Answer Sheet

Q1) 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?

✓ 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.
References: https://docs.microsoft.com/en-us/office365/securitycompliance/customize-a-built-in-sensitive-information-type
● Elevate access for global administrators in Azure AD.
● Upgrade the pricing tier of the Security Center to Standard.
● Enable integration with Microsoft Cloud App Security.

Q2) You are testing an Azure Kubernetes Service (AKS) cluster. The cluster is configured as shown in the exhibit.
You plan to deploy the cluster to production. You disable HTTP application routing.
You need to implement application routing that will provide reverse proxy and TLS termination for AKS services by using a single IP address.
What should you do?

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

Q3)

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

An administrator named Admin1 has access to the following identities:

An OpenID-enabled user account
A Hotmail account
An account in contoso.com
An account in an Azure AD tenant named fabrikam.com

You plan to use Azure Account Center to transfer the ownership of Sub1 to Admin1.

To which accounts can you transfer the ownership of Sub1?

● contoso.com only
● contoso.com, fabrikam.com, and Hotmail only
✓ contoso.com and fabrikam.com only
Explanation:-When you transfer billing ownership of your subscription to an account in another Azure AD tenant, you can move the subscription to the new account's tenant. If you do so, all users, groups, or service principals who had role based access (RBAC) to manage subscriptions and its resources lose their access. Only the user in the new account who accepts your transfer request will have access to manage the resources. You can make these transfers:
From a work or school account to another work or school account.
From a Microsoft account to a work or school account.
From a Microsoft account to another Microsoft account.
The target account must be a valid Azure Commerce account to be a valid target for transfers. For new accounts, you are asked to create an Azure Commerce account when signing in to the Azure Enterprise portal. For existing accounts, you must first create a new Azure subscription before the account is eligible. You can't make a transfer from a work or school account to a Microsoft account. When you complete a subscription transfer, Microsoft updates the account owner.

https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/ea-portal-get-started#change-account-owner
● contoso.com, fabrikam.com, Hotmail, and OpenID-enabled user account

---

Q4) Your company plans to create separate subscriptions for each department. Each subscription will be associated to the same Azure Active Directory (Azure AD) tenant.
You need to configure each subscription to have the same role assignments.
What should you use?

● Azure Policy
● Azure AD Privileged Identity Management (PIM)
✓ Azure Blueprints
Explanation:-Just as a blueprint allows an engineer or an architect to sketch a project's design parameters, Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements.
Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:
• Role Assignments
• Policy Assignments
• Azure Resource Manager templates
• Resource Groups
Reference: https://docs.microsoft.com/en-us/azure/governance/blueprints/overview

● Azure Security Center

Q5)

Your network contains an on-premises Active Directory domain named corp.contoso.com.

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

You sync all on-premises identities to Azure AD.

You need to prevent users who have a givenName attribute that starts with TEST from being synced to Azure AD. The solution must minimize administrative effort.

What should you use?

✓ Synchronization Rules Editor
Explanation:-Use the Synchronization Rules Editor and write attribute-based filtering rule.
References: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration
● Web Service Configuration Tool
● the Azure AD Connect wizard
● Active Directory Users and Computers

Q6) Your network contains an Active Directory forest named contoso.com. The forest contains a single domain.
You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
You plan to deploy Azure AD Connect and to integrate Active Directory and the Azure AD tenant.
You need to recommend an integration solution that meets the following requirements:
• Ensures that password policies and user logon restrictions apply to user accounts that are synced to the tenant
• Minimizes the number of servers required for the solution.
Which authentication method should you include in the recommendation?

● password hash synchronization with seamless single sign-on (SSO)
✓ pass-through authentication with seamless single sign-on (SSO)
Explanation:-Pass Through Authentication. The reason being:
1. Ensures that password policies and user logon restrictions apply to user accounts that are synced to the tenant >> Pass-Through Authentication enforce on-premises user account states, password policies, and sign-in hours.
2. Minimizes the number of servers required for the solution. >> Pass-through needs a lightweight agent to be installed one (or more) on-premises servers.
References: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta
● federated identity with Active Directory Federation Services (AD FS)
● Managed Domain environment

Q7) You have an Azure subscription named Subscription1 that contains a virtual network named VNet1. VNet1 is in a resource group named RG1.
Subscription1 has a user named User1. User1 has the following roles:
• Reader
• Security Admin
• Security Reader
You need to ensure that User1 can assign the Reader role for VNet1 to other users.
What should you do?

