Topic 1 - Question Set 1

Question #1 *Topic 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. Most Voted

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) Most Voted

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 Most Voted

B. Azure AD Privileged Identity Management (PIM)

C. Conditional Access policies

D. Azure Arc

E. Azure AD enterprise applications Most Voted

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. Most Voted

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%)

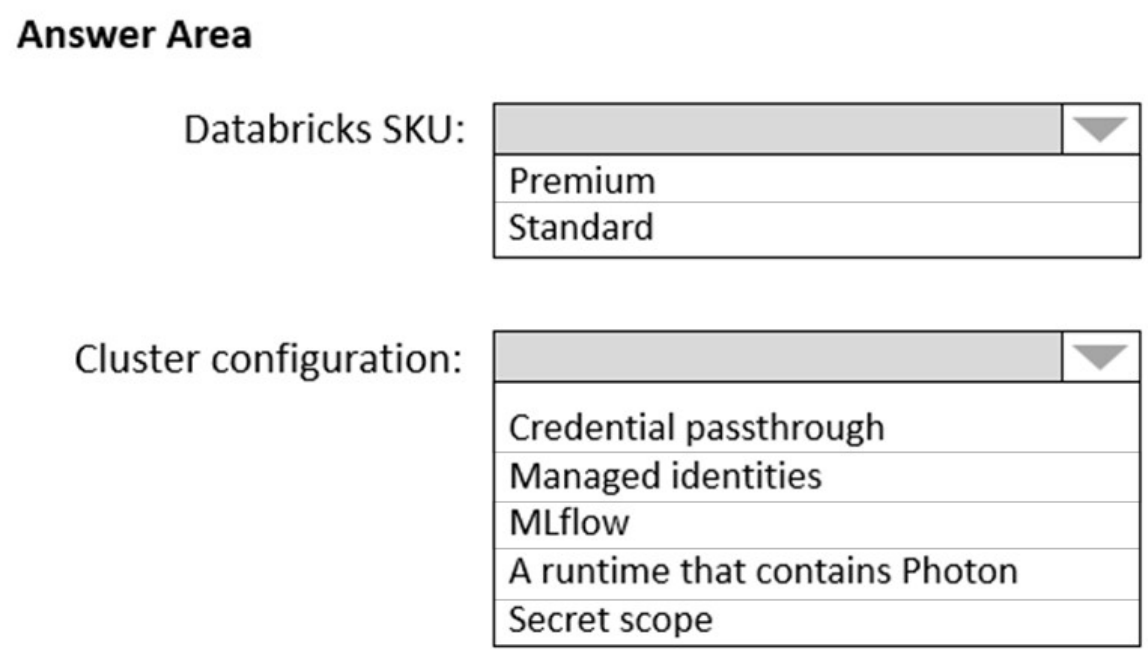
Question #5 *Topic 1*

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.

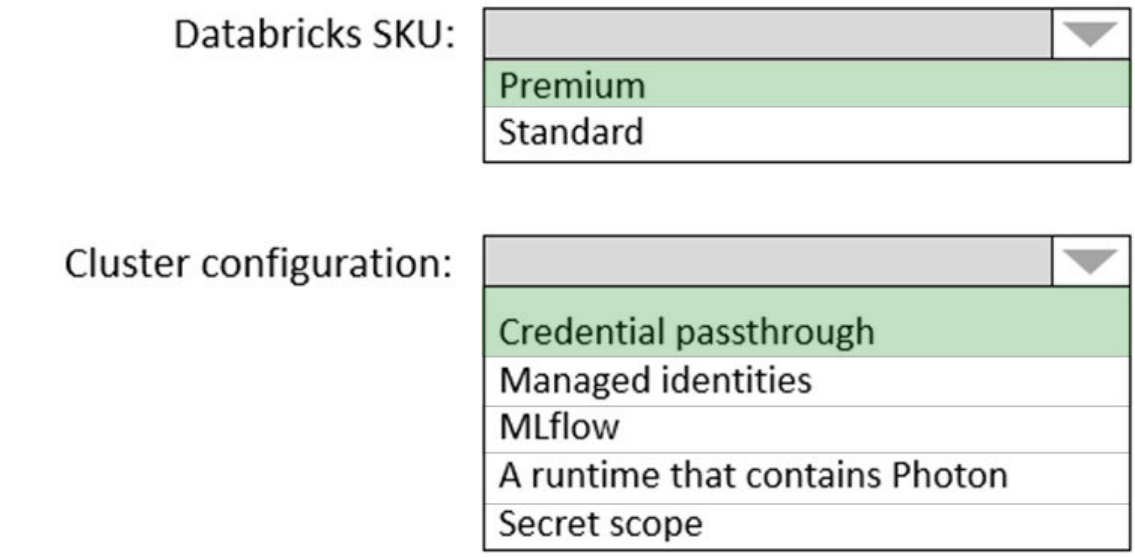
What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



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 Most Voted

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 Most Voted

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 Most Voted

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

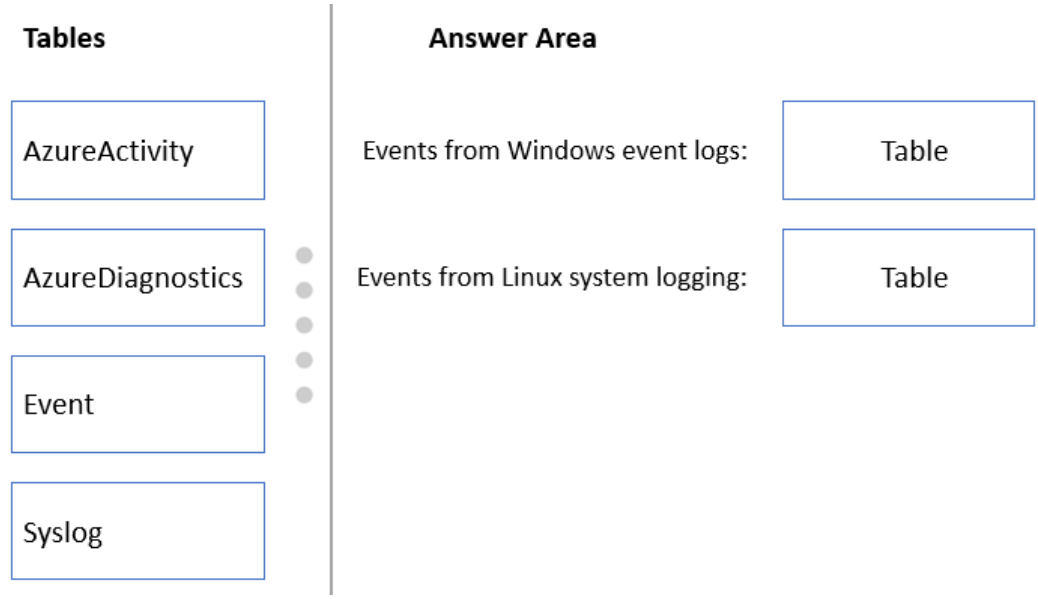
Community vote distribution
A (100%)

Question #10 *Topic 1*

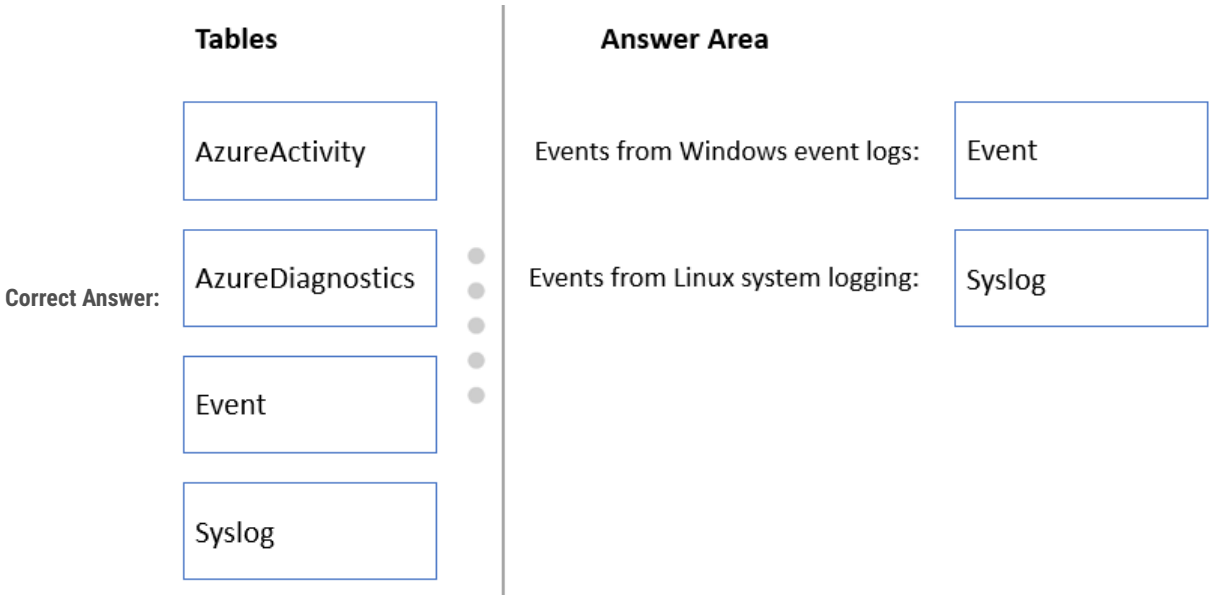
DRAG DROP -
You have an Azure subscription. The subscription contains Azure virtual machines that run Windows Server 2016 and Linux.
You need to use Azure Monitor to design an alerting strategy for security-related events.
Which Azure Monitor Logs tables should you query? To answer, drag the appropriate 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

