

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
- D. compute resources
- E. resource groups
- F. management groups

**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%)

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:

Features

Answer Area

a public Azure Load Balancer

a managed identity

an internal Azure Load Balancer

a Conditional Access policy

an Azure App Service plan

Azure AD Application Proxy

an Azure AD enterprise application



Correct Answer:

Features

Answer Area

a public Azure Load Balancer

a managed identity

an internal Azure Load Balancer

an Azure App Service plan

Azure AD Application Proxy

an Azure AD enterprise application

a Conditional Access policy



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
- 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%)

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

**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%)

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.

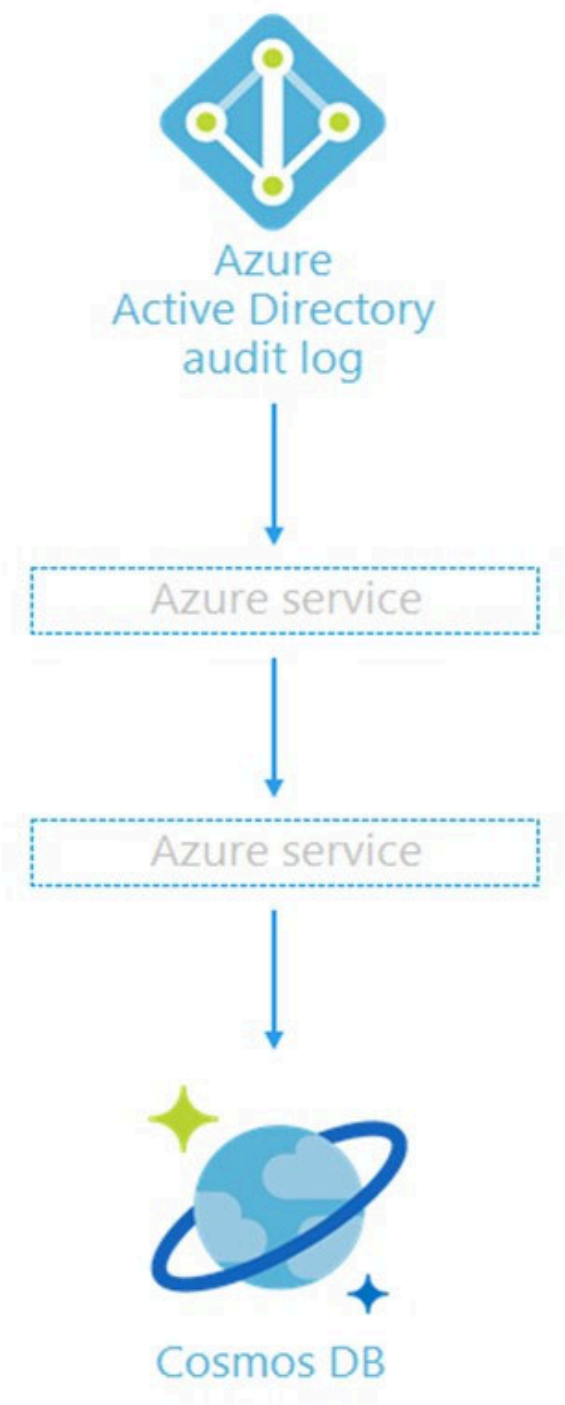
NOTE: Each correct selection is worth one point.

Select and Place:

**Azure Services**

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

**Answer Area**



Correct Answer:

### Azure Services

Azure Event Grid

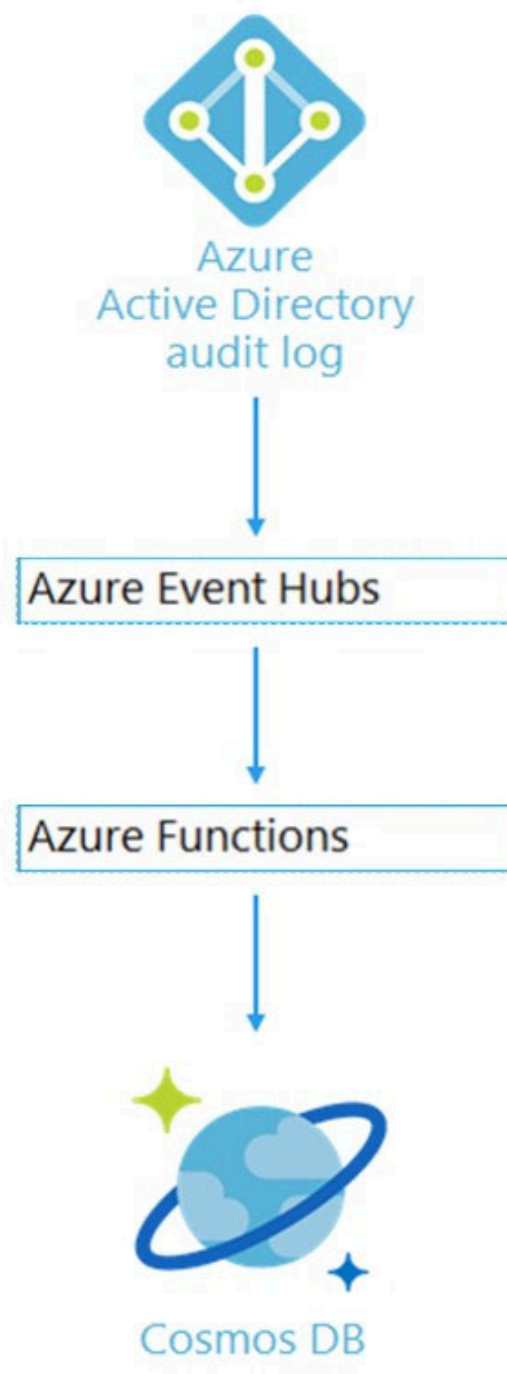
Azure Event Hubs

Azure Functions

Azure Monitor Logs

Azure Notification Hubs

### Answer Area



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>

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

**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%)

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>



## 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	<ul style="list-style-type: none"><li>Review the membership of administrative roles and require users to provide a justification for continued membership.</li><li>Get alerts about changes in administrator assignments.</li><li>See a history of administrator activation, including which changes administrators made to Azure resources.</li></ul>
Development	<ul style="list-style-type: none"><li>Enable the applications to access Key Vault and retrieve keys for use in code.</li></ul>
Quality Assurance	<ul style="list-style-type: none"><li>Receive temporary administrator access to create and configure additional web apps in the test environment.</li></ul>

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

**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

Correct Answer:

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>