● Remove User1 from the Security Reader and Reader roles for Subscription1.
● Assign User1 the Network Contributor role for VNet1.
✓ Assign User1 the Owner role for VNet1.
● Remove User1 from the Security Reader and Reader roles for Subscription1. Assign User1 the Contributor role for Subscription1.

Q8) You have an Azure Active Directory (Azure AD) tenant.
You have an existing Azure AD conditional access policy named Policy1. Policy1 enforces the use of Azure AD-joined devices when members of the Global
Administrators group authenticate to Azure AD from untrusted locations.
You need to ensure that members of the Global Administrators group will also be forced to use multi-factor authentication when authenticating from untrusted locations.
What should you do?

● From multi-factor authentication page, modify the service settings.
● From the Azure portal, modify session control of Policy1.
✓ From the Azure portal, modify grant control of Policy1.
● From multi-factor authentication page, modify the user settings.

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
● 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.
Note: Signals are emitted by the target resource and can be of several types. Metric, Activity log, Application Insights, and Log.
References: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-metric

● Activity Log

Q10) You have an Azure Subscription named Sub1.
You have an Azure Storage account named Sa1 in a resource group named RG1.
Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies.
You discover that unauthorized users accessed both the file service and the blob service.
You need to revoke all access to Sa1.
Solution: You generate new SASs.
Does this meet the goal?

● Correct

✓ Incorrect

Explanation:-Instead you should create a new stored access policy.
To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately affects all of the shared access signatures associated with it.
References: https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

---

Q11) You have an Azure Subscription named Sub1.
You have an Azure Storage account named Sa1 in a resource group named RG1.
Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies.
You discover that unauthorized users accessed both the file service and the blob service.
You need to revoke all access to Sa1.
Solution: You create a new stored access policy.
Does this meet the goal?

✓ Correct

Explanation:-To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately effects all of the shared access signatures associated with it.
References: https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

● Incorrect

Q12) You have an Azure subscription.
You create an Azure web app named Contoso1812 that uses an S1 App service plan.
You create a DNS record for www.contoso.com that points to the IP address of Contoso1812.
You need to ensure that users can access Contoso1812 by using the https://www.contoso.com URL.
Which two actions should you perform? Each correct answer presents part of the solution.

● Turn on the system-assigned managed identity for Contoso1812.

✓ Add a hostname to Contoso1812.

Explanation:-You can configure Azure DNS to host a custom domain for your web apps. For example, you can create an Azure web app and have your users access it using either www.contoso.com or contoso.com as a fully qualified domain name (FQDN).
To do this, you have to create three records: A root "A" record pointing to contoso.com A root "TXT" record for verification A "CNAME" record for the www name that points to the A record

● Scale out the App Service plan of Contoso1812.

● Add a deployment slot to Contoso1812.

● Scale up the App Service plan of Contoso1812.

✓ Upload a PFX file to Contoso1812

Explanation:-To use HTTPS, you need to upload a PFX file to the Azure Web App. The PFX file will contain the SSL certificate required for HTTPS.
References: https://docs.microsoft.com/en-us/azure/dns/dns-web-sites-custom- domain

---

Q13) You have an Azure subscription named Sub1.
You have an Azure Storage account named Sa1 in a resource group named RG1.
Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies.
You discover that unauthorized users accessed both the file service and the blob service.
You need to revoke all access to Sa1.
Solution: You create a lock on Sa1.
Does this meet the goal?

● Correct

✓ Incorrect

Explanation:-To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately affects all of the shared access signatures associated with it.
References: https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

---

Q14) You have a hybrid configuration of Azure Active Directory (Azure AD).
You have an Azure HDInsight cluster on a virtual network.
You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.
You need to configure the environment to support the planned authentication.
Solution: You deploy Azure Active Directory Domain Services (Azure AD DS) to the Azure subscription.
Does this meet the goal?

● Correct
✓ Incorrect

Explanation:-Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.
Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:
• Create Azure Virtual Network.
• Create a custom DNS server in the Azure Virtual Network.
• Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.
• Configure forwarding between the custom DNS server and your on-premises DNS server.
References: https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

---

Q15) You are planning on rolling out Privilege Identity Management (PIM) to the IT and Dev department. Which of the following licenses should be assigned to your directory to enable this functionality? Select all that apply.

