Question #1

You have an Azure subscription that contains a custom application named Application1. Application1 was developed by an external company named Fabrikam,
Ltd. Developers at Fabrikam were assigned role-based access control (RBAC) permissions to the Application1 components. All users are licensed for the
Microsoft 365 E5 plan.
You need to recommend a solution to verify whether the Fabrikam developers still require permissions to Application1. The solution must meet the following requirements:
☞ To the manager of the developers, send a monthly email message that lists the access permissions to Application1.
☞ If the manager does not verify an access permission, automatically revoke that permission.
☞ Minimize development effort.
What should you recommend?

A. In Azure Active Directory (Azure AD), create an access review of Application1.

B. Create an Azure Automation runbook that runs the Get-AzRoleAssignment cmdlet.

C. In Azure Active Directory (Azure AD) Privileged Identity Management, create a custom role assignment for the Application1 resources.

D. Create an Azure Automation runbook that runs the Get-AzureADUserAppRoleAssignment cmdlet.

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-user-access-with-access-reviews

Community vote distribution

A (100%)

Question #2 *Topic 1*

You have an Azure subscription. The subscription has a blob container that contains multiple blobs.
Ten users in the finance department of your company plan to access the blobs during the month of April.
You need to recommend a solution to enable access to the blobs during the month of April only.
Which security solution should you include in the recommendation?

A. shared access signatures (SAS)

B. Conditional Access policies

C. certificates

D. access keys

Correct Answer: *A*
Shared Access Signatures (SAS) allows for limited-time fine grained access control to resources. So you can generate URL, specify duration (for month of April) and disseminate URL to 10 team members. On May 1, the SAS token is automatically invalidated, denying team members continued access.
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview

Community vote distribution

A (100%)

Question #3 *Topic 1*

You have an Azure Active Directory (Azure AD) tenant that syncs with an on-premises Active Directory domain.
You have an internal web app named WebApp1 that is hosted on-premises. WebApp1 uses Integrated Windows authentication.
Some users work remotely and do NOT have VPN access to the on-premises network.
You need to provide the remote users with single sign-on (SSO) access to WebApp1.
Which two features should you include in the solution? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Azure AD Application Proxy

B. Azure AD Privileged Identity Management (PIM)

C. Conditional Access policies

D. Azure Arc

E. Azure AD enterprise applications

F. Azure Application Gateway

Correct Answer: *AE*
A: Application Proxy is a feature of Azure AD that enables users to access on-premises web applications from a remote client. Application Proxy includes both the
Application Proxy service which runs in the cloud, and the Application Proxy connector which runs on an on-premises server.
You can configure single sign-on to an Application Proxy application.
E: Add an on-premises app to Azure AD
Now that you've prepared your environment and installed a connector, you're ready to add on-premises applications to Azure AD.
1. Sign in as an administrator in the Azure portal.
2. In the left navigation panel, select Azure Active Directory.
3. Select Enterprise applications, and then select New application.
4. Select Add an on-premises application button which appears about halfway down the page in the On-premises applications section.
Alternatively, you can select Create your own application at the top of the page and then select Configure Application Proxy for secure remote access to an on-premise application.
5. In the Add your own on-premises application section, provide the following information about your application.
6. Etc.
Incorrect:
Not C: Conditional Access policies are not required.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-add-on-premises-application

Community vote distribution

AE (95%) 3%

Question #4 *Topic 1*

You have an Azure Active Directory (Azure AD) tenant named contoso.com that has a security group named Group1. Group1 is configured for assigned membership. Group1 has 50 members, including 20 guest users.
You need to recommend a solution for evaluating the membership of Group1. The solution must meet the following requirements:
☞ The evaluation must be repeated automatically every three months.
☞ Every member must be able to report whether they need to be in Group1.
☞ Users who report that they do not need to be in Group1 must be removed from Group1 automatically.
☞ Users who do not report whether they need to be in Group1 must be removed from Group1 automatically.
What should you include in the recommendation?

A. Implement Azure AD Identity Protection.

B. Change the Membership type of Group1 to Dynamic User.

C. Create an access review.

D. Implement Azure AD Privileged Identity Management (PIM).

Correct Answer: *C*
Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User's access can be reviewed on a regular basis to make sure only the right people have continued access.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

Community vote distribution

C (98%)

HOTSPOT -

You plan to deploy Azure Databricks to support a machine learning application. Data engineers will mount an Azure Data Lake Storage account to the Databricks file system. Permissions to folders are granted directly to the data engineers.