Question #11 *Topic 1*

You are designing a large Azure environment that will contain many subscriptions.
You plan to use Azure Policy as part of a governance solution.
To which three scopes can you assign Azure Policy definitions? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Azure Active Directory (Azure AD) administrative units

B. Azure Active Directory (Azure AD) tenants

C. subscriptions Most Voted

D. compute resources

E. resource groups Most Voted

F. management groups Most Voted

Correct Answer: *CEF*
Azure Policy evaluates resources in Azure by comparing the properties of those resources to business rules. Once your business rules have been formed, the policy definition or initiative is assigned to any scope of resources that Azure supports, such as management groups, subscriptions, resource groups, or individual resources.
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/overview

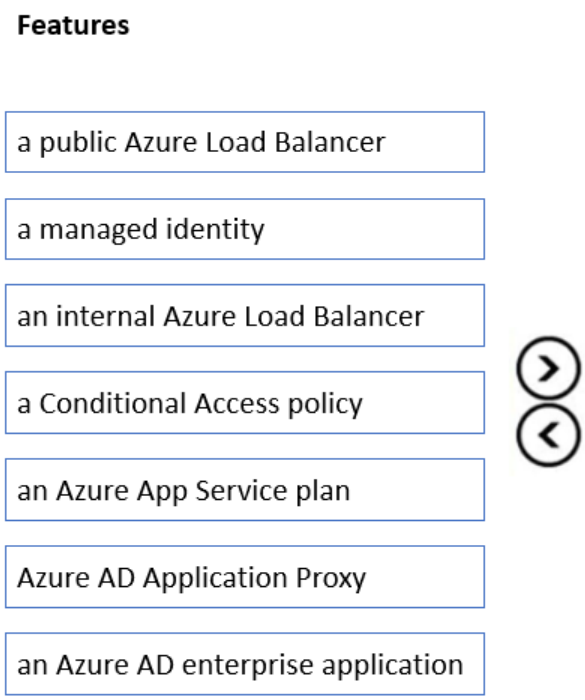
Community vote distribution
CEF (100%)

Question #12 *Topic 1*

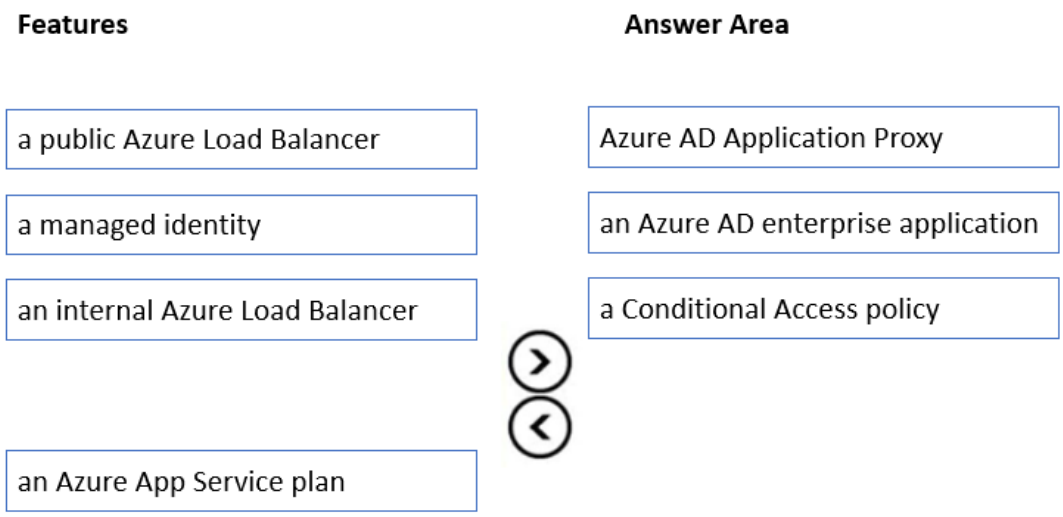
DRAG DROP -
Your on-premises network contains a server named Server1 that runs an ASP.NET application named App1.
You have a hybrid deployment of Azure Active Directory (Azure AD).
You need to recommend a solution to ensure that users sign in by using their Azure AD account and Azure Multi-Factor Authentication (MFA) when they connect to App1 from the internet.
Which three features should you recommend be deployed and configured in sequence? To answer, move the appropriate features from the list of

features to the answer area and arrange them in the correct order.

Select and Place:



Correct Answer:



Step 1: Azure AD Application Proxy

Start by enabling communication to Azure data centers to prepare your environment for Azure AD Application Proxy.

Step 2: an Azure AD enterprise application

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. Etc.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-add-on-premises-application

Question #13 *Topic 1*

You need to recommend a solution to generate a monthly report of all the new Azure Resource Manager (ARM) resource deployments in your Azure subscription.
What should you include in the recommendation?

A. Azure Activity Log Most Voted

B. Azure Advisor

C. Azure Analysis Services

D. Azure Monitor action groups

Correct Answer: *A*
Activity logs are kept for 90 days. You can query for any range of dates, as long as the starting date isn't more than 90 days in the past.
Through activity logs, you can determine:
- what operations were taken on the resources in your subscription
- who started the operation
- when the operation occurred
- the status of the operation
- the values of other properties that might help you research the operation

Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/view-activity-logs

Community vote distribution
A (100%)

Question #14 *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: Install and configure the Azure Monitoring agent and the Dependency Agent on all the virtual machines. Use VM insights in Azure Monitor to analyze the network traffic.
Does this meet the goal?

A. Yes

B. No Most Voted

Correct Answer: *B*
Use the Azure Monitor agent if you need to:
Collect guest logs and metrics from any machine in Azure, in other clouds, or on-premises.
Use the Dependency agent if you need to:
Use the Map feature VM insights or the Service Map solution.
Note: Instead use 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 https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview#dependency-agent

Community vote distribution
B (100%)

Question #15 *Topic 1*

DRAG DROP -
You need to design an architecture to capture the creation of users and the assignment of roles. The captured data must be stored in Azure Cosmos DB.
Which services should you include in the design? To answer, drag the appropriate services to the correct targets. Each service 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.

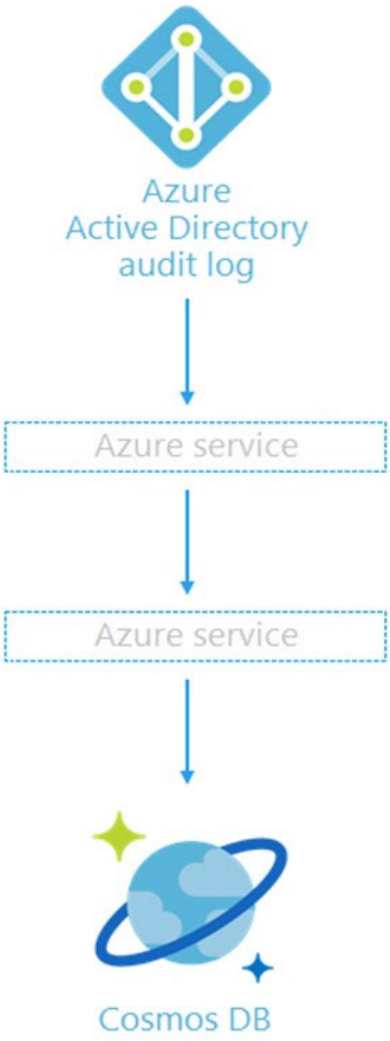
NOTE: Each correct selection is worth one point.

Select and Place:

