Braindump2go Guarantee All Exams 100% Pass One Time!

- **Vendor:** Microsoft
- **Exam Code:** AZ-500
- **Exam Name:** Microsoft Azure Security Technologies
- **New Updated Questions from Braindump2go**
- **(Updated in September/2021)**

Visit Braindump2go and Download Full Version AZ-500 Exam Dumps

QUESTION 307
Your company recently created an Azure subscription.
You have been tasked with making sure that a specified user is able to implement Azure AD Privileged Identity Management (PIM).
Which of the following is the role you should assign to the user?

A. The Global administrator role.
B. The Security administrator role.
C. The Password administrator role.
D. The Compliance administrator role.

Answer: A
Explanation:
To start using PIM in your directory, you must first enable PIM.
1. Sign in to the Azure portal as a Global Administrator of your directory.
You must be a Global Administrator with an organizational account (for example, @yourdomain.com), not a Microsoft account (for example, @outlook.com), to enable PIM for a directory.
Scenario: Technical requirements include: Enable Azure AD Privileged Identity Management (PIM) for contoso.com
Reference:
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-getting-started

QUESTION 308
Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
Your company has an Active Directory forest with a single domain, named weylandindustries.com. They also have an Azure Active Directory (Azure AD) tenant with the same name.
You have been tasked with integrating Active Directory and the Azure AD tenant. You intend to deploy Azure AD Connect.
Your strategy for the integration must make sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant, and that the amount of necessary servers are reduced.
Solution: You recommend the use of pass-through authentication and seamless SSO with password hash synchronization.
Does the solution meet the goal?

A. Yes
B. No

Answer: B
Explanation:

For pass-through authentication, you need one or more (we recommend three) lightweight agents installed on existing servers. These agents must have access to your on-premises Active Directory Domain Services, including your on-premises AD domain controllers. They need outbound access to the Internet and access to your domain controllers. For this reason, it's not supported to deploy the agents in a perimeter network.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

QUESTION 309
Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
Your company has an Active Directory forest with a single domain, named weylandindustries.com. They also have an Azure Active Directory (Azure AD) tenant with the same name.
You have been tasked with integrating Active Directory and the Azure AD tenant. You intend to deploy Azure AD Connect.
Your strategy for the integration must make sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant, and that the amount of necessary servers are reduced.
Solution: You recommend the use of federation with Active Directory Federation Services (AD FS).
Does the solution meet the goal?

A. Yes
B. No

Answer: B
Explanation:
A federated authentication system relies on an external trusted system to authenticate users. Some companies want to reuse their existing federated system investment with their Azure AD hybrid identity solution. The maintenance and management of the federated system falls outside the control of Azure AD.
It's up to the organization by using the federated system to make sure it's deployed securely and can handle the authentication load.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

QUESTION 310
Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
Your company has an Active Directory forest with a single domain, named weylandindustries.com. They also have an Azure Active Directory (Azure AD) tenant with the same name.
You have been tasked with integrating Active Directory and the Azure AD tenant. You intend to deploy Azure AD Connect.
Your strategy for the integration must make sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant, and that the amount of necessary servers are reduced.
Solution: You recommend the use of password hash synchronization and seamless SSO.
Does the solution meet the goal?

A. Yes
B. No

Answer: A
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.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

QUESTION 311
Your company has an Active Directory forest with a single domain, named weylandindustries.com. They also have an

Azure Active Directory (Azure AD) tenant with the same name.
After syncing all on-premises identities to Azure AD, you are informed that users with a givenName attribute starting with LAB should not be allowed to sync to Azure AD.
Which of the following actions should you take?

