SC-900^{Q&As}

Microsoft Security Compliance and Identity Fundamentals

Pass Microsoft SC-900 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/sc-900.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

Instant Download After Purchase

100% Money Back Guarantee

365 Days Free Update

800,000+ Satisfied Customers

QUESTION 1

HOTSPOT

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
With Advanced Audit in Microsoft 365, you can identify when email items were accessed.	○	○
Advanced Audit in Microsoft 365 supports the same retention period of audit logs as core auditing.	○	○
Advanced Audit in Microsoft 365 allocates customer-dedicated bandwidth for accessing audit data.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
With Advanced Audit in Microsoft 365, you can identify when email items were accessed.	○	○
Advanced Audit in Microsoft 365 supports the same retention period of audit logs as core auditing.	○	○
Advanced Audit in Microsoft 365 allocates customer-dedicated bandwidth for accessing audit data.	○	○

Box 1: Yes

The MailItemsAccessed event is a mailbox auditing action and is triggered when mail data is accessed by mail protocols and mail clients.

Box 2: No

![Pass2Lead](https://Pass2Lead.com)
Basic Audit retains audit records for 90 days.

Advanced Audit retains all Exchange, SharePoint, and Azure Active Directory audit records for one year. This is accomplished by a default audit log retention policy that retains any audit record that contains the value of Exchange, SharePoint,

or AzureActiveDirectory for the Workload property (which indicates the service in which the activity occurred) for one year.

Box 3: yes

Advanced Audit in Microsoft 365 provides high-bandwidth access to the Office 365 Management Activity API.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/advanced-audit?view=o365-worldwide

https://docs.microsoft.com/en-us/microsoft-365/compliance/auditing-solutions-overview?view=o365-worldwide#licensing-requirements

https://docs.microsoft.com/en-us/office365/servicedescriptions/microsoft-365-service-descriptions/microsoft-365-tenantlevel-services-licensing-guidance/microsoft-365-security-compliance-licensing-guidance#advanced-audit

---

QUESTION 2

HOTSPOT

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Windows Hello for Business can use the Microsoft Authenticator app as an authentication method.	○	○
Windows Hello for Business can use a PIN code as an authentication method.	○	○
Windows Hello for Business authentication information syncs across all the devices registered by a user.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
Windows Hello for Business can use the Microsoft Authenticator app as an authentication method.	○	◉
Windows Hello for Business can use a PIN code as an authentication method.	◉	○
Windows Hello for Business authentication information syncs across all the devices registered by a user.	○	◉

Box 1: No

The Microsoft Authenticator app helps you sign in to your accounts when you\'re using two-factor verification. Two-factor verification helps you to use your accounts more securely because passwords can be forgotten, stolen, or compromised.

Two-factor verification uses a second factor like your phone to make it harder for other people to break in to your account.

Box 2: Yes

In Windows 10, Windows Hello for Business replaces passwords with strong two-factor authentication on devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN.

Box 3: No

Windows Hello credentials are based on certificate or asymmetrical key pair. Windows Hello credentials can be bound to the device, and the token that is obtained using the credential is also bound to the device.

Reference: https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview

---

QUESTION 3

You have a Microsoft OneDrive for Business folder that contains the files shown in the following table.

Type	Number of files
.jpg	50
.docx	300
.txt	50
.zip	20

In Microsoft Cloud App Security, you create a file policy to automatically apply a classification. What is the effect of applying the policy?

A. The policy will apply to only the .docx and .txt files. The policy will classify the files within 24 hours.

![Pass2Lead](https://Pass2Lead.com)
B. The policy will apply to all the files. The policy will classify only 100 files daily.

C. The policy will apply to only the .docx files. The policy will classify only 100 files daily.

D. The policy will apply to only the .docx and .txt files. The policy will classify the files immediately.

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/cloud-app-security/azip-integration

QUESTION 4

You need to ensure repeatability when creating new resources in an Azure subscription. What should you use?

A. Microsoft Sentinel

B. Azure Policy

C. Azure Batch

D. Azure Blueprints

Correct Answer: D

Using Azure Blueprints for repeatable deploy and update operations.

Sometimes, using policies is just not enough. Reasons may vary—the number of projects is too big to govern via policies, they become obstacles because you cannot enforce a particular rule, or you find complex designs with them to be just too complicated. For all of those scenarios, Microsoft has prepared an additional tool for Azure administrators called Azure Blueprints. They are like sketches for buildings—you can set collect all required artifacts in one place and use it for multiple deployments. With this feature, you can orchestrate multiple deployments and shorten the time needed to achieve a coherent architecture. If you are familiar with ARM templates, you may find Azure Blueprints much easier to understand as they offer similar functionalities to Resource Manager. On the other hand, it is a great tool for preserving a connection between a blueprint and a deployment or manage multiple subscriptions at once.

Reference: https://subscription.packtpub.com/book/cloud-and-networking/9781838551452/2/ch02lvl1sec13/using-azure-blueprints-for-repeatable-deploy-and-update-operations

QUESTION 5

HOTSPOT You are implementing Microsoft Office 365 Message Encryption (OME) for a Microsoft 365 tenant named contoso.com. You need to meet the following requirements:

1.

All email to a domain named fabrikam.com must be encrypted automatically.

2.

Encrypted emails must expire seven days after they are sent.

![Pass2Lead](https://Pass2Lead.com)
What should you configure 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

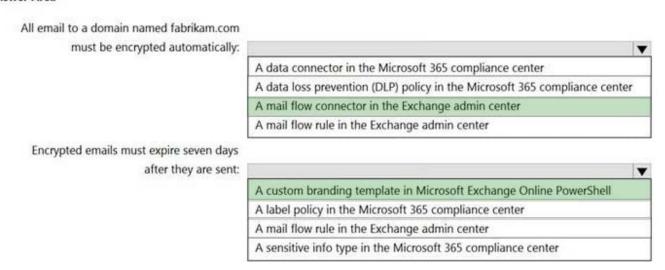All email to a domain named fabrikam.com must be encrypted automatically: ▼

A data connector in the Microsoft 365 compliance center
A data loss prevention (DLP) policy in the Microsoft 365 compliance center
A mail flow connector in the Exchange admin center
A mail flow rule in the Exchange admin center

Encrypted emails must expire seven days after they are sent: ▼

A custom branding template in Microsoft Exchange Online PowerShell
A label policy in the Microsoft 365 compliance center
A mail flow rule in the Exchange admin center
A sensitive info type in the Microsoft 365 compliance center

Correct Answer:

Answer Area

All email to a domain named fabrikam.com must be encrypted automatically: ▼

A data connector in the Microsoft 365 compliance center
A data loss prevention (DLP) policy in the Microsoft 365 compliance center
A mail flow connector in the Exchange admin center
A mail flow rule in the Exchange admin center

Encrypted emails must expire seven days after they are sent: ▼

A custom branding template in Microsoft Exchange Online PowerShell
A label policy in the Microsoft 365 compliance center
A mail flow rule in the Exchange admin center
A sensitive info type in the Microsoft 365 compliance center