

45 questions in 45 minutes

Question #1

Topic 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
All Azure Active Directory (Azure AD) license editions include the same features.	<input type="radio"/>	<input type="radio"/>
You can manage an Azure Active Directory (Azure AD) tenant by using the Azure portal.	<input type="radio"/>	<input type="radio"/>
You must deploy Azure virtual machines to host an Azure Active Directory (Azure AD) tenant.	<input type="radio"/>	<input type="radio"/>

Hide Solution

Discussion 30

Correct Answer:

**Answer Area**

Statements	Yes	No
All Azure Active Directory (Azure AD) license editions include the same features.	<input type="radio"/>	<input checked="" type="radio"/>
You can manage an Azure Active Directory (Azure AD) tenant by using the Azure portal.	<input checked="" type="radio"/>	<input type="radio"/>
You must deploy Azure virtual machines to host an Azure Active Directory (Azure AD) tenant.	<input type="radio"/>	<input checked="" type="radio"/>

### Answer Area

Correct Answer:

- Azure Blueprints
- Azure Policy
- The Microsoft Cloud Adoption Framework for Azure
- A resource lock

provides best practices from Microsoft employees, partners, and customers, including tools and guidance to assist in an Azure deployment.

Reference:

<https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/get-started/>

Correct Answer:

### Answer Area

Statements	Yes	No
Applying system updates increases an organization's secure score in Microsoft Defender for Cloud	<input checked="" type="radio"/>	<input type="radio"/>
The secure score in Microsoft Defender for Cloud can evaluate resources across multiple Azure subscriptions	<input checked="" type="radio"/>	<input type="radio"/>
Enabling multi-factor authentication (MFA) increases an organization's secure score in Microsoft Defender for Cloud	<input checked="" type="radio"/>	<input type="radio"/>

Box 1: Yes -

System updates reduces security vulnerabilities, and provide a more stable environment for end users. Not applying updates leaves unpatched vulnerabilities and results in environments that are susceptible to attacks.

Box 2: Yes -

Box 3: Yes -

If you only use a password to authenticate a user, it leaves an attack vector open. With MFA enabled, your accounts are more secure.

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/secure-score-security-controls>

### Question #7

Which score measures an organization's progress in completing actions that help reduce risks associated to data protection and regulatory standards?

- A. Microsoft Secure Score
- B. Productivity Score
- C. Secure score in Azure Security Center
- D. Compliance score **Most Voted**

### Question #9


Topic 1

Which Microsoft portal provides information about how Microsoft cloud services comply with regulatory standard, such as International Organization for Standardization (ISO)?

- A. the Microsoft Endpoint Manager admin center
- B. Azure Cost Management + Billing
- C. Microsoft Service Trust Portal **Most Voted**
- D. the Azure Active Directory admin center

Hide Solution

Discussion 24

**Correct Answer:** C 

The Microsoft Service Trust Portal contains details about Microsoft's implementation of controls and processes that protect our cloud services and the customer data therein.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-service-trust-portal?view=o365-worldwide>

Community vote distribution

C (100%)

Correct Answer:

### Answer Area

▼
Archiving
Compressing
Deduplicating
Encrypting

a file makes the data in the file readable and usable to viewers that have the appropriate key.

Correct Answer:

### Answer Area

Statements	Yes	No
Digitally signing a document requires a private key.	<input checked="" type="radio"/>	<input type="radio"/>
Verifying the authenticity of a digitally signed document requires the public key of the signer.	<input checked="" type="radio"/>	<input type="radio"/>
Verifying the authenticity of a digitally signed document requires the private key of the signer.	<input checked="" type="radio"/>	<input type="radio"/>

Box 1: Yes -

A certificate is required that provides a private and a public key.

Box 2: Yes -

The public key is used to validate the private key that is associated with a digital signature.

Box 3: Yes -

The private key, or rather the password to the private key, validates the identity of the signer.

Reference:

<https://support.microsoft.com/en-us/office/obtain-a-digital-certificate-and-create-a-digital-signature-e3d9d813-3305-4164-a820-2e063d86e512>

<https://docs.microsoft.com/en-us/dynamics365/fin-ops-core/fin-ops/organization-administration/electronic-signature-overview>

### Answer Area

Correct Answer:

When users sign in to the Azure portal, they are first

assigned permissions.  
authenticated.  
authorized.  
resolved.

Correct Answer:

### Answer Area

is the process of identifying whether a signed-in user can access a specific resource.

Authentication  
Authorization  
Federation  
Single sign-on (SSO)

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/overview-authentication-authorization>

Correct Answer:

### Answer Area

#### Statements

Yes

No

Azure AD Connect can be used to implement hybrid identity.

☒☐

Hybrid identity requires the implementation of two Microsoft 365 tenants.

☐☒

Authentication of hybrid identifies requires the synchronization of Active Directory Domain Services (AD DS) and Azure Active Directory (Azure AD).

