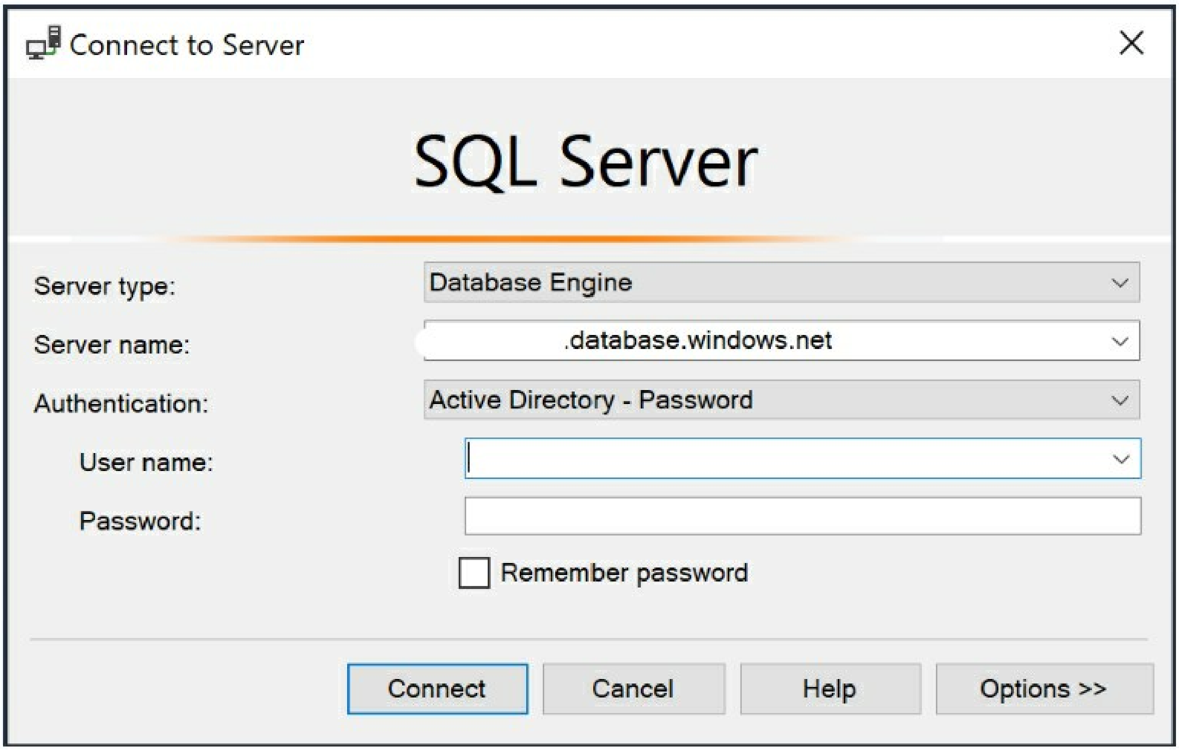
Answer Sheet

Q1)

You're like the most awesome SQL DBA ever. You connect to your Azure SQL Database using SSMS and authenticate using the dialog as in the exhibit.



Server type: Database Engine

Server name: .database.windows.net

Authentication: Active Directory - Password

User name:

Password:

□ Remember password

Which user account credentials do you supply?

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

Q2)

You need to ensure that data is secured in transit for a web application on your Azure subscription.

Which of the following is required? Each answer is part of the solution and you have to minimize costs. (Choose 4)

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

Create a self-signed certificate - no, this is not supported with app service.
Create SSL bindings - yes, to ensure the all browser comms are encrypted to the web app.
Deploy Azure Application Gateway - no, this is not required to enable TLS, but you might want to deploy it to provide additional layer of security.

✓ Upload a certificate to Azure Key Vault

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

Q3)

Your organisation has a new regulatory requirement that all cloud VM deployments must meet the Center for Internet Security Hardened Benchmarks.

How can you ensure that this requirement is met while minimising costs, downtime and administrative effort?

Each option represents part of the solution and is not listed in order.

Select each of the options that you should do.

✓ Redeploy non-compliant VMs

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

✓ Review compliance against Azure Policy

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

● Download CIS-compliant VM images from www.cisecurity.org

✓ Assign a custom Azure Policy

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

● Assign a built-in Azure Policy

✓ Choose a CIS VM image when creating new VMs

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

Q4) You have a preconfigured Kay Vault and VM. Which of the following steps do you have to perform to apply ADE to a VM?

✓ Use the Set-AzVMDiskEncryptionExtension PowerShell commandlet

Explanation:-Enable the key vault for volume encryption.
Use the Set-AzVMDiskEncryptionExtension PowerShell commandlet.
https://docs.microsoft.com/en-us/azure/security/azure-disk-encryption-windows-powershell-quickstart

● Enable the key vault for virtual machines deployment

● Enable the key vault for volume encryption

● Use the New-AzKeyvault PowerShell commandlet

● Use the Get-AzKeyvault PowerShell commandlet

Q5)

A certain user is in scope for the global information protection policy in AIP as well as for a number of other policies. These policies have conflicting settings.

