Vendor: Microsoft

Exam Code: SC-300

Exam Name: Microsoft Identity and Access Administrator

Version: DEMO

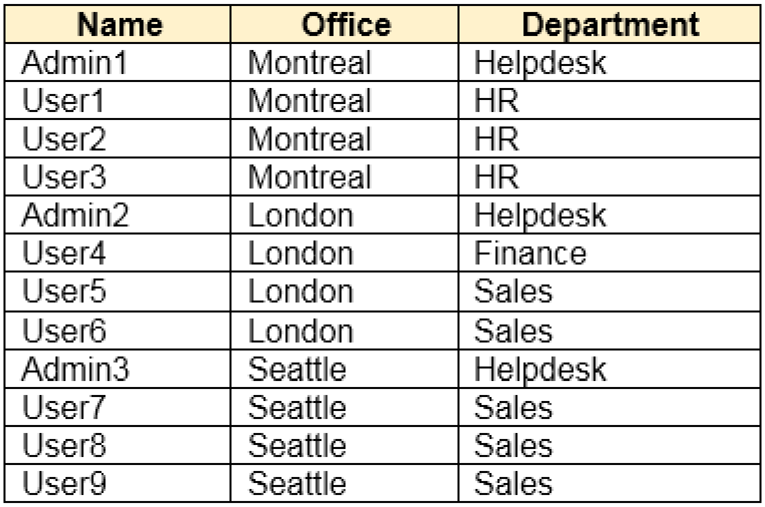
QUESTION 1
Case Study 1 - Contoso, Ltd

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

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment
The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named Contoso_Resources. The Contoso_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the users shown in the following table.



Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Existing Environment. Microsoft 365/Azure Environment
Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

- Microsoft Office 365 Enterprise E5
- Enterprise Mobility + Security
- Windows 10 Enterprise E3
- Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

- The users in the London office have the Microsoft 365 Phone System license unassigned.
- The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

You need to sync the ADatum users. The solution must meet the technical requirements.

What should you do?

A. From the Microsoft Azure Active Directory Connect wizard, select Customize synchronization options.
B. From PowerShell, run Set-ADSyncScheduler.
C. From PowerShell, run Start-ADSyncSyncCycle.
D. From the Microsoft Azure Active Directory Connect wizard, select Change user sign-in.

Answer: A
Explanation:
You need to select Customize synchronization options to configure Azure AD Connect to sync the Adatum organizational unit (OU).

Reference:
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering#filtering-options
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-whatis#azure-ad-connect-sync-topics

QUESTION 2
Case Study 2 - Litware, Inc

Overview
Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identify Environment
The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

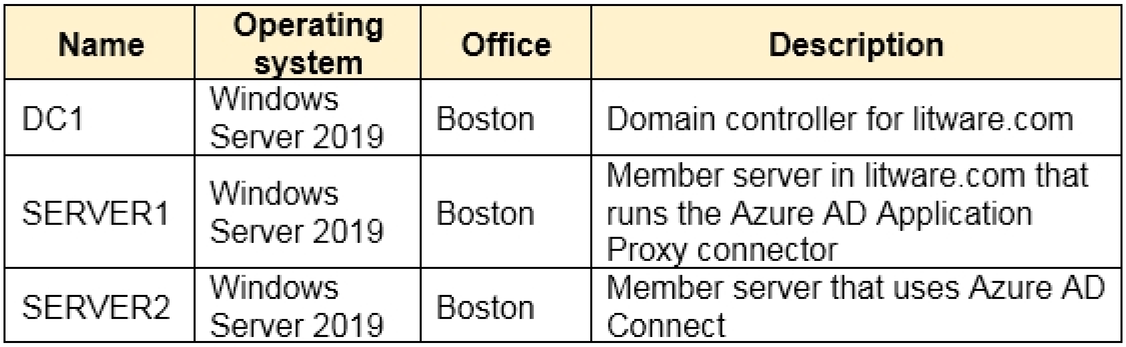
Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment
All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.



Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

You need to meet the authentication requirements for leaked credentials.

What should you do?

A. Enable password hash synchronization in Azure AD Connect.
B. Configure Azure AD Password Protection.
C. Configure an authentication method policy in Azure AD.
D. Enable federation with PingFederate in Azure AD Connect.

