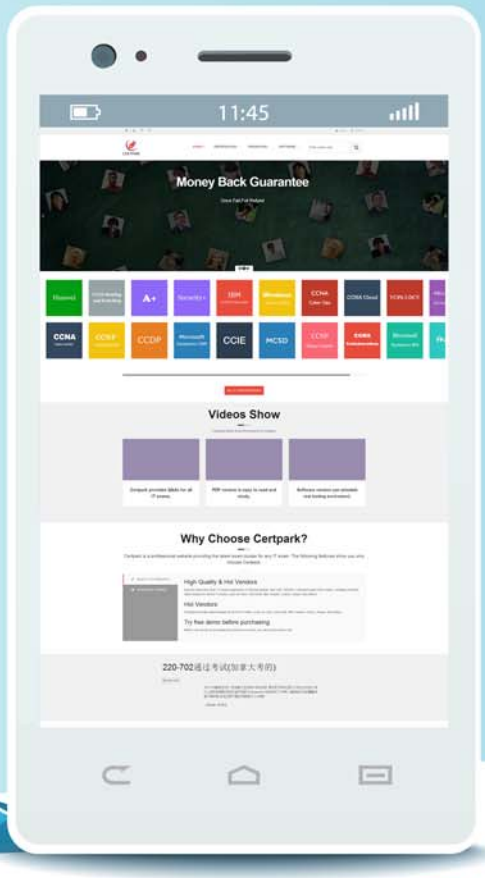
CERTPARK

QUESTION & ANSWER

CERTPARK.COM

Accurate Study Guides,
High Passing Rate!
provides update
free of charge
in one year!



https://www.certpark.com

Exam : **MS-100**

Title : Microsoft 365 Identity and Services

Version : DEMO

1. Topic 1, Contoso, Ltd

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answer and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview
Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The offices have the users and devices shown in the following table.

Office	Users	Laptops	Desktops	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso recently purchased a Microsoft 365 E5 subscription.

Existing Environment
The network contains an Active directory forest named contoso.com and a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.
You recently configured the forest to sync to the Azure AD tenant.
You add and then verify adatum.com as an additional domain name.
All servers run Windows Server 2016.
All desktop computers and laptops run Windows 10 Enterprise and are joined to contoso.com.
All the mobile devices in the Montreal and Seattle offices run Android. All the mobile devices in the New York office run iOS.

Contoso has the users shown in the following table.

Name	Role
User1	*None*
User2	*None*
User3	Customer Lockbox access approver
User4	*None*

Contoso has the groups shown in the following table.

Name	Type	Membership rule
Group1	Assigned	*Not applicable*
Group 2	Dynamic	(user.department –eq "Finance")

Microsoft Office 365 licenses are assigned only to Group2.
The network also contains external users from a vendor company who have Microsoft accounts that use a suffix of @outlook.com.

Requirements
Planned Changes
Contoso plans to provide email addresses for all the users in the following domains:
- East.adatum.com
- Contoso.adatum.com
- Humongousinsurance.com