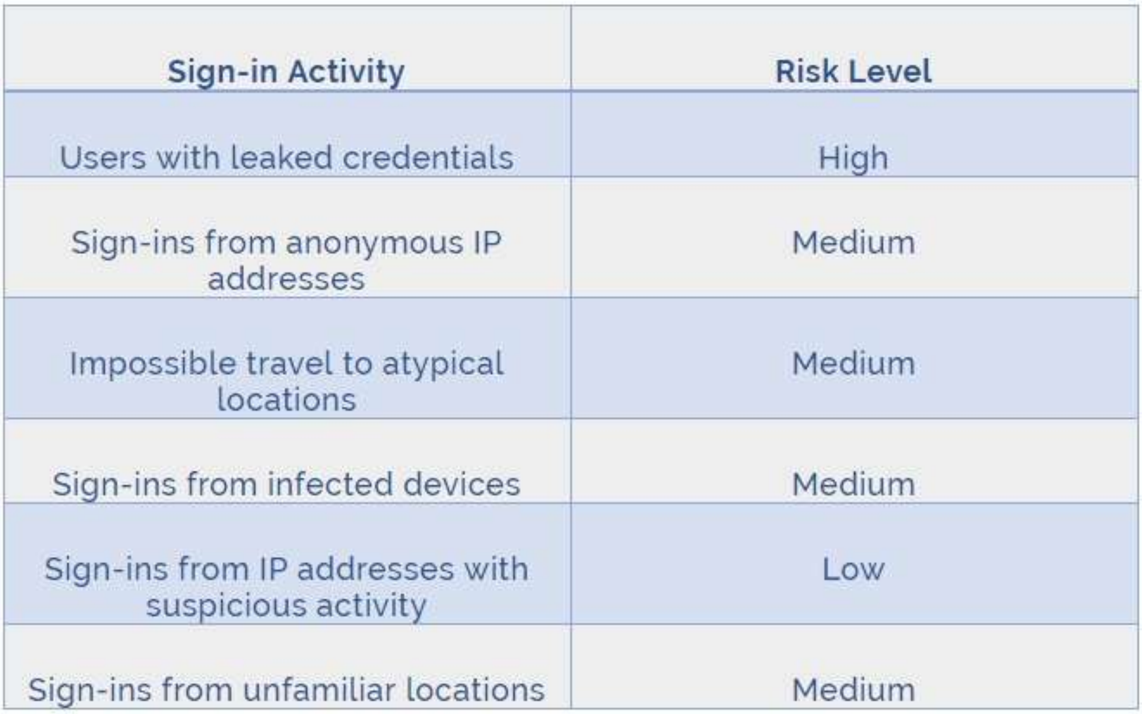
A. You should make use of the Synchronization Rules Editor to create an attribute-based filtering rule.
B. You should configure a DNAT rule on the Firewall.
C. You should configure a network traffic filtering rule on the Firewall.
D. You should make use of Active Directory Users and Computers to create an attribute-based filtering rule.

Answer: A
Explanation:
Use the Synchronization Rules Editor and write attribute-based filtering rule.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration

QUESTION 312
You have been tasked with applying conditional access policies for your company's current Azure Active Directory (Azure AD).
The process involves assessing the risk events and risk levels.
Which of the following is the risk level that should be configured for users that have leaked credentials?

A. None
B. Low
C. Medium
D. High

Answer: D
Explanation:
These six types of events are categorized in to 3 levels of risks ?High, Medium&; Low:



Sign-in Activity	Risk Level
Users with leaked credentials	High
Sign-ins from anonymous IP addresses	Medium
Impossible travel to atypical locations	Medium
Sign-ins from infected devices	Medium
Sign-ins from IP addresses with suspicious activity	Low
Sign-ins from unfamiliar locations	Medium

Reference:
http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/

QUESTION 313
You have been tasked with applying conditional access policies for your company's current Azure Active Directory (Azure AD).
The process involves assessing the risk events and risk levels.
Which of the following is the risk level that should be configured for sign ins that originate from IP addresses with dubious activity?