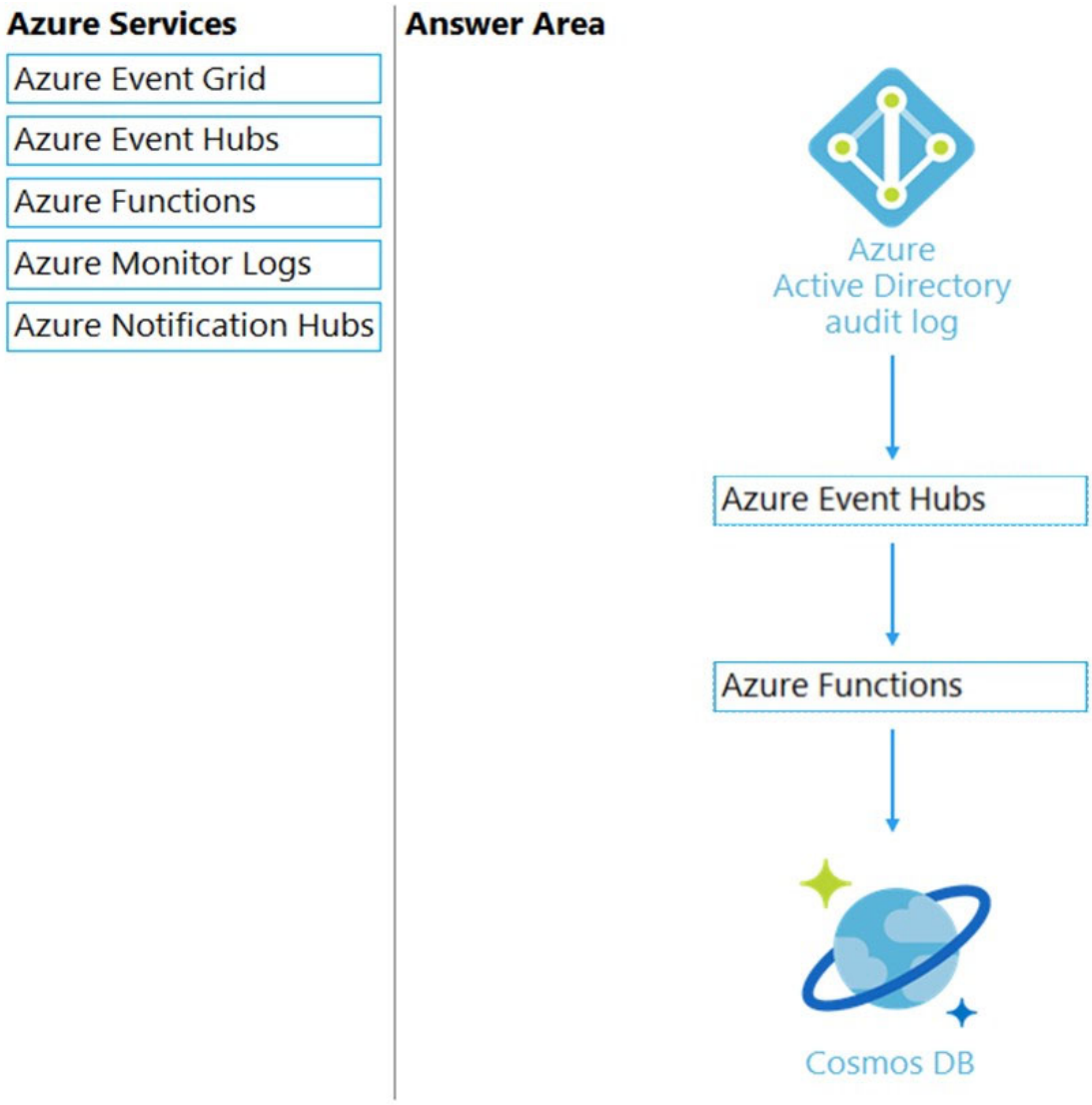
Azure Services

- Azure Event Grid
- Azure Event Hubs
- Azure Functions
- Azure Monitor Logs
- Azure Notification Hubs

Answer Area



Correct Answer:



Box 1: Azure Event Hubs -

You can route Azure Active Directory (Azure AD) activity logs to several endpoints for long term retention and data insights.

The Event Hub is used for streaming.

Box 2: Azure Function -

Use an Azure Function along with a cosmos DB change feed, and store the data in Cosmos DB.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-activity-logs-azure-monitor

Question #16 *Topic 1*

Your company, named Contoso, Ltd., implements several Azure logic apps that have HTTP triggers. The logic apps provide access to an on-premises web service.
Contoso establishes a partnership with another company named Fabrikam, Inc.
Fabrikam does not have an existing Azure Active Directory (Azure AD) tenant and uses third-party OAuth 2.0 identity management to authenticate its users.
Developers at Fabrikam plan to use a subset of the logic apps to build applications that will integrate with the on-premises web service of Contoso.
You need to design a solution to provide the Fabrikam developers with access to the logic apps. The solution must meet the following requirements:
- Requests to the logic apps from the developers must be limited to lower rates than the requests from the users at Contoso.
- The developers must be able to rely on their existing OAuth 2.0 provider to gain access to the logic apps.
- The solution must NOT require changes to the logic apps.
- The solution must NOT use Azure AD guest accounts.

What should you include in the solution?

A. Azure Front Door

B. Azure AD Application Proxy

C. Azure AD business-to-business (B2B)

D. Azure API Management Most Voted

Correct Answer: *D*
Many APIs support OAuth 2.0 to secure the API and ensure that only valid users have access, and they can only access resources to which they're entitled. To use Azure API Management's interactive developer console with such APIs, the service allows you to configure your service instance to work with your OAuth 2.0 enabled API.
Incorrect:
Azure AD business-to-business (B2B) uses guest accounts.
Azure AD Application Proxy is for on-premises scenarios.
Reference:
https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-oauth2

Community vote distribution
D (100%)

Question #17 *Topic 1*

HOTSPOT -
You have an Azure subscription that contains 300 virtual machines that run Windows Server 2019.
You need to centrally monitor all warning events in the System logs of the virtual machines.
What should you include in the solution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Resource to create in Azure:
- An event hub
- A Log Analytics workspace
- A search service
- A storage account

Configuration to perform on the virtual machines:
- Create event subscriptions
- Configure Continuous delivery
- Install the Azure Monitor agent
- Modify the membership of the Event Log Readers group

Correct Answer:

Answer Area

Resource to create in Azure:
- An event hub
- **A Log Analytics workspace**
- A search service
- A storage account

Configuration to perform on the virtual machines:
- Create event subscriptions
- Configure Continuous delivery
- **Install the Azure Monitor agent**
- Modify the membership of the Event Log Readers group

Box 1: A Log Analytics workspace

Send resource logs to a Log Analytics workspace to enable the features of Azure Monitor Logs.

You must create a diagnostic setting for each Azure resource to send its resource logs to a Log Analytics workspace to use with Azure Monitor Logs.

Box 2: Install the Azure Monitor agent

Use the Azure Monitor agent if you need to:

Collect guest logs and metrics from any machine in Azure, in other clouds, or on-premises.

Manage data collection configuration centrally

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/resource-logs https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview#azure-monitor-agent

Question #18 *Topic 1*

HOTSPOT -

You have several Azure App Service web apps that use Azure Key Vault to store data encryption keys.

Several departments have the following requests to support the web app:

Department	Request
Security	• Review the membership of administrative roles and require users to provide a justification for continued membership. • Get alerts about changes in administrator assignments. • See a history of administrator activation, including which changes administrators made to Azure resources.
Development	• Enable the applications to access Key Vault and retrieve keys for use in code.
Quality Assurance	• Receive temporary administrator access to create and configure additional web apps in the test environment.

Which service should you recommend for each department's request? To answer, configure the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Security:
- Azure AD Privileged Identity Management
- Azure Managed Identity
- Azure AD Connect
- Azure AD Identity Protection

Development:
- Azure AD Privileged Identity Management
- Azure Managed Identity
- Azure AD Connect
- Azure AD Identity Protection

Quality Assurance:
- Azure AD Privileged Identity Management
- Azure Managed Identity
- Azure AD Connect
- Azure AD Identity Protection

Correct Answer:

Answer Area

Security:
- Azure AD Privileged Identity Management
- Azure Managed Identity
- Azure AD Connect
- Azure AD Identity Protection

Development:
- Azure AD Privileged Identity Management
- Azure Managed Identity
- Azure AD Connect
- Azure AD Identity Protection

Quality Assurance:
- Azure AD Privileged Identity Management
- Azure Managed Identity
- Azure AD Connect
- Azure AD Identity Protection

Box 1: Azure AD Privileged Identity Management

Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or

misused access permissions on resources that you care about. Here are some of the key features of Privileged Identity Management:
Provide just-in-time privileged access to Azure AD and Azure resources
Assign time-bound access to resources using start and end dates
Require approval to activate privileged roles
Enforce multi-factor authentication to activate any role
Use justification to understand why users activate
Get notifications when privileged roles are activated
Conduct access reviews to ensure users still need roles
Download audit history for internal or external audit
Prevents removal of the last active Global Administrator role assignment

Box 2: Azure Managed Identity -
Managed identities provide an identity for applications to use when connecting to resources that support Azure Active Directory (Azure AD) authentication.
Applications may use the managed identity to obtain Azure AD tokens. With Azure Key Vault, developers can use managed identities to access resources. Key
Vault stores credentials in a secure manner and gives access to storage accounts.
Box 3: Azure AD Privileged Identity Management
Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about. Here are some of the key features of Privileged Identity Management:
Provide just-in-time privileged access to Azure AD and Azure resources
Assign time-bound access to resources using start and end dates
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

Question #19 *Topic 1*

HOTSPOT -
Your company has the divisions shown in the following table.

Division	Azure subscription	Azure Active Directory (Azure AD) tenant
East	Sub1, Sub2	East.contoso.com
West	Sub3, Sub4	West.contoso.com

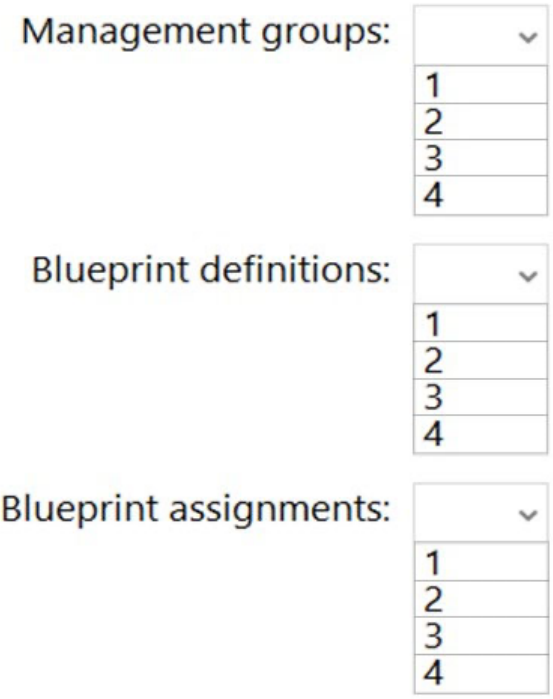
You plan to deploy a custom application to each subscription. The application will contain the following:
- A resource group
- An Azure web app
- Custom role assignments
- An Azure Cosmos DB account

You need to use Azure Blueprints to deploy the application to each subscription.
What is the minimum number of objects required to deploy the application? To answer, select the appropriate options in the answer area.