● Azure AD P1
✓ Azure AD P2

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

● EMS E3
✓ EMS E5

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

✓ Microsoft 365 M5

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

---

Q16) Your network contains an Active Directory forest named contoso.com. You have an Azure Directory (Azure AD) tenant named contoso.com.
You plan to configure synchronization by using the Express Settings installation option in Azure AD Connect.
You need to identify which roles and groups are required to perform the planned configuration. The solution must use the principle of least privilege.
Which two roles and groups should you identify? Each correct answer presents part of the solution.

● the Domain Admins group in Active Directory
● the Security administrator role in Azure AD
✓ the Global administrator role in Azure AD

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

● the User administrator role in Azure AD
✓ the Enterprise Admins group in Active Directory

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

---

Q17) 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).
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 Intune 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?

✓ Correct

Explanation:-This option is correct, 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

● Incorrect

Q18) 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).
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? Select 2 methods.

✓ 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

● Manager

● Location

✓ 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

Q19) 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).
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?

✓ 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

● Privilege Identity Management

● Identity Protection

Q20) 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).
Correct or Incorrect: You can configure an Azure Conditional Access policy for client applications like Microsoft Word.

● Correct

✓ Incorrect

Explanation:-This option is correct, 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

Q21) 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).
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? Choose all that apply.

● Android

● iOS

● Windows Phone

● macOS

✓ All of these

Explanation:-All of these are correct. 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

Q22) 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).
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?

● Correct
✓ Incorrect

Explanation:-This option is correct as 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

---

Q23) 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).
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? Select all that apply.

● The work or school account used in the configuration wizard to setup directory synchronization has been deleted, disabled or password expired
● The admin account used for directory synchronization was changed
● There are network connection issues
● Directory synchronization service has stopped
✓ All of these

Explanation:-All of these is correct as 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

---

Q24) 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).
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?

✓ Correct

Explanation:-This option is correct as 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

● Incorrect

Q25) 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).
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?

● Correct
✓ Incorrect
Explanation:-This option is correct. 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

---

Q26) You have a hybrid configuration of Azure Active Directory (Azure AD).
You have an Azure HDInsight cluster on a virtual network.
You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.
You need to configure the environment to support the planned authentication.
Solution: You deploy an Azure AD Application Proxy.
Does this meet the goal?

● Correct
✓ Incorrect
Explanation:-Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.
Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:
• Create Azure Virtual Network.
• Create a custom DNS server in the Azure Virtual Network.
• Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.
• Configure forwarding between the custom DNS server and your on-premises DNS server.
Reference: https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

---

Q27) You have an Azure Subscription named Sub1.
You have an Azure Storage account named Sa1 in a resource group named RG1.
Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies.
You discover that unauthorized users accessed both the file service and the blob service.
You need to revoke all access to Sa1.
Solution: You regenerate the access keys.
Does this meet the goal?

● Correct
✓ Incorrect
Explanation:-Instead you should create a new stored access policy.
To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately affects all of the shared access signatures associated with it.
Reference: https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

---

Q28) You have a hybrid configuration of Azure Active Directory (Azure AD). You have an Azure SQL Database instance that is configured to support Azure AD authentication.
Database developers must connect to the database instance and authenticate by using their on-premises Active Directory account.
You need to ensure that developers can connect to the instance by using Microsoft SQL Server Management Studio. The solution must minimize authentication prompts.
Which authentication method should you recommend?

✓ Active Directory - Password
Explanation:-Use Active Directory password authentication when connecting with an Azure AD principal name using the Azure AD managed domain.
Use this method to authenticate to SQL DB/DW with Azure AD for native or federated Azure AD users. A native user is one explicitly created in Azure AD and being authenticated using user name and password, while a federated user is a Windows user whose domain is federated with Azure AD. The latter method (using user & password) can be used when a user wants to use their windows credential, but their local machine is not joined with the domain (for example, using a remote access). In this case, a Windows user can indicate their domain account and password and can authenticate to SQL DB/DW using federated credentials.
References: https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure
● Active Directory - Universal with MFA support
● SQL Server Authentication
● Active Directory - Integrated

Q29) You plan to use Azure Resource Manager templates to perform multiple deployments of identically configured Azure virtual machines. The password for the administrator account of each deployment is stored as a secret in different Azure key vaults.
You need to identify a method to dynamically construct a resource ID that will designate the key vault containing the appropriate secret during each deployment.
The name of the key vault and the name of the secret will be provided as inline parameters.
What should you use to construct the resource ID?

