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.

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

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

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.

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

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

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

You have been tasked with delegate administrative access to your company's Azure key vault.  
You have to make sure that a specific user is able to add and delete certificates in 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. A key vault access policy
* B. Azure policy
* C. Azure AD Privileged Identity Management (PIM)
* D. Azure DevOps

You have an Azure virtual machine that runs Windows Server R2.  
You plan to deploy and configure an Azure Key vault, and enable Azure Disk Encryption for the virtual machine.  
Which of the following is TRUE with regards to Azure Disk Encryption for a Windows VM?

* A. It is supported for basic tier VMs.
* B. It is supported for standard tier VMs.
* C. It is supported for VMs configured with software-based RAID systems.
* D. It is supported for VMs configured with Storage Spaces Direct (S2D).

You want to gather logs from a large number of Windows Server 2016 computers using Azure Log Analytics.  
You are configuring an Azure Resource Manager template to deploy the Microsoft Monitoring Agent to all the servers automatically.  
Which of the following should be included in the template? (Choose all that apply.)

* A. WorkspaceID
* B. AzureADApplicationID
* C. WorkspaceKey
* D. StorageAccountKey

You have a sneaking suspicion that there are users trying to sign in to resources which are inaccessible to them.  
You decide to create an Azure Log Analytics query to confirm your suspicions. The query will detect unsuccessful user sign-in attempts from the last few days.  
You want to make sure that the results only show users who had failed to sign-in more than five times.  
Which of the following should be included in your query?

* A. The EventID and CountIf() parameters.
* B. The ActivityID and CountIf() parameters.
* C. The EventID and Count() parameters.
* D. The ActivityID and Count() parameters.

**KUSTO Query**

let timeframe = 1d; SecurityEvent | where TimeGenerated > ago(1d) | where AccountType == 'User' and EventID == 4625 // 4625 - failed log in | summarize failed\_login\_attempts=count(), latest\_failed\_login=arg\_max(TimeGenerated, Account) by Account | where failed\_login\_attempts > 5 | project-away Account1

Your company's Azure subscription includes a hundred virtual machines that have Azure Diagnostics enabled.  
You have been tasked with retrieving the identity of the user that removed a virtual machine fifteen days ago. You have already accessed Azure Monitor.  
Which of the following options should you use?

* A. Application Log
* B. Metrics
* C. Activity Log
* D. Logs

DRAG DROP -  
Your company has an Azure SQL database that has Always Encrypted enabled.  
You are required to make the relevant information available to application developers to allow them to access data in the database.  
Which two of the following options should be made available? Answer by dragging the correct options from the list to the answer area.  
Select and Place:  
