ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Topic 1, 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.

Identity 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 gu est accounts in the litware.com tenant.

Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection polices 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.

On-premises Environment

The on-premises network contains the severs 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.

Delegation Requirements

Litware identifies the following delegation requirements:

* Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).
* Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant
* Use custom catalogs and custom programs for Identity Governance.
- Ensure that User1 can create enterprise applications in Azure AD. Use the principle of least privilege.

Licensing Requirements

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to Microsoft 365 group that he appropriate license assigned.

Management Requirement

Litware wants to create a group named LWGroup1 will contain all the Azure AD user accounts for

Litware but exclude all the Azure AD guest accounts.

Authentication Requirements

Litware identifies the following authentication requirements:

- Implement multi-factor authentication (MFA) for all Litware users.
- Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.
- Implement a banned password list for the litware.com forest.
- Enforce MFA when accessing on-premises applications.
- Automatically detect and remediate externally leaked credentials

Access Requirements

Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Monitoring Requirements

Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

Question: 1

You need to meet the authentication requirements for leaked credentials.
What should you do?

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

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security/fundamentals/steps-secure-identity

Question: 2

You need to configure the MFA settings for users who connect from the Boston office. The solution must meet the authentication requirements and the access requirements.
What should you configure?

A. named locations that have a private IP address range
B. named locations that have a public IP address range
C. trusted IPs that have a public IP address range
D. trusted IPs that have a private IP address range

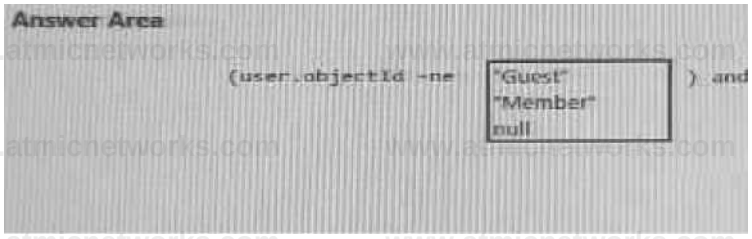
Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

Location offer your country set, IP ranges MFA trusted IP and corporate network VPN gateway IP address: This is the public IP address of the VPN device for your on-premises network. The VPN device requires an IPv4 public IP address. Specify a valid public IP address for the VPN device to which you want to connect. It must be reachable by Azure Client Address space: List the IP address ranges that you want routed to the local on-premises network through this gateway. You can add multiple address space ranges. Make sure that the ranges you specify here do not overlap with ranges of other networks your virtual network connects to, or with the address ranges of the virtual network itself.

Question: 3

HOTSPOT
You need to create the LWGroup1 group to meet the management requirements.
How should you complete the dynamic membership rule? To answer, drag the appropriate values to the correct targets. Each value may be used once, more than once, or not at all. You many need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:

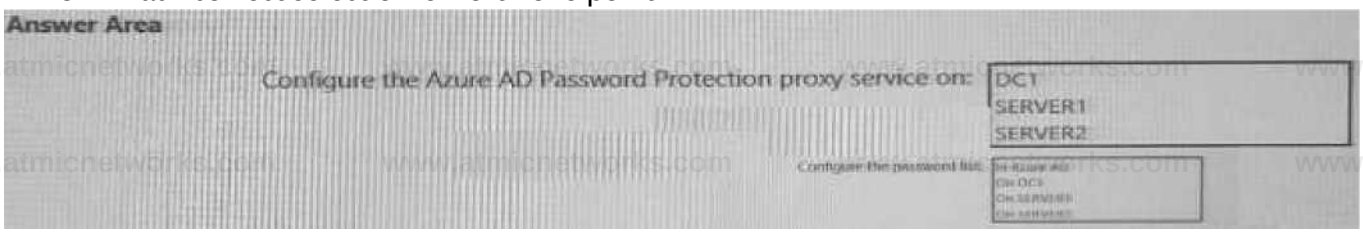
Null "Member"

Question: 4

HOTSPOT

You need to implement password restrictions to meet the authentication requirements.
You install the Azure AD password Protection DC agent on DC1.
What should you do next? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

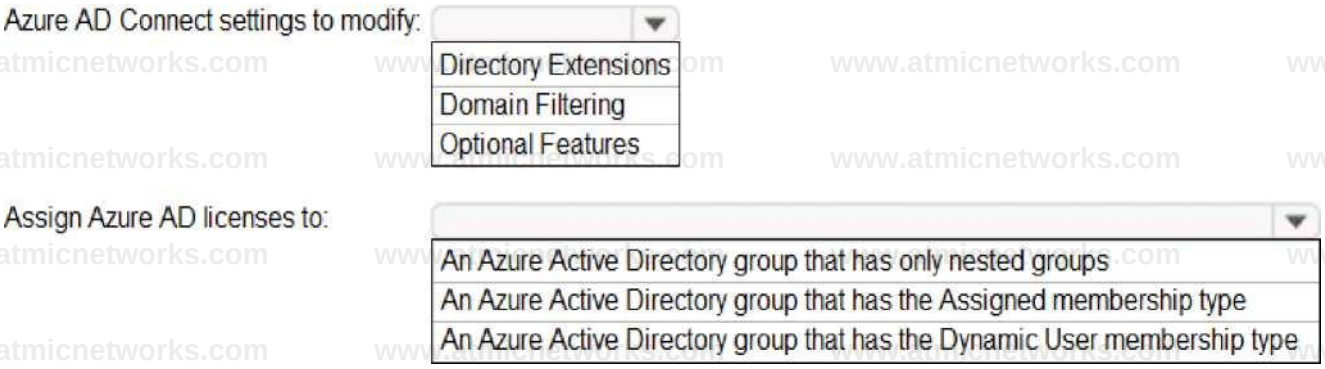
Server1
On DC1

Question: 5

HOTSPOT

You need to configure the assignment of Azure AD licenses to the Litware users. The solution must meet the licensing requirements.What should you do? To answer, select the appropriate options in the answer area.

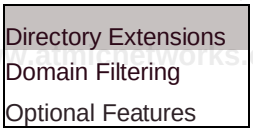
NOTE:Each correct selection is worth one point.



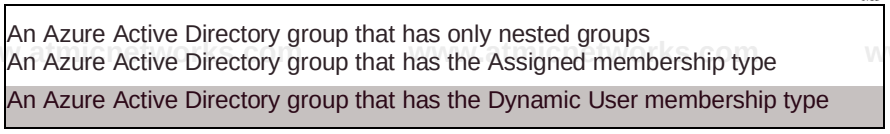
Answer:

Explanation:

Azure AD Connect settings to modify:



Assign Azure AD licenses to:



Litware recently added a custom user attribute namedLWLicensesto the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of theLWLicensesattribute. Users who have the appropriate value forLWLicensesmust be added automatically to

a Microsoft 365 group that has the appropriate licenses assigned.

Question: 6

HOTSPOT

You need to identify which roles to use for managing role assignments. The solution must meet the delegation requirements.

What should you do? To answer, select the appropriate options in the answer area.

NOTE:Each correct selection is worth one point.

To manage Azure AD built-in role assignments, use:

▼
Global administrator
Privileged role administrator
Security administrator
User access administrator

Answer:

To manage Azure built-in role assignments, use:▼ Global administrator Privileged role administrator Security administrator User access administrator

Explanation:

To manage Azure AD built-in role assignments, use:

- Global administrator
- **Privileged role administrator**
- Security administrator
- User access administrator

To manage Azure built-in role assignments, use:

- Global administrator
- Privileged role administrator
- Security administrator
- **User access administrator**

Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal

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

Question: 7

HOTSPOT

You need to implement on-premises application and SharePoint Online restrictions to meet the authentication requirements and the access requirements.What should you do? To answer, select the appropriate options in the answer area.

NOTE:Each correct selection is worth one point.

For on-premises applications:

Configure Cloud App Security policies.
Modify the User consent settings for the enterprise applications.
Publish the applications by using Azure AD Application Proxy.

For SharePoint Online:

Configure Cloud App Security policies.
Modify the User consent settings for the enterprise applications.
Publish an application by using Azure AD Application Proxy.

Answer:

Explanation:

For on-premises applications:

Configure Cloud App Security policies.
Modify the User consent settings for the enterprise applications.
Publish the applications by using Azure AD Application Proxy.

For SharePoint Online:

Configure Cloud App Security policies.
Modify the User consent settings for the enterprise applications.
Publish an application by using Azure AD Application Proxy.

Question: 8

You need to configure the detection of multi-staged attacks to meet the monitoring requirements. What should you do?