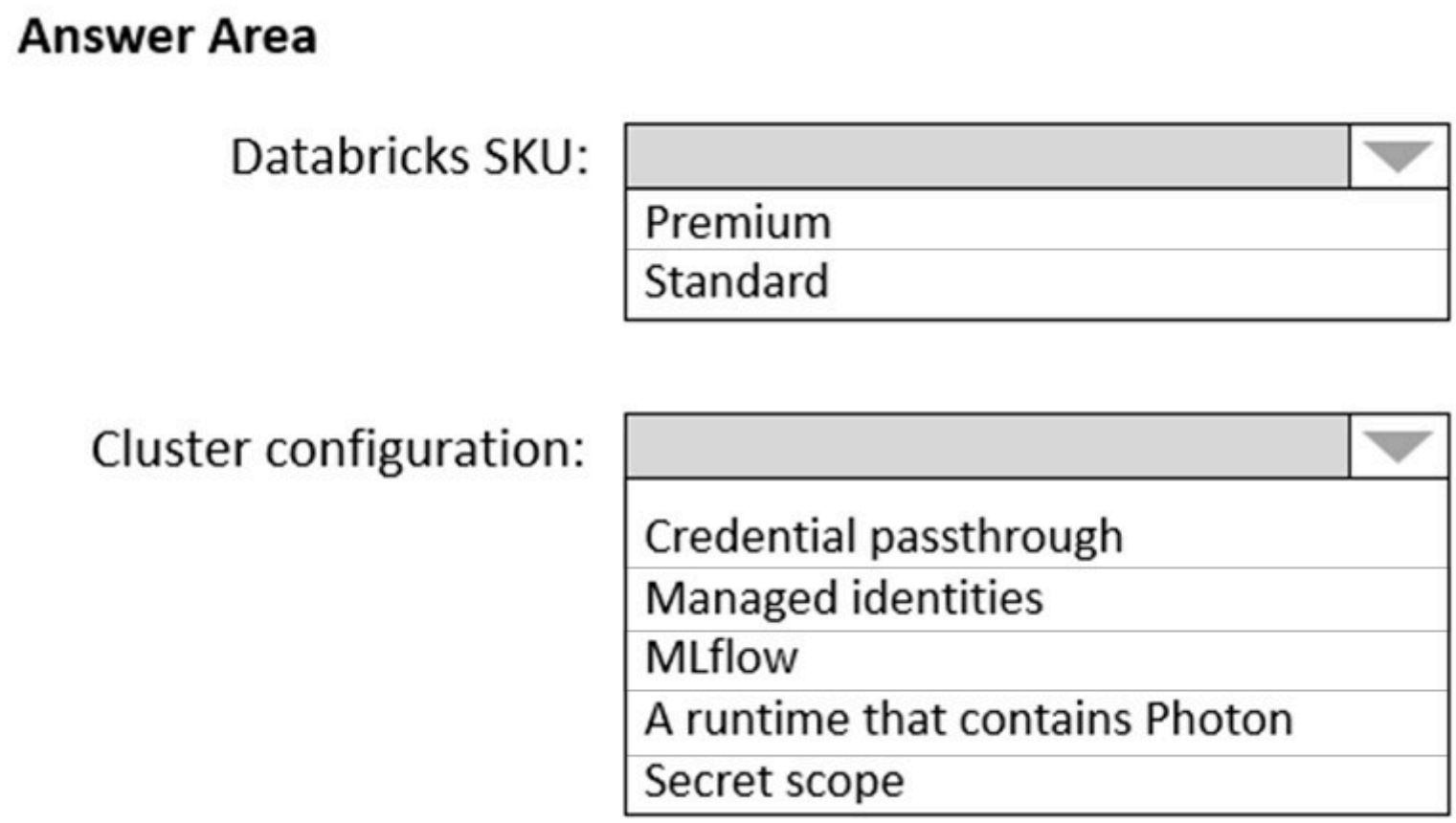
You need to recommend a design for the planned Databrick deployment. The solution must meet the following requirements:

- Ensure that the data engineers can only access folders to which they have permissions.
- Minimize development effort.
- Minimize costs.