Which settings are effectively applied to the user?

● The least restrictive policy

✓ The last policy on the list

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

● The most restrictive policy

● The first policy on the list

Q6)

Using a connection string containing the access key in an application configuration filr to access an Azure storage account is considered insecure. Microsoft recommends to use Azure Key vault to store the connection string for use with the applicaiton.

How does Azure Key vault ensure that only authorised accounts get to access the connection string? Each answer is part of the solution.

● Network Security Group

✓ Azure RBAC

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

✓ Azure AD App registration

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

● Built-in firewall

● Azure Application Gateway with Web Application Firewall

Q7) 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 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?

✓ Correct

Explanation:-This option is correct, “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

● Incorrect

Q8) 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 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?

● Owner role

● 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

● Security administrator role

Q9) 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 the On-premises data gateway to the on-premises network. Does this meet the goal?

✓ 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 cust

● Correct

**Q10) 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 login 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)

Explanation:-Password hash synchronization requires the least effort regarding deployment, maintenance, and infrastructure. This level of effort typically applies to organizations that only need their users to sign in to Office 365, SaaS apps, and other Azure AD-based resources. When turned on, password hash synchronization is part of the Azure AD Connect sync process and runs every two minutes. Incorrect Answers: A: A federated authentication system relies on an external trusted system to authenticate users

● pass-through authentication with seamless single sign-on (SSO)

● federated identity with Active Directory Federation Services (AD FS)

Q11) 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?

● Web Service Configuration Tool

● the Azure AD Connect wizard

● Active Directory Users and Computers

✓ Synchronization Rules Editor

Explanation:-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?

Q12) 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 Blueprints

✓ Azure AD Privileged Identity Management (PIM)

Explanation:-The Azure AD Privileged Identity Management (PIM) service also allows Privileged Role Administrators to make permanent admin role assignments.

● Azure Policy

● Azure Security Center

Q13) 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?

● Scale out the App Service plan of Contoso1812.

✓ Scale up the App Service plan of 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 E: To map a custom DNS name to a web app, the web app's App Service plan must be a

● 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 E: To map a custom DNS name to a web app, the web app's App Service plan must be a paid tier (Shared, Basic, Standard, Premium or Consumption for Azure Refer: https://docs.microsoft.com/en-us/azure/dns/dns-web-sites-custom-domain

---

Q14) What are the three items you have to configure when creating an Azure Monitor Alert Rule?

● Notification

✓ Condition

Explanation:-Resource, condition and action. Notification can be configured as an action. Condition contains the signal and alert logic.

● Subscription

✓ Action

Explanation:-Resource, condition and action. Notification can be configured as an action. Condition contains the signal and alert logic.

● Resource group

✓ Resource

Explanation:-Resource, condition and action. Notification can be configured as an action. Condition contains the signal and alert logic.

Q15)

You have a storage account named "BlobStore" and you have noticed that anyone can access this storage account over the internet.

You need to secure this storage account so that only users from the Head Office with IP 197.145.42.202/32 can access this storage account, however you still require anonymous access over the internet to the storage metrics for this account.

Which 2 options should you configure?

● Configure Allow access from all networks
✓ Configure IP ranges under the firewall section and specify 197.145.42.202/32
● Allow trusted Microsoft services to access this storage account
● Configure Allow access from selected networks and specify 197.145.42.202/32

Explanation:-You need to specify the public IP address range you want to allow under the firewall section for the storage account. You need to allow only read access to storage metrics from any network. https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security

✓ Allow read access to storage metrics from any network

Q16) You plan on deploying anti-malware solution to your LOB application VM via security extension. Is it possible to add the anti-malware security extension on top of the built-in Windows Defender anti-malware solution running locally on the VM?

✓ Correct

Explanation:-It is possible to add the Azure VM Antimalware extension. It is to be noted that Windows Server 2016 OS has Windows Defender built-in by default which protects against malware. However, if you run the Azure VM Antimalware extension on top of Windows Defender, the extension will apply any optional configuration policies to be used by Windows Defender and that the extension will not deploy any additional antimalware services. https://docs.microsoft.com/en-us/azure/security/azure-security-antimalware

● Incorrect

Q17) 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?

✓ 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

✓ 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

● Enable the system assigned managed identity for the VM using the Azure Active Directory blade
✓ 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

✓ 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

✓ The application connects to the SQL server using the Access token

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

---

Q18) When creating a new AIP label, what four areas can be configured?