A. Customize the Azure Sentinel rule logic.
B. Create a workbook.
C. Add Azure Sentinel data connectors.

D. Add an Azure Sentinel playbook.

Answer: A

Explanation:

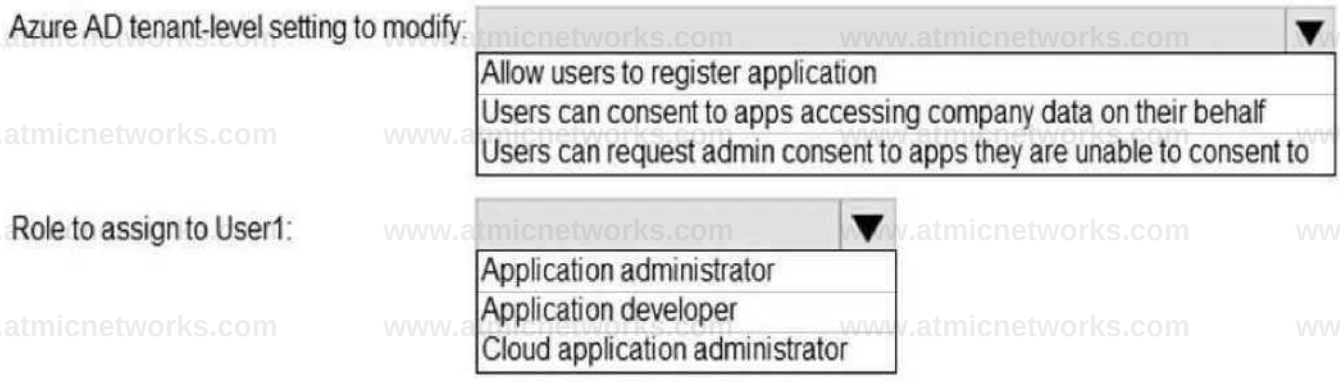
Question: 9

HOTSPOT

You need to configure app registration in Azure AD to meet the delegation 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:

Azure AD tenant-level setting to modify: i

Allow users to register application
Users can consent to apps accessing company data on their behalf
Users can request admin consent to apps they are unable to consent to

Role to assign to Useri: |

Application administrator Application developer Cloud application administrator

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles

Question: 10

You need to track application access assignments by using Identity Governance. The solution must meet the delegation requirements.

What should you do first?

A. Modify the User consent settings for the enterprise applications.
B. Create a catalog.
C. Create a program.
D. Modify the Admin consent requests settings for the enterprise applications.

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management- overview

Topic 2, Contoso, Ltd

Overview

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

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

Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contos.com. The domain contains an organizational unit (OU) named Contoso_Resources. The Contoso_Resoureces 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

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 E5

Project Plan 3

Azure AD Connect is configured between azure AD and Active Directory Domain Serverless (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 user have all licenses assigned besides following exception:
The users in the London office have the Microsoft 365 admin center to manually assign licenses. All user have 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 project administrator roles.
Problem Statements
Contoso identifies the following issues:

- Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
- The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
- The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
- Currently, the helpdesk administrators can perform tasks by using the: User administrator role without justification or approval.
- When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

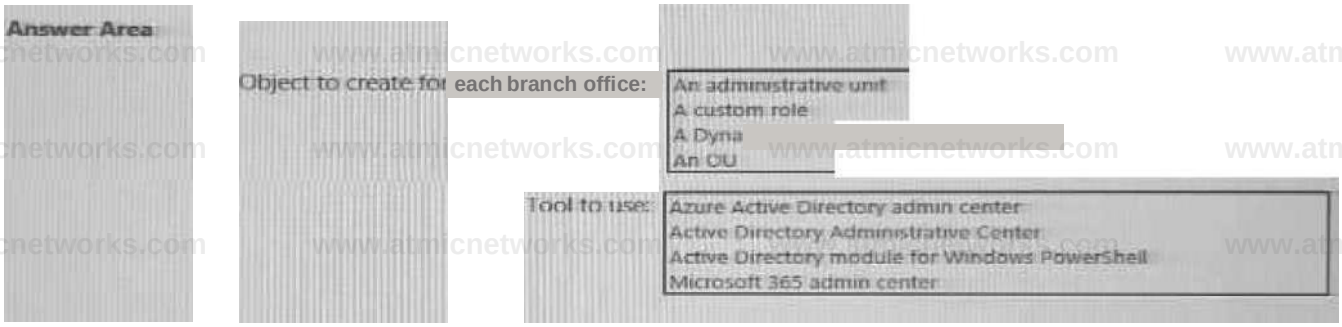
Planned Changes
Contoso plans to implement the following changes.
Implement self-service password reset (SSPR). Analyze Azure audit activity logs by using Azure Monitor-Simplify license allocation for new users added to the tenant. Collaborate with the users at Fabrikam on a joint marketing campaign. Configure the User administrator role to require justification and approval to activate.
Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.
Contoso plans to acquire a company named Corporation. One hundred new A Datum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle. Technical Requirements
Contoso identifies the following technical requirements:

- AH users must be synced from AD DS to the contoso.com Azure AD tenant.
- App1 must have a redirect URI pointed to https://contoso.com/auth-response.
- License allocation for new users must be assigned automatically based on the location of the user.
- Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
- Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
- The helpdesk administrators must be able to manage licenses for only the users in their respective office.
- Users must be forced to change their password if there is a probability that the users' identity was compromised.

Question: 11

HOTSPOT
You need to meet the technical requirements for license management by the helpdesk administrators.

What should you create first, and which tool should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Object to create for each branch office:

- An administrative unit
- A custom role
- A Dynamic User security group
- An OU

Tool to use:

- Azure Active Directory admin center
- Active Directory Administrative Center
- Active Directory module for Windows PowerShell
- Microsoft 365 admin center

Question: 12

You need to locate licenses to the

A. Datum users. The solution must need the technical requirements.

Which type of object should you create?

A. A Dynamo User security group

B. An OU

C. A distribution group

D. An administrative unit

Answer: D

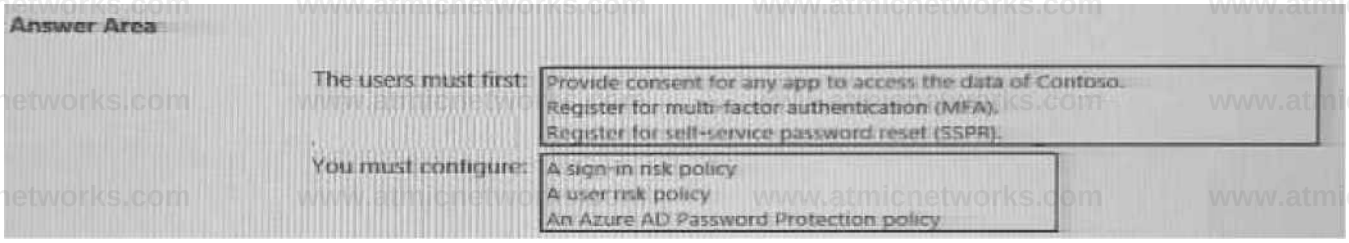
Explanation:

Question: 13

HOTSPOT

You need to meet the technical requirements for the probability that user identifies were compromised.

What should the users do first, and what should you configure? To answer, select the appropriate options in the answer area.



NOTE: Each correct selection is worth one point.

Answer:

Explanation:

Register for multi-factor authentication (MFA). A user risk policy

Question: 14

You need to meet the planned changes for the User administrator role.

What should you do?

A. Create an access review.

B. Modify Role settings

C. Create an administrator unit.

D. Modify Active Assignments.

Answer: D

Explanation:

Role Setting details is where you need to be: Role setting details - User Administrator
Privileged Identity Management | Azure AD roles
Default Setting State

Require justification on activation Yes
Require ticket information on activation No
On activation, require Azure MFA Yes
Require approval to activate No
Approvers None

Question: 15

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 A datum organizational unit (OU).

Question: 16

HOTSPOT

You need to meet the technical requirements for the probability that user identities were compromised.

What should the users do first, and what should you configure? To answer, select the appropriate options in the answer area.

NOTE:Each correct selection is worth one point.

The users must first:

Provide consent for any app to access the data of Contoso.
Register for multi-factor authentication (MFA).
Register for self-service password reset (SSPR).

You must configure:

A sign-in risk policy
A user risk policy
An Azure AD Password Protection policy

Answer:

Explanation:

The users must first:

Provide consent for any app to access the data of Contoso
Register for multi-factor authentication (MFA).
Register for self-service password reset (SSPR).

You must configure:

A sign-in risk policy
A user risk policy
An Azure AD Password Protection policy

Reference:

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

Question: 17

You need to meet the planned changes and technical requirements for App1. What should you implement?

A. a policy set in Microsoft Endpoint Manager
B. an app configuratifon policy in Microsoft Endpoint Manager
C. an app registration in Azure AD
D. Azure AD Application Proxy

Answer: C

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app

Question: 18

You create a Log Analytics workspace.
You need to implement the technical requirements for auditing.
What should you configure in Azure AD?