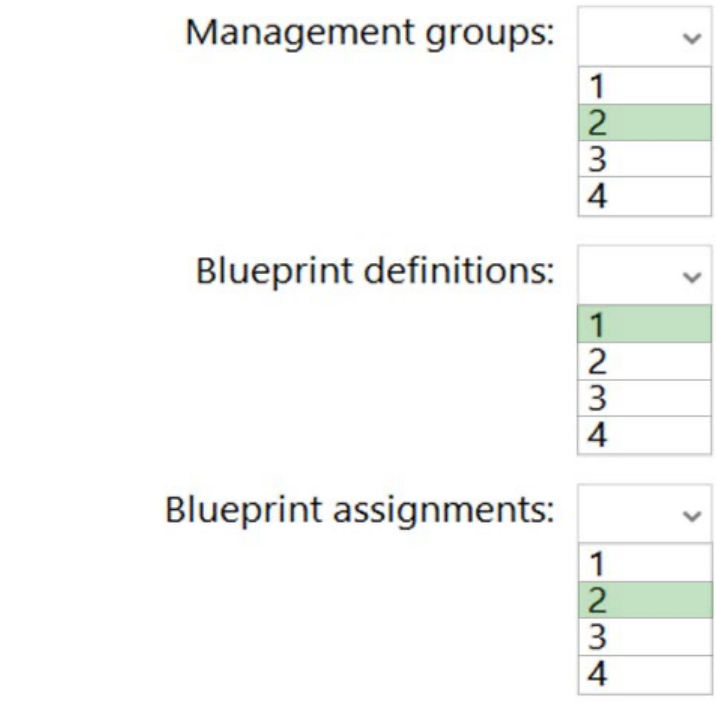
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



Answer Area



Correct Answer:

Box 1: 2 -

One management group for each Azure AD tenant

Azure management groups provide a level of scope above subscriptions.

All subscriptions within a management group automatically inherit the conditions applied to the management group.

All subscriptions within a single management group must trust the same Azure Active Directory tenant.

Box 2: 1 -

One single blueprint definition can be assigned to different existing management groups or subscriptions.

When creating a blueprint definition, you'll define where the blueprint is saved. Blueprints can be saved to a management group or subscription that you have
Contributor access to. If the location is a management group, the blueprint is available to assign to any child subscription of that management group.

Box 3: 2 -

Blueprint assignment -
Each Published Version of a blueprint can be assigned (with a max name length of 90 characters) to an existing management group or subscription.
Assigning a blueprint definition to a management group means the assignment object exists at the management group. The deployment of artifacts still targets a subscription.
Reference:
https://docs.microsoft.com/en-us/azure/governance/management-groups/overview https://docs.microsoft.com/en-us/azure/governance/blueprints/overview

Question #20 *Topic 1*

HOTSPOT -
You need to design an Azure policy that will implement the following functionality:
- For new resources, assign tags and values that match the tags and values of the resource group to which the resources are deployed.
- For existing resources, identify whether the tags and values match the tags and values of the resource group that contains the resources.
- For any non-compliant resources, trigger auto-generated remediation tasks to create missing tags and values.

The solution must use the principle of least privilege.
What should you include in the design? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Azure Policy effect to use:
- Append
- EnforceOPAConstraint
- EnforceRegoPolicy
- Modify

Azure Active Directory (Azure AD) object and role-based access control (RBAC) role to use for the remediation tasks:
- A managed identity with the Contributor role
- A managed identity with the User Access Administrator role
- A service principal with the Contributor role
- A service principal with the User Access Administrator role

Correct Answer:

Answer Area

Azure Policy effect to use:
- Append
- EnforceOPAConstraint
- EnforceRegoPolicy
- **Modify**

Azure Active Directory (Azure AD) object and role-based access control (RBAC) role to use for the remediation tasks:
- **A managed identity with the Contributor role**
- A managed identity with the User Access Administrator role
- A service principal with the Contributor role
- A service principal with the User Access Administrator role

Box 1: Modify -

Modify is used to add, update, or remove properties or tags on a subscription or resource during creation or update. A common example is updating tags on resources such as costCenter. Existing non-compliant resources can be remediated with a remediation task. A single Modify rule can have any number of operations. Policy assignments with effect set as Modify require a managed identity to do remediation.

Incorrect:

* The following effects are deprecated: EnforceOPAConstraint EnforceRegoPolicy

* Append is used to add additional fields to the requested resource during creation or update. A common example is specifying allowed IPs for a storage resource.

Append is intended for use with non-tag properties. While Append can add tags to a resource during a create or update request, it's recommended to use the

Modify effect for tags instead.

Box 2: A managed identity with the Contributor role

The managed identity needs to be granted the appropriate roles required for remediating resources to grant the managed identity.

Contributor - Can create and manage all types of Azure resources but can't grant access to others.

Incorrect:

User Access Administrator: lets you manage user access to Azure resources.

Reference:

https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects https://docs.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

Question #21 *Topic 1*

HOTSPOT -

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Account Kind	Location

storage1	Azure Storage account	Storage (general purpose v1)	East US
storage2	Azure Storage account	StorageV2 (general purpose v2)	East US
Workspace1	Azure Log Analytics workspace	**Not applicable**	East US
Workspace2	Azure Log Analytics workspace	**Not applicable**	East US
Hub1	Azure event hub	**Not applicable**	East US

You create an Azure SQL database named DB1 that is hosted in the East US Azure region.

To DB1, you add a diagnostic setting named Settings1. Settings1 archive SQLInsights to storage1 and sends SQLInsights to Workspace1.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Hot Area:

Answer Area

Statements	Yes	No
You can add a new diagnostic setting that archives SQLInsights logs to storage2.	○	○
You can add a new diagnostic setting that sends SQLInsights logs to Workspace2.	○	○
You can add a new diagnostic setting that sends SQLInsights logs to Hub1.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
You can add a new diagnostic setting that archives SQLInsights logs to storage2.	○	○
You can add a new diagnostic setting that sends SQLInsights logs to Workspace2.	○	○
You can add a new diagnostic setting that sends SQLInsights logs to Hub1.	○	○

Box 1: Yes -

A single diagnostic setting can define no more than one of each of the destinations. If you want to send data to more than one of a particular destination type (for example, two different Log Analytics workspaces), then create multiple settings.

Each resource can have up to 5 diagnostic settings.

Note: This diagnostic telemetry can be streamed to one of the following Azure resources for analysis.

* Log Analytics workspace
* Azure Event Hubs
* Azure Storage

Box 2: Yes -

Box 3: Yes -

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/diagnostic-settings https://docs.microsoft.com/en-us/azure/azure-sql/database/metrics-diagnostic-telemetry-logging-streaming-export-configure?tabs=azure-portal

Question #22 *Topic 1*

You plan to deploy an Azure SQL database that will store Personally Identifiable Information (PII).
You need to ensure that only privileged users can view the PII.
What should you include in the solution?

A. dynamic data masking Most Voted

B. role-based access control (RBAC)

C. Data Discovery & Classification

D. Transparent Data Encryption (TDE)

Correct Answer: *A*
Dynamic data masking limits sensitive data exposure by masking it to non-privileged users.
Dynamic data masking helps prevent unauthorized access to sensitive data by enabling customers to designate how much of the sensitive data to reveal with minimal impact on the application layer. It's a policy-based security feature that hides the sensitive data in the result set of a query over designated database fields, while the data in the database is not changed.
Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/database/dynamic-data-masking-overview

Community vote distribution
A (100%)

Question #23 *Topic 1*

You plan to deploy an app that will use an Azure Storage account.
You need to deploy the storage account. The storage account must meet the following requirements:
- Store the data for multiple users.
- Encrypt each user's data by using a separate key.
- Encrypt all the data in the storage account by using customer-managed keys.

What should you deploy?

A. files in a premium file share storage account
B. blobs in a general purpose v2 storage account Most Voted
C. blobs in an Azure Data Lake Storage Gen2 account
D. files in a general purpose v2 storage account

Correct Answer: *B*
You can specify a customer-provided key on Blob storage operations. A client making a read or write request against Blob storage can include an encryption key on the request for granular control over how blob data is encrypted and decrypted.
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption

Community vote distribution
B (94%) 6%

Question #24 *Topic 1*

HOTSPOT -
You have an Azure App Service web app that uses a system-assigned managed identity.
You need to recommend a solution to store the settings of the web app as secrets in an Azure key vault. The solution must meet the following requirements:
- Minimize changes to the app code.
- Use the principle of least privilege.

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:

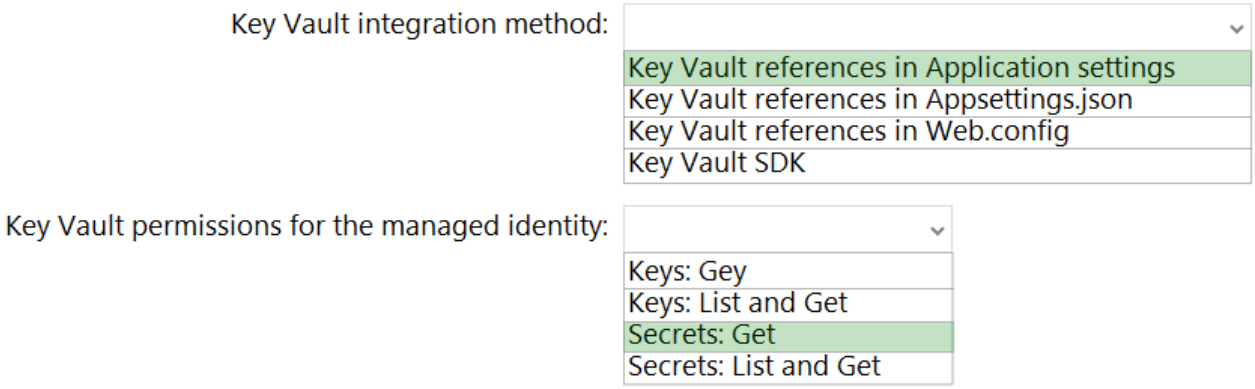
Answer Area

Key Vault integration method:
- Key Vault references in Application settings
- Key Vault references in Appsettings.json
- Key Vault references in Web.config
- Key Vault SDK

Key Vault permissions for the managed identity:
- Keys: Gey
- Keys: List and Get
- Secrets: Get
- Secrets: List and Get

Correct Answer:

Answer Area



Box 1: Key Vault references in Application settings

Source Application Settings from Key Vault.