● a key vault access policy
✓ a linked template
Explanation:-you can dynamically generate the resource ID for a key vault secret by using a linked template.
Reference: https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter?tabs=azure-cli#reference-secrets-with-dynamic-id
https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter?tabs=azure-cli
● a parameters file
● an automation account

Q30) You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
An administrator named Admin1 has access to the following identities:
• An OpenID-enabled user account
• A Hotmail account
• An account in contoso.com
• An account in an Azure AD tenant named fabrikam.com
You plan to use Azure Account Center to transfer the ownership of Sub1 to Admin1.
To which accounts can you transfer the ownership of Sub1?

● contoso.com only
● contoso.com, fabrikam.com, and Hotmail only
✓ contoso.com and fabrikam.com only

Explanation:-When you transfer billing ownership of your subscription to an account in another Azure AD tenant, you can move the subscription to the new account's tenant. If you do so, all users, groups, or service principals who had role based access (RBAC) to manage subscriptions and its resources lose their access. Only the user in the new account who accepts your transfer request will have access to manage the resources.
Reference: https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer
https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer#transferring-subscription-to-an-account-in-another-azure-ad-tenant

● contoso.com, fabrikam.com, Hotmail, and OpenID-enabled user account

---

Q31) You have Azure Resource Manager templates that you use to deploy Azure virtual machines.
You need to disable unused Windows features automatically as instances of the virtual machines are provisioned.
What should you use?

● device configuration policies in Microsoft Intune
✓ an Azure Desired State Configuration (DSC) virtual machine extension

Explanation:-You can use Azure Automation State Configuration to manage Azure VMs (both Classic and Resource Manager), on-premises VMs, Linux machines, AWS VMs, and on-premises physical machines.
Note: Azure Automation State Configuration provides a DSC pull server similar to the Windows Feature DSC-Service so that target nodes automatically receive configurations, conform to the desired state, and report back on their compliance. The built-in pull server in Azure Automation eliminates the need to set up and maintain your own pull server. Azure Automation can target virtual or physical Windows or Linux machines, in the cloud or on-premises.
Reference: https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started

● application security groups
● Azure Logic Apps
● security policies in Azure Security Center
● Azure Advisor

Q32) You are configuring an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry.
You need to use the auto-generated service principal to authenticate to the Azure Container Registry.
What should you create?

● an Azure Active Directory (Azure AD) group
✓ an Azure Active Directory (Azure AD) role assignment

Explanation:-When you create an AKS cluster, Azure also creates a service principal to support cluster operability with other Azure resources. You can use this auto-generated service principal for authentication with an ACR registry. To do so, you need to create an Azure AD role assignment that grants the cluster's service principal access to the container registry.
References: https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-auth-aks

● an Azure Active Directory (Azure AD) user
● a secret in Azure Key Vault

Q33) You have an Azure subscription named Sub1.
You create a virtual network that contains one subnet. On the subnet, you provision the virtual machines shown in the following table.
Currently, you have not provisioned any network security groups (NSGs).
You need to implement network security to meet the following requirements:
• Allow traffic to VM4 from VM3 only.
• Allow traffic from the Internet to VM1 and VM2 only.
• Minimize the number of NSGs and network security rules.
How many NSGs and network security rules should you create?

● 2 NSGs and 2 Network security rules
✓ 2 NSGs and 3 Network security rules

Explanation:-You cannot specify multiple service tags or application groups) in a security rule.
References: https://docs.microsoft.com/en-us/azure/virtual-network/security-overview

● 1 NSG and 2 Network security rules
● 2 NSGs and 4 Network security rules

Q34) You have the Azure virtual machines shown in the following table.
You create an Azure Log Analytics workspace named Analytics1 in RG1 in the East US region.
Which virtual machines can be enrolled in Analytics1?

● VM1 only
● VM1, VM2, and VM3 only
✓ VM1, VM2, VM3, and VM4

Explanation:-You can monitor Azure VMs in any region. The VMs themselves aren't limited to the regions supported by the Log Analytics workspace. So region doesn't matter. You can enable multiple Azure VMs or virtual machine scale sets across a specified subscription or resource group
So we can create Log analytics in US region and install agents on machines on any region then with providing Log Analytics Workspace key and

connection we can collect data from any machine in any region.
References https://docs.microsoft.com/en-us/azure/azure-monitor/insights/vminsights-enable-overview

● VM1 and VM4 only

Q35) You use Azure Security Center for the centralized policy management of three Azure subscriptions.
You use several policy definitions to manage the security of the subscriptions.
You need to deploy the policy definitions as a group to all three subscriptions.
Solution: You create a policy definition and assignments that are scoped to resource groups.
Does this meet the goal?