A. Company branding
B. Diagnostics settings
C. External Identities
D. App registrations

Answer: D

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/overview-monitoring

Question: 19

HOTSPOT

You need to implement the planned changes and technical requirements for the marketing department.

What should you do? To answer, select the appropriate options in the answer area.

NOTE:Each correct selection is worth one point.

To configure user access:
- An access package
- An access review
- A conditional access policy

To enable collaboration with fabrikam.com:
- An accepted domain
- A connected organization
- A custom domain name

Answer:

Explanation:

To configure user access:
- An access package
- An access review
- A conditional access policy

To enable collaboration with fabrikam.com:
- An accepted domain
- A connected organization
- A custom domain name

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management- organization

Question: 20

You need to allocate licenses to the new users from
A. Datum. The solution must meet the technical requirements.
Which type of object should you create?

A. a distribution group
B. a Dynamic User security group
C. an administrative unit
D. an OU

Answer: C

Explanation:

Topic 3, A. Datum CorpOverview

Overview

A. Datum Corporation is a consulting company in Montreal.

A. Datum recently acquired a Vancouver-based company named Litware, Inc.

A Datum Environment

The on-premises network of A. Datum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

A. Datum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect

A. Datum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.

The tenant contains the users shown in the following table.

Problem Statements

A. Datum identifies the following issues:

- Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit.
- A recent security incident reveals that several users leaked their credentials, a suspicious browser was used for a sign-in, and resources were accessed from an anonymous IP address,
- When you attempt to assign the Device Administrators role To IT_Group1, the group does NOT appear in the selection list.
- Anyone in the organization can invite guest users, including other guests and non-administrators.
- The helpdesk spends too much time resetting user passwords.
- Users currently use only passwords for authentication.

Requirements

A, Datum plans to implement the following changes;

- Configure self-service password reset {SSPR}.
- Configure multi-factor authentication (MFA) for all users.
- Configure an access review for an access package named Package1.
- Require admin approval for application access to organizational data.
- Sync the AD DS users and groupsoflitware.com with the Azure AD tenant.
  - Ensure that only users that are assigned specific admin roles can invite guest users.
  - Increase the maximum number of devices that can be joined or registered to Azure AD to 10.

Technical Requirements

A. Datum identifies the following technical requirements:

- Users assigned the User administrator role must be able to request permission to use the role when needed for up to one year.
- Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.
- Users must provide one authentication method to reset their password by using SSPR. Available methods must include:
  - Email
  - Phone

- Security questions
- The Microsoft Authenticator app
- Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.
- The principle of least privilege must be used.

Question: 21

You need to implement the planned changes for litware.com. What should you configure?

A. Azure AD Connect cloud sync between the Azure AD tenant and litware.com
B. Azure AD Connect to include the litware.com domain
C. staging mode in Azure AD Connect for the litware.com domain

Answer: C

Explanation:

Question: 22

You need implement the planned changes for application access to organizational dat a. What should you configure?

A. authentication methods
B. the User consent settings
C. access packages
D. an application proxy

Answer: B

Explanation:

Question: 23

You implement the planned changes for SSPR.

What occurs when User3 attempts to use SSPR? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Number of authentication methods required:

Authentication methods that can be used:

Answer: See the explanation

Explanation:

Answer is

Answer Area

Number of authentication methods required: *2*

Authentication methods that can be used: Email and phone only

Question: 24

DRAG DROP

You need to resolve the recent security incident issues.

What should you configure for each incident? To answer, drag the appropriate policy types to the correct issues. Each policy type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Policy Types

An authentication method policy

A Conditional Access policy

A sign in risk policy

A user risk po icy

Answer Area

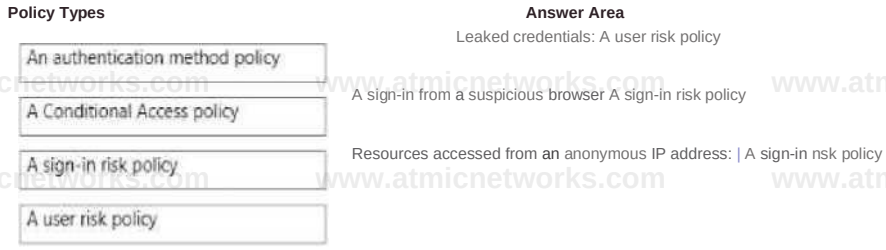
Leaked credentials,

A siqn-m from a suspicious browser

Resources accessed from an anonymous IP address:

Answer

Explanation:



Question: 25

You need to resolve the issue of the sales department users. What should you configure for the Azure AD tenant?

A. the User settings
B. the Device settings
C. the Access reviews settings
D. Security defaults

Answer: A

Explanation:

Question: 26

You need to resolve the issue of I-.Group1. What should you do first?

A. Recreate the IT-Group 1 group.
B. Change Membership type of IT-Group1 to Dynamic Device
C. Add an owner to IT_Group1.
D. Change Membership type of IT-Group1 to Dynamic User

Answer: A

Explanation:

Question: 27

You need to implement the planned changes for Package1. Which users can create and manage the access review?

A. User3 only
B. User4 only
C. User5 only
D. User3 and User4
E. User3 and User5

F. User4and User5

Answer: E

Explanation:

Question: 28

You need to resolve the issue of the guest user invitations. What should you do for the Azure AD tenant?

A. Configure the Continuous access evaluation settings.
B. Modify the External collaboration settings.
C. Configure the Access reviews settings.
D. Configure a Conditional Access policy.

Answer: C

Explanation:

Question: 29

You need to modify the settings of the User administrator role to meet the technical requirements. Which two actions should you perform for the role? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Select Require justification on activation
B. Set all assignments to Active
C. Set all assignments to Eligible
D. Modify the Expire eligible assignments after setting.
E. Select Require ticket information on activation.

Answer: C,D

Explanation:

Topic 4, Misc. Questions

Question: 30

Your company has an Azure Active Directory (Azure AD) tenant named contosri.com. The company has the business partners shown in the following table.

Name	Description
Fabrikam, Inc.	An Azure AD tenant that has two verified domains named fabrikam.com and adatum.com
Litware, Inc.	A third-party identity provider that uses the domain names of litwareinc.com and contoso.com

users can request access by using package 1.
Users at Fabrikam and Litware use ail then respective domain names for email addresses.

You plan to create an access package named packaqe1 that will be accessible only to the Fabrikam and Litware users.
You need to configure connected organizations for Fabrikam and litware so that any of their users can request access by using package1.
What is the minimum of connected organization that you should create.

A. 1
B. 2
C. 3
D. 4

Answer: C

Explanation:

Question: 31

You have an Azure subscription that contains the resources shown in the following table.

Name	Type
Group 1	Group that has the Assigned membership type
App1	Enterprise application in Azure Active Directory (Azure AD)
Contributor	Azure subscription role
Rolel	Azure Active Directory (Azure AD) role

For which resources can you create an access review?

A. Group1, App1, Contributor, and Role1
B. Hotel and Contributor only
C. Group1, Role1, and Contributor only
D. Group1 only

Answer: A

Explanation:

Access reviews require an Azure AD Premium P2 license.

Access reviews for Group1 and App1 can be configured in Azure AD Access Reviews.

Access reviews for the Contributor role and Role1 would need to be configured in Privileged Identity Management (PIM). PIM is included in Azure AD Premium P2.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim- how-to-start-security-review?toc=/azure/active-directory/governance/toc.json

https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

Question: 32

You have an Azure Active Directory (Azure AD) tenant that uses conditional access policies. You plan to use third-party security information and event management (SIEM) to analyze conditional access usage.
You need to download the Azure AD log that contains conditional access policy data.
What should you export from Azure AD?