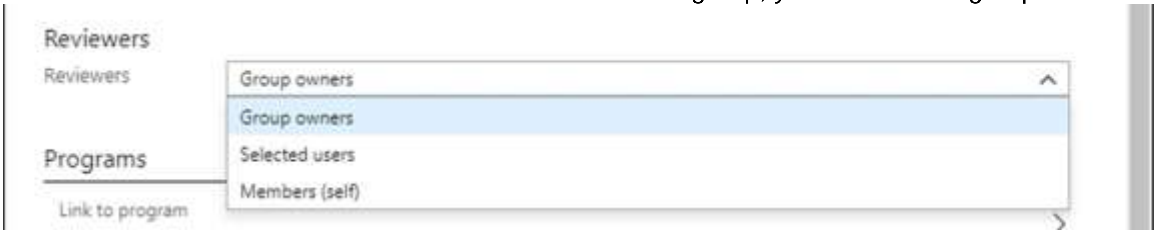
A. None
B. Low
C. Medium
D. High

Answer: C
Explanation:
http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/

QUESTION 314
You have been tasked with configuring an access review, which you plan to assigned to a new collection of reviews.
You also have to make sure that the reviews can be reviewed by resource owners.
You start by creating an access review program and an access review control.
You now need to configure the Reviewers.
Which of the following should you set Reviewers to?

A. Selected users.
B. Members (Self).
C. Group Owners.
D. Anyone.

Answer: C
Explanation:
In the Reviewers section, select either one or more people to review all the users in scope. Or you can select to have the members review their own access. If the resource is a group, you can ask the group owners to review.



Reviewers

Reviewers: Group owners

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review
https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-programs-controls

QUESTION 315
Your company recently created an Azure subscription. You have, subsequently, been tasked with making sure that you are able to secure Azure AD roles by making use of Azure Active Directory (Azure AD) Privileged Identity Management (PIM).
Which of the following actions should you take FIRST?

A. You should sign up Azure Active Directory (Azure AD) Privileged Identity Management (PIM) for Azure AD roles.
B. You should consent to Azure Active Directory (Azure AD) Privileged Identity Management (PIM).
C. You should discover privileged roles.
D. You should discover resources.

Answer: B
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started

QUESTION 316
You need to consider the underlined segment to establish whether it is accurate.
You have been tasked with creating a different subscription for each of your company's divisions. However, the subscriptions will be linked to a single Azure Active Directory (Azure AD) tenant.
You want to make sure that each subscription has identical role assignments.
You make use of Azure AD Privileged Identity Management (PIM).
Select "No adjustment required" if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

A. No adjustment required
B. Azure Blueprints
C. Conditional access policies
D. Azure DevOps

Answer: A
Explanation:
The Azure AD Privileged Identity Management (PIM) service also allows Privileged Role Administrators to make permanent admin role assignments.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-add-role-to-user

QUESTION 317
Your company has an Azure Container Registry.
You have been tasked with assigning a user a role that allows for the uploading of images to the Azure Container Registry. The role assigned should not require more privileges than necessary.
Which of the following is the role you should assign?

A. Owner
B. Contributor
C. AcrPush
D. AcrPull

Answer: C
Explanation:
https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-roles

QUESTION 318
Your company has an Azure Container Registry.
You have been tasked with assigning a user a role that allows for the downloading of images from the Azure Container Registry. The role assigned should not require more privileges than necessary.
Which of the following is the role you should assign?

A. Reader
B. Contributor
C. AcrDelete
D. AcrPull

Answer: A
Explanation:
Reference:
https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-roles

QUESTION 319

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your Company's Azure subscription includes a virtual network that has a single subnet configured.

You have created a service endpoint for the subnet, which includes an Azure virtual machine that has Ubuntu Server 18.04 installed.

You are preparing to deploy Docker containers to the virtual machine. You need to make sure that the containers can access Azure Storage resources and Azure SQL databases via the service endpoint.

You need to perform a task on the virtual machine prior to deploying containers.

Solution: You create an application security group.

Does the solution meet the goal?

A. Yes
B. No

Answer: B

QUESTION 320

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your Company's Azure subscription includes a virtual network that has a single subnet configured.

You have created a service endpoint for the subnet, which includes an Azure virtual machine that has Ubuntu Server 18.04 installed.

You are preparing to deploy Docker containers to the virtual machine. You need to make sure that the containers can access Azure Storage resources and Azure SQL databases via the service endpoint.

You need to perform a task on the virtual machine prior to deploying containers.

Solution: You create an AKS Ingress controller.

Does the solution meet the goal?