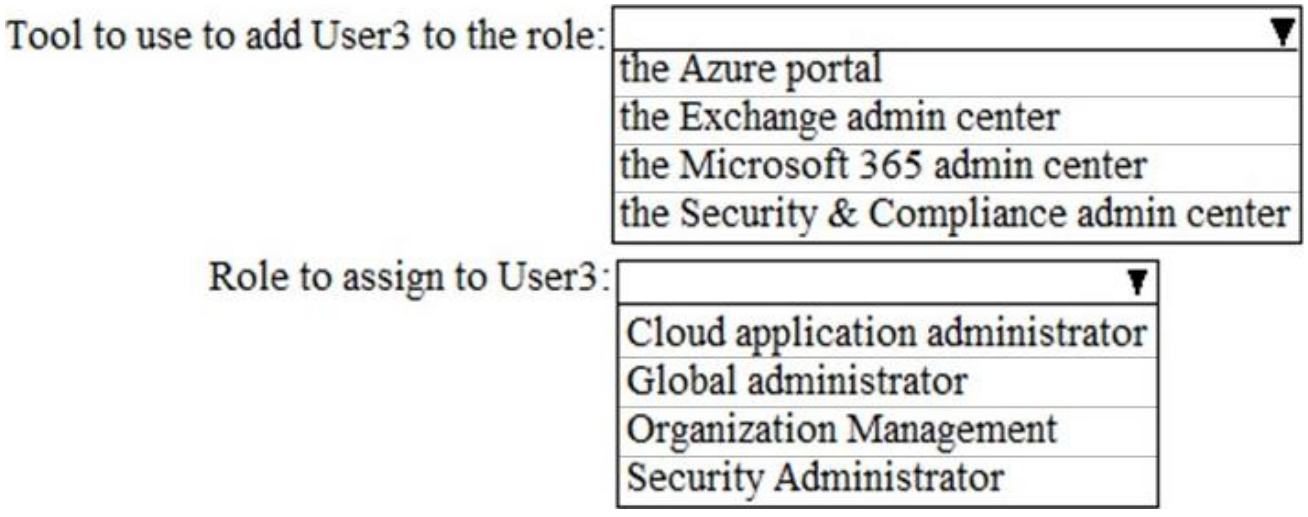
Technical Requirements
Contoso identifies the following technical requirements:
- All new users must be assigned Office 365 licenses automatically.
- The principle of least privilege must be used whenever possible.

Security Requirements
Contoso identifies the following security requirements:
- Vendors must be able to authenticate by using their Microsoft account when accessing Contoso resources.
- User2 must be able to view reports and schedule the email delivery of security and compliance reports.
- The members of Group1 must be required to answer a security question before changing their password.
- User3 must be able to manage Office 365 connectors.
- User4 must be able to reset User3 password.

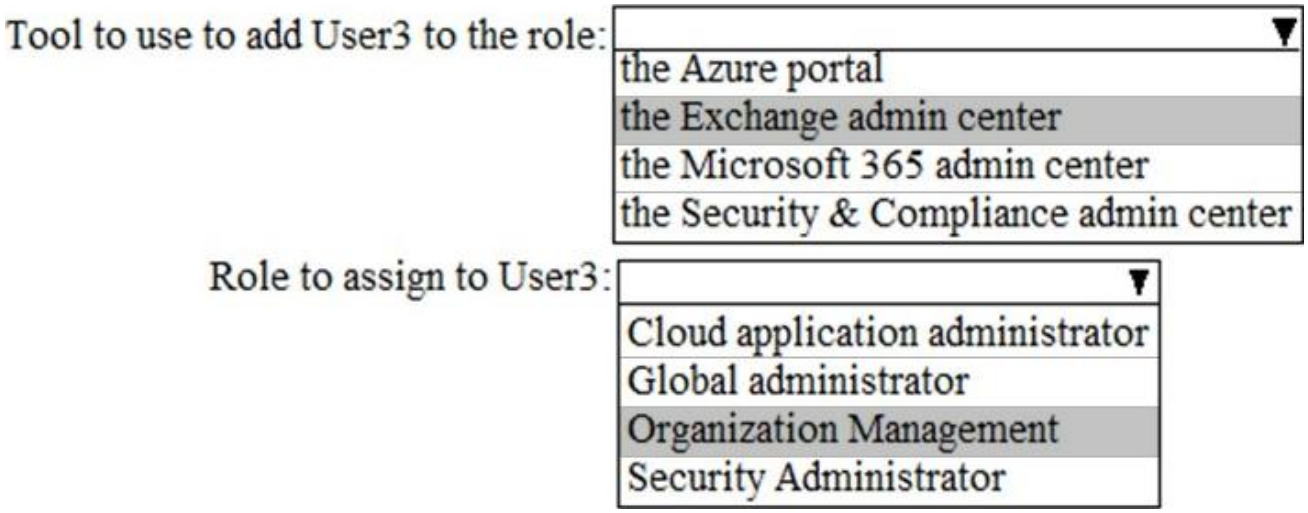
You need to meet the security requirement for Group1.
What should you do?
A. Configure all users to sign in by using multi-factor authentication.