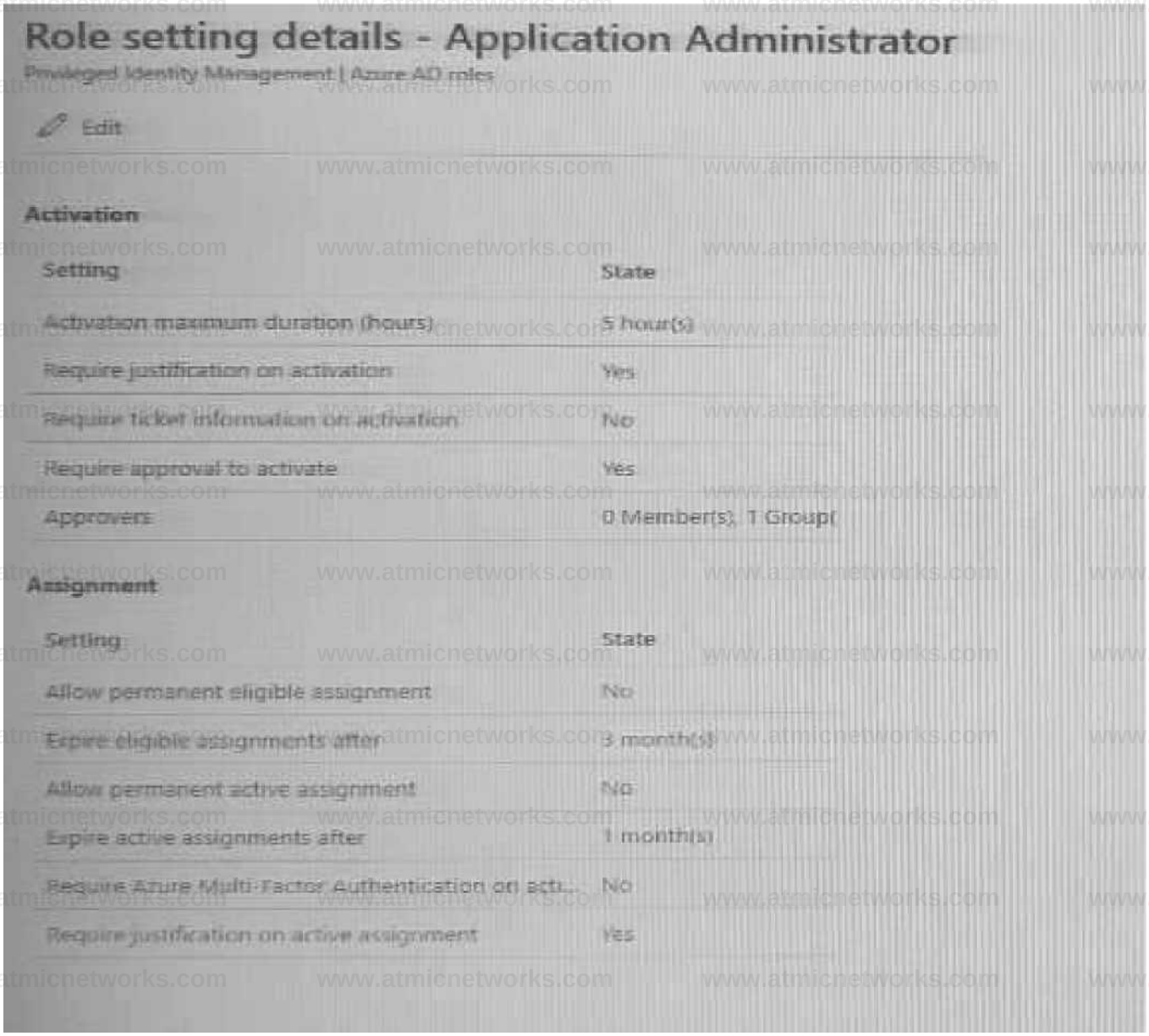
A. sign-ins in JSON format
B. sign-ins in CSV format
C. audit logs in JSON format
D. audit logs in CSV format

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-audit-logs

Question: 33

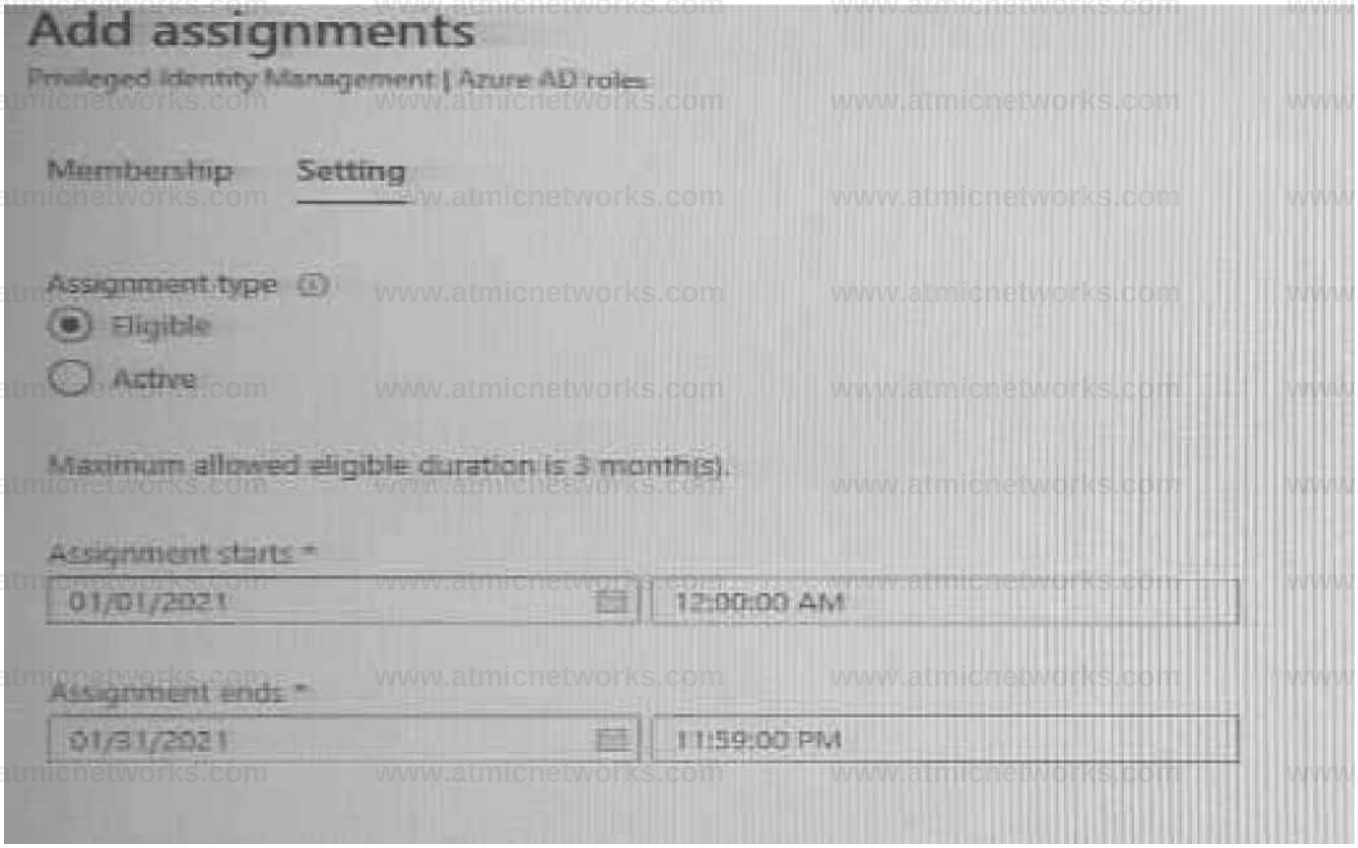
HOTSPOT
You have an Azure Active Directory (Azure AD) tenant that contains three users named User1, User1, and User3,
You create a group named Group1. You add User2 and User3 to Group1.
You configure a role in Azure AD Privileged identity Management (PIM) as shown in the application administrator exhibit.
(Click the application Administrator tab.)



Group1 is configured as the approver for the application administrator role.

You configure User2to be eligible for the application administrator role.

For User1, you add an assignment to the Application administrator role as shown in the Assignment exhibit. (Click Assignment tab)



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

NOTE: Each correct selection is worth one point.

Answer Area

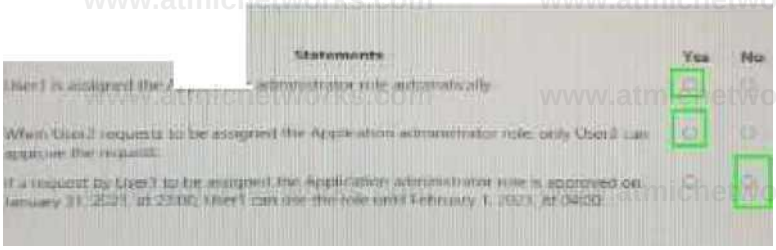
Statements	Yes	No
User! is assigned I he Application administrator role automatically.		
When User? requests to be assigned the Application administrator role, only Users cun approve the request		
It a request by User! to be assigned tin- Application administrator role Is approved on January 31 2.021, at 23-00, Usr*rt can use the role until February I. 2021. at 04:00.		

Answer:

Explanation:

Answer:

RMHH .ilw** •



Question: 34

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

You need to review the Azure AD sign-ins log to investigate sign ins that occurred in the past. For how long does Azure AD store events in the sign-in log?