Key Vault references can be used as values for Application Settings, allowing you to keep secrets in Key Vault instead of the site config. Application Settings are securely encrypted at rest, but if you need secret management capabilities, they should go into Key Vault.

To use a Key Vault reference for an app setting, set the reference as the value of the setting. Your app can reference the secret through its key as normal. No code changes are required.

Box 2: Secrets: Get -

In order to read secrets from Key Vault, you need to have a vault created and give your app permission to access it.

1. Create a key vault by following the Key Vault quickstart.
2. Create a managed identity for your application.
3. Key Vault references will use the app's system assigned identity by default, but you can specify a user-assigned identity.
4. Create an access policy in Key Vault for the application identity you created earlier. Enable the "Get" secret permission on this policy.

Reference:

https://docs.microsoft.com/en-us/azure/app-service/app-service-key-vault-references https://docs.microsoft.com/en-us/azure/app-service/app-service-key-vault-references

Question #25 *Topic 1*

You plan to deploy an application named App1 that will run on five Azure virtual machines. Additional virtual machines will be deployed later to run App1.

You need to recommend a solution to meet the following requirements for the virtual machines that will run App1:

- Ensure that the virtual machines can authenticate to Azure Active Directory (Azure AD) to gain access to an Azure key vault, Azure Logic Apps instances, and an Azure SQL database.
- Avoid assigning new roles and permissions for Azure services when you deploy additional virtual machines.
- Avoid storing secrets and certificates on the virtual machines.
- Minimize administrative effort for managing identities.

Which type of identity should you include in the recommendation?

A. a system-assigned managed identity

B. a service principal that is configured to use a certificate

C. a service principal that is configured to use a client secret

D. a user-assigned managed identity Most Voted

Correct Answer: *D*

Managed identities provide an identity for applications to use when connecting to resources that support Azure Active Directory (Azure AD) authentication.

A user-assigned managed identity:

Can be shared.

The same user-assigned managed identity can be associated with more than one Azure resource.

Common usage:

Workloads that run on multiple resources and can share a single identity.

For example, a workload where multiple virtual machines need to access the same resource.

Incorrect:

Not A: A system-assigned managed identity can't be shared. It can only be associated with a single Azure resource.

Typical usage:

Workloads that are contained within a single Azure resource.

Workloads for which you need independent identities.

For example, an application that runs on a single virtual machine.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

Community vote distribution

D (100%)

Question #26 *Topic 1*

You have the resources shown in the following table:

Name	Type
AS1	Azure Synapse Analytics instance
CDB1	Azure Cosmos DB SQL API account

CDB1 hosts a container that stores continuously updated operational data.

You are designing a solution that will use AS1 to analyze the operational data daily.

You need to recommend a solution to analyze the data without affecting the performance of the operational data store.

What should you include in the recommendation?

A. Azure Cosmos DB change feed

B. Azure Data Factory with Azure Cosmos DB and Azure Synapse Analytics connectors

C. Azure Synapse Link for Azure Cosmos DB Most Voted

D. Azure Synapse Analytics with PolyBase data loading

Correct Answer: *C*

Azure Synapse Link for Azure Cosmos DB creates a tight integration between Azure Cosmos DB and Azure Synapse Analytics. It enables customers to run near real-time analytics over their operational data with full performance isolation from their transactional workloads and without an ETL pipeline.

Reference:

https://docs.microsoft.com/en-us/azure/cosmos-db/synapse-link-frequently-asked-questions

Community vote distribution

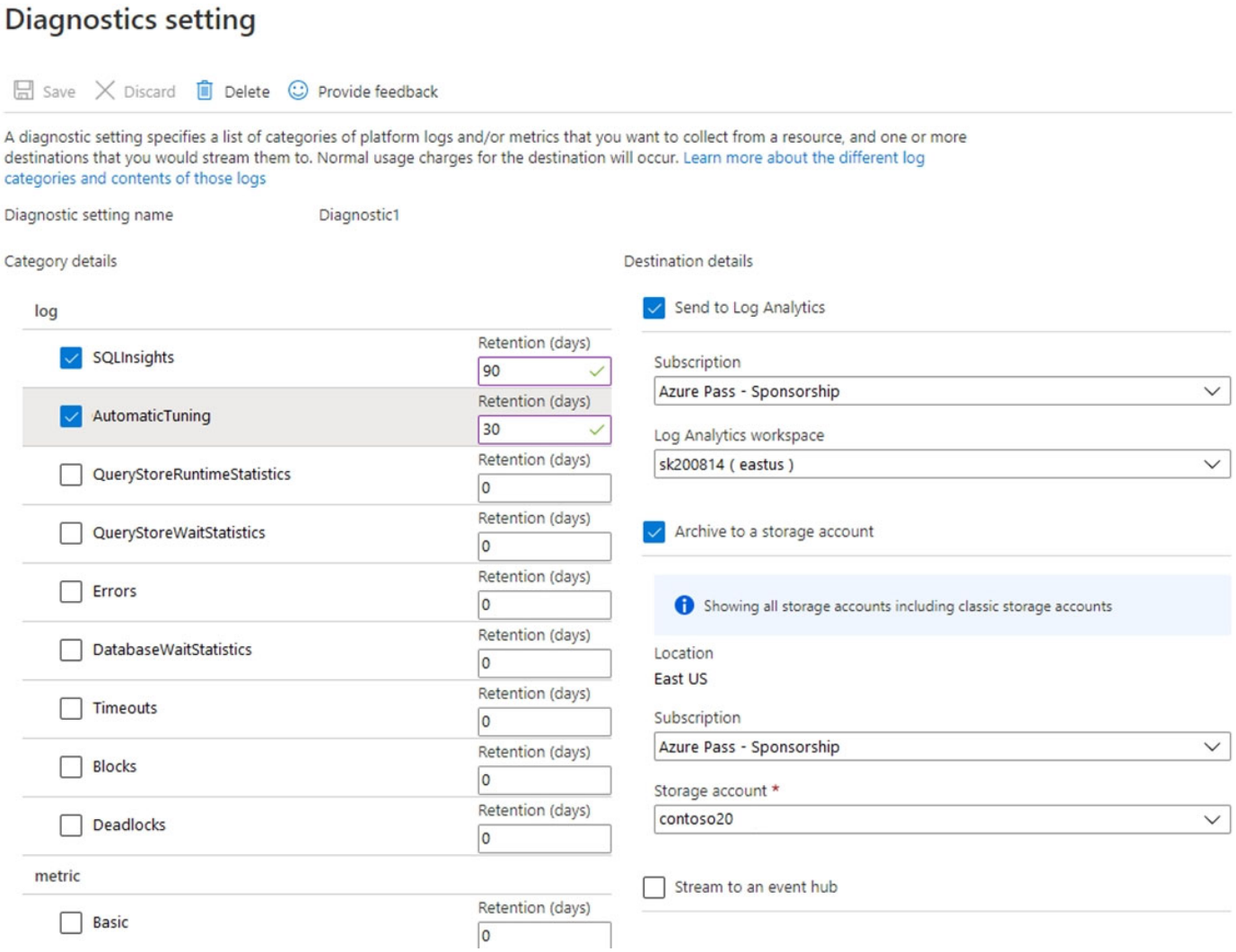
C (100%)

Question #27 *Topic 1*

HOTSPOT -

You deploy several Azure SQL Database instances.

You plan to configure the Diagnostics settings on the databases as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

The amount of time that SQLInsights data will be stored in blob storage is **[answer choice]**.

- 30 days
- 90 days
- 730 days
- indefinite

The maximum amount of time that SQLInsights data can be stored in Azure Log Analytics is **[answer choice]**.

- 30 days
- 90 days
- 730 days
- indefinite

Answer Area

The amount of time that SQLInsights data will be stored in blob storage is **[answer choice]**.

30 days
90 days

Question #28 *Topic 1*

You have an application that is used by 6,000 users to validate their vacation requests. The application manages its own credential store. Users must enter a username and password to access the application. The application does NOT support identity providers.
You plan to upgrade the application to use single sign-on (SSO) authentication by using an Azure Active Directory (Azure AD) application registration.
Which SSO method should you use?