Answer: A
Explanation:
Password hash synchronization
Risk detections like leaked credentials require the presence of password hashes for detection to occur. For more information about password hash synchronization, see the article, Implement password hash synchronization with Azure AD Connect sync.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#password-hash-synchronization

QUESTION 3
You have an Azure Active Directory (Azure AD) tenant named contoso.com.

You plan to bulk invite Azure AD business-to-business (B2B) collaboration users.

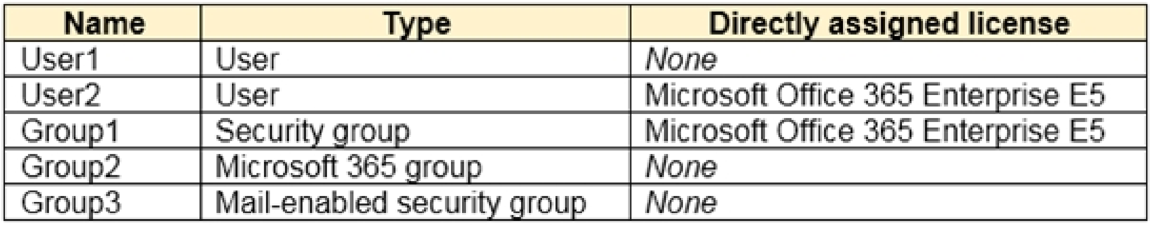
Which two parameters must you include when you create the bulk invite? Each correct answer presents part of the solution

NOTE: Each correct selection is worth one point.

A. email address
B. redirection URL
C. username
D. shared key
E. password

Answer: AB
Explanation:
Required values are:
Email address to invite - the user who will receive an invitation
Redirection url - the URL to which the invited user is forwarded after accepting the invitation. If you want to forward the user to the My Apps page, you must change this value to https://myapps.microsoft.com or https://myapplications.microsoft.com.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/tutorial-bulk-invite#invite-guest-users-in-bulk

QUESTION 4
You have an Azure Active Directory (Azure AD) tenant that contains the objects shown in the following table.



Name	Type	Directly assigned license
User1	User	*None*
User2	User	Microsoft Office 365 Enterprise E5
Group1	Security group	Microsoft Office 365 Enterprise E5
Group2	Microsoft 365 group	*None*
Group3	Mail-enabled security group	*None*

Which objects can you add as members to Group3?

A. User2 and Group2 only
B. User2, Group1, and Group2 only
C. User1, User2, Group1 and Group2
D. User1 and User2 only
E. User2 only

Answer: E
Explanation:
In the M365 admin center, only users can be added to the mail-enabled security group.
You can only add licensed users to the group, unlicensed users won't even show up on the member select page.
Reference:
https://bitsizedbytes.wordpress.com/2018/12/10/distribution-security-and-office-365-groups-nesting/

QUESTION 5
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure Active Directory (Azure AD) tenant that syncs to an Active Directory forest.

You discover that when a user account is disabled in Active Directory, the disabled user can still authenticate to Azure AD for up to 30 minutes.

You need to ensure that when a user account is disabled in Active Directory, the user account is immediately prevented from authenticating to Azure AD.

Solution: You configure pass-through authentication.

Does this meet the goal?

A. Yes
B. No

Answer: A
Explanation:
Azure Active Directory (Azure AD) Pass-through Authentication allows your users to sign in to both on-premises and cloud-based applications by using the same passwords. Pass-through Authentication signs users in by validating their passwords directly against on-premises Active Directory.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

QUESTION 6
You have an Azure Active Directory (Azure AD) tenant that contains a user named SecAdmin1. SecAdmin1 is assigned the Security administrator role.

SecAdmin1 reports that she cannot reset passwords from the Azure AD Identity Protection portal.

You need to ensure that SecAdmin1 can manage passwords and invalidate sessions on behalf of non-administrative users. The solution must use the principle of least privilege.

Which role should you assign to SecAdmin1?

A. Authentication administrator
B. Helpdesk administrator
C. Privileged authentication administrator
D. Security operator

Answer: B
Explanation:
Authentication administrator: can reset passwords for non-admins but can't invalidate sessions.
Helpdesk administrator: Users with this role can change passwords, invalidate refresh tokens, manage service requests, and monitor service health. Invalidating a refresh token forces the user to sign in again.
Privileged Authentication Administrator: can reset all passwords (admins & non-admins) but can't invalidate any sessions.
Security Operator: can't reset any passwords.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#authentication-administrator
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#helpdesk-administrator
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#privileged-authentication-administrator

https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#security-operator

QUESTION 7
You configure a new Microsoft 365 tenant to use a default domain name of contoso.com.

