DBCLOUD
EXAMS

QUESTIONS & ANSWERS

verified



Technology Provider: Microsoft
Exam: Microsoft Cybersecurity Architect
Number of questions in the database: 237
Exam Version: NOV.2026

Topic 1 - Question Set 1

Question #1*Topic 1*

Your company has a Microsoft 365 ES subscription.
The Chief Compliance Officer plans to enhance privacy management in the working environment.
You need to recommend a solution to enhance the privacy management. The solution must meet the following requirements:
☞ Identify unused personal data and empower users to make smart data handling decisions.
☞ Provide users with notifications and guidance when a user sends personal data in Microsoft Teams.
☞ Provide users with recommendations to mitigate privacy risks.
What should you include in the recommendation?

- A. communication compliance in insider risk management
- B. Microsoft Viva Insights
- C. Privacy Risk Management in Microsoft Priva
- D. Advanced eDiscovery

Correct Answer: *C*
Privacy Risk Management in Microsoft Priva gives you the capability to set up policies that identify privacy risks in your Microsoft 365 environment and enable easy remediation. Privacy Risk Management policies are meant to be internal guides and can help you:
Detect overexposed personal data so that users can secure it.
Spot and limit transfers of personal data across departments or regional borders.
Help users identify and reduce the amount of unused personal data that you store.
Incorrect:
Not B: Microsoft Viva Insights provides personalized recommendations to help you do your best work. Get insights to build better work habits, such as following through on commitments made to collaborators and protecting focus time in the day for uninterrupted, individual work.
Not D: The Microsoft Purview eDiscovery (Premium) solution builds on the existing Microsoft eDiscovery and analytics capabilities. eDiscovery (Premium) provides an end-to-end workflow to preserve, collect, analyze, review, and export content that's responsive to your organization's internal and external investigations.
Reference:
https://docs.microsoft.com/en-us/privacy/priva/risk-management

Respuesta por mayor votación de la comunidad

C (100%)

https://dbcloud.academy/

Question #2*Topic 1*

You have an Azure subscription that has Microsoft Defender for Cloud enabled.
Suspicious authentication activity alerts have been appearing in the Workload protections dashboard.
You need to recommend a solution to evaluate and remediate the alerts by using workflow automation. The solution must minimize development effort.
What should you include in the recommendation?

- A. Azure Monitor webhooks
- B. Azure Event Hubs
- C. Azure Functions apps
- D. Azure Logics Apps

Correct Answer: *D*
The workflow automation feature of Microsoft Defender for Cloud feature can trigger Logic Apps on security alerts, recommendations, and changes to regulatory compliance.
Note: Azure Logic Apps is a cloud-based platform for creating and running automated workflows that integrate your apps, data, services, and systems. With this platform, you can quickly develop highly scalable integration solutions for your enterprise and business-to-business (B2B) scenarios.
Incorrect:
Not C: Using Azure Functions apps would require more effort.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation

Respuesta por mayor votación de la comunidad

D (100%)

Question #3*Topic 1*

Your company is moving a big data solution to Azure.
The company plans to use the following storage workloads:
⇨ Azure Storage blob containers
⇨ Azure Data Lake Storage Gen2

Azure Storage file shares -
▪
⇨ Azure Disk Storage
Which two storage workloads support authentication by using Azure Active Directory (Azure AD)?
Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

- A. Azure Storage file shares
- B. Azure Disk Storage
- C. Azure Storage blob containers

https://dbcloud.academy/

- D. Azure Data Lake Storage Gen2

Correct Answer: *CD*
C: Azure Storage supports using Azure Active Directory (Azure AD) to authorize requests to blob data. With Azure AD, you can use Azure role-based access control (Azure RBAC) to grant permissions to a security principal, which may be a user, group, or application service principal. The security principal is authenticated by Azure AD to return an OAuth 2.0 token. The token can then be used to authorize a request against the Blob service.
You can scope access to Azure blob resources at the following levels, beginning with the narrowest scope:
* An individual container. At this scope, a role assignment applies to all of the blobs in the container, as well as container properties and metadata.
* The storage account.
* The resource group.
* The subscription.
* A management group.
D: You can securely access data in an Azure Data Lake Storage Gen2 (ADLS Gen2) account using OAuth 2.0 with an Azure Active Directory (Azure AD) application service principal for authentication. Using a service principal for authentication provides two options for accessing data in your storage account:
A mount point to a specific file or path

Direct access to data -
Incorrect:
Not A: To enable AD DS authentication over SMB for Azure file shares, you need to register your storage account with AD DS and then set the required domain properties on the storage account. To register your storage account with AD DS, create an account representing it in your AD DS.
Reference:
https://docs.microsoft.com/en-us/azure/storage/blobs/authorize-access-azure-active-directory
https://docs.microsoft.com/en-us/azure/databricks/data/data-sources/azure/adls-gen2/azure-datalake-gen2-sp-access

Respuesta por mayor votación de la comunidad

CD (75%)

AD (25%)

Question #4*Topic 1*

HOTSPOT -
Your company is migrating data to Azure. The data contains Personally Identifiable Information (PII).
The company plans to use Microsoft Information Protection for the PII data store in Azure.
You need to recommend a solution to discover PII data at risk in the Azure resources.
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.

https://dbcloud.academy/

Hot Area:

Answer Area

To connect the Azure data sources to Microsoft Information Protection:

- Azure Purview
- Endpoint data loss prevention
- Microsoft Defender for Cloud Apps
- Microsoft Information Protection

To triage security alerts related to resources that contain PII data:

- Azure Monitor
- Endpoint data loss prevention
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps

Correct Answer:

Answer Area

To connect the Azure data sources to Microsoft Information Protection:

- Azure Purview
- Endpoint data loss prevention
- Microsoft Defender for Cloud Apps
- Microsoft Information Protection

To triage security alerts related to resources that contain PII data:

- Azure Monitor
- Endpoint data loss prevention
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps

Box 1: Azure Purview -
Microsoft Purview is a unified data governance service that helps you manage and govern your on-

https://dbcloud.academy/