● Correct
✓ Incorrect

Explanation:-References: https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-management-groups/

Q36) You have an Azure Subscription. The subscription contains 50 virtual machines that run Windows Server 2012 R2 or Windows Server 2016.
You need to deploy Microsoft Antimalware to the virtual machines.
Solution: You add an extension to each virtual machine.
Does this meet the goal?

✓ Correct

Explanation:-You can use Visual Studio to enable and configure the Microsoft Antimalware service. This entails selecting Microsoft Antimalware extension from the dropdown list under Installed Extensions and click Add to configure with default antimalware configuration.
References: https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware

● Incorrect

Q37) 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.
References: https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware

Q38) From Azure Security Center, you create a custom alert rule.
You need to configure which users will receive an email message when the alert is triggered.
What should you do?

✓ From Azure Monitor, create an action group.

Explanation:-Reference: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/action-groups

● From Security Center, modify the Security policy settings of the Azure subscription.
● From Azure Active Directory (Azure AD), modify the members of the Security Reader role group.
● From Security Center, modify the alert rule.

Q39) You have an Azure subscription that contains the virtual networks shown in the following table.
The subscription contains the virtual machines shown in the following table.
On NIC1, you configure an application security group named ASG1.br>On which other network interfaces can you configure ASG1?

● NIC2, NIC3, NIC4, and NIC5
✓ NIC2 and NIC3 only

Explanation:-Only network interfaces in NVET1, which consists of Subnet11 and Subnet12, can be configured in ASG1, as all network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in.
Reference: https://azure.microsoft.com/es-es/blog/applicationsecuritygroups/

● NIC2 only
● NIC2, NIC3, and NIC4 only

Q40) You have 15 Azure virtual machines in a resource group named RG1.
All virtual machines run identical applications.
You need to prevent unauthorized applications and malware from running on the virtual machines.
What should you do?

● Apply an Azure policy to RG1.
✓ From Azure Security Center, configure adaptive application controls.

Explanation:-Adaptive application control is an intelligent, automated end-to-end application whitelisting solution from Azure Security Center. It helps you control which applications can run on your Azure and non-Azure VMs (Windows and Linux), which, among other benefits, helps harden your VMs against malware. Security Center uses machine learning to analyze the applications running on your VMs and helps you apply the specific whitelisting rules using this intelligence.
Reference: https://docs.microsoft.com/en-us/azure/security-center/security-center-adaptive-application

● Configure Azure Active Directory (Azure AD) Identity Protection.
● Apply a resource lock to RG1.

Q41) You plan to deploy Azure container instances.
You have a containerized application that validates credit cards. The application is comprised of two containers: an application

container and a validation container.
The application container is monitored by the validation container. The validation container performs security checks by making requests to the application container and waiting for responses after every transaction.
You need to ensure that the application container and the validation container are scheduled to be deployed together. The containers must communicate to each other only on ports that are not externally exposed.
What should you include in the deployment?

● application security groups
● network security groups (NSGs)
● management groups
✓ container groups

Explanation:-Azure Container Instances supports the deployment of multiple containers onto a single host using a container group. A container group is useful when building an application sidecar for logging, monitoring, or any other configuration where a service needs a second attached process.
Reference: https://docs.microsoft.com/en-us/azure/container-instances/container-instances-container-groups

---

Q42) You use Azure Security Center for the centralized policy management of three Azure subscriptions.
You use several policy definitions to manage the security of the subscriptions.
You need to deploy the policy definitions as a group to all three subscriptions.
Solution: You create a policy initiative and assignments that are scoped to resource groups.
Does this meet the goal?

● Correct
✓ Incorrect

Explanation:-Instead use a management group.
Management groups in Microsoft Azure solve the problem of needing to impose governance policy on more than one Azure subscription simultaneously.
Reference: https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-management-groups/

Q43) 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?

✓ 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.
References: https://docs.microsoft.com/en-us/office365/securitycompliance/customize-a-built-in-sensitive-information-type

● Elevate access for global administrators in Azure AD.
● Change Azure Security Center to use Standard-tier-pricing.
● Enable integration with Microsoft Cloud App Security.