What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

Databricks SKU: Premium / Standard

Correct Answer:

Cluster configuration: Credential passthrough / Managed identities / MLflow / A runtime that contains Photon / Secret scope

Box 1: Premium -

Premium Databricks SKU is required for credential passhtrough.

Box 2: Credential passthrough -

Athenticate automatically to Azure Data Lake Storage Gen1 (ADLS Gen1) and Azure Data Lake Storage Gen2 (ADLS Gen2) from Azure Databricks clusters using the same Azure Active Directory (Azure AD) identity that you use to log into Azure Databricks. When you enable Azure Data Lake Storage credential passthrough for your cluster, commands that you run on that cluster can read and write data in Azure Data Lake

Storage without requiring you to configure service principal credentials for access to storage.
Reference:
https://docs.microsoft.com/en-us/azure/databricks/security/credential-passthrough/adls-passthrough

Question #6 *Topic 1*

HOTSPOT -

You plan to deploy an Azure web app named App1 that will use Azure Active Directory (Azure AD) authentication.

App1 will be accessed from the internet by the users at your company. All the users have computers that run Windows 10 and are joined to Azure AD.

You need to recommend a solution to ensure that the users can connect to App1 without being prompted for authentication and can access App1 only from company-owned computers.

What should you recommend for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

The users can connect to App1 without being prompted for authentication:

- An Azure AD app registration
- An Azure AD managed identity
- Azure AD Application Proxy

The users can access App1 only from company-owned computers:

- A Conditional Access policy
- An Azure AD administrative unit
- Azure Application Gateway
- Azure Blueprints
- Azure Policy

Correct Answer:

Answer Area

The users can connect to App1 without being prompted for authentication:

- An Azure AD app registration
- An Azure AD managed identity
- Azure AD Application Proxy

The users can access App1 only from company-owned computers:

- A Conditional Access policy
- An Azure AD administrative unit
- Azure Application Gateway
- Azure Blueprints
- Azure Policy

Box 1: An Azure AD app registration

Azure active directory (AD) provides cloud based directory and identity management services.You can use azure AD to manage users of your application and authenticate access to your applications using azure active directory.

You register your application with Azure active directory tenant.

Box 2: A conditional access policy

Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action.

By using Conditional Access policies, you can apply the right access controls when needed to keep your organization secure and stay out of your user's way when not needed.

Reference:
https://codingcanvas.com/using-azure-active-directory-authentication-in-your-web-application/ https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

Question #7 *Topic 1*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company deploys several virtual machines on-premises and to Azure. ExpressRoute is deployed and configured for on-premises to Azure connectivity.
Several virtual machines exhibit network connectivity issues.
You need to analyze the network traffic to identify whether packets are being allowed or denied to the virtual machines.
Solution: Use Azure Traffic Analytics in Azure Network Watcher to analyze the network traffic.
Does this meet the goal?

A. Yes
B. No

Correct Answer: *B*
Instead use Azure Network Watcher IP Flow Verify, which allows you to detect traffic filtering issues at a VM level.
Note: IP flow verify checks if a packet is allowed or denied to or from a virtual machine. The information consists of direction, protocol, local IP, remote IP, local port, and remote port. If the packet is denied by a security group, the name of the rule that denied the packet is returned. While any source or destination IP can be chosen, IP flow verify helps administrators quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment.
Reference:
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview

Community vote distribution

B (95%) 5%

Question #8 *Topic 1*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company deploys several virtual machines on-premises and to Azure. ExpressRoute is deployed and configured for on-premises to Azure connectivity.
Several virtual machines exhibit network connectivity issues.
You need to analyze the network traffic to identify whether packets are being allowed or denied to the virtual machines.
Solution: Use Azure Advisor to analyze the network traffic.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead use Azure Network Watcher IP Flow Verify, which allows you to detect traffic filtering issues at a VM level.
Note: IP flow verify checks if a packet is allowed or denied to or from a virtual machine. The information consists of direction, protocol, local IP, remote IP, local port, and remote port. If the packet is denied by a security group, the name of the rule that denied the packet is returned. While any source or destination IP can be chosen, IP flow verify helps administrators quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment.
Reference:
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview

Community vote distribution

B (100%)

