SC-300^Q&As

Microsoft Identity and Access Administrator

Pass Microsoft SC-300 Exam with 100% Guarantee

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

QUESTION 1

You have an Azure AD tenant that contains two users named User1 and User2. You plan to perform the following actions:

1.

Create a group named Group1.

2.

Add User1 and User2 to Group1.

3.

Assign Azure AD roles to Group1.

You need to create Group1.

Which two settings can you use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Group type: Microsoft 365 - Membership type: Assigned

B. Group type: Security - Membership type: Assigned

C. Group type: Security - Membership type: Dynamic User

D. Group type: Microsoft 365 - Membership type: Dynamic User

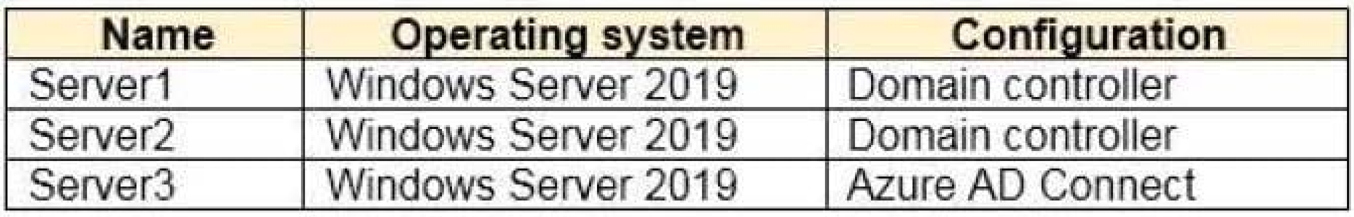
E. Group type: Security - Membership type: Dynamic Device

Correct Answer: AB

QUESTION 2

You have a Microsoft 365 tenant.

The Azure Active Directory (Azure AD) tenant syncs to an on-premises Active Directory domain. The domain contains the servers shown in the following table.



Name	Operating system	Configuration
Server1	Windows Server 2019	Domain controller
Server2	Windows Server 2019	Domain controller
Server3	Windows Server 2019	Azure AD Connect

The domain controllers are prevented from communicating to the internet.

You implement Azure AD Password Protection on Server1 and Server2.

You deploy a new server named Server4 that runs Windows Server 2019.

You need to ensure that Azure AD Password Protection will continue to work if a single server fails.

What should you implement on Server4?

A. Azure AD Connect

B. Azure AD Application Proxy

C. Password Change Notification Service (PCNS)

D. the Azure AD Password Protection proxy service

Correct Answer: D

Reference: https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premisesdeploy

QUESTION 3

Your company has a Microsoft 365 tenant.

The company has a call center that contains 300 users. In the call center, the users share desktop computers and might use a different computer every day. The call center computers are NOT configured for biometric identification.

The users are prohibited from having a mobile phone in the call center.

You need to require multi-factor authentication (MFA) for the call center users when they access Microsoft 365 services.

What should you include in the solution?

A. a named network location

B. the Microsoft Authenticator app

C. Windows Hello for Business authentication

D. FIDO2 tokens

Correct Answer: D

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless

QUESTION 4

You have a Microsoft 365 E5 subscription.

You create a user named User1.

You need to ensure that User1 can update the status of Identity Secure Score improvement actions.

Solution: You assign the User Administrator role to User1.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

QUESTION 5

You have a Microsoft 365 tenant.

All users must use the Microsoft Authenticator app for multi-factor authentication (MFA) when accessing Microsoft 365 services.

Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a sign-in request.

You need to block the users automatically when they report an MFA request that they did not Initiate.

Solution: From the Azure portal, you configure the Fraud alert settings for multi-factor authentication (MFA).

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

The fraud alert feature lets users report fraudulent attempts to access their resources. When an unknown and suspicious MFA prompt is received, users can report the fraud attempt using the Microsoft Authenticator app or through their phone.

The following fraud alert configuration options are available:

1.

Automatically block users who report fraud.

2.

Code to report fraud during initial greeting.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings