-ins from Android and iOS. When logging in the guest users must also use MFA.

Which technology should you implement to accomplish this goal?

- Privilege Identity Management
- ✅ Conditional Access

Explanation:-Conditional Access is correct as this allows rules to be created that specifies specific criteria when signing in which can then grant access, request additional authentication or even decline the request when logging in from a platform that is denied. Privilege Identity management will not suffice as this enables users to activate additional roles with their identity like Global Admin or access to resources in Azure. MFA by itself will not suffice as there is limited options, either enabled, enforced or disabled and no automatic intelligence associated with it. Identity Protection will not suffice as this is mainly associated with risky sign ins and not blocking users from logging in via specific rule sets created like blocking specific platforms etc. https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

- Identity Protection

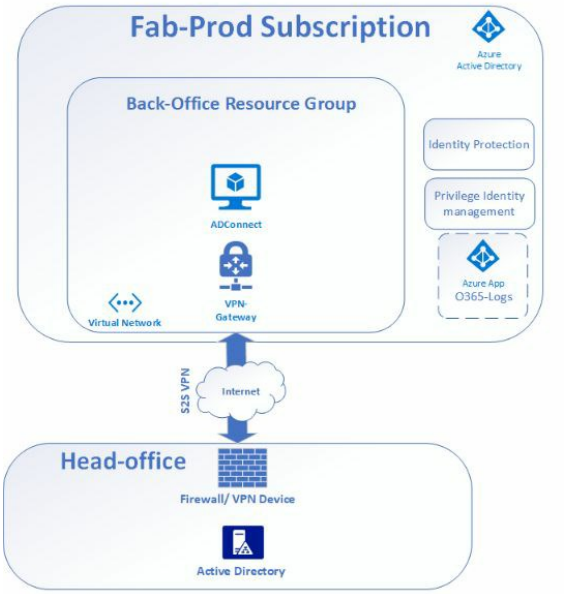
Comprehension:

Fabrikam Inc. has adopted Azure as their cloud platform. Fabrikam currently has a hybrid identity model which is supported by ADConnect. Within the Azure environment, there is 1 subscription labeled **"Fab-Prod"** which has a resource group labeled **"Back-Office"**. The "Back-Office" resource group has the following resources:

1. **"ADConnect"** VM is running on a standard A2M spec VM

2. **"VPN-Gateway"** is the VPN gateway which is configured for Site-to-Site VPN (Azure to on-premises)

There are 250 Azure Active Directory user accounts which has the Office E5 licenses assigned to each user individually. The Azure tenant is configured for Privilege Identity Management and has 3 global administrator accounts (Admin01, Admin02 and Admin03) enrolled which is used to manage the environment, these administrator accounts have EMS E5 license associated to each account. Admin01 is the subscription owner for the "Fab-Prod" subscription and permissions are handled via Privilege Identity Management (PIM).



Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than once correct solution, while others might not have a correct solution.

Q6) Correct or Incorrect: You can configure an Azure Conditional Access policy for client applications like Microsoft Word.

Incorrect

Explanation:-You cannot specify a conditional access policy for a client application like Word or Outlook. Conditional Access policy sets requirements for accessing a service. It's enforced when authentication to that service occurs. The policy is not set directly on a client application.
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/faqs

Correct

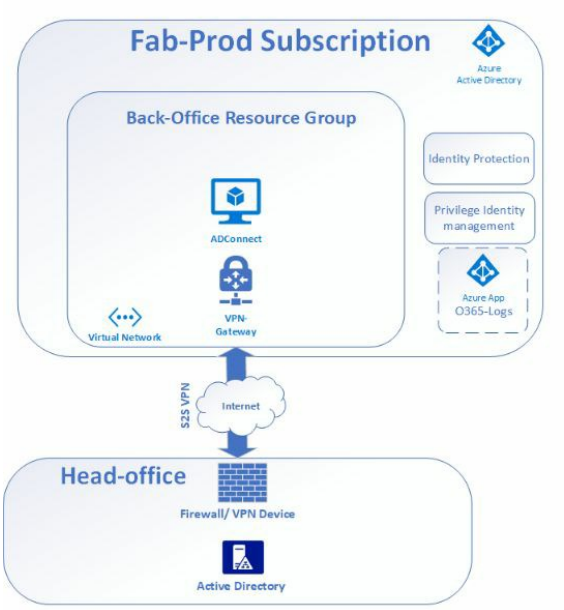
Comprehension:

Fabrikam Inc. has adopted Azure as their cloud platform. Fabrikam currently has a hybrid identity model which is supported by ADConnect. Within the Azure environment, there is 1 subscription labeled **"Fab-Prod"** which has a resource group labeled **"Back-Office"**. The "Back-Office" resource group has the following resources:

1. **"ADConnect"** VM is running on a standard A2M spec VM

2. **"VPN-Gateway"** is the VPN gateway which is configured for Site-to-Site VPN (Azure to on-premises)

There are 250 Azure Active Directory user accounts which has the Office E5 licenses assigned to each user individually. The Azure tenant is configured for Privilege Identity Management and has 3 global administrator accounts (Admin01, Admin02 and Admin03) enrolled which is used to manage the environment, these administrator accounts have EMS E5 license associated to each account. Admin01 is the subscription owner for the "Fab-Prod" subscription and permissions are handled via Privilege Identity Management (PIM).



Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than once correct solution, while others might not have a correct solution.

Q7)

You are planning on rolling out a new Azure AD Conditional Access policy to restrict access to only specific device platforms.

Which of the following device platforms are supported by conditional access?

macOS

Explanation:-Conditional Access policies supports the following device platforms: Android, iOS, Windows Phone, Windows, macOS.
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/technical-reference

Windows Phone

Explanation:-Conditional Access policies supports the following device platforms: Android, iOS, Windows Phone, Windows, macOS.
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/technical-reference

iOS

Explanation:-Conditional Access policies supports the following device platforms: Android, iOS, Windows Phone, Windows, macOS.
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/technical-reference

Android

Explanation:-Conditional Access policies supports the following device platforms: Android, iOS, Windows Phone, Windows, macOS.
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/technical-reference

---

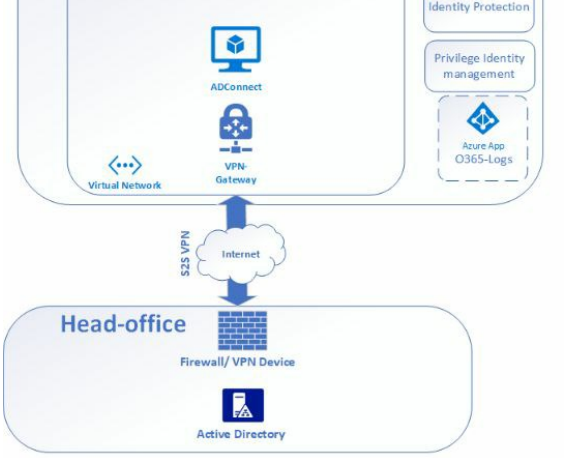
Comprehension:

Fabrikam Inc. has adopted Azure as their cloud platform. Fabrikam currently has a hybrid identity model which is supported by ADConnect. Within the Azure environment, there is 1 subscription labeled **"Fab-Prod"** which has a resource group labeled **"Back-Office"**. The "Back-Office" resource group has the following resources:

1. **"ADConnect"** VM is running on a standard A2M spec VM

2. **"VPN-Gateway"** is the VPN gateway which is configured for Site-to-Site VPN (Azure to on-premises)

There are 250 Azure Active Directory user accounts which has the Office E5 licenses assigned to each user individually. The Azure tenant is configured for Privilege Identity Management and has 3 global administrator accounts (Admin01, Admin02 and Admin03) enrolled which is used to manage the environment, these administrator accounts have EMS E5 license associated to each account. Admin01 is the subscription owner for the "Fab-Prod" subscription and permissions are handled via Privilege Identity Management (PIM).



Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than once correct solution, while others might not have a correct solution.

Q8)

The security department has requested that when configuring Single Sign On (SSO) for hybrid users that all user passwords are passed through the on-premises Active Directory domain controller for validation.

Solution: You configure Password Hash Sync and enable single sign on (SSO) with the ADConnect tool.

Does this solution meet the goal?

✅ Incorrect

Explanation:-You will need to configure “Pass through Authentication” as this option allows user passwords to be passed through to the on-premises AD domain controller for validation. “Password hash sync” is incorrect as this will store a hash of the password in the cloud and authentication occurs in the cloud instead of on-premises. Enabling single sign on is correct as this is supported with “password Hash Sync” and “Pass through Authentication” and is a requirement for SSO. https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom

⚪ Correct

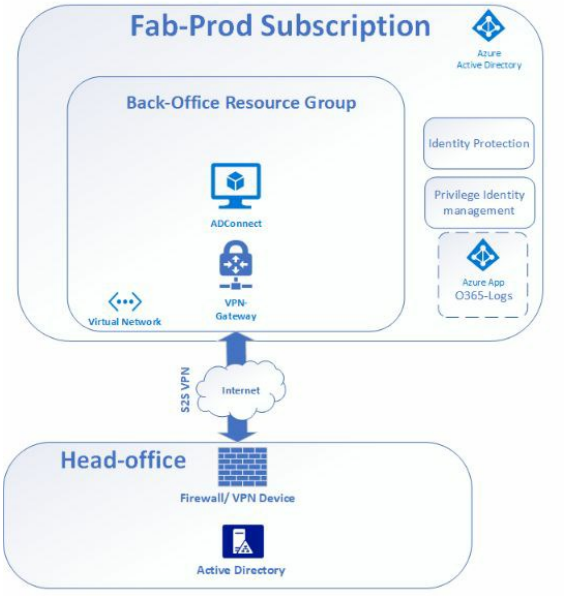
Comprehension:

Fabrikam Inc. has adopted Azure as their cloud platform. Fabrikam currently has a hybrid identity model which is supported by ADConnect. Within the Azure environment, there is 1 subscription labeled **“Fab-Prod”** which has a resource group labeled **“Back-Office”**. The “Back-Office” resource group has the following resources:

1. **“ADConnect”** VM is running on a standard A2M spec VM

2. **“VPN-Gateway”** is the VPN gateway which is configured for Site-to-Site VPN (Azure to on-premises)

There are 250 Azure Active Directory user accounts which has the Office E5 licenses assigned to each user individually. The Azure tenant is configured for Privilege Identity Management and has 3 global administrator accounts (Admin01, Admin02 and Admin03) enrolled which is used to manage the environment, these administrator accounts have EMS E5 license associated to each account. Admin01 is the subscription owner for the “Fab-Prod” subscription and permissions are handled via Privilege Identity Management (PIM).



Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than once correct solution, while others might not have a correct solution.

Q9)

Currently the on-premises identities are synced to Azure AD via the ADConnect tool installed on the “ADConnect” server which is connected to the on-premises network via the Site-to-Site VPN. The ADConnect tool has been configured and has been syncing identities for the past month without issue, however you received an email message saying “Azure Active Directory" (Azure AD) didn’t register a synchronization attempt in the last 24 hours.

What could be the cause?

✅ Directory synchronization service has stopped

Explanation:-They can be possible causes of the identities not synching to Azure AD via the ADConnect tool. There are 2 methods to troubleshoot this issue: Method 1: Manually verify that the service is started and that the admin account can sign in, Method 2: Resolve the problem with the logon account for the directory synchronization service. https://support.microsoft.com/en-za/help/2882421/directory-synchronization-to-azure-active-directory-stops-or-you-re-wa

✅ There are network connection issues

Explanation:-They can be possible causes of the identities not synching to Azure AD via the ADConnect tool. There are 2 methods to troubleshoot this issue: Method 1: Manually verify that the service is started and that the admin account can sign in, Method 2: Resolve the problem with the logon account for the directory synchronization service. https://support.microsoft.com/en-za/help/2882421/directory-synchronization-to-azure-active-directory-stops-or-you-re-wa

✅ The admin account used for directory synchronization was changed

Explanation:-They can be possible causes of the identities not synching to Azure AD via the ADConnect tool. There are 2 methods to troubleshoot this issue: Method 1: Manually verify that the service is started and that the admin account can sign in, Method 2: Resolve the problem with the logon account for the directory synchronization service. https://support.microsoft.com/en-za/help/2882421/directory-synchronization-to-azure-active-directory-stops-or-you-re-wa

✅ The work or school account used in the configuration wizard to setup directory synchronization has been deleted, disabled or password expired

Explanation:-They can be possible causes of the identities not synching to Azure AD via the ADConnect tool. There are 2 methods to troubleshoot this issue: Method 1: Manually verify that the service is started and that the admin account can sign in, Method 2: Resolve the problem with the logon account for the directory synchronization service. https://support.microsoft.com/en-za/help/2882421/directory-synchronization-to-azure-active-directory-stops-or-you-re-wa

---

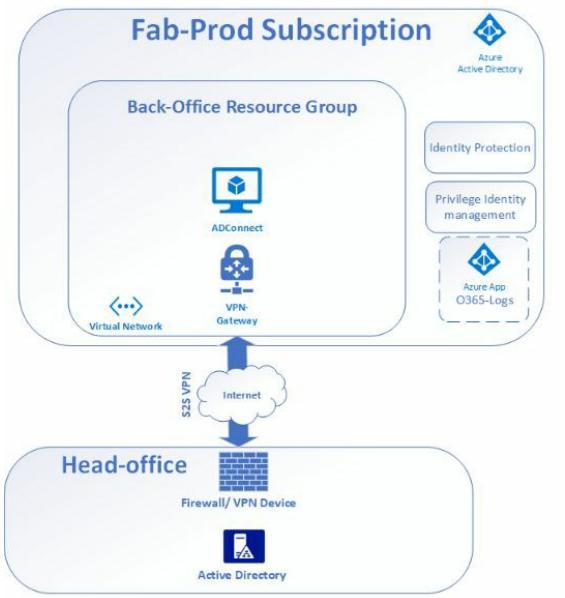
Comprehension:

Fabrikam Inc. has adopted Azure as their cloud platform. Fabrikam currently has a hybrid identity model which is supported by ADConnect. Within the Azure environment, there is 1 subscription labeled **"Fab-Prod"** which has a resource group labeled **"Back-Office"**. The "Back-Office" resource group has the following resources:

1. **"ADConnect"** VM is running on a standard A2M spec VM

2. **"VPN-Gateway"** is the VPN gateway which is configured for Site-to-Site VPN (Azure to on-premises)

There are 250 Azure Active Directory user accounts which has the Office E5 licenses assigned to each user individually. The Azure tenant is configured for Privilege Identity Management and has 3 global administrator accounts (Admin01, Admin02 and Admin03) enrolled which is used to manage the environment, these administrator accounts have EMS E5 license associated to each account. Admin01 is the subscription owner for the "Fab-Prod" subscription and permissions are handled via Privilege Identity Management (PIM).



Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than once correct solution, while others might not have a correct solution.

Q10)

You have been requested to evaluate the security posture of all identities in Azure Active Directory.

You need to provide the following information per user:

Risk level

Risk events

Current status

Solution: You configure Azure AD Identity Protection.

Does this solution meet the goal?

⚪ Incorrect

✅ Correct

Explanation:-Identity Protection allows you to view risk level, risk events and current status. Identity Protection also allows you to mitigate risky sign-ins by blocking sign-ins or requiring multi-factor authentication challenges. https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview

---

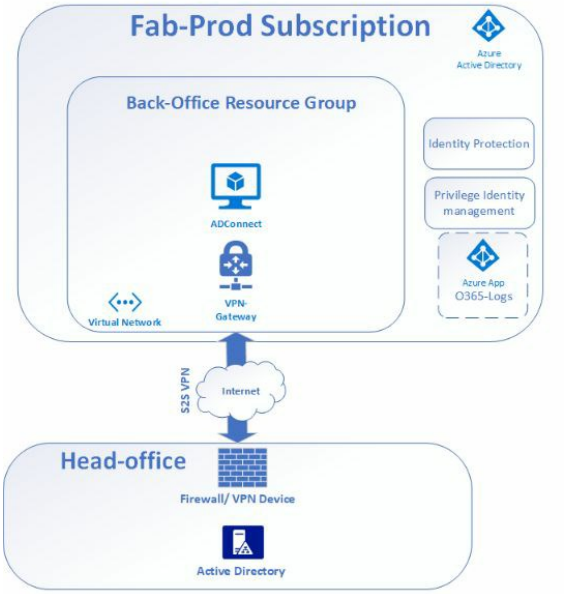
Comprehension:

Fabrikam Inc. has adopted Azure as their cloud platform. Fabrikam currently has a hybrid identity model which is supported by ADConnect. Within the Azure environment, there is 1 subscription labeled **"Fab-Prod"** which has a resource group labeled **"Back-Office"**. The "Back-Office" resource group has the following resources:

1. **"ADConnect"** VM is running on a standard A2M spec VM

2. **"VPN-Gateway"** is the VPN gateway which is configured for Site-to-Site VPN (Azure to on-premises)

There are 250 Azure Active Directory user accounts which has the Office E5 licenses assigned to each user individually. The Azure tenant is configured for Privilege Identity Management and has 3 global administrator accounts (Admin01, Admin02 and Admin03) enrolled which is used to manage the environment, these administrator accounts have EMS E5 license associated to each account. Admin01 is the subscription owner for the "Fab-Prod" subscription and permissions are handled via Privilege Identity Management (PIM).



Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than once correct solution, while others might not have a correct solution.

Q11)

You have been requested to create a new Azure AD application labeled "Office365-logging" which needs to retrieve information about user, admin and policy actions and events from Office 365. This app needs to support both work and school accounts including personal Microsoft accounts.

Solution: You create an Azure AD V1.0 endpoint

Does this solution meet the goal?

✅ Incorrect

Explanation:-You will need an Azure AD V2.0 endpoint as the V1.0 endpoint does not support personal Microsoft accounts (it only supports work and school accounts). https://docs.microsoft.com/en-us/graph/auth-overview

⚪ Correct

Q12) Correct or Incorrect: you can deploy a VM in the same virtual network where your Azure Kubernetes Cluster is running?

✅ Correct

Explanation:-you can deploy a VM to the same VNet where a Kubernetes cluster is running, however the VM can't be deployed to the same subnet as the Kubernetes cluster. https://docs.microsoft.com/en-us/azure/aks/configure-azure-cni?toc=%2Fazure%2Fvirtual-network%2Ftoc.json

⚪ Incorrect

Q13) Correct or Incorrect: you can deploy a VM in the same subnet where your Azure Kubernetes Cluster is running?

⚪ Correct

✅ Incorrect

Explanation:-You cannot deploy a VM to the same subnet where a Kubernetes cluster is running, however the VM can be deployed to the same VNet. https://docs.microsoft.com/en-us/azure/aks/configure-azure-cni?toc=%2Fazure%2Fvirtual-network%2Ftoc.json

---

Q14) Which of the following security concerns are relevant to container solutions?

✅ Poisoned images

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

versions of software with known vulnerabilities. https://azure.microsoft.com/mediahandler/files/resourcefiles/container-security-in-microsoft-azure/Open%20Container%20Security%20in%20Microsoft%20Azure.pdf

✅ Container breakouts

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

✅ Denial-of-service attacks

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

✅ Kernel Exploits

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

---

Q15)

You need to delegate access to a system administrator to a specific VM labeled "LOB-VM" in the Production resource group. The system administrator should have full control over the VM but should not be able to grant additional users' access. The resource group is home to a combination of resources across different departments.

You need to grant RBAC access with strict security in mind.

Which is the correct RBAC configuration?

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

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

---

Q16)

You need to ensure that all current and future resources that are compliant are enrolled into Azure Security Center.

Solution: You configure an Azure policy on the subscription level.

Does this solution meet the goal?

✅ Correct

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

⚪ Incorrect

Q17)

You need to harden your Docker containers.

Solution: You enable AppArmor.

Does this solution meet the goal?

✅ Correct

Explanation:-You can use AppArmor, SELinux, GRSEC or another appropriate hardening system. https://docs.docker.com/engine/security/security/

⚪ Incorrect

Q18)

You have inherited an Azure environment which has plenty of resource groups. You have been tasked to manage access, policies and compliance for the subscriptions in an efficient manner.

Solution: You decide to make use of RBAC.

Does this solution meet the goal?

- Correct
- ✅ Incorrect

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

Q19)

You need to limit outbound HTTPS traffic to specific fully qualified domain names (FQDN).

Which of the following technologies support this?

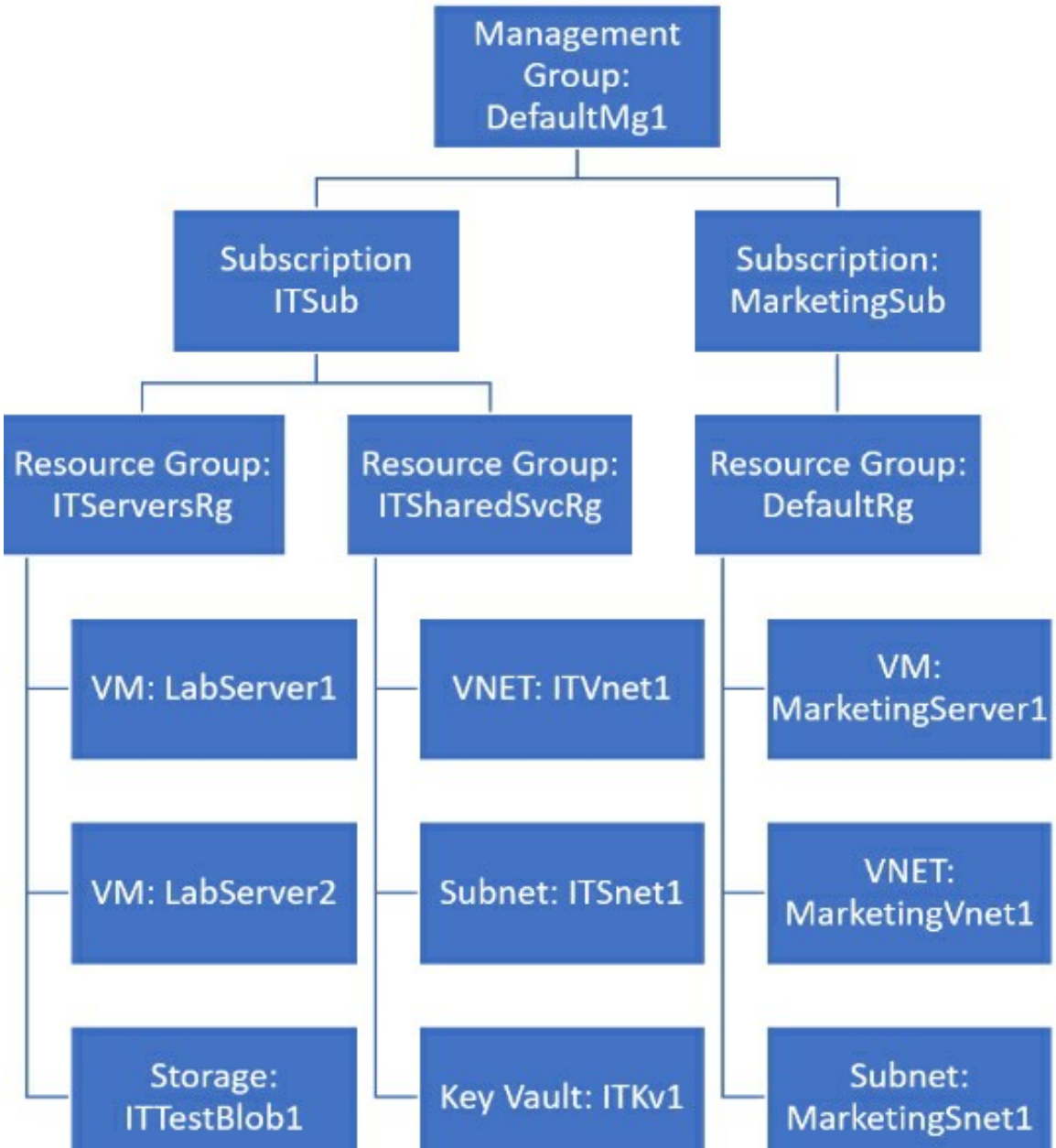
- Application Security Groups (ASG)
- ✅ Azure Firewall

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

- Network Security Groups (NSG)
- Just-in-time VM access (JIT VM Access)

Q20)

See the structure in the exhibit.



The following assignments 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:

✅ LabServer2: Contributor
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.
⚪ MarketingServer1: Contributor
⚪ MarketingServer1: None
✅ ITKv1: Reader
Explanation:-Role assignments are inherited by the child objects of the scope.
Role assignments are cumulative on overlap.
✅ MarketingServer1: Reader
Explanation:-Role assignments are inherited by the child objects of the scope.
Role assignments are cumulative on overlap.

Q21)

You have a hybrid Azure AD deployment and have just deployed an Azure SQL Database.You have deployed a custom application to a newly created VM (VM1) and you want the application to use the VM's system-assigned managed identity to access the Azure SQL Database. You have a user named User1 that wants to use the application.

What steps do you perform to accomplish your goal?

✅ Give the user permissions in the database using ALTER ROLE db_datareader ADD MEMBER [VM1]
Explanation:-Managed identities for Azure resources like VMs and registered apps enjoys quite a focus in the exam - you should know the concept, how to configure them (VMs, registered apps, SQL server etc.) and what the usage patterns are. https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-sql
✅ Create a contained database user specifying the VM managed identity in the database using CREATE USER [VM1] FROM EXTERNAL PROVIDER
Explanation:-Managed identities for Azure resources like VMs and registered apps enjoys quite a focus in the exam - you should know the concept, how to configure them (VMs, registered apps, SQL server etc.) and what the usage patterns are. https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-sql
✅ Enable the system assigned managed identity for the VM using the VM Identity blade
Explanation:-Managed identities for Azure resources like VMs and registered apps enjoys quite a focus in the exam - you should know the concept, how to configure them (VMs, registered apps, SQL server etc.) and what the usage patterns are. https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-sql
✅ Enable AD authentication on the Active Directory Admin blade of the SQL server
Explanation:-Managed identities for Azure resources like VMs and registered apps enjoys quite a focus in the exam - you should know the concept, how to configure them (VMs, registered apps, SQL server etc.) and what the usage patterns are. https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-sql
✅ Create a Azure AD user account that will serve as the SQL server administrator and assign the AD role of user
Explanation:-Managed identities for Azure resources like VMs and registered apps enjoys quite a focus in the exam - you should know the concept, how to configure them (VMs, registered apps, SQL server etc.) and what the usage patterns are. https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-sql
⚪ The application connects to the SQL server using the VM user account

---

Q22)

You need to configure temporary access to an Azure VM on port 22, the solution should manage the inbound rules automatically in the back end and remove the rules when the time period expires.

Which of the following technologies should you configure?

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

---

Q23)

You are configuring security for data in transit for an Azure App Service.

Which of the following security tasks should be performed?

Choose all that apply, do not choose any that does not apply.

- ✅ Test HTTPS
- ✅ Upload SSL Certificate
- ✅ Bind SSL Certificate

Explanation:-All the answer options should be configured for Azure App Service. See: https://docs.microsoft.com/en-us/azure/app-service/app-service-web-tutorial-custom-ssl

- ✅ HTTPS enforced
- ✅ Minimum TLS version enforced
- ⚪ None of these

Q24) What Azure resource is used when creating a security playbook?

- ✅ Azure Logic App

Explanation:-Security playbooks in Azure Security Center is based on an Azure Logic App

- ⚪ Azure Security Center
- ⚪ Azure Log Analytics
- ⚪ Azure Function
- ⚪ Azure Container Instance

Q25)

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

You need to deploy Microsoft Antimalware to the virtual machines.

Solution: You connect to each virtual machine and add a Windows feature.

Does this meet the goal?

- ⚪ Correct
- ✅ Incorrect

Explanation:-Microsoft Antimalware is deployed as an extension and not a feature.

Q26)

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

You are assigned the Global administrator role for the tenant. You are responsible for managing Azure Security Center settings.

You need to create a custom sensitivity label.

What should you do first?

- ⚪ Elevate access for global administrators in Azure AD.
- ⚪ Change Azure Security Center to use Standard-tier-pricing.
- ✅ Create a custom sensitive information type.

Explanation:-First, you need to create a new sensitive information type because you can't directly modify the default rules.

- ⚪ Enable integration with Microsoft Cloud App Security.

Q27)

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?

- ✅ Don't create a conditional access policy
- ⚪ 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
- ⚪ None of these
- ⚪ Create a conditional access policy, choose all users, choose all cloud apps, choose grant access and require MFA, enable policy

---

Q28)

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.

- ⚪ Add the AAD Global administrator's account to the "MFA bypass" group
- ✅ 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

- Create a AAD conditional access policy that grants access to the "MFA bypass" group for all applications
- Nothing; the MFA bypass group is a built-in MFA lock-out failsafe
- There is no way to bypass an AAD conditional access policy

Q29) Which of the following Azure tools can help mature the security baseline specific to securing virtual networks?

- ✅ Azure portal

Explanation:-Azure portal is correct as you can use the portal to mature network policies and processes. Azure policy is also correct as you can enforce policies that supports security baselines. Key Vault, Azure AD, Azure Security Center and Azure Monitor does not contribute to the security baseline for securing virtual networks. https://docs.microsoft.com/bs-latn-ba/azure/architecture/cloud-adoption/governance/security-baseline/toolchain

- Azure Security Center
- Azure Key Vault
- ✅ Azure policy

Explanation:-Azure portal is correct as you can use the portal to mature network policies and processes. Azure policy is also correct as you can enforce policies that supports security baselines. Key Vault, Azure AD, Azure Security Center and Azure Monitor does not contribute to the security baseline for securing virtual networks. https://docs.microsoft.com/bs-latn-ba/azure/architecture/cloud-adoption/governance/security-baseline/toolchain

- Azure AD
- Azure Monitor

Q30)

You notice a recommendation in the Azure Security Center to add a vulnerability assessment solution to your Azure virtual machines.

Which of the following options are Azure Security Center-integrated solutions to the recommendation. (Select two)

- ✅ Qualys

Explanation:-Azure Security Center supports Qualys and Rapid7 as integrated vulnerability assessment solutions. Nessus is not currently integrated with Azure Security Center. Azure Log Analytics, Azure Monitor and Microsoft ATA are not vulnerability assessment solutions related to this ASC recommendation. See: https://docs.microsoft.com/en-us/azure/security-center/security-center-vulnerability-assessment-recommendations

- Azure Log Analytics
- Nessus
- ✅ Rapid7

Explanation:-Azure Security Center supports Qualys and Rapid7 as integrated vulnerability assessment solutions. Nessus is not currently integrated with Azure Security Center. Azure Log Analytics, Azure Monitor and Microsoft ATA are not vulnerability assessment solutions related to this ASC recommendation. See: https://docs.microsoft.com/en-us/azure/security-center/security-center-vulnerability-assessment-recommendations

- Microsoft Advanced Threat Analytics
- Azure Monitor

Q31)

You have synchronized your IT departments on-premises identities with Azure AD via the AD Connect tool.

You need to onboard the rest of the on-premises users with the least amount of effort.

What should you do?

- Restart the ADConnect VM
- Uninstall and re-install the ADConnect tool
- ✅ Re-run the ADConnect tool

Explanation:-Re-run ADConnect tool is correct, this will allow you to customize the synchronization properties to add additional Object Unit filtering. Uninstall and re-install ADConnect is incorrect as this will take more effort than to re-run the ADConnect tool. Stopping the synchronization service is incorrect as this will stop all configured identities from synching. Restarting the ADConnect VM is incorrect as this will not enable you to onboard the additional users. https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-installation-wizard

- Stop the synchronization service

Q32)

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

You need to update a certificate that has become stale in the CONTOSOvault which is called “WebsiteCertificate” via an API call to the Key Vault.

Which statement below is correct?

- POST http://CONTOSOvault.vault.azure.net/certificates/WebsiteCertificate/3d31d7b36c942ad83ef36fc?api-version=7.0
- POST https://CONTOSOvault.vault.azure.net/certificates/WebsiteCertificate/3d31d7b36c942ad83ef36fc?api-version=7.0
- ✅ PATCH https://CONTOSOvault.vault.azure.net/certificates/WebsiteCertificate/3d31d7b36c942ad83ef36fc?api-version=7.0

Explanation:-PATCH is correct https://CONTOSOvault.vault.azure.net/certificates/WebsiteCertificate/3d31d7b36c942ad83ef36fc?api-version=7.0 is correct as this follows the correct way to update a specific certificate in the Azure Key Vault via API call. Here is the way the statement is used in general: PATCH {vaultBaseUrl}/certificates/{certificate-name}/{certificate-version}?api-version=7.0. using HTTP will not suffice as the Key Vaults use HTTPS by default and POST is not the correct action. https://docs.microsoft.com/en-us/rest/api/keyvault/updatecertificate/updatecertificate

- PATCH http://CONTOSOvault.vault.azure.net/certificates/WebsiteCertificate/3d31d7b36c942ad83ef36fc?api-version=7.0

Q33)

You are the administrator for the Contoso financial group. You are responsible for all storage accounts in Azure. You have been tasked to share limited access to the Blob files in storage account "Company_function" with another company for a limited time.

The other company should only be able to list and read the data in the blob storage. The other company's administrator is familiar with Azure Storage Explorer and want you to share secure access with him by using this tool.

Which information should you configure and give the administrator?

- Create Shared Access Signature for "Company_function" and configure the following: read and list permissions, service access to Blobs. Send the administrator the SAS URI to be used in Storage Explorer
- Provide the administrator with the storage name and key
- Create Shared Access Signature for "Company_function" and configure the following: start and expiry time, read and write permissions, service access to Blobs. Send the administrator the SAS URI to be used in Storage Explorer.
- ✅ Create Shared Access Signature for "Company_function" and configure the following: start and expiry time, read and list permissions, service access to Blobs. Send the administrator the SAS URI to be used in Storage Explorer

Explanation:-You need to create a Shared Access Signature for "Company_function" and configure start and expiry time as this is part of the time limitation request, list and read permissions are the least intrusive and blob storage is correct. The administrator should be able to use the SAS URI to configure access in Storage Explorer in their side. Option 1 is incorrect as there is write permissions assigned. Option 3 is incorrect as there is no time limitation set. Option 4 is incorrect as sending a storage name and key will not provide limited access as required. https://docs.microsoft.com/en-us/azure/storage/common/storage-dotnet-shared-access-signature-part-1

Q34)

Azure backup can be configured to backup on-premises VMs.

What is used to ensure data is encrypted at rest?

- Azure Recovery Services
- Transparent Data Encryption
- ✅ Passphrase

Explanation:-When using Azure backup to backup on-premises VMs a passphrase is used along with AES256 to encrypt the backup. See: https://docs.microsoft.com/en-us/azure/backup/backup-azure-backup-faq#encryption

- Azure Recovery Vault
- Azure Storage Service Encryption

Q35)

You are the administrator for the ACME banking group. You are responsible for managing the key vault in Azure. You need to create a new certificate in the ACMEvault with a key size of 2018 and that cannot be reused via an API call which should be called ACMEcertificate.

Which statement below is correct?

- GET https://ACMEvault.vault.azure.net/certificates/ACMEcertificate/create?api-version=7.0
- POST http://ACMEvault.vault.azure.net/certificates/ACMEcertificate/create?api-version=7.0
- SET https://ACMEvault.vault.azure.net/certificates/ACMEcertificate/create?api-version=7.0
- ✅ POST https://ACMEvault.vault.azure.net/certificates/ACMEcertificate/create?api-version=7.0

Explanation:-POST {https://ACMEvault.vault.azure.net}/certificates/{ACMEcertificate}/create?api-version=7.0 is correct as this follows the correct way to create a new certificate. Here is the way the statement is used in general: POST {vaultBaseUrl}/certificates/{certificate-name}/create?api-version=7.0. It uses HTTPS by default, GET and SET are incorrect when creating a new certificate. https://docs.microsoft.com/en-us/rest/api/keyvault/createcertificate/createcertificate

---

Q36)

Which of the following Azure tools can help mature the security baseline specific to detecting malicious activity?

Select all that apply.

- ✅ Azure Monitor

Explanation:-Azure Security Center is correct as this tool allows you to mature the policies and processes in your Azure environment. Azure monitor is correct as this tool can also be used in maturing polices and processes regarding security baselines in Azure. The Azure portal, Key vault, Azure AD and Azure policy cannot be used as a tool regarding a security baseline when detecting malicious activity in your Azure environment. https://docs.microsoft.com/bs-latn-ba/azure/architecture/cloud-adoption/governance/security-baseline/toolchain

- Azure policy
- Azure Key Vault
- ✅ Azure Security Center

Explanation:-Azure Security Center is correct as this tool allows you to mature the policies and processes in your Azure environment. Azure monitor is correct as this tool can also be used in maturing polices and processes regarding security baselines in Azure. The Azure portal, Key vault, Azure AD and Azure policy cannot be used as a tool regarding a security baseline when detecting malicious activity in your Azure environment. https://docs.microsoft.com/bs-latn-ba/azure/architecture/cloud-adoption/governance/security-baseline/toolchain

- Azure portal
- Azure AD

Q37)

You are in the process of creating an Azure container registry via CLI in the "MyRG" resource group.

Complete the following command to create the container registry labeled "MyContainer001".

Az (1) create –resource group MyRG –(2) MyContainer001 (3) –Basic

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

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

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

Q38)

You plan to secure remote access from your on-premises network to your AKS cluster which is deployed to an existing Azure VNet.

The solution should have the lowest possible latency and very high network speeds.

Solution: You implement a Site-to-Site VPN solution.

Does this solution meet the goal?

- Correct
- ✅ Incorrect

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

---

Q39)

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

Choose the correct list of steps to accomplish your goals.

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

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

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

---

Q40) Which of the following is true for an Azure Security Center incident?

- Any high-severity alert (not low-severity or medium-severity alerts)
- A single alert with a high probability of being a true positive
- ✅ An aggregation of alerts that align with kill chain patterns

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

- A single alert detected by more than one ASC detection mechanism
- An alert detected by Azure Advanced Threat Protection

Q41)

You are the security administrator for your Azure subscription and are reviewing the security alerts as listed in Azure Security Center.

You select one of the high-severity alerts and select the resource identified by the alert as being attacked.

What response options are available to you?

- ✅ Click run playbooks on the alert details pane

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

- ✅ Click investigate on the alert details pane

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

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

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

---

Q42)

You create an Azure Information Protection classification policy that defines a number of classification levels. You configure labels for general, sensitive and confidential. You configure the visual marker for the confidential label as watermark. A few weeks later you change the policy by creating sub labels for the confidential class as Confidential \ All Employees and Confidential \ Recipients Only.

You configure the visual marker for each of these as footer.

When the Confidential \ All Employees classification is applied to the document, which of the following visual marking(s) is/are applied?

- None
- Footer and Watermark
- Watermark
- ✔ Footer

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