Question #9 *Topic 1*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company deploys several virtual machines on-premises and to Azure. ExpressRoute is deployed and configured for on-premises to Azure connectivity.
Several virtual machines exhibit network connectivity issues.
You need to analyze the network traffic to identify whether packets are being allowed or denied to the virtual machines.
Solution: Use Azure Network Watcher to run IP flow verify to analyze the network traffic.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
Azure Network Watcher IP Flow Verify allows you to detect traffic filtering issues at a VM level.
IP flow verify checks if a packet is allowed or denied to or from a virtual machine. The information consists of direction, protocol, local IP, remote IP, local port, and remote port. If the packet is denied by a security group, the name of the rule that denied the packet is returned. While any source or destination IP can be chosen,
IP flow verify helps administrators quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment.
Reference:
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview

Community vote distribution

A (100%)

DRAG DROP -

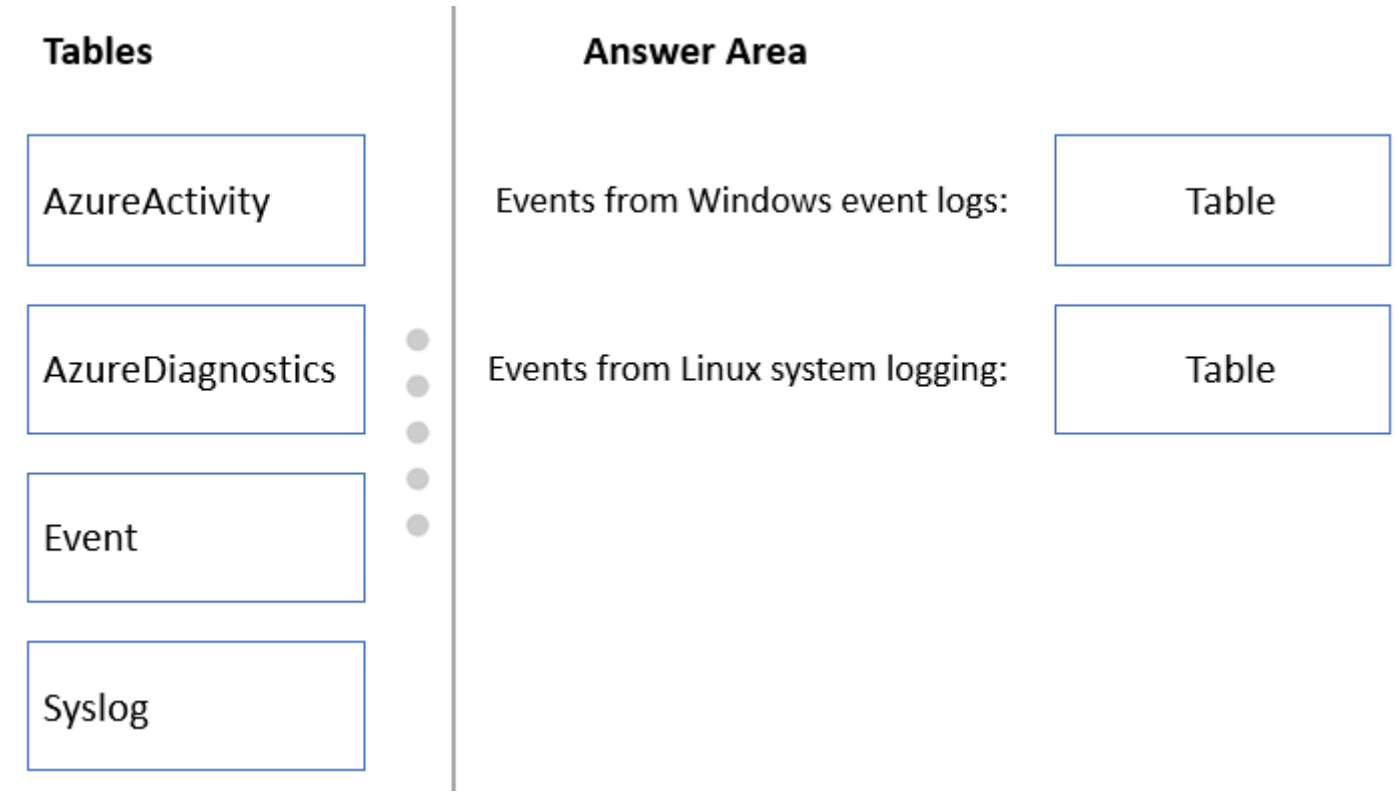
You have an Azure subscription. The subscription contains Azure virtual machines that run Windows Server 2016 and Linux.