A. 14 days
B. 30 days
C. 90 days
D. 365 days

Answer: B

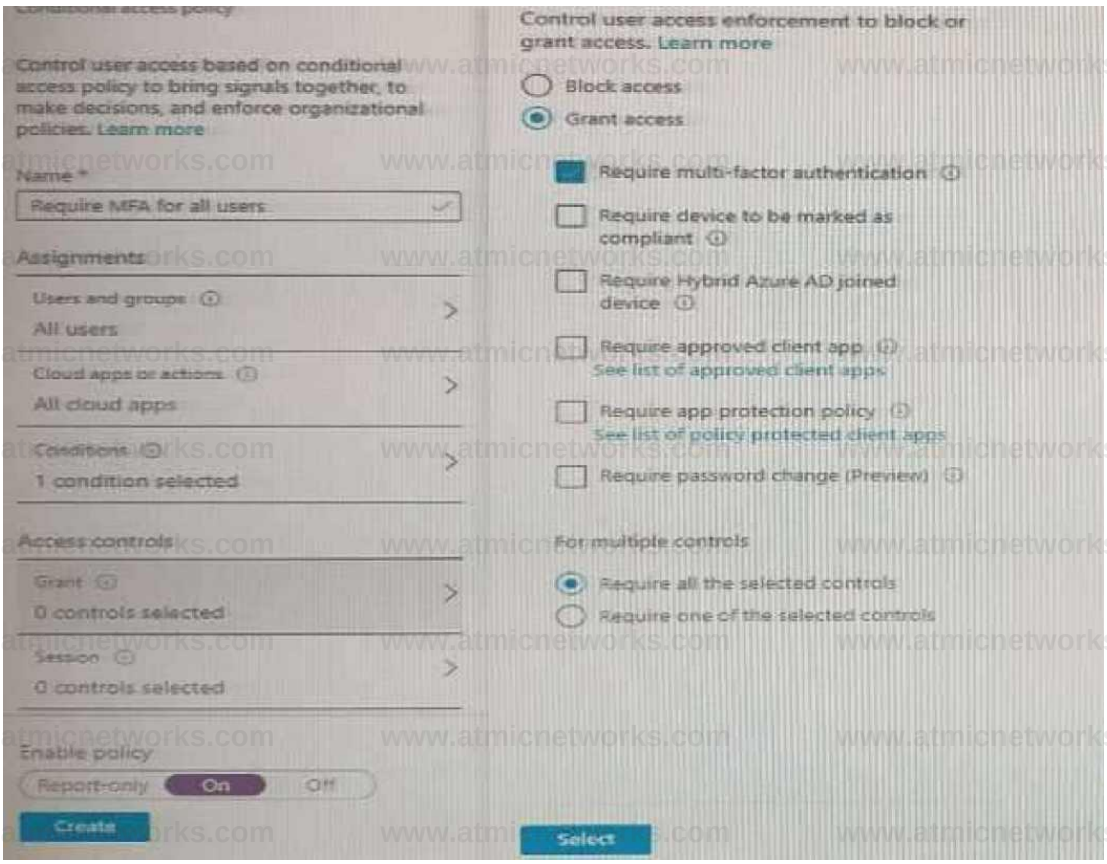
Explanation:

Question: 35

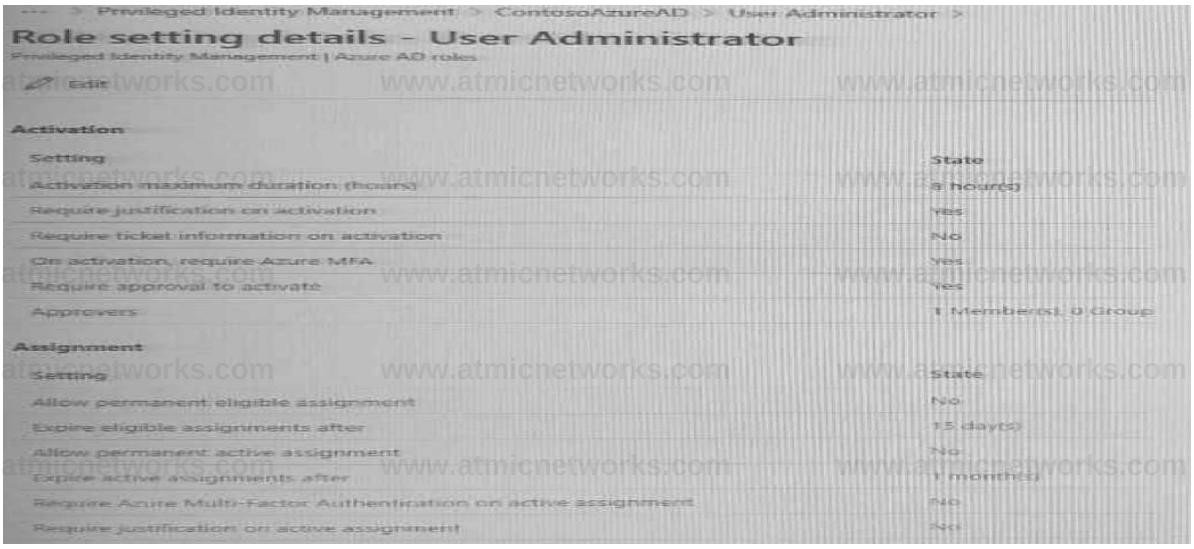
HOTSPOT

You have a Microsoft 365 tenant.

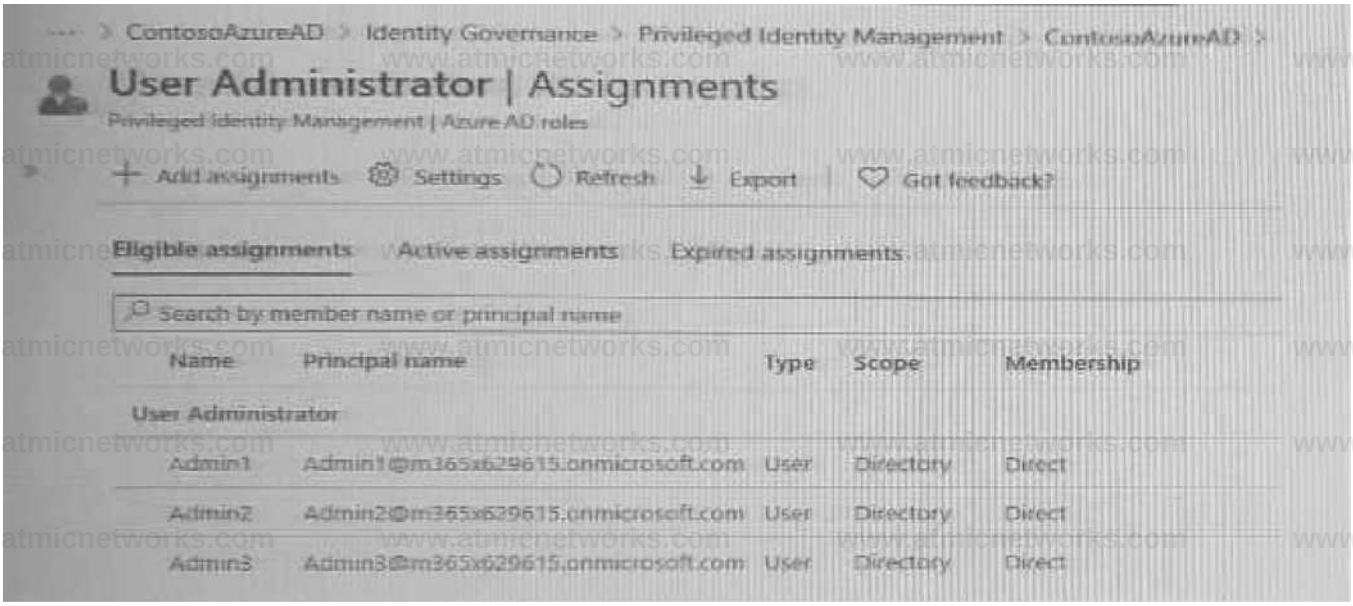
You configure a conditional access policy as shown in the Conditional Access policy exhibit. (Click the Conditional Access policy tab.)