You need to ensure that you can control access to Microsoft 365 resources by using conditional access policies.

What should you do first?

A. Disable the User consent settings.
B. Disable Security defaults.
C. Configure a multi-factor authentication (MFA) registration policy.
D. Configure password protection for Windows Server Active Directory.

Answer: B
Explanation:
If your tenant was created on or after October 22, 2019, it is possible security defaults are already enabled in your tenant. To protect all of our users, security defaults are being rolled out to all new tenants created.
To enable CAP you have to disable Security defaults.
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults

QUESTION 8
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

Answer: D
Explanation:
FIDO2 security device (biometrics, PIN, and NFC)
User can access device based on organization controls and authenticate based on PIN, biometrics using devices such as USB security keys and NFC-enabled smartcards, keys, or wearables.
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless

QUESTION 9
You have an Azure Active Directory (Azure AD) tenant named contoso.com.

All users who run applications registered in Azure AD are subject to conditional access policies.

You need to prevent the users from using legacy authentication.

What should you include in the conditional access policies to filter out legacy authentication attempts?

A. a cloud apps or actions condition
B. a user risk condition
C. a client apps condition
D. a sign-in risk condition

Answer: C
Explanation:
Directly blocking legacy authentication
The easiest way to block legacy authentication across your entire organization is by configuring a Conditional Access policy that applies specifically to legacy authentication clients and blocks access.
Conditional Access policies apply to all client apps by default Client apps.
By default, all newly created Conditional Access policies will apply to all client app types even if the client apps condition is not configured.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication

QUESTION 10
You have an Azure Active Directory (Azure AD) tenant.

You open the risk detections report.

Which risk detection type is classified as a user risk?

A. impossible travel
B. anonymous IP address
C. atypical travel
D. leaked credentials

Answer: D
Explanation:
Leaked credentials indicates that the user's valid credentials have been leaked.
Note:
There are several versions of this question in the exam. The question can have other incorrect answer options, including the following:
- password spray
- malicious IP address
- unfamiliar sign-in properties

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks

QUESTION 11
You have a Microsoft 365 tenant.

All users have computers that run Windows 10. Most computers are company-owned and joined to Azure Active Directory (Azure AD). Some computers are user-owned and are only registered in Azure AD.

You need to prevent users who connect to Microsoft SharePoint Online on their user-owned computer from downloading or syncing files. Other users must NOT be restricted.

Which policy type should you create?

A. a Microsoft Cloud App Security activity policy that has Microsoft Office 365 governance actions configured
B. an Azure AD conditional access policy that has session controls configured
C. an Azure AD conditional access policy that has client apps conditions configured
D. a Microsoft Cloud App Security app discovery policy that has governance actions configured

Answer: B
Explanation:
You need to use "Use app enforced restrictions" from the "Session" control of the CA.
https://docs.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices

QUESTION 12
You have an Azure Active Directory (Azure AD) tenant that syncs to an Active Directory domain.

The on-premises network contains a VPN server that authenticates to the on-premises Active Directory domain. The VPN server does NOT support Azure Multi-Factor Authentication (MFA).

You need to recommend a solution to provide Azure MFA for VPN connections.

What should you include in the recommendation?

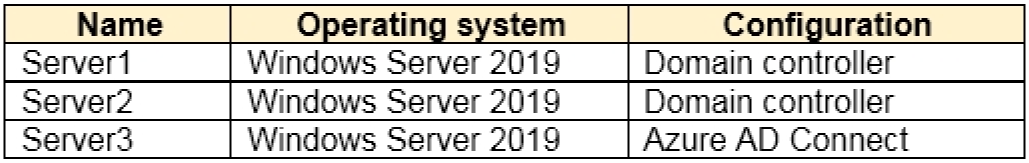
A. Azure AD Application Proxy
B. an Azure AD Password Protection proxy
C. Network Policy Server (NPS)
D. a pass-through authentication proxy

Explanation:
NPS (Network Policy and Access Service) is like a middle man between the VPN client and Azure MFA. The NPS role is installed on a domain-joined server or the domain controller and is configured to authenticate and authorize RADIUS requests from the VPN client.
The VPN should be configured to use RADIUS authentication and point to the NPS server.
The MFA NPS extension is installed anywhere but the VPN server. When a user/VPN client attempts to authenticate, it sends a RADIUS request to the NPS server through the VPN which performs the primary authentication and then triggers the NPS Extension for secondary authentication.