Q44) You have an Azure subscription named Sub1 that contains the virtual machines shown in the following table.
You need to ensure that the virtual machines in RG1 have the Remote Desktop port closed until an authorized user requests access.
What should you configure?

● Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
● an application security group
● Azure Active Directory (Azure AD) conditional access
✓ just in time (JIT) VM access

Explanation:-Just-in-time (JIT) virtual machine (VM) access can be used to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.
Note: When just-in-time is enabled, Security Center locks down inbound traffic to your Azure VMs by creating an NSG rule. You select the ports on the VM to which inbound traffic will be locked down. These ports are controlled by the just-in-time solution.
When a user requests access to a VM, Security Center checks that the user has Role-Based Access Control (RBAC) permissions that permit them to successfully request access to a VM. If the request is approved, Security Center automatically configures the Network Security Groups (NSGs) and Azure Firewall to allow inbound traffic to the selected ports and requested source IP addresses or ranges, for the amount of time that was specified. After the time has expired, Security
Center restores the NSGs to their previous states. Those connections that are already established are not being interrupted, however.
Reference: https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time

---

Q45) You have an Azure subscription that contains the virtual machines shown in the following table.
From Azure Security Center, you turn on Auto Provisioning.
You deploy the virtual machines shown in the following table.
On which virtual machines is the Log Analytics agent installed?

● VM3 only
● VM1 and VM3 only
● VM3 and VM4 only
✓ VM1, VM2, VM3, and VM4

Explanation:-When automatic provisioning is On, Security Center provisions the Log Analytics Agent on all supported Azure VMs and any new ones that are created.
Supported Operating systems include: Ubuntu 14.04 LTS (x86/x64), 16.04 LTS (x86/x64), and 18.04 LTS (x64) and Windows Server 2008 R2, 2012, 2012 R2, 2016, version 1709 and 1803
Reference: https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection

---

Q46) 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?

● an application permission without 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.
References: https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-access-web-apis
● a delegated permission that requires admin consent
● an application permission that requires admin consent

Q47) Your company has an Azure subscription named Sub1 that is associated to an Azure Active Directory Azure (Azure AD) tenant named contoso.com.
The company develops a mobile application named App1. App1 uses the OAuth 2 implicit grant type to acquire Azure AD access tokens.
You need to register App1 in Azure AD.
What information should you obtain from the developer to register the application?

✓ a redirect URI
Explanation:-For Native Applications you need to provide a Redirect URI, which Azure AD will use to return token responses.
References: https://docs.microsoft.com/en-us/azure/active-directory/develop/v1-protocols-oauth-code
● a reply URL
● a key
● an application ID

Q48) From the Azure portal, you are configuring an Azure policy.
You plan to assign policies that use the DeployIfNotExist, AuditIfNotExist, Append, and Deny effects.
Which effect requires a managed identity for the assignment?

● AuditIfNotExist
● Append
✓ DeployIfNotExist
Explanation:-When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity.
References: https://docs.microsoft.com/bs-latn-ba/azure/governance/policy/how-to/remediate-resources
● Deny

Q49) You have an Azure subscription that contains an Azure key vault named Vault1.
In Vault1, you create a secret named Secret1.
An application developer registers an application in Azure Active Directory (Azure AD).
You need to ensure that the application can use Secret1.
What should you do?

✓ In Azure AD, create a role.
Explanation:-Azure Key Vault provides a way to securely store credentials and other keys and secrets, but your code needs to authenticate to Key Vault to retrieve them.
Managed identities for Azure resources overview makes solving this problem simpler, by giving Azure services an automatically managed identity in Azure Active
Directory (Azure AD). You can use this identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without having any credentials in your code.
Example: How a system-assigned managed identity works with an Azure VM
After the VM has an identity, use the service principal information to grant the VM access to Azure resources. To call Azure Resource Manager, use role-based access control (RBAC) in Azure AD to assign the appropriate role to the VM service principal. To call Key Vault, grant your code access to the specific secret or key in Key Vault.
References: https://docs.microsoft.com/en-us/azure/key-vault/quick-create-net
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview
● In Azure Key Vault, create a key.
● In Azure Key Vault, create an access policy.
● In Azure AD, enable Azure AD Application Proxy.

Q50) You have an Azure SQL database.
You implement Always Encrypted.
You need to ensure that application developers can retrieve and decrypt data in the database.br>Which two pieces of information should you provide to the developers? Each correct answer presents part of the solution.