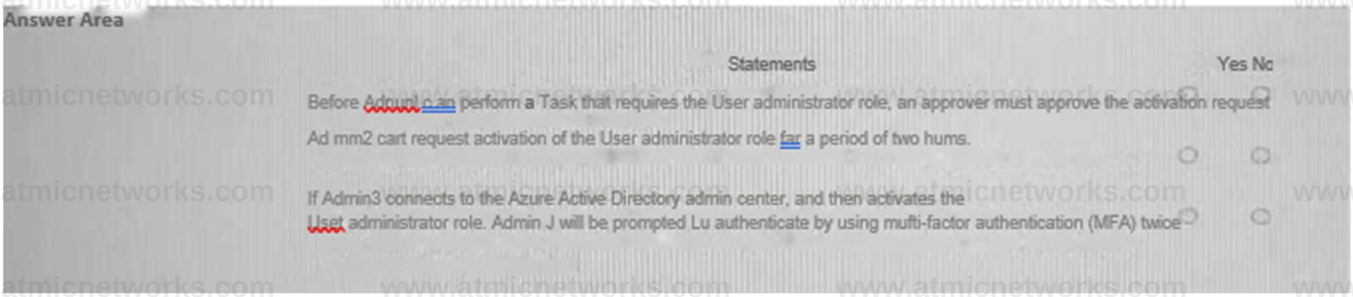
You view the User administrator role settings as shown in the Role setting details exhibit. (Click the Role setting details tab.)



You view the User administrator role assignments as shown in the Role assignments exhibit. (Click the Role assignments lab.)



For each of the following statement, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.



Yes

Yes

No

Answer:

Question: 36

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

Name	Type	
USLTI	User	
GuesU	Guest	
Identity'	Managed identity	

Which objects can you add as eligible in Azure Privileged identity Management (PIM) for an Azure AD role?

A. User1 only
B. User1 and Identity1 only
C. User1. Guest1, and Identity
D. User1 and Guest1 only

Answer: D

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim- deployment-plan

Question: 37

HOTSPOT

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com. The company has a business partner named Fabrikam, Inc.

Fabrikam uses Azure AD and has two verified domain names of fabrikam.com and litwareinc.com.

Both domain names are used for Fabrikam email addresses.

You plan to create an access package named package1 that will be accessible only to the users at Fabrikam.

You create a connected organization for Fabrikam.

You need to ensure that the package1 will be accessible only to users who have fabrikam.com email addresses.

What should you do? To answer, select the appropriate options in the answer area.

NOTE:Each correct selection is worth one point.

To allow access for users who have fabnkam com email addresses, configure: ▼

- An access package assignment in Identity Governance
- An access package policy in Identity Governance
- A conditional access policy in Azure AD
- The External collaboration settings in Azure AD

To block access for users who have litwareinc com email addresses, configure: ▼

- An access package assignment in Identity Governance
- An access package policy in Identity Governance
- A conditional access policy in Azure AD
- The External collaboration settings in Azure AD

Answer:

Explanation:

To allow access for users who have fabnkam.com email addresses, configure

- An access package assignment in Identity Governance
- An access package policy in Identity Governance
- A conditional access policy in Azure AD
- The External collaboration settings in Azure AD

To block access for users who have htwareinc.com email addresses, configure: ▼

- An access package assignment in Identity Governance
- An access package policy in Identity Governance
- A conditional access policy in Azure AD
- The External collaboration settings in Azure AD

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management- access-package-request-policy

https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management- access-package-create

Question: 38

You have a Microsoft 365 tenant.

You need to ensure that you tan view Azure Active Directory (Azure AD) audit log information by using Azure Monitor.

What should you do first?

A. Run the Get-AzureADAuditDirectoryLogs cmdlet.
B. Create an Azure AD workbook.
C. Run the Set-AzureADTenantDetail cmdlet.
D. Modify the Diagnostics settings for Azure AD.

Answer: D

Explanation:

Question: 39

HOTSPOT

You have a Microsoft 365 tenant that contains a group named Group1 as shown in the Group1 exhibit. (Click theGroup1tab.)

```
PS C:\> Get-AzureADGroup -    .;       ';"J: .: ." | Get-AzureADGroupowner

Objectld                              DisplayName     UserPrincipalName                  UserType

a7f7d405-636f-4493-b971-5c2b7al31blc Admin            admin@M365x629615.onmicrosoft.com Member

PS C:\> Get-AzureADGroup s : .r ch.' : 1 r.:      :: .: " | GetAzureADGroupMember | ft displayname^

DisplayName

Userl
User4
Group3
```

You create an enterprise application named App1 as shown in the App1 Properties exhibit. (Click theApp1 Propertiestab.)

Dashboard > ContosoAzureAD > Enterprise applications > App1

'I[1] App1| Properties

Enterprise Application «

£ Overview

Q Deployment Plan

X Diagnose and solve problems

Manage

'I' Properties

A Owners

& Roles and administrators IPrev.

A Users and groups

3 Single sign-on

£ Provisioning

r Application proxy

C Self-service

Security

Conditional Access

4« Permissions

0 Token encryption

Activity

3 Sign-ms

^ Save X Discard § Delete ^? Got feedback?

Enabled for users to sign-in? Yes No

Name App1

Homepage URL https://app1.m365x629615.onmicrosoft.com/

Logo AP

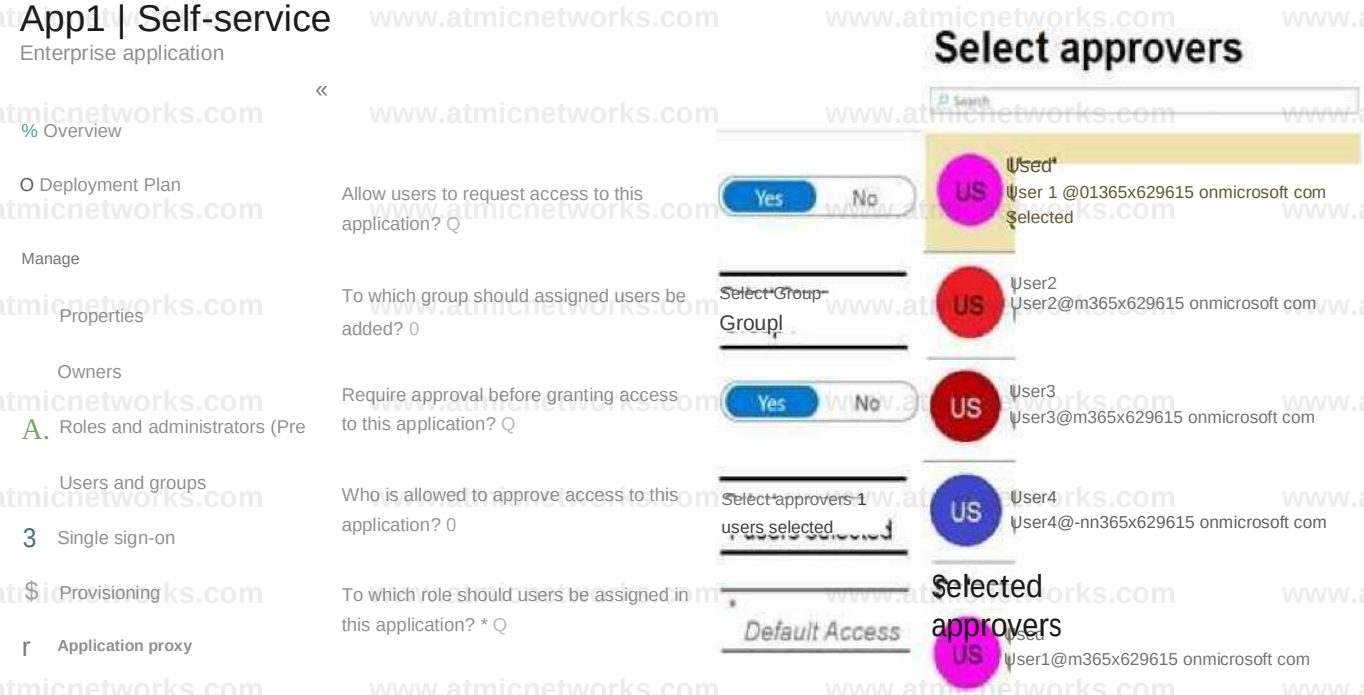
Select a file

User access URL https://myapps.microsoft.com/signin/App1/09df58d6-d29d-40de-b0d...

Application ID 0	09df58d6-d29d-40de-b0d0-321fdc63c665
Object ID ©	03709d22-7e61-4007-a2a0-04dbdff269cd
Terms of Service Uri ©	Publisher did not provide this information
Privacy Statement Uri 0	Publisher did not provide this information
Reply URL 0	https://contoso.com/App1/logon
User assignment required?	No
Visible to users? 0	Yes flW

You configure self-service for App1 as shown in the App1 Self-service exhibit. (Click theApp1 Selfservicetab.)

Dashoboard ContosoAzureAD > Enterprise applications > App1



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
The members of Group3 can access App1 without first being approved by User1.	○	○
After you configure self-service for App1, the owner of Group1 is User1.	○	○
App1 appears in the Microsoft Office 365 app launcher of User4.	○	○

Answer:

Explanation:

No
No
Yes

a) When you assign a group to an application, only users in the group will have access. The assignment does not cascade to nested groups.

b) Tested in lab, existing owners will be replaced. Also direct assignment (resource owner) is path of least privilege. (replicated in test)

c) Application setting 'visible to users' is set to No, then no users see this application on their My Apps portal and O365 launcher.