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-nps-extension-vpn

QUESTION 13
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

Answer: D
Explanation:
The AzureAD Password Protection proxy service initiates an outbound connection (Port 443) to Azure to pull the banned password list.
The downloaded banned password list is pulled by the agent installed on DCs.
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy

QUESTION 14
You have an Azure Active Directory (Azure AD) tenant.

You create an enterprise application collection named HR Apps that has the following settings:

```
- Applications: App1, App2, App3
- Owners: Admin1
- Users and groups: HRUsers
```

All three apps have the following Properties settings:

```
- Enabled for users to sign in: Yes
- User assignment required: Yes
- Visible to users: Yes
```

Users report that when they go to the My Apps portal, they only see App1 and App2.

You need to ensure that the users can also see App3.

What should you do from App3?

A. From Users and groups, add HRUsers.
B. From Single sign-on, configure a sign-on method.
C. From Properties, change User assignment required to No.
D. From Permissions, review the User consent permissions.

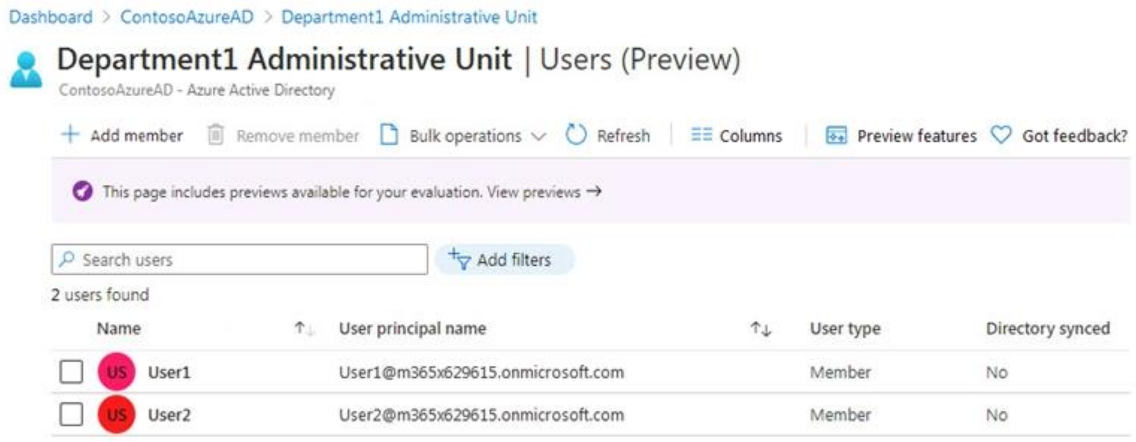
Answer: A
Explanation:
User assignment and Visible to Users goes hand in hand for this.
If Visible to Users is set to Yes then this is the explanation from the 'i' next to it:
If this option is set to yes, then assigned users will see the application on My Apps and O365 app launcher. If this option is set to no, then no users will see this application on their My Apps and O365 launcher. Assigned User is the key here.
Unless the users are assigned to the app, then No one will see the application on their MyApps or O365 Launcher.

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal
https://docs.microsoft.com/en-us/azure/active-directory/user-help/my-applications-portal-workspaces

QUESTION 15
Hotspot Question

You have an Azure Active Directory (Azure AD) tenant that contains an administrative unit named Department1.

Department1 has the users shown in the Users exhibit. (Click the Users tab.)


Dashboard > ContosoAzureAD > Department1 Administrative Unit

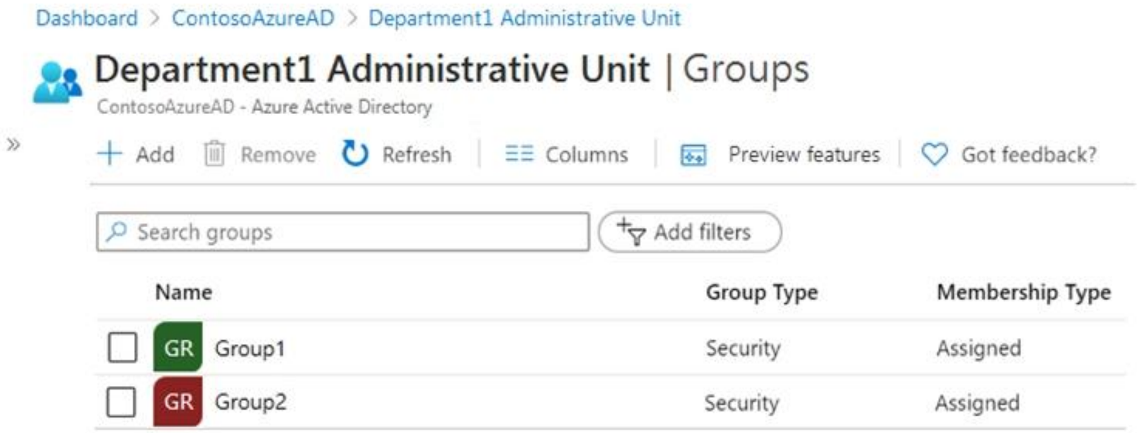
Department1 Administrative Unit | Users (Preview)
ContosoAzureAD - Azure Active Directory

This page includes previews available for your evaluation. View previews →

2 users found

	Name	User principal name	User type	Directory synced
□	US User1	User1@m365x629615.onmicrosoft.com	Member	No
□	US User2	User2@m365x629615.onmicrosoft.com	Member	No

Department1 has the groups shown in the Groups exhibit. (Click the Groups tab.)

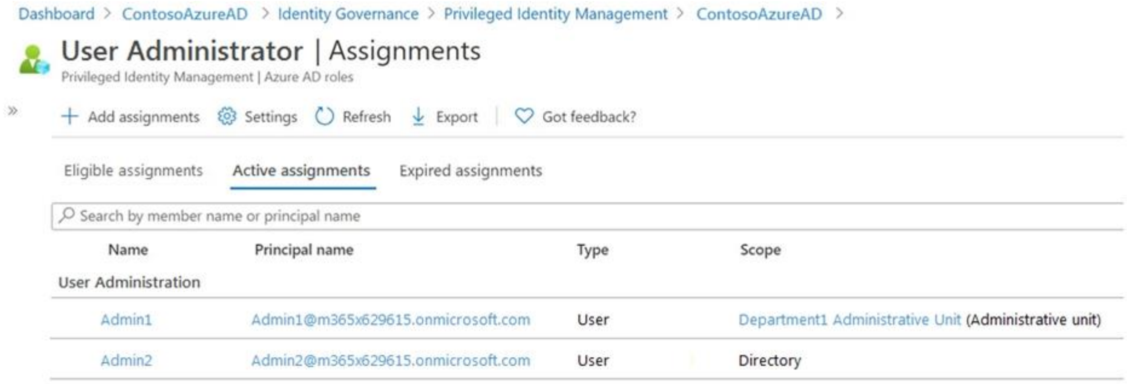


Department1 Administrative Unit | Groups

ContosoAzureAD - Azure Active Directory

	Name	Group Type	Membership Type
□	GR Group1	Security	Assigned
□	GR Group2	Security	Assigned

Department1 has the user administrator assignments shown in the Assignments exhibit. (Click the Assignments tab.)