A. Yes
B. No

Answer: B

QUESTION 321

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your Company's Azure subscription includes a virtual network that has a single subnet configured.

You have created a service endpoint for the subnet, which includes an Azure virtual machine that has Ubuntu Server 18.04 installed.

You are preparing to deploy Docker containers to the virtual machine. You need to make sure that the containers can access Azure Storage resources and Azure SQL databases via the service endpoint.

You need to perform a task on the virtual machine prior to deploying containers.

Solution: You install the container network interface (CNI) plug-in.

Does the solution meet the goal?

A. Yes
B. No

Answer: A

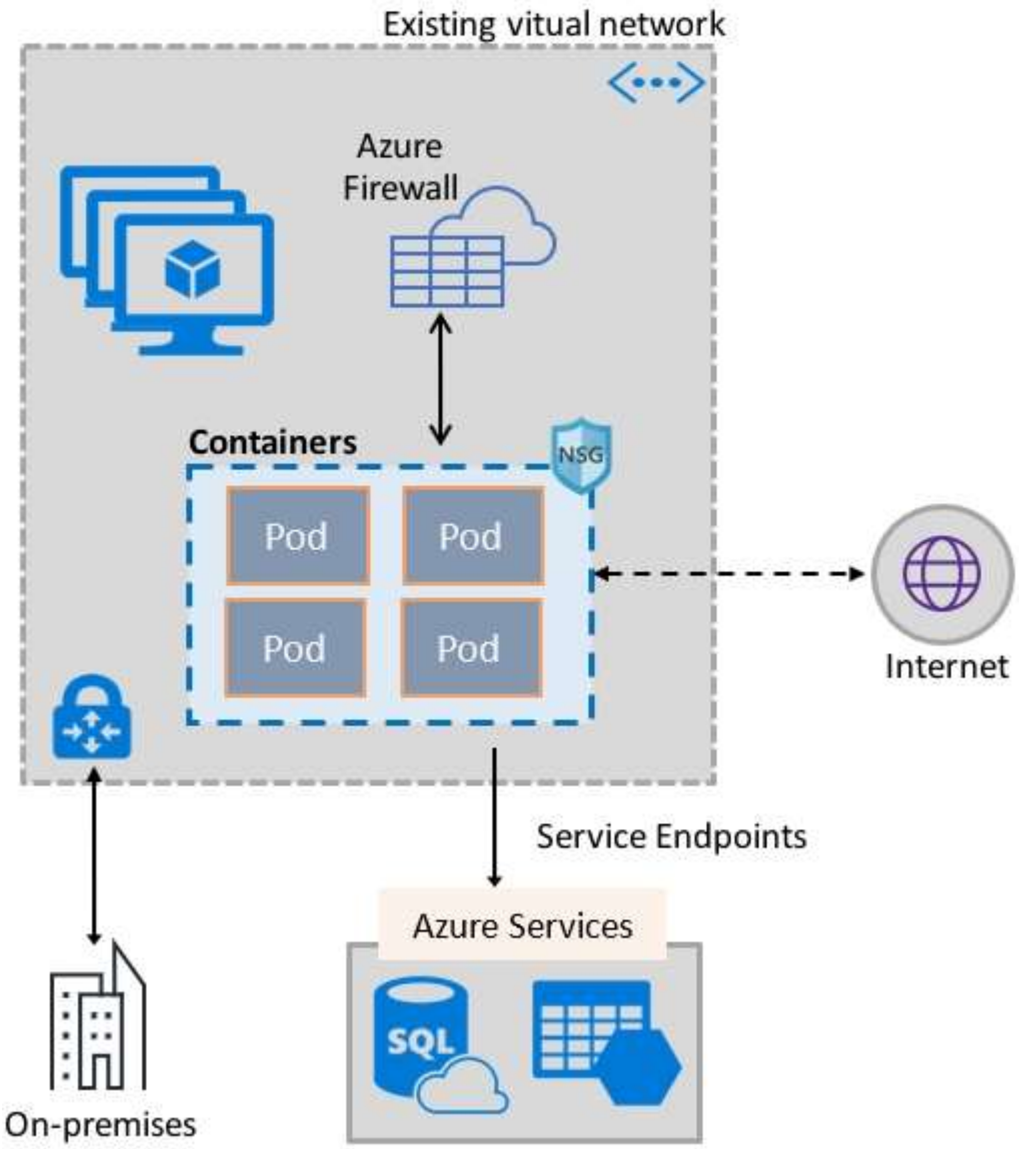
Explanation:

The Azure Virtual Network container network interface (CNI) plug-in installs in an Azure Virtual Machine.

The plug-in supports both Linux and Windows platform.

The plug-in assigns IP addresses from a virtual network to containers brought up in the virtual machine, attaching them to the virtual network, and connecting them directly to other containers and virtual network resources. The plug-in doesn't rely on overlay networks, or routes, for connectivity, and provides the same performance as virtual machines.

The following picture shows how the plug-in provides Azure Virtual Network capabilities to Pods:



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

QUESTION 322
You make use of Azure Resource Manager templates to deploy Azure virtual machines.
You have been tasked with making sure that Windows features that are not in use, are automatically inactivated when instances of the virtual machines are provisioned.
Which of the following actions should you take?

A. You should make use of Azure DevOps.
B. You should make use of Azure Automation State Configuration.
C. You should make use of network security groups (NSG).
D. You should make use of Azure Blueprints.

Answer: B
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

QUESTION 323
Your company's Azure subscription includes Windows Server 2016 Azure virtual machines.
You are informed that every virtual machine must have a custom antimalware virtual machine extension installed. You are writing the necessary code for a policy that will help you achieve this.
Which of the following is an effect that must be included in your code?

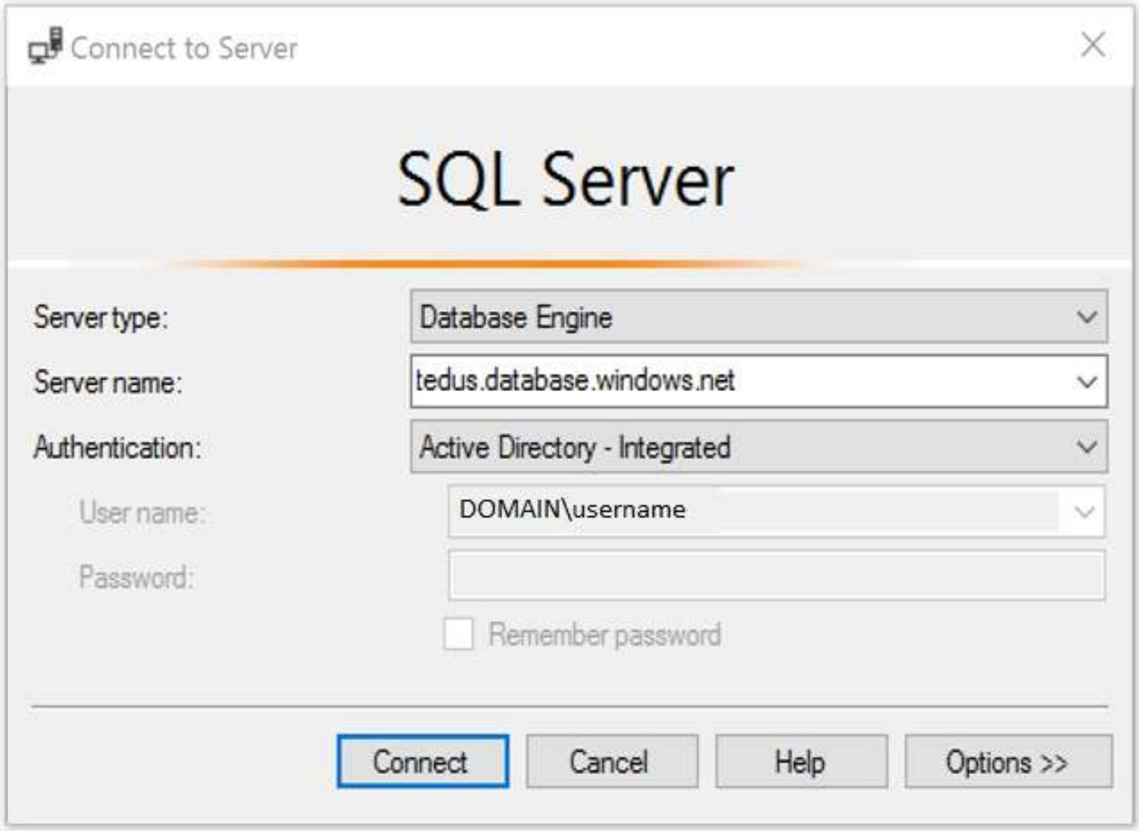
A. Disabled
B. Modify
C. AuditIfNotExists
D. DeployIfNotExists