A. header-based

B. SAML

C. password-based Most Voted

D. OpenID Connect

Correct Answer: *C*
Password - On-premises applications can use a password-based method for SSO. This choice works when applications are configured for Application Proxy.
With password-based SSO, users sign in to the application with a username and password the first time they access it. After the first sign-on, Azure AD provides the username and password to the application. Password-based SSO enables secure application password storage and replay using a web browser extension or mobile app. This option uses the existing sign-in process provided by the application, enables an administrator to manage the passwords, and doesn't require the user to know the password.
Incorrect:
Choosing an SSO method depends on how the application is configured for authentication. Cloud applications can use federation-based options, such as OpenID
Connect, OAuth, and SAML.
Federation - When you set up SSO to work between multiple identity providers, it's called federation.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-single-sign-on

Community vote distribution
C (100%)

Question #29 *Topic 1*

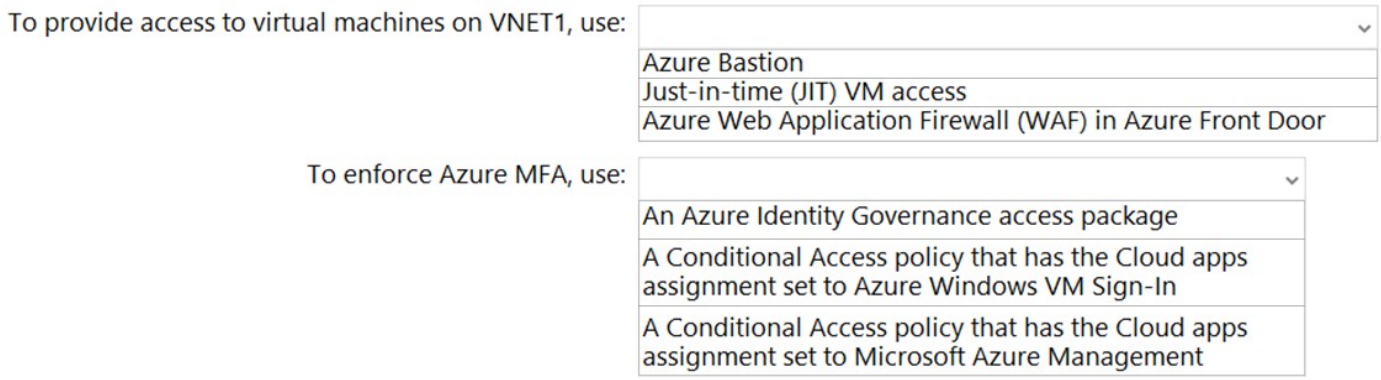
HOTSPOT -
You have an Azure subscription that contains a virtual network named VNET1 and 10 virtual machines. The virtual machines are connected to VNET1.
You need to design a solution to manage the virtual machines from the internet. The solution must meet the following requirements:
- Incoming connections to the virtual machines must be authenticated by using Azure Multi-Factor Authentication (MFA) before network connectivity is allowed.
- Incoming connections must use TLS and connect to TCP port 443.
- The solution must support RDP and SSH.

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

NOTE: Each correct selection is worth one point.

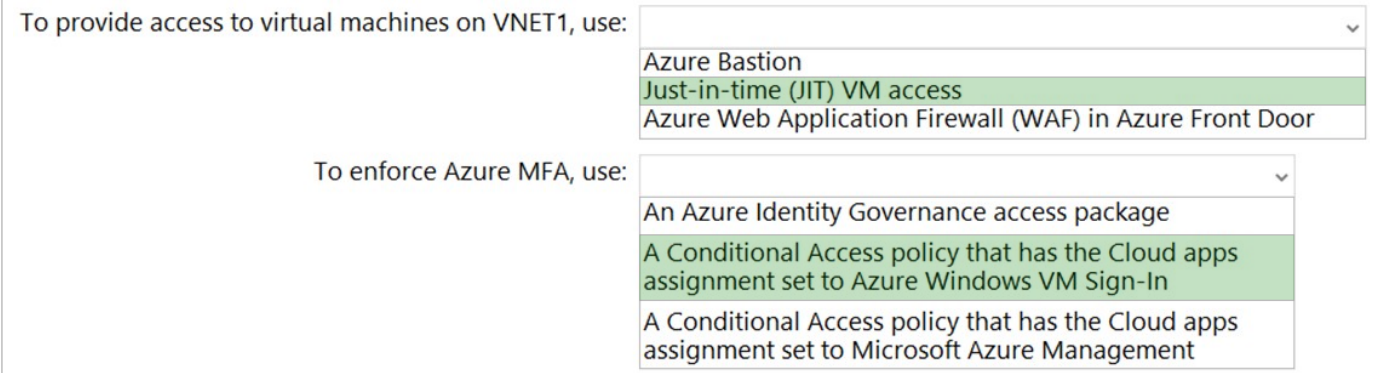
Hot Area:

Answer Area



Correct Answer:

Answer Area



Box 1: Just-in-time (JIT) VN access

Lock down inbound traffic to your Azure Virtual Machines with Microsoft Defender for Cloud's just-in-time (JIT) virtual machine (VM) access feature. This reduces exposure to attacks while providing easy access when you need to connect to a VM.

Note: Threat actors actively hunt accessible machines with open management ports, like RDP or SSH. Your legitimate users also use these ports, so it's not practical to keep them closed.

When you enable just-in-time VM access, you can select the ports on the VM to which inbound traffic will be blocked.

To solve this dilemma, Microsoft Defender for Cloud offers JIT. With JIT, you can lock down the inbound traffic to your VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.

Box 2: A conditional Access policy that has Cloud Apps assignment set to Azure Windows VM Sign-In

You can enforce Conditional Access policies such as multi-factor authentication or user sign-in risk check before authorizing access to Windows VMs in Azure that are enabled with Azure AD sign in. To apply Conditional Access policy, you must select the "Azure Windows VM Sign-In" app from the cloud apps or actions assignment option and then use Sign-in risk as a condition and/or require multi-factor authentication as a grant access control.

Reference:

https://docs.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-overview https://docs.microsoft.com/en-us/azure/active-directory/devices/howto-vm-sign-in-azure-ad-windows

Question #30 *Topic 1*

You are designing an Azure governance solution.
All Azure resources must be easily identifiable based on the following operational information: environment, owner, department and cost center.
You need to ensure that you can use the operational information when you generate reports for the Azure resources.
What should you include in the solution?

A. an Azure data catalog that uses the Azure REST API as a data source

B. an Azure management group that uses parent groups to create a hierarchy

C. an Azure policy that enforces tagging rules Most Voted

D. Azure Active Directory (Azure AD) administrative units

Correct Answer: *C*
You apply tags to your Azure resources, resource groups, and subscriptions to logically organize them into a taxonomy. Each tag consists of a name and a value pair.
You use Azure Policy to enforce tagging rules and conventions. By creating a policy, you avoid the scenario of resources being deployed to your subscription that don't have the expected tags for your organization. Instead of manually applying tags or searching for resources that aren't compliant, you create a policy that automatically applies the needed tags during deployment.
Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-policies

Community vote distribution
C (100%)

Question #31 *Topic 1*

A company named Contoso, Ltd. has an Azure Active Directory (Azure AD) tenant that is integrated with Microsoft 365 and an Azure subscription.
Contoso has an on-premises identity infrastructure. The infrastructure includes servers that run Active Directory Domain Services (AD DS) and Azure AD Connect.
Contoso has a partnership with a company named Fabrikam. Inc. Fabrikam has an Active Directory forest and a Microsoft 365 tenant. Fabrikam has the same on- premises identity infrastructure components as Contoso.
A team of 10 developers from Fabrikam will work on an Azure solution that will be hosted in the Azure subscription of Contoso. The developers must be added to the Contributor role for a resource group in the Contoso subscription.
You need to recommend a solution to ensure that Contoso can assign the role to the 10 Fabrikam developers. The solution must ensure that the Fabrikam developers use their existing credentials to access resources
What should you recommend?

A. In the Azure AD tenant of Contoso. create cloud-only user accounts for the Fabrikam developers.

B. Configure a forest trust between the on-premises Active Directory forests of Contoso and Fabrikam.

C. Configure an organization relationship between the Microsoft 365 tenants of Fabrikam and Contoso.

D. In the Azure AD tenant of Contoso, create guest accounts for the Fabnkam developers. Most Voted

Correct Answer: *D*
You can use the capabilities in Azure Active Directory B2B to collaborate with external guest users and you can use Azure RBAC to grant just the permissions that guest users need in your environment.
Incorrect:
Not B: Forest trust is used for internal security, not external access.
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-external-users

Community vote distribution
D (94%) 4%

Question #32 *Topic 1*

Your company has the divisions shown in the following table.

Division	Azure subscription	Azure Active Directory (Azure AD) tenant
East	Sub1	Contoso.com
West	Sub2	Fabrikam.com

Sub1 contains an Azure App Service web app named App1. App1 uses Azure AD for single-tenant user authentication. Users from contoso.com can authenticate to App1.
You need to recommend a solution to enable users in the fabrikam.com tenant to authenticate to App1.
What should you recommend?

A. Configure the Azure AD provisioning service.

B. Enable Azure AD pass-through authentication and update the sign-in endpoint.

C. Use Azure AD entitlement management to govern external users. Most Voted

D. Configure Azure AD join.

Correct Answer: *A*
You can enable automatic user provisioning for your multi-tenant application in Azure Active Directory.
Automatic user provisioning is the process of automating the creation, maintenance, and removal of user identities in target systems like your software-as-a- service applications.
Azure AD provides several integration paths to enable automatic user provisioning for your application.
* The Azure AD Provisioning Service manages the provisioning and deprovisioning of users from Azure AD to your application (outbound provisioning) and from your application to Azure AD (inbound provisioning). The service connects to the System for Cross-Domain Identity Management (SCIM) user management API endpoints provided by your application.
* Microsoft Graph
* The Security Assertion Markup Language Just in Time (SAML JIT) user provisioning.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/app-provisioning/isv-automatic-provisioning-multi-tenant-apps

Community vote distribution
C (100%)