☒☐

Correct Answer:

Statements	Yes	No
Enabling multi-factor authentication (MFA) increases the Microsoft Secure Score.	<input checked="" type="radio"/>	<input type="radio"/>
A higher Microsoft Secure Score means a lower identified risk level in the Microsoft 365 tenant.	<input checked="" type="radio"/>	<input type="radio"/>
Microsoft Secure Score measures progress in completing actions based on controls that include key regulations and standards for data protection and governance.	<input checked="" type="radio"/>	<input type="radio"/>

Box 1: Yes -

Microsoft Secure Score has updated improvement actions to support security defaults in Azure Active Directory, which make it easier to help protect your organization with pre-configured security settings for common attacks.

If you turn on security defaults, you'll be awarded full points for the following improvement actions:

Ensure all users can complete multi-factor authentication for secure access (9 points)

Require MFA for administrative roles (10 points)

Enable policy to block legacy authentication (7 points)

Box 2: Yes -

Each improvement action is worth 10 points or less, and most are scored in a binary fashion. If you implement the improvement action, like create a new policy or turn on a specific setting, you get 100% of the points. For other improvement actions, points are given as a percentage of the total configuration.

Note: Following the Secure Score recommendations can protect your organization from threats. From a centralized dashboard in the Microsoft 365 Defender portal, organizations can monitor and work on the security of their Microsoft 365 identities, apps, and devices.

Box 3: Yes -

Microsoft Secure Score is a measurement of an organization's security posture, with a higher number indicating more improvement actions taken.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score>



### Question #28

What can you use to provide a user with a two-hour window to complete an administrative task in Azure?

- A. Azure Active Directory (Azure AD) Privileged Identity Management (PIM) **Most Voted**
- B. Azure Multi-Factor Authentication (MFA)
- C. Azure Active Directory (Azure AD) Identity Protection
- D. conditional access policies

### Question #29

In a hybrid identity model, what can you use to sync identities between Active Directory Domain Services (AD DS) and Azure Active Directory (Azure AD)?

- A. Active Directory Federation Services (AD FS)
- B. Microsoft Sentinel
- C. Azure AD Connect **Most Voted**
- D. Azure AD Privileged Identity Management (PIM)

### Correct Answer:

#### Answer Area

With Windows Hello for Business, a user's biometric data used for authentication

- is stored on an external device.
- is stored on a local device only.
- is stored in Azure Active Directory (Azure AD).
- is replicated to all the devices designated by the user.

Biometrics templates are stored locally on a device.

Reference:

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

Which Azure Active Directory (Azure AD) feature can you use to evaluate group membership and automatically remove users that no longer require membership in a group?

- A. access reviews **Most Voted**
- B. managed identities
- C. conditional access policies
- D. Azure AD Identity Protection

### Answer Area

**Correct Answer:**

Statements	Yes	No
Conditional access policies can use the device state as a signal.	<input checked="" type="radio"/>	<input type="radio"/>
Conditional access policies apply before first-factor authentication is complete.	<input type="radio"/>	<input checked="" type="radio"/>
Conditional access policies can trigger multi-factor authentication (MFA) if a user attempts to access a specific application.	<input checked="" type="radio"/>	<input type="radio"/>

Box 1: Yes -

Box 2: No -

Conditional Access policies are enforced after first-factor authentication is completed.

Box 3: Yes -

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview>



Correct Answer:

### Answer Area

▼

Microsoft Defender for Cloud Apps
Microsoft Defender for Endpoint
Microsoft Defender for Identity
Microsoft Defender for Office 365

is a cloud-based solution that leverages on-premises Active Directory signals to identify, detect, and investigate advanced threats.

Reference:

<https://docs.microsoft.com/en-us/defender-for-identity/what-is>

#### Question #40

Which Azure Active Directory (Azure AD) feature can you use to provide just-in-time (JIT) access to manage Azure resources?

- A. conditional access policies
- B. Azure AD Identity Protection
- C. Azure AD Privileged Identity Management (PIM) **Most Voted**
- D. authentication method policies

#### Question #41

Which three authentication methods can be used by Azure Multi-Factor Authentication (MFA)? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. text message (SMS) **Most Voted**
- B. Microsoft Authenticator app **Most Voted**
- C. email verification
- D. phone call **Most Voted**
- E. security question

Which Microsoft 365 feature can you use to restrict communication and the sharing of information between members of two departments at your organization?

- A. sensitivity label policies
- B. Customer Lockbox
- C. information barriers **Most Voted**
- D. Privileged Access Management (PAM)

Correct Answer:

### Answer Area



Statements	Yes	No
Conditional access policies can be applied to global administrators.	<input checked="" type="radio"/>	<input type="radio"/>
Conditional access policies are evaluated before a user is authenticated.	<input type="radio"/>	<input checked="" type="radio"/>
Conditional access policies can use a device platform, such as Android or iOS, as a signal.	<input checked="" type="radio"/>	<input type="radio"/>

Box 1: Yes -

Conditional access policies can be applied to all users

Box 2: No -

Conditional access policies are applied after first-factor authentication is completed.