You need to use Azure Monitor to design an alerting strategy for security-related events.

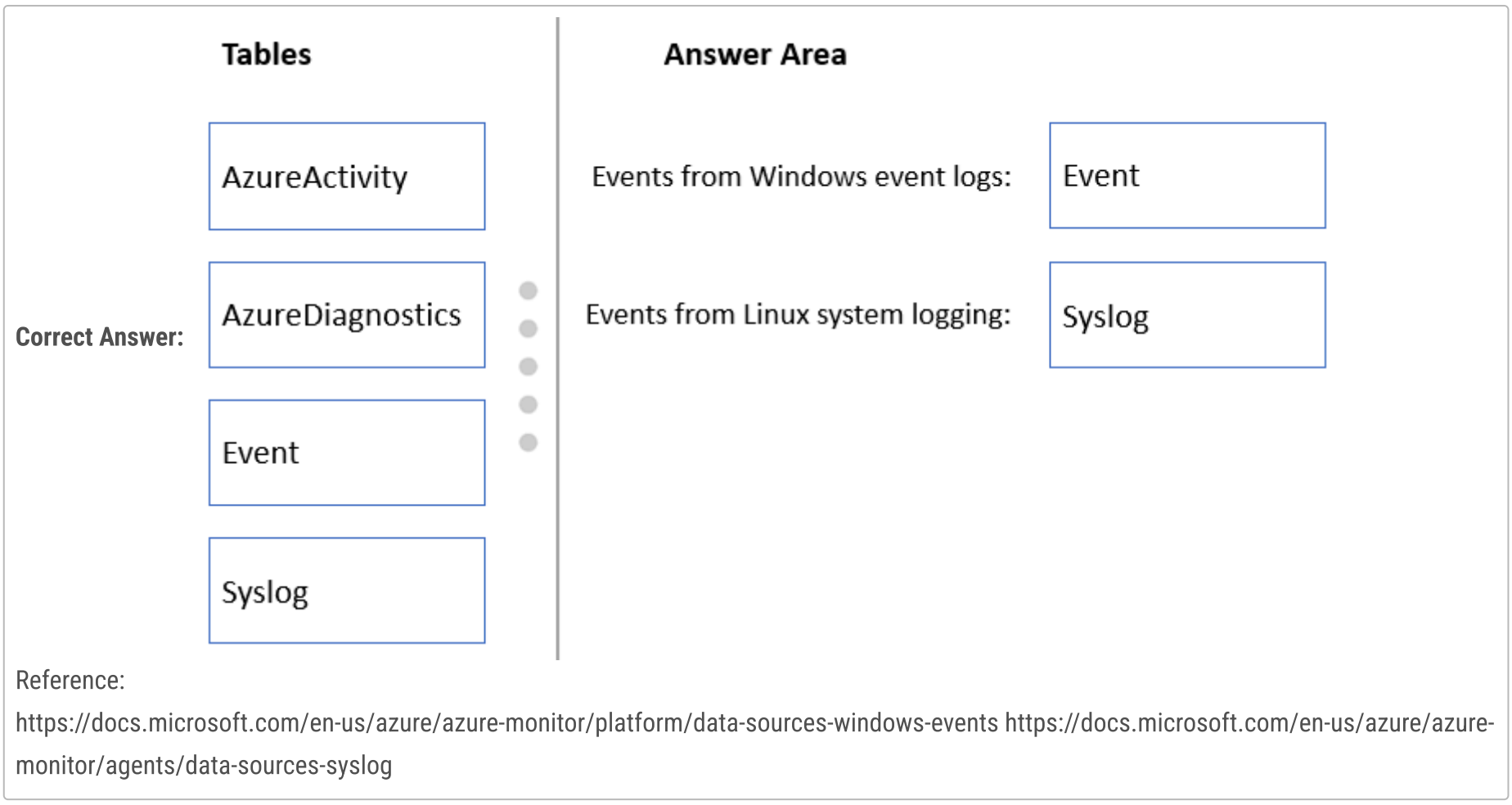
Which Azure Monitor Logs tables should you query? To answer, drag the appropriate tables to the correct log types. Each table may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-sources-windows-events https://docs.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-syslog