Question #33 *Topic 1*

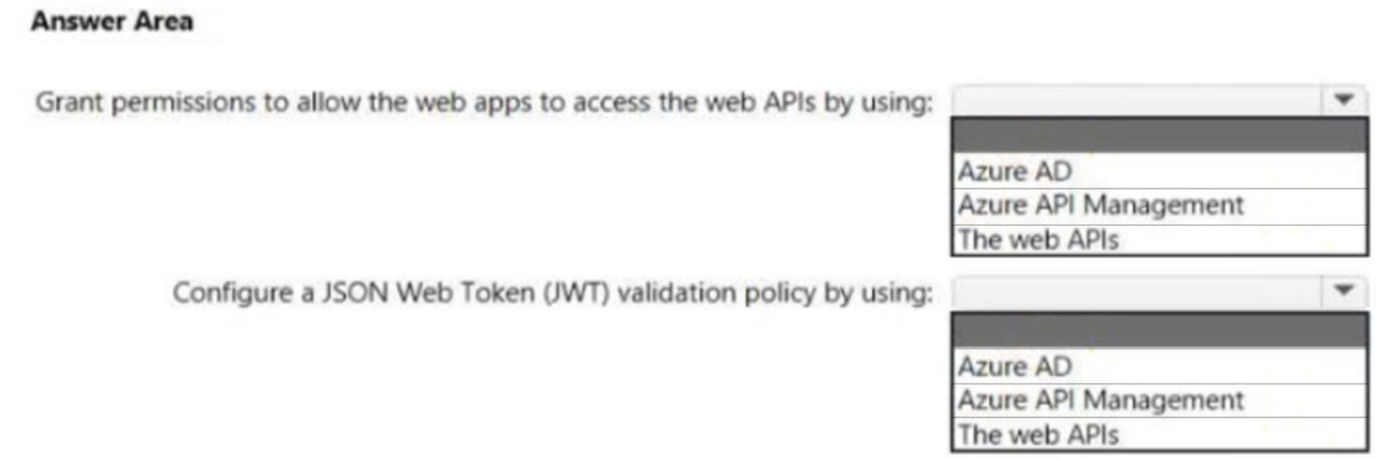
HOTSPOT -
Your company has 20 web APIs that were developed in-house.
The company is developing 10 web apps that will use the web APIs. The web apps and the APIs are registered in the company s Azure Active Directory (Azure
AD) tenant. The web APIs are published by using Azure API Management.
You need to recommend a solution to block unauthorized requests originating from the web apps from reaching the web APIs. The solution must meet the following requirements:
⇨ Use Azure AD-generated claims.
Minimize configuration and management effort.

▪

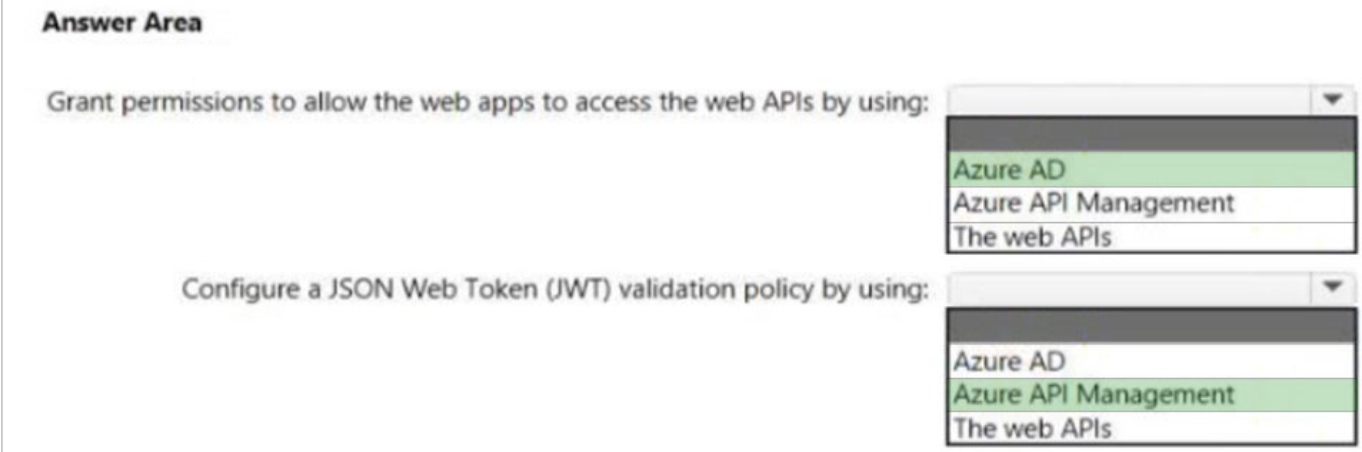
What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: Azure AD -

Grant permissions in Azure AD.

Box 2: Azure API Management -

Configure a JWT validation policy to pre-authorize requests.

Pre-authorize requests in API Management with the Validate JWT policy, by validating the access tokens of each incoming request. If a request does not have a valid token, API Management blocks it.

Reference:

https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-protect-backend-with-aad

Question #34 *Topic 1*

You need to recommend a solution to generate a monthly report of all the new Azure Resource Manager (ARM) resource deployments in your Azure subscription.
What should you include in the recommendation?

A. Azure Log Analytics Most Voted

B. Azure Arc

C. Azure Analysis Services

D. Application Insights

Correct Answer: *A*
The Activity log is a platform log in Azure that provides insight into subscription-level events. Activity log includes such information as when a resource is modified or when a virtual machine is started.
Activity log events are retained in Azure for 90 days and then deleted.
For more functionality, you should create a diagnostic setting to send the Activity log to one or more of these locations for the following reasons: to Azure Monitor Logs for more complex querying and alerting, and longer retention (up to two years) to Azure Event Hubs to forward outside of Azure to Azure Storage for cheaper, long-term archiving
Note: Azure Monitor builds on top of Log Analytics, the platform service that gathers log and metrics data from all your resources. The easiest way to think about it is that Azure Monitor is the marketing name, whereas Log Analytics is the technology that powers it.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log

Community vote distribution
A (100%)

Question #35 *Topic 1*

Your company has the divisions shown in the following table.

Division	Azure subscription	Azure Active Directory (Azure AD) tenant
East	Sub1	Contoso.com
West	Sub2	Fabrikam.com

Sub1 contains an Azure App Service web app named App1. App1 uses Azure AD for single-tenant user authentication. Users from contoso.com can authenticate to App1.
You need to recommend a solution to enable users in the fabrikam.com tenant to authenticate to App1.
What should you recommend?

A. Configure the Azure AD provisioning service.

B. Configure assignments for the fabrikam.com users by using Azure AD Privileged Identity Management (PIM).

C. Use Azure AD entitlement management to govern external users. Most Voted

D. Configure Azure AD Identity Protection.

Correct Answer: *C*
Entitlement management is an identity governance capability that enables organizations to manage identity and access lifecycle at scale by automating access request workflows, access assignments, reviews, and expiration. Entitlement management allows delegated non-admins to create access packages that external users from other organizations can request access to. One and multi-stage approval workflows can be configured to evaluate requests, and provision users for time-limited access with recurring reviews. Entitlement management enables policy-based provisioning and deprovisioning of external accounts.

Note: Access Packages -
An access package is the foundation of entitlement management. Access packages are groupings of policy-governed resources a user needs to collaborate on a project or do other tasks. For example, an access package might include: access to specific SharePoint sites. enterprise applications including your custom in-house and SaaS apps like Salesforce.
Microsoft Teams.
Microsoft 365 Groups.
Incorrect:
Not A: Automatic provisioning refers to creating user identities and roles in the cloud applications that users need access to. In addition to creating user identities, automatic provisioning includes the maintenance and removal of user identities as status or roles change.
Not B: Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about. Here are some of the key features of Privileged Identity Management:
Provide just-in-time privileged access to Azure AD and Azure resources
Assign time-bound access to resources using start and end dates
Etc.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/6-secure-access-entitlement-managment
https://docs.microsoft.com/en-us/azure/active-directory/app-provisioning/how-provisioning-works https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

Community vote distribution
C (100%)

Question #36 *Topic 1*

You are developing an app that will read activity logs for an Azure subscription by using Azure Functions.

You need to recommend an authentication solution for Azure Functions. The solution must minimize administrative effort.

What should you include in the recommendation?

A. an enterprise application in Azure AD

B. system-assigned managed identities Most Voted

C. shared access signatures (SAS)

D. application registration in Azure AD

Correct Answer: *B*

Community vote distribution

B (100%)

Question #37 *Topic 1*

Your company has the divisions shown in the following table.

Division	Azure subscription	Azure AD tenant
East	Sub1	Contoso.com
West	Sub2	Fabrikam.com

Sub1 contains an Azure App Service web app named App1. App1 uses Azure AD for single-tenant user authentication. Users from contoso.com can authenticate to App1.

You need to recommend a solution to enable users in the fabrikam.com tenant to authenticate to App1.

What should you recommend?

A. Configure Azure AD join.

B. Use Azure AD entitlement management to govern external users. Most Voted

C. Enable Azure AD pass-through authentication and update the sign-in endpoint.

D. Configure assignments for the fabrikam.com users by using Azure AD Privileged Identity Management (PIM).

Correct Answer: *B*

Community vote distribution

B (100%)

Question #38 *Topic 1*

Your company has the divisions shown in the following table.

Division	Azure subscription	Azure AD tenant
East	Sub1	Contoso.com
West	Sub2	Fabrikam.com

Sub1 contains an Azure App Service web app named App1. App1 uses Azure AD for single-tenant user authentication. Users from contoso.com can authenticate to App1.

You need to recommend a solution to enable users in the fabrikam.com tenant to authenticate to App1.

What should you recommend?

A. Configure Azure AD join.

B. Configure Azure AD Identity Protection.

C. Use Azure AD entitlement management to govern external users. Most Voted

D. Configure assignments for the fabrikam.com users by using Azure AD Privileged Identity Management (PIM).

Correct Answer: *C*

Community vote distribution

C (100%)

Question #39 *Topic 1*

You need to recommend a solution to generate a monthly report of all the new Azure Resource Manager (ARM) resource deployments in your Azure subscription.

What should you include in the recommendation?

A. Azure Activity Log Most Voted

B. Azure Arc

C. Azure Analysis Services

D. Azure Monitor metrics

Correct Answer: *A*

Community vote distribution

A (100%)

Question #40 *Topic 1*

HOTSPOT

-

You have an Azure subscription that contains an Azure key vault named KV1 and a virtual machine named VM1. VM1 runs Windows Server 2022: Azure Edition.