● a stored access policy
● a shared access signature (SAS)
✓ the column encryption key
Explanation:-Always Encrypted uses two types of keys: column encryption keys and column master keys. A column encryption key is used to encrypt data in an encrypted column. A column master key is a key-protecting key that encrypts one or more column encryption keys.
References: https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine
● user credentials
✓ the column master key
Explanation:-Always Encrypted uses two types of keys: column encryption keys and column master keys. A column encryption key is used to encrypt data in an encrypted column. A column master key is a key-protecting key that encrypts one or more column encryption keys.
References: https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine

Q51) You have a hybrid configuration of Azure Active Directory (Azure AD).
All users have computers that run Windows 10 and are hybrid Azure AD joined.

You have an Azure SQL database that is configured to support Azure AD authentication.
Database developers must connect to the SQL database by using Microsoft SQL Server Management Studio (SSMS) and authenticate by using their on-premises Active Directory account.
You need to tell the developers which authentication method to use to connect to the SQL database from SSMS. The solution must minimize authentication prompts.
Which authentication method should you instruct the developers to use?

● SQL Login
● Active Directory "" Universal with MFA support
✓ Active Directory "" Integrated

Explanation:-Azure AD can be the initial Azure AD managed domain. Azure AD can also be an on-premises Active Directory Domain Services that is federated with the Azure AD.
Using an Azure AD identity to connect using SSMS or SSDT
The following procedures show you how to connect to a SQL database with an Azure AD identity using SQL Server Management Studio or SQL Server Database Tools.
Active Directory integrated authentication
Use this method if you are logged in to Windows using your Azure Active Directory credentials from a federated domain.
1. Start Management Studio or Data Tools and in the Connect to Server (or Connect to Database Engine) dialog box, in the Authentication box, select Active Directory - Integrated. No password is needed or can be entered because your existing credentials will be presented for the connection.
2. Select the Options button, and on the Connection Properties page, in the Connect to database box, type the name of the user database you want to connect to. (The AD domain name or tenant ID" option is only supported for Universal with MFA connection options, otherwise it is greyed out.)
References: https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/sql-database/sql-database-aad-authentication-configure.md

● Active Directory "" Password

Q52) You have an Azure SQL Database server named SQL1.
You plan to turn on Advanced Threat Protection for SQL1 to detect all threat detection types.
Which action will Advanced Threat Protection detect as a threat?

● A user updates more than 50 percent of the records in a table.
✓ A user attempts to sign as select * from table1.

Explanation:-Advanced Threat Protection can detect potential SQL injections: This alert is triggered when an active exploit happens against an identified application vulnerability to SQL injection. This means the attacker is trying to inject malicious SQL statements using the vulnerable application code or stored procedures.
References: https://docs.microsoft.com/en-us/azure/sql-database/sql-database-threat-detection-overview

● A user is added to the db_owner database role.
● A user deletes more than 100 records from the same table.

Q53) You have 10 virtual machines on a single subnet that has a single network security group (NSG).
You need to log the network traffic to an Azure Storage account.
Which two actions should you perform? Each correct answer presents part of the solution.

● Install the Network Performance Monitor solution.
✓ Enable Azure Network Watcher.

Explanation:-A network security group (NSG) enables you to filter inbound traffic to, and outbound traffic from, a virtual machine (VM). You can log network traffic that flows through an NSG with Network Watcher's NSG flow log capability. Steps include:
• Create a VM with a network security group
• Enable Network Watcher and register the Microsoft.Insights provider
• Enable a traffic flow log for an NSG, using Network Watcher's NSG flow log capability
• Download logged data
• View logged data
Reference: https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-portal

● Enable diagnostic logging for the NSG.
✓ Enable NSG flow logs.

Explanation:-A network security group (NSG) enables you to filter inbound traffic to, and outbound traffic from, a virtual machine (VM). You can log network traffic that flows through an NSG with Network Watcher's NSG flow log capability. Steps include:
• Create a VM with a network security group
• Enable Network Watcher and register the Microsoft.Insights provider
• Enable a traffic flow log for an NSG, using Network Watcher's NSG flow log capability
• Download logged data
• View logged data
Reference: https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-portal

● Create an Azure Log Analytics workspace.

Q54) 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?

✓ Workflow automation

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

● Azure Logic Apps Designer
● Azure Monitor
● Azure DevOps
● Azure Application Insights