● General
✓ Common

Explanation:-Common: Name and description
Marking: Visual marking, header, footer, watermark
Protection: Encryption key selection, permissions, expiration
Conditions: Built-in or custom REGEX pattern matching

✓ Marking

Explanation:-Common: Name and description
Marking: Visual marking, header, footer, watermark
Protection: Encryption key selection, permissions, expiration
Conditions: Built-in or custom REGEX pattern matching

✓ Protection

Explanation:-Common: Name and description
Marking: Visual marking, header, footer, watermark
Protection: Encryption key selection, permissions, expiration
Conditions: Built-in or custom REGEX pattern matching

● Encryption
✓ Conditions

Explanation:-Common: Name and description

Marking: Visual marking, header, footer, watermark
Protection: Encryption key selection, permissions, expiration
Conditions: Built-in or custom REGEX pattern matching

Q19) See the exhibit.
You have a corporate compliance requirement that mandates bring your own key for all storage accounts for data at rest encryption. Which area would you use to configure this?

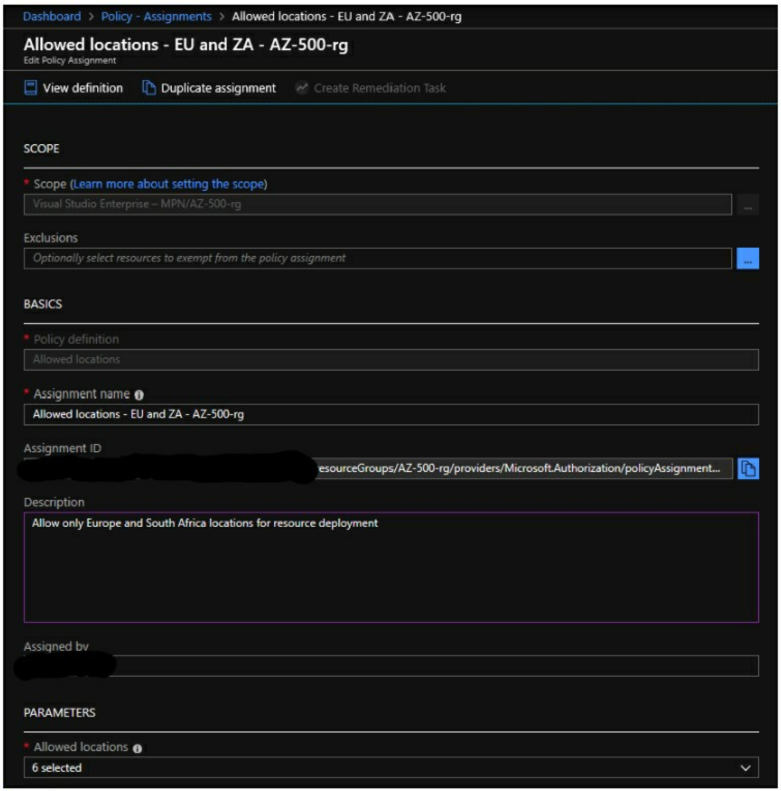
● Access control (IAM)
● Data transfer
● Access keys
✓ Encryption
Explanation:-You can use the Encryption configiuration option to configure BYOK for a storage account with integration with Azure Key Vault.
● Shared access signature

Q20) In Azure Information Protection there are three types of key scenarios. Match the key scenario with the technology used to create and maintain the keys. Choose 3.

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

Q21)

You create an Azure Policy assignment as in the exhibit.



Dashboard > Policy - Assignments > Allowed locations - EU and ZA - AZ-500-rg

Allowed locations - EU and ZA - AZ-500-rg
Edit Policy Assignment

View definition | Duplicate assignment | Create Remediation Task

SCOPE

* Scope (Learn more about setting the scope)
Visual Studio Enterprise – MPN/AZ-500-rg

Exclusions
Optionally select resources to exempt from the policy assignment

BASICS

* Policy definition
Allowed locations

* Assignment name
Allowed locations - EU and ZA - AZ-500-rg

Assignment ID
[redacted]esourceGroups/AZ-500-rg/providers/Microsoft.Authorization/policyAssignment...

Description
Allow only Europe and South Africa locations for resource deployment

Assigned bv
[redacted]

PARAMETERS

* Allowed locations
6 selected

For each of the following, select all the statements which are true.

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

Non-compliant resources are reported on the Azure Policy compliance blade - True.
Non-compliant resources are stopped - False.
Non-compliant resources are deleted - False.

● Non-compliant resources are deleted

Q22)

You are creating a custom RBAC role and want to restrict all but a few allowable actions to the new role.

What section of the role definition JSON file do you configure?

● NotActions

✓ Actions

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

● DataActions

● NotDataActions

● AssignableScopes

Q23)

You want to ensure the use of trusted container images in your organisation.

Which two of the following options should you choose?

● Azure container instances

✓ Docker trusted registry

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

✓ Azure container registry

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

● Docker hub

● Azure Kubernetes Service

● Azure Key Vault

Q24) Correct or Incorrect: Azure SQL Database encrypts sensitive data using the column encryption key (CEK) in a Always Encrypted deployment.

● Correct

✓ Incorrect

Explanation:-The Always Encrypted enabled client driver running on the client is responsible for encryption and decryption of data before it is sent to the database.
https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine?view=sql-server-2017#how-it-works