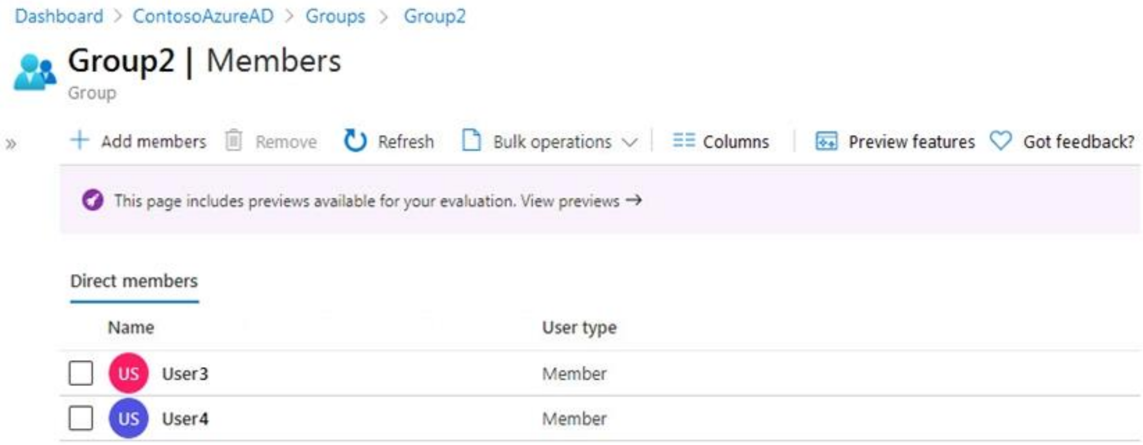

Dashboard > ContosoAzureAD > Identity Governance > Privileged Identity Management > ContosoAzureAD >
+ Add assignments
Settings
Refresh
Export
Got feedback?
Eligible assignments
Active assignments
Expired assignments
Search by member name or principal name

User Administrator | Assignments

Privileged Identity Management | Azure AD roles

Name	Principal name	Type	Scope
User Administration			
Admin1	Admin1@m365x629615.onmicrosoft.com	User	Department1 Administrative Unit (Administrative unit)
Admin2	Admin2@m365x629615.onmicrosoft.com	User	Directory

The members of Group2 are shown in the Group2 exhibit. (Click the Group2 tab.)



Group2 | Members

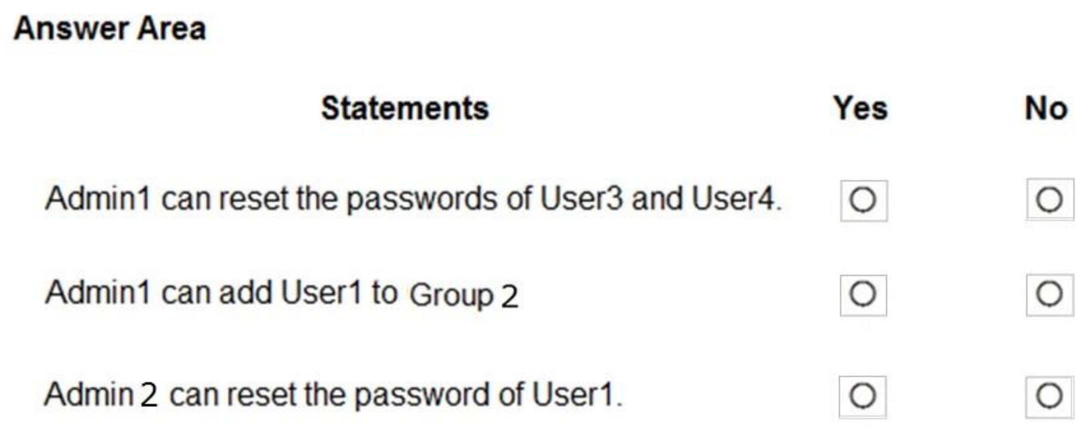
Group

This page includes previews available for your evaluation. View previews →

	Name	User type
□	US User3	Member
□	US User4	Member

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

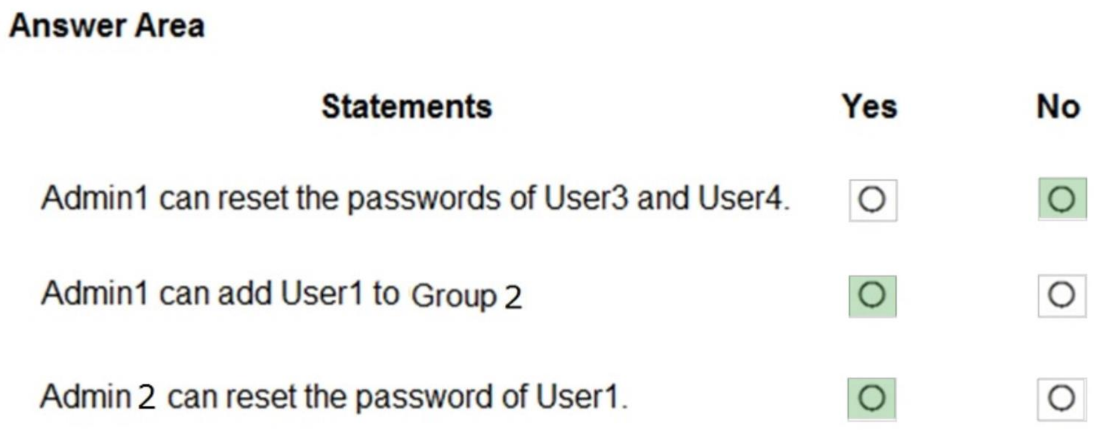
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
Admin1 can reset the passwords of User3 and User4.	○	○
Admin1 can add User1 to Group 2	○	○
Admin 2 can reset the password of User1.	○	○