B. Modify the properties of Group1.
C. Assign Group1 a management role.
D. Modify the Password reset properties of the Azure AD tenant.
Answer: D
Explanation:
References: ☞ The members of Group1 must be required to answer a security question before changing their password.
If SSPR (Self Service Password Reset) is enabled, you must select at least one of the following options for the authentication methods. Sometimes you hear these options referred to as "gates."
Mobile app notification
Mobile app code
Email
Mobile phone
Office phone
Security questions
You can specify the required authentication methods in the Password reset properties of the Azure AD tenant. In this case, you should set the required authentication method to be ‘Security questions’.
Reference: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks

2.HOTSPOT
You need to meet the security requirements for User3. The solution must meet the technical requirements.
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer:



Explanation:

☞ User3 must be able to manage Office 365 connectors.

☞ The principle of least privilege must be used whenever possible.

Office 365 connectors are configured in the Exchange Admin Center.

You need to assign User3 the Organization Management role to enable User3 to manage Office 365 connectors.

A Global Admin could manage Office 365 connectors but the Organization Management role has less privilege.

3.You need to meet the security requirement for the vendors.

What should you do?

A. From the Azure portal, add an identity provider.

B. From Azure Cloud Shell, run the New-AzureADUser cmdlet and specify the –UserPrincipalName parameter.

C. From the Azure portal, create guest accounts.

D. From Azure Cloud Shell, run the New-AzureADUser cmdlet and specify the –UserType parameter.

Answer: C

Explanation:

☞ Vendors must be able to authenticate by using their Microsoft account when accessing Contoso resources.

You can invite guest users to the directory, to a group, or to an application. After you invite a user through any of these methods, the invited user's account is added to Azure Active Directory (Azure AD), with a user type of Guest. The guest user must then redeem their invitation to access resources. An invitation of a user does not expire.

The invitation will include a link to create a Microsoft account. The user can then authenticate using their Microsoft account. In this question, the vendors already have Microsoft accounts so they can authenticate using them.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/b2b/add-users-administrator

4.You need to assign User2 the required roles to meet the security requirements and the technical requirements.

To which two roles should you assign User2? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.
A. the Exchange View-only Organization Management role
B. the Microsoft 365 Records Management role
C. the Exchange Online Help Desk role
D. the Microsoft 365 Security Reader role
E. the Exchange Online Compliance Management role
Answer: D,E
Explanation:
☞ User2 must be able to view reports and schedule the email delivery of security and compliance reports.
The Security Reader role can view reports but not schedule the email delivery of security and compliance reports.
The Exchange Online Compliance Management role can schedule the email delivery of security and compliance reports.
Reference: https://docs.microsoft.com/en-us/exchange/permissions-exo/permissions-exo

5.You need to meet the security requirement for the vendors.
What should you do?
A. From the Azure portal, modify the authentication methods.
B. From Azure Cloud Shell, run the New-AzureADMSInvitation and specify the –InvitedIserEmailAddress cmdlet.
C. From Azure Cloud Shell, run the Set-MsolUserPrincipalName and specify the –tenantID parameter.
D. From the Azure portal, add an identity provider.
Answer: B
Explanation:
☞ Vendors must be able to authenticate by using their Microsoft account when accessing Contoso resources.
You can invite guest users to the directory, to a group, or to an application. After you invite a user through any of these methods, the invited user's account is added to Azure Active Directory (Azure AD), with a user type of Guest. The guest user must then redeem their invitation to access resources. An invitation of a user does not expire.
The invitation will include a link to create a Microsoft account. The user can then authenticate using their Microsoft account. In this question, the vendors already have Microsoft accounts so they can authenticate using them.
In this solution, we are creating guest account invitations by using the New-AzureADMSInvitation cmdlet and specifying the –InvitedUserEmailAddress parameter.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/b2b/add-users-administrator
https://docs.microsoft.com/en-us/powershell/module/azuread/new-azureadmsinvitation?view=azureadps-2.0