Box 3: Yes -

Users with devices of specific platforms or marked with a specific state can be used when enforcing Conditional Access policies.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview>

### Question #48

You have an Azure subscription.

You need to implement approval-based, time-bound role activation.

What should you use?

- A. Windows Hello for Business
- B. Azure Active Directory (Azure AD) Identity Protection
- C. access reviews in Azure Active Directory (Azure AD)
- D. Azure Active Directory (Azure AD) Privileged Identity Management (PIM) **Most Voted**

### Answer Area

Correct Answer:

Statements	Yes	No
Global administrators are exempt from conditional access policies	<input type="radio"/>	<input checked="" type="radio"/>
A conditional access policy can add users to Azure Active Directory (Azure AD) roles	<input type="radio"/>	<input checked="" type="radio"/>
Conditional access policies can force the use of multi-factor authentication (MFA) to access cloud apps	<input checked="" type="radio"/>	<input type="radio"/>

Reference:

Correct Answer:

### Answer Area

When using multi-factor authentication (MFA), a password is considered something you

are

have

know

share

Correct Answer:

### Answer Area

You can use

classifications

incidents

policies

Secure score

in the Microsoft 365 Defender portal to identify devices that are affected by an alert.

Correct Answer:

### Answer Area

You can use

Reports

Hunting

Attack simulator

Incidents

in the Microsoft 365 security center to view an aggregation of alerts that relate to the same attack.

### Answer Area

#### Statements

Yes

No

Correct Answer:

Network security groups (NSGs) can deny inbound traffic from the internet.

☒☐

Network security groups (NSGs) can deny outbound traffic to the internet.

☒☐

Network security groups (NSGs) can filter traffic based on IP address, protocol, and port.

☒☐

You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview>

Correct Answer:

### Answer Area

In Microsoft Sentinel, you can automate common tasks by using

deep investigation tools.

hunting search-and-query tools.

playbooks.

workbooks.

Correct Answer:

### Answer Area

Statements	Yes	No
Microsoft Defender for Endpoint can protect Android devices.	<input checked="" type="radio"/>	<input type="radio"/>
Microsoft Defender for Endpoint can protect Azure virtual machines that run Windows 10.	<input checked="" type="radio"/>	<input type="radio"/>
Microsoft Defender for Endpoint can protect Microsoft SharePoint Online sites and content from viruses.	<input type="radio"/>	<input checked="" type="radio"/>

### Question #72

Topic 1

What can you use to provide threat detection for Azure SQL Managed Instance?

- A. Microsoft Secure Score
- B. application security groups
- C. Microsoft Defender for Cloud **Most Voted**
- D. Azure Bastion



### Question #77

What should you use in the Microsoft 365 Defender portal to view security trends and track the protection status of identities?

A. Attack simulator

B. Reports **Most Voted**

C. Hunting

D. Incidents

[Hide Solution](#)

[Discussion](#) 4

### Question #79

To which type of resource can Azure Bastion provide secure access?

A. Azure Files

B. Azure SQL Managed Instances

C. Azure virtual machines **Most Voted**

D. Azure App Service

### Question #88

What can you use to deploy Azure resources across multiple subscriptions in a consistent manner?

A. Microsoft Defender for Cloud

B. Azure Blueprints **Most Voted**

C. Microsoft Sentinel

D. Azure Policy

#### Answer Area

Correct Answer:

Azure Active Directory (Azure AD) Identity Protection can add users to groups based on the users' risk level.

Azure Active Directory (Azure AD) Identity Protection can detect whether user credentials were leaked to the public.

Azure Active Directory (Azure AD) Identity Protection can be used to invoke Multi-Factor Authentication based on a user's risk level.

#### Statements

Yes

No

☐☒☒☐☒☐

Box 1: No -

Box 2: Yes -

Leaked Credentials indicates that the user's valid credentials have been leaked.

Box 3: Yes -

Multi-Factor Authentication can be required based on conditions, one of which is user risk.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection> <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks> <https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa>

## Question #91

Which Microsoft 365 compliance center feature can you use to identify all the documents on a Microsoft SharePoint Online site that contain a specific key word?

A. Audit

B. Compliance Manager

C. Content Search **Most Voted**


D. Alerts

Hide Solution



Discussion

9

**Correct Answer:** C 

The Content Search tool in the Security & Compliance Center can be used to quickly find email in Exchange mailboxes, documents in SharePoint sites and OneDrive locations, and instant messaging conversations in Skype for Business.

The first step is to starting using the Content Search tool to choose content locations to search and configure a keyword query to search for specific items.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/search-for-content?view=o365-worldwide>

Correct Answer:

### Answer Area

	▼
Azure Defender	
The Microsoft 365 compliance center	
The Microsoft Defender portal	
Microsoft Endpoint Manager	

provides a central location for managing information protection, information governance, and data loss prevention (DLP) policies.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/microsoft-365-compliance-center?view=o365-worldwide>