Answer:



Answer Area

Statements	Yes	No
Admin1 can reset the passwords of User3 and User4.	○	[✓ ○]
Admin1 can add User1 to Group 2	[✓ ○]	○
Admin 2 can reset the password of User1.	[✓ ○]	○

Explanation:
Admin1 and Admin2 are not members of Administrative group(Department1). However Admin1 has User administrator role scope for Department1 and Admin2 has User administrator role scope for the whole directory
User 1 And User 2 are users of Department1
Group1(No members) and Group2(User 3 and User4 are members) are groups of Department1.

Box 1: No
Admin1 cannot reset the password for User 3 and User4 because they are part of group2.(User admin role assigned to admin unit cannot reset password of users present inside the group. Admin1 can reset the password of User1 and User2 who are not part of any groups inside the admin unit)

Box 2: Yes
Admin1 can add/remove users to the GROUPS present inside the admin unit (Admin1 cannot add/remove users from USERS section)

Box 3: Yes
Admin2 is User admin at directory scope ,hence can reset password of any uses except the password of global admin/higher power roles

QUESTION 16

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Active Directory forest that syncs to an Azure Active Directory (Azure AD) tenant.

You discover that when a user account is disabled in Active Directory, the disabled user can still authenticate to Azure AD for up to 30 minutes.

You need to ensure that when a user account is disabled in Active Directory, the user account is immediately prevented from authenticating to Azure AD.

Solution: You configure Azure AD Password Protection.

Does this meet the goal?

A. Yes
B. No

Answer: B
Explanation:
Azure AD Password Protection
With this feature, you can use the same checks for passwords in AzureAD on your on-premises Active Directory implementation.
You can enforce both the Microsoft Global Banned Passwords and Custom banned-passwords list stored in Azure AD tenant.
The DC agent software must be installed on all DCs in a domain.

QUESTION 17
You have an Azure Active Directory (Azure AD) tenant.
For the tenant, Users can register applications is set to No.
A user named Admin1 must deploy a new cloud app named App1.
You need to ensure that Admin1 can register App1 in Azure AD. The solution must use the principle of least privilege.

Which role should you assign to Admin1?

A. Managed Application Contributor for Subscription1.
B. Application developer in Azure AD.
C. Cloud application administrator in Azure AD.
D. App Configuration Data Owner for Subscription1.

Answer: B
Explanation:
Application Developer can create application registrations independent of the 'Users can register applications' setting.
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

QUESTION 18
You have an Azure Active Directory (Azure AD) tenant named contoso.com that has Azure AD Identity Protection enabled.
You need to implement a sign-in risk remediation policy without blocking user access.
What should you do first?

A. Configure access reviews in Azure AD.
B. Enforce Azure AD Password Protection.
C. Configure self-service password reset (SSPR) for all users.
D. Implement multi-factor authentication (MFA) for all users.

Answer: D
Explanation:
To implement a sign-in risk remediation policy.
When a sign in risk policy triggers:
Azure AD MFA can be triggered, allowing to user to prove it's them by using one of their registered authentication methods, resetting the sign in risk.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies

QUESTION 19
You create a conditional access policy that blocks access when a user triggers a high-severity sign-in alert.
You need to test the policy under the following conditions:

```
- A user signs in from another country.
- A user triggers a sign-in risk.
```

What should you use to complete the test?

A. the Conditional Access What If tool
B. sign-ins logs in Azure Active Directory (Azure AD)
C. the activity logs in Microsoft Defender for Cloud Apps
D. access reviews in Azure Active Directory (Azure AD)

Answer: A
Explanation:
The Azure AD conditional access What if tool allows you to understand the impact of your conditional access policies on your environment. Instead of test driving your policies by performing multiple sign-ins manually, this tool enables you to evaluate a simulated sign-in of a user. The simulation estimates the impact this sign-in has on your policies and generates a simulation report. The report does not only list the applied conditional access policies but also classic policies if they exist.

Reference:
https://azure.microsoft.com/en-us/updates/azure-ad-conditional-access-what-if-tool-is-now-available

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**