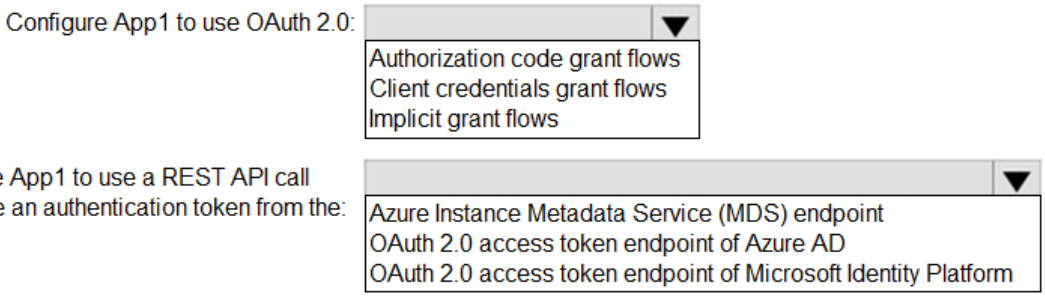
You plan to deploy an ASP.Net Core-based application named App1 to VM1.

You need to configure App1 to use a system-assigned managed identity to retrieve secrets from KV1. The solution must minimize development effort.

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

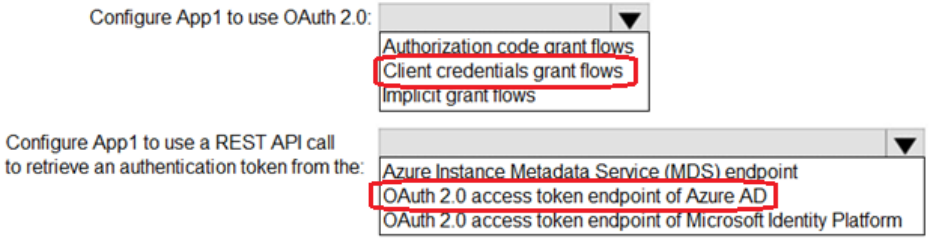
NOTE: Each correct selection is worth one point.

Answer Area



Correct Answer:

Answer Area



Question #41 *Topic 1*

Your company has the divisions shown in the following table.

Division	Azure subscription	Azure AD tenant
East	Sub1	Contoso.com
West	Sub2	Fabrikam.com

Sub1 contains an Azure App Service web app named App1. App1 uses Azure AD for single-tenant user authentication. Users from contoso.com can authenticate to App1.

You need to recommend a solution to enable users in the fabrikam.com tenant to authenticate to App1.

What should you recommend?

A. Configure Azure AD join.

B. Configure Azure AD Identity Protection.

C. Configure a Conditional Access policy.

D. Configure Supported account types in the application registration and update the sign-in endpoint. Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Question #42 *Topic 1*

You have an Azure AD tenant named contoso.com that has a security group named Group1. Group1 is configured for assigned memberships. 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. Most Voted

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

Correct Answer: *D*

Community vote distribution

C (97%)

Question #43 *Topic 1*

HOTSPOT
-

You have an Azure subscription named Sub1 that is linked to an Azure AD tenant named contoso.com.

You plan to implement two ASP.NET Core apps named App1 and App2 that will be deployed to 100 virtual machines in Sub1. Users will sign in to App1 and App2 by using their contoso.com credentials.

App1 requires read permissions to access the calendar of the signed-in user. App2 requires write permissions to access the calendar of the signed-in user.

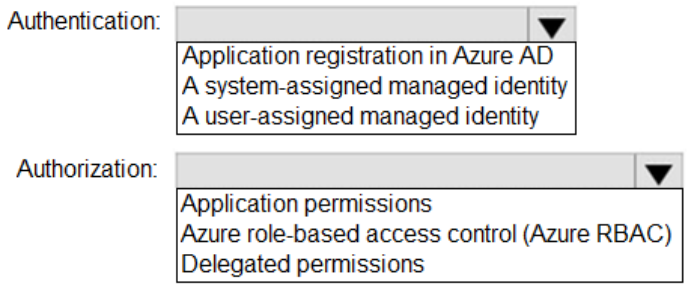
You need to recommend an authentication and authorization solution for the apps. The solution must meet the following requirements:

• Use the principle of least privilege.
• Minimize administrative effort.

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

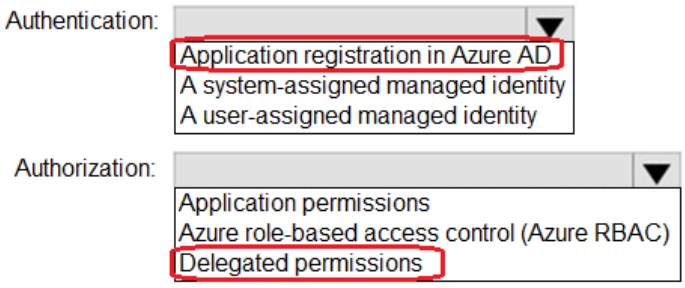
NOTE: Each correct selection is worth one point.

Answer Area



Correct Answer:

Answer Area



Question #44 *Topic 1*

Your company has the divisions shown in the following table.

Division	Azure subscription	Azure AD tenant
East	Sub1	Contoso.com
West	Sub2	Fabrikam.com

Sub1 contains an Azure App Service web app named App1. App1 uses Azure AD for single-tenant user authentication. Users from contoso.com can authenticate to App1.

You need to recommend a solution to enable users in the fabrikam.com tenant to authenticate to App1.

What should you recommend?

A. Enable Azure AD pass-through authentication and update the sign-in endpoint.

B. Use Azure AD entitlement management to govern external users. Most Voted

C. Configure assignments for the fabrikam.com users by using Azure AD Privileged Identity Management (PIM).

D. Configure Azure AD Identity Protection.

Correct Answer: *B*

Community vote distribution

B (100%)

Question #45 *Topic 1*

Your company has the divisions shown in the following table.

Division	Azure subscription	Azure AD tenant
East	Sub1	Contoso.com
West	Sub2	Fabrikam.com

Sub1 contains an Azure App Service web app named App1. App1 uses Azure AD for single-tenant user authentication. Users from contoso.com can authenticate to App1.

You need to recommend a solution to enable users in the fabrikam.com tenant to authenticate to App1.

What should you recommend?

A. Configure the Azure AD provisioning service.

B. Enable Azure AD pass-through authentication and update the sign-in endpoint.

C. Configure Supported account types in the application registration and update the sign-in endpoint. Most Voted

D. Configure Azure AD join.

Correct Answer: *C*

Community vote distribution

C (100%)

Question #46 *Topic 1*

HOTSPOT

-

You have an Azure AD tenant that contains a management group named MG1.

You have the Azure subscriptions shown in the following table.

Name	Management group
Sub1	MG1
Sub2	MG2
Sub3	Tenant Root Group

The subscriptions contain the resource groups shown in the following table.

Name	Subscription
RG1	Sub1
RG2	Sub2
RG3	Sub3

The subscription contains the Azure AD security groups shown in the following table.

Name	Member of
Group1	Group3
Group2	Group3
Group3	*None*

The subscription contains the user accounts shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

You perform the following actions:

Assign User3 the Contributor role for Sub1.
Assign Group1 the Virtual Machine Contributor role for MG1.
Assign Group3 the Contributor role for the Tenant Root Group.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can create a new virtual machine in RG1.	○	○
User2 can grant permissions to Group2.	○	○
User3 can create a storage account in RG2.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1 can create a new virtual machine in RG1.	●	○
User2 can grant permissions to Group2.	○	●
User3 can create a storage account in RG2.	●	○

Question #47 *Topic 1*

Your company has the divisions shown in the following table.

Division	Azure subscription	Azure AD tenant
East	Sub1	Contoso.com
West	Sub2	Fabrikam.com

Sub1 contains an Azure App Service web app named App1. App1 uses Azure AD for single-tenant user authentication. Users from contoso.com can authenticate to App1.

You need to recommend a solution to enable users in the fabrikam.com tenant to authenticate to App1.

What should you recommend?

A. Configure Azure AD Identity Protection.

B. Configure assignments for the fabrikam.com users by using Azure AD Privileged Identity Management (PIM).

C. Configure Supported account types in the application registration and update the sign-in endpoint. Most Voted

D. Configure a Conditional Access policy.

Correct Answer: *C*

Community vote distribution

C (100%)

Question #48 *Topic 1*

Your company has the divisions shown in the following table.

Division	Azure subscription	Azure AD tenant
East	Sub1	Contoso.com
West	Sub2	Fabrikam.com

Sub1 contains an Azure App Service web app named App1. App1 uses Azure AD for single-tenant user authentication. Users from contoso.com can authenticate to App1.

You need to recommend a solution to enable users in the fabrikam.com tenant to authenticate to App1.

What should you recommend?

A. Use Azure AD entitlement management to govern external users. Most Voted

B. Enable Azure AD pass-through authentication and update the sign-in endpoint.

C. Configure a Conditional Access policy.

D. Configure assignments for the fabrikam.com users by using Azure AD Privileged Identity Management (PIM).

Correct Answer: *A*

Community vote distribution

A (100%)

Question #49 *Topic 1*

You have an Azure subscription that contains 1,000 resources.

You need to generate compliance reports for the subscription. The solution must ensure that the resources can be grouped by department.

What should you use to organize the resources?

A. application groups and quotas

B. Azure Policy and tags Most Voted

C. administrative units and Azure Lighthouse

D. resource groups and role assignments

Correct Answer: *B*

Community vote distribution

B (100%)

Question #50 *Topic 1*

You need to recommend a solution to generate a monthly report of all the new Azure Resource Manager (ARM) resource deployments in your Azure subscription.

What should you include in the recommendation?

A. Azure Arc

B. Azure Monitor metrics

C. Azure Advisor

D. Azure Log Analytics Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Next Questions →