

# DUMPS ARENA

## Microsoft 365 Administrator Exam

Microsoft MS-102

Version Demo

Total Demo Questions: 15

Total Premium Questions: 357

Buy Premium PDF

<https://dumpsarena.co>

[sales@dumpsarena.co](mailto:sales@dumpsarena.co)

[sales@dumpsarena.co](mailto:sales@dumpsarena.co)  
[dumpsarena.co](https://dumpsarena.co)

**QUESTION NO: 1**

What is the maximum retention period for deleted Microsoft 365 tenant users?

- A. 30 days
- B. 60 days
- C. 120 days
- D. 90 days

**ANSWER: D**

**Explanation:**

The maximum retention period for deleted Microsoft 365 tenant users is 90 days.

**QUESTION NO: 2**

What is the purpose of Azure AD Connect?

- A. To implement network security
- B. To manage virtual machines
- C. To synchronize on-premises identities to Azure AD
- D. To manage Azure resources

**ANSWER: C**

**Explanation:**

Azure AD Connect is used to synchronize on-premises identities to Azure AD.

**QUESTION NO: 3**

Which of the following is a benefit of using Azure AD for identity and access management?

- A. All of the above
- B. Self-service password reset for end-users
- C. Automated password expiration and reset

D. Centralized identity management and synchronization

**ANSWER: A**

**Explanation:**

Azure AD provides centralized identity management and synchronization, automated password expiration and reset, and self-service password reset for end-users.

**QUESTION NO: 4**

What is an incident in Microsoft Defender for Endpoint?

- A. A user error
- B. A hardware failure in an endpoint
- C. A security event that could compromise the confidentiality, integrity, or availability of data or systems
- D. A software malfunction on an endpoint

**ANSWER: C**

**Explanation:**

An incident in Microsoft Defender for Endpoint is a security event that could compromise the confidentiality, integrity, or availability of data or systems.

**QUESTION NO: 5**

What is the purpose of Microsoft Defender for Endpoint?

- A. Identity and access management
- B. Endpoint protection
- C. Email protection
- D. Network protection

**ANSWER: B**

**Explanation:**

Microsoft Defender for Endpoint provides next-generation antivirus, EDR, and advanced attack surface reduction capabilities for endpoint protection.

**QUESTION NO: 6**

What is the maximum number of users that can be added to a single Microsoft 365 group?

- A. 250 users
- B. 50 users
- C. 100 users
- D. 500 users

**ANSWER: A****Explanation:**

A single Microsoft 365 group can have a maximum of 250 users.

**QUESTION NO: 7**

What is the name of the group that defines the policies for data sources in Microsoft Purview?

- A. Data source group
- B. Data policy group
- C. Data classification group
- D. Data governance group

**ANSWER: D****Explanation:**

The data governance group is responsible for defining policies for data sources in Microsoft Purview.

**QUESTION NO: 8**

What is the maximum number of devices a single user can install Microsoft 365 Apps for enterprise on?

- A. 5
- B. 1
- C. Unlimited
- D. 10

**ANSWER: A****Explanation:**

Each user can install Microsoft 365 Apps for enterprise on up to five devices.

**QUESTION NO: 9**

What is Azure AD tenant?

- A. A container for an organization's users, groups, applications, and devices
- B. An authentication mechanism that uses multi-factor authentication
- C. A tool that enables IT administrators to manage user accounts and groups
- D. A feature that allows IT administrators to manage access to resources at a granular level

**ANSWER: A****Explanation:**

An Azure AD tenant is a container for an organization's users, groups, applications, and devices.

**QUESTION NO: 10**

What is the maximum number of users allowed in a Microsoft 365 Business Basic plan?

- A. 10,000
- B. 1000
- C. 500
- D. 300

**ANSWER: D****Explanation:**

The Microsoft 365 Business Basic plan is limited to 300 users.

**QUESTION NO: 11**

Which feature in Microsoft Defender for Office 365 provides protection against advanced email threats such as phishing?

- A. Safe Links
- B. Exchange Online Protection

C. Advanced Threat Protection

D. Safe Attachments

**ANSWER: C**

**Explanation:**

Advanced Threat Protection in Microsoft Defender for Office 365 provides protection against advanced email threats such as phishing, malware, and spear-phishing.

**QUESTION NO: 12**

Which of the following best describes role-based access control (RBAC) in Azure?

A. Identity-based management of directory services

B. Policy-based management of access rights

C. Group-based management of server clusters

D. Resource-based management of cloud services

**ANSWER: B**

**Explanation:**

Azure uses policy-based management of access rights via its role-based access control (RBAC) system, which lets you define roles with specific permissions.

**QUESTION NO: 13**

What is the difference between Azure AD B2C and Azure AD B2B?

A. Azure AD B2C and Azure AD B2B are the same thing.

B. Azure AD B2C is used for authenticating internal users while Azure AD B2B is used for authenticating external users.

C. Azure AD B2C is used for authenticating customers while Azure AD B2B is used for authenticating partners.

D. Azure AD B2C is used for authenticating external users while Azure AD B2B is used for authenticating internal users.

**ANSWER: D**

**Explanation:**

Azure AD B2C is used for authenticating external users while Azure AD B2B is used for authenticating internal users.

**QUESTION NO: 14**

What is a Threat Intelligence?

- A. It's information that helps organizations identify and prevent security threats.
- B. It's a feature of Microsoft Defender ATP that scans email attachments for malware.
- C. It's a machine-learning algorithm that detects suspicious behavior.
- D. It's a type of virus that targets Microsoft 365 services.

**ANSWER: A**

**Explanation:**

Threat Intelligence is a type of information that helps organizations identify and prevent potential security threats, by providing context and insights to security events.

**QUESTION NO: 15**

What is the primary benefit of integrating existing apps with Microsoft 365 services?

- A. Streamlined workflows
- B. Lower development costs
- C. Improved scalability
- D. Enhanced user interface

**ANSWER: A**

**Explanation:**

Integrating existing apps with Microsoft 365 services can improve workflows and streamline processes.