Reference

a) https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group- access-portal

b) maybehttps://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-manage-groups

c) https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-properties#visible-to-users

Question: 40

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

Answer: A

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles

Reply Uri 0

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE:Each correct selection is worth one point.Question: 42

Your company requires that users request access before they can access corporate applications.

You register a new enterprise application named MyApp1 in Azure Active Dilatory (Azure AD) and configure single sign-on (SSO) for MyApp1.

Which settings should you configure next for MyApp1?

A. Self-service
B. Provisioning
C. Roles and administrators
D. Application proxy

Answer: A

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access

Question: 43

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

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

- Applications: Appl. App?, App3
- Owners: Admin 1
- Users and groups: HRUsers

AH 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 sue App1 and App2-You need to ensure that the users can also see App3. What should you do from App3?

What should you do from App3?

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

Answer: A

Explanation:

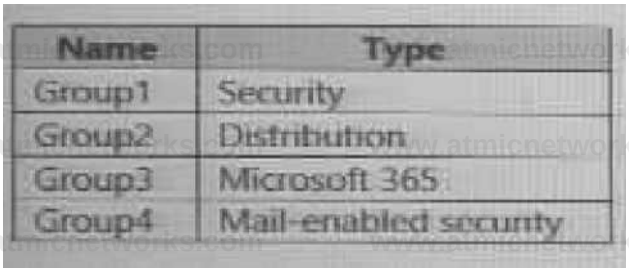
Reference:

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: 44

You have a Microsoft 365 tenant.
The Azure Active Directory (Azure AD) tenant contains the groups shown in the following table.



Name	Type
Group1	Security
Group2	Distribution
Group3	Microsoft 365
Group4	Mail-enabled security

In Azure AD. you add a new enterprise application named Appl. Which groups can you assign to App1?

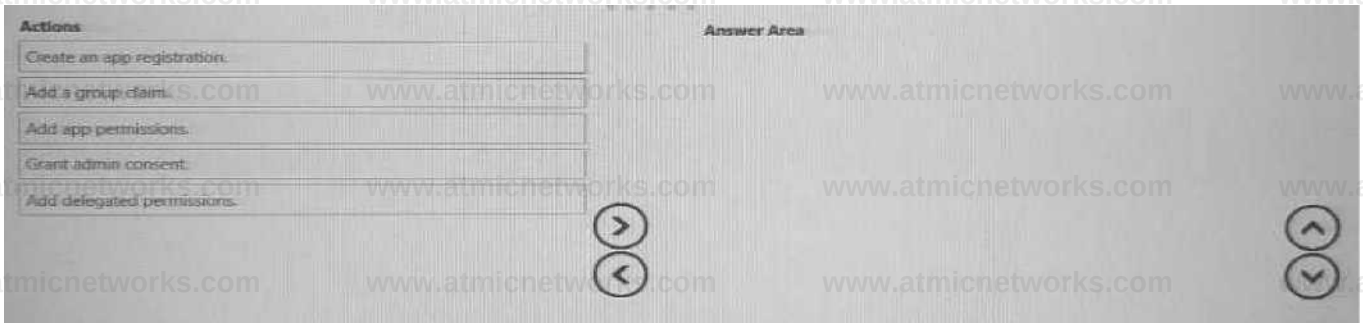
A. Group1 and Group2 only
B. Group2 only
C. Group3 only
D. Group1 only
E. Group1 and Group4

Answer: C

Explanation:

Question: 45

DRAG DROP
Your company has an Azure Active Directory (Azure AD) tenant named contoso.com.
The company is developing a web service named App1.
You need to ensure that App1 can use Microsoft Graph to read directory data in contoso.com.
Which three actions should yon perform in sequence? To answer, move the appropriate actions from the list of actions to the



answer area and arrange them In the correct order.

Answer:

Explanation:

Create an app registration:

Your app must be registered with the Microsoft identity platform and be authorized by either a user or an administrator for access to the Microsoft Graph resources it needs.

Grant admin consent:

Higher-privileged permissions require administrator consent.

Add app permissions:

After the consents to permissions for your app, your app can acquire access tokens that represent the app's permission to access a resource in some capacity. Encoded inside the access token is every permission that your app has been granted for that resource.

Reference:

https://docs.microsoft.com/en-us/graph/auth/auth-concepts

Question: 48

You configure a new Microsoft 36S tenant to use a default domain name of contosso.com.

You need to ensure that you can control access to Microsoft 365 resource-, by using conditional access policy.

What should you do first?

A. Disable the User consent settings.
B. Disable Security defaults.
C. Configure a multi-factor authentication (MI A) registration policy1.
D. Configure password protection for Windows Server Active Directory.

Answer: B

Explanation:

Question: 49

You have an Azure Active Directory (Azure AD) tenant named conto.so.com that has Azure AD Identity Protection enabled. You need to Implement a sign-in risk remediation policy without blocking access.

What should you do first?

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

Answer: C

Explanation:

MFA and SSPR are both required. However, MFA is required first.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity- protection-remediate-unblock

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment

Question: 50

You have an Azure Active Directory (Azure AD) tenant that syncs to an Active Directory forest. The tenant-uses through authentication.
A corporate security policy states the following:
Domain controllers must never communicate directly to the internet.
Only required software must be- installed on servers.
The Active Directory domain contains the on-premises servers shown in the following table.

Name	Description
Server1	Domain controller (PDC emulator)
Server2	Domain controller (infrastructure master)
Server3	Azure AD Connect server
Server4	Unassigned member server

You need to ensure that users can authenticate to Azure AD if a server fails.
On which server should you install an additional pass-through authentication agent?

A. Server2
B. Server4
C. Server1
D. Server3

Answer: B

Explanation:
Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-quick-start

Question: 51

HOTSPOT
You have a Microsoft 36S tenant.
You create a named location named HighRiskCountries that contains a list of high-risk countries.
You need to limit the amount of time a user can stay authenticated when connecting from a high-risk country.
What should you configure in a conditional access policy? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Configure 1-fighHiskCnuntries by using:

A cloud upp oi action
A condition
A grant control
A ■.,",Miiii control

Canfigure Sign in frequency by using:

A cloud app or action
A condition
A t|Nfii control
A session control

Answer:

Explanation:

Configure HighRiskCountnes by using:

A cloud app or action A condition
A grant control
A session control

Configure Sign-in frequency by using:

A cloud app or action
A condition
A grant control
A session control

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional- access-session

Question: 52

You have an Azure Active Directory (Azure AD) tenant.
You configure self-service password reset (SSPR) by using the following settings:

- Require users to register when signing in: Yes

- Number of methods required to reset: 1

What is a valid authentication method available to users?

A. home prions
B. mobile app notification
C. a mobile app code
D. an email to an address in your organization

Answer: D

Explanation:

Question: 53

You have a Microsoft 365 tenant.

You currently allow email clients that use Basic authentication to conned to Microsoft Exchange Online. You need to ensure that users can connect t to Exchange only run email clients that use Modern authentication protocols.

What should you implement?

You need to ensure that use Modern authentication

A. a compliance policy in Microsoft Endpoint Manager
B. a conditional access policy in Azure Active Directory (Azure AD)
C. an application control profile in Microsoft Endpoint Manager
D. an OAuth policy in Microsoft Cloud App Security

Answer: C

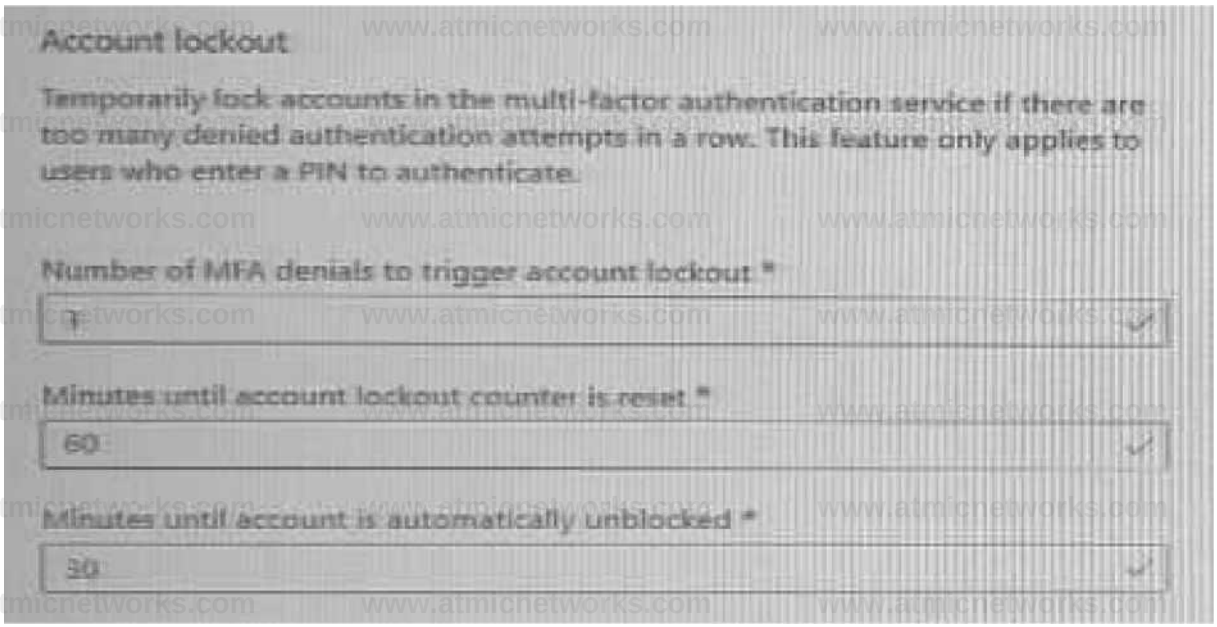
Explanation:

Question: 54

HOTSPOT

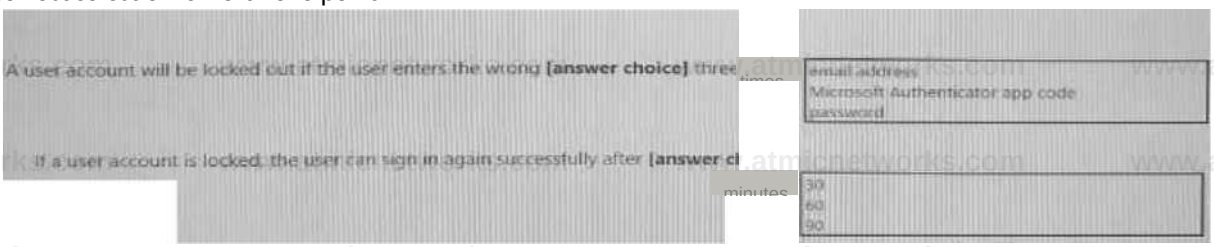
You have an Azure Active Directory (Azure AD) tenant that has multi-factor authentication (MFA) enabled.

The account lockout settings are configured as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

App code 60

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

Question: 55

HOTSPOT

You have a Microsoft 365 tenant.

You need to identify users who have leaked credentials. The solution must meet the following requirements.

- Identity sign-Ins by users who ate suspected of having leaked credentials.
- Rag the sign-ins as a high risk event.
- Immediately enforce a control to mitigate the risk, while still allowing the user to access applications.

What should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

To classify leaked credentials as high-risk, use:

- Azure Active Directory (Azure AD) Identity Protection
- Azure Active Directory (Azure AD) Privileged Identity Management (PIM) Identity Governance
- Self-service password reset (SSPR)

To trigger remediation, use: ▼

- Client apps not using Modern authentication
- Device state
- Sign-in risk User location User risk

To mitigate the risk, select: ▼

- Apply app enforced restrictions
- Block access
- Grant access but require app protection policy
- Grant access but require password change

Answer:

Explanation:

To classify leaked credentials as high-risk, use:

- Azure Active Directory (Azure AD) Identity Protection
- Azure Active Directory (Azure AD) Privileged Identity Management (PIM) Identity Governance
- Self-service password reset (SSPR)

To tngger remediation, use: ▼

- Client apps not using Modern authentication
- Device state
- Sign-in risk User location
- User risk

To mitigate the risk, select: ▼

- Apply app enforced restrictions
- Block access
- Grant access but require app protection policy
- Grant access but require password change

Reference:

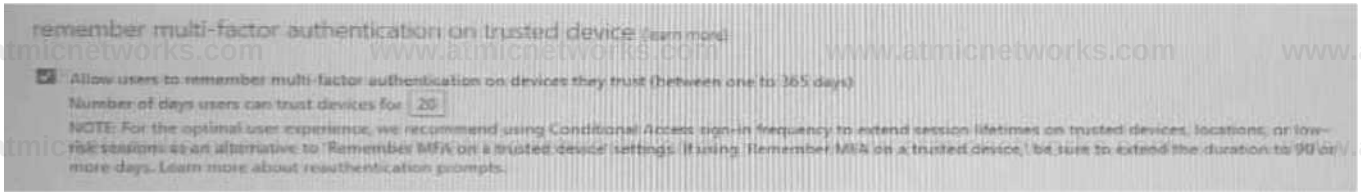
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity- protection-risks

Question: 56

You create the Azure Active Directory (Azure AD) users shown in the following table.

Name	Multi-factor auth status	Device
User1	Disabled	Device1
User2	Enabled	Device2
User3	Enforced	Device3

On February 1, 2021, you configure the multi-factor authentication (MFA) settings as shown in the following exhibit.



The users authentication to Azure AD on their devices as shown in the following table.

Date	User
February 2, 2021	User1
February 5, 2021	User2
February 21, 2021	User1

On February 26, 2021, what will the multi-factor auth status be for each user?

A)

Name	Multi-factor auth status
User1	Disabled
User2	Enabled
User3	Enforced

B)

Name	Multi-factor auth status
User1	Enabled
User2	Enabled
User3	Enabled

C)

Name	Multi-factor auth status
User1	Enforced
User2	Enforced
User3	Enforced

D)

Name	Multi-factor auth status
User1	Disabled
User2	Enforced
User3	Enforced

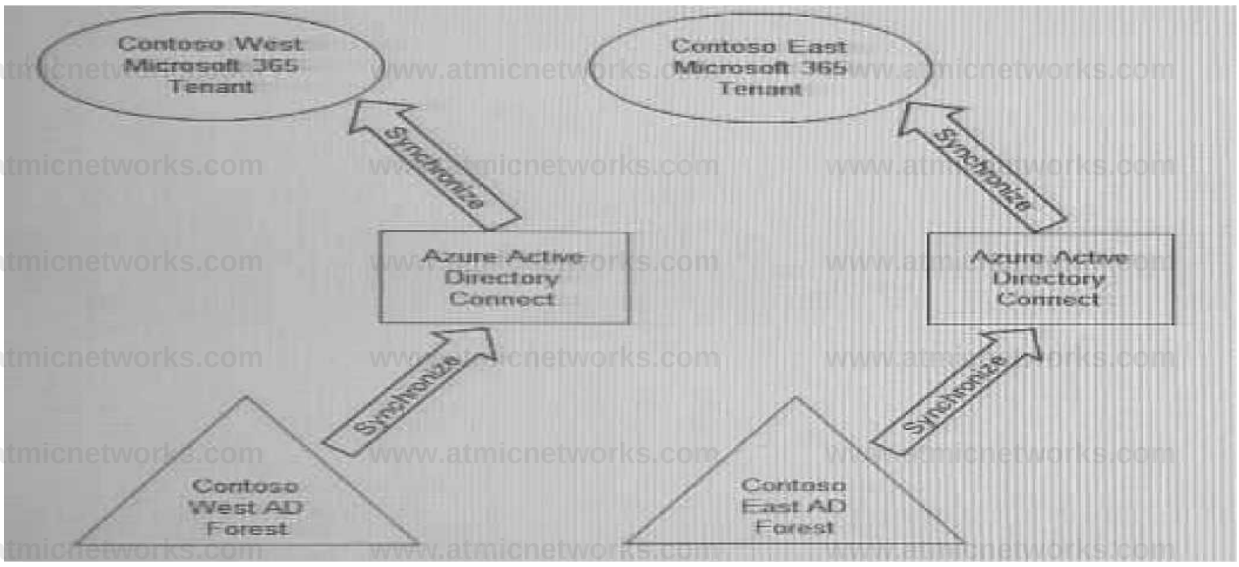
A. Option A B. Option B C. Option C D. Option D

Answer: B

Explanation:

Question: 57

Your company has two divisions named Contoso East and Contoso West. The Microsoft 365 identity architecture tor both divisions is shown in the following exhibit.



You need to assign users from the Contoso East division access to Microsoft SharePoint Online sites in the Contoso West tenant. The solution must not require additional Microsoft 3G5 licenses.
What should you do?

A. Configure the exiting Azure AD Connect server in Contoso Cast to sync the Contoso East Active Directory forest to the Contoso West tenant.
B. Configure Azure AD Application Proxy in the Contoso West tenant.
C. Deploy a second Azure AD Connect server to Contoso East and configure the server to sync the Contoso East Active Directory forest to the Contoso West tenant.
D. Invite the Contoso East users as guests in the Contoso West tenant.

Answer: A