Answer: D
Explanation:
DeployIfNotExists executes a template deployment when the condition is met.
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects

QUESTION 324
Your company makes use of Azure Active Directory (Azure AD) in a hybrid configuration. All users are making use of hybrid Azure AD joined Windows 10 computers.
You manage an Azure SQL database that allows for Azure AD authentication.
You need to make sure that database developers are able to connect to the SQL database via Microsoft SQL Server Management Studio (SSMS). You also need to make sure the developers use their on-premises Active Directory account for authentication. Your strategy should allow for authentication prompts to be kept to a minimum.
Which of the following is the authentication method the developers should use?

A. Azure AD token.
B. Azure Multi-Factor authentication.
C. Active Directory integrated authentication.
D. Active Directory integrated authentication.

Answer: C
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.



Connect to Server

SQL Server

Server type: Database Engine

Server name: tedus.database.windows.net

Authentication: Active Directory - Integrated

User name: DOMAIN\username

Password:

□ Remember password

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.)

QUESTION 325
You have been tasked with enabling Advanced Threat Protection for an Azure SQL Database server.
Advanced Threat Protection must be configured to identify all types of threat detection.
Which of the following will happen if when a faulty SQL statement is generate in the database by an application?

A. A Potential SQL injection alert is triggered.
B. A Vulnerability to SQL injection alert is triggered.
C. An Access from a potentially harmful application alert is triggered.
D. A Brute force SQL credentials alert is triggered.

Answer: B
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/sql-database/sql-database-threat-detection-overview

QUESTION 326
Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
You are in the process of creating an Azure Kubernetes Service (AKS) cluster. The Azure Kubernetes Service (AKS) cluster must be able to connect to an Azure Container Registry.
You want to make sure that Azure Kubernetes Service (AKS) cluster authenticates to the Azure Container Registry by making use of the auto-generated service principal.
Solution: You create an Azure Active Directory (Azure AD) role assignment.
Does the solution meet the goal?

A. Yes

B. No

Answer: A
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.
Reference:
https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-auth-aks

QUESTION 327
Your company has an Azure subscription that includes two virtual machines, named VirMac1 and VirMac2, which both have a status of Stopped (Deallocated). The virtual machines belong to different resource groups, named ResGroup1 and ResGroup2.
You have also created two Azure policies that are both configured with the virtualMachines resource type. The policy configured for ResGroup1 has a policy definition of Not allowed resource types, while the policy configured for ResGroup2 has a policy definition of Allowed resource types.
You then create a Read-only resource lock on VirMac1, as well as a Read-only resource lock on ResGroup2.
Which of the following is TRUE with regards to the scenario? (Choose all that apply.)

A. You will be able to start VirMac1.
B. You will NOT be able to start VirMac1.
C. You will be able to create a virtual machine in ResGroup2.
D. You will NOT be able to create a virtual machine in ResGroup2.

Answer: BC
Explanation:
https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking

QUESTION 328
You have been tasked with delegate administrative access to your company's Azure key vault.
You have to make sure that a specific user can set advanced access policies for the key vault. You also have to make sure that access is assigned based on the principle of least privilege.
Which of the following options should you use to achieve your goal?

A. Azure Information Protection
B. RBAC
C. Azure AD Privileged Identity Management (PIM)
D. Azure DevOps

Answer: B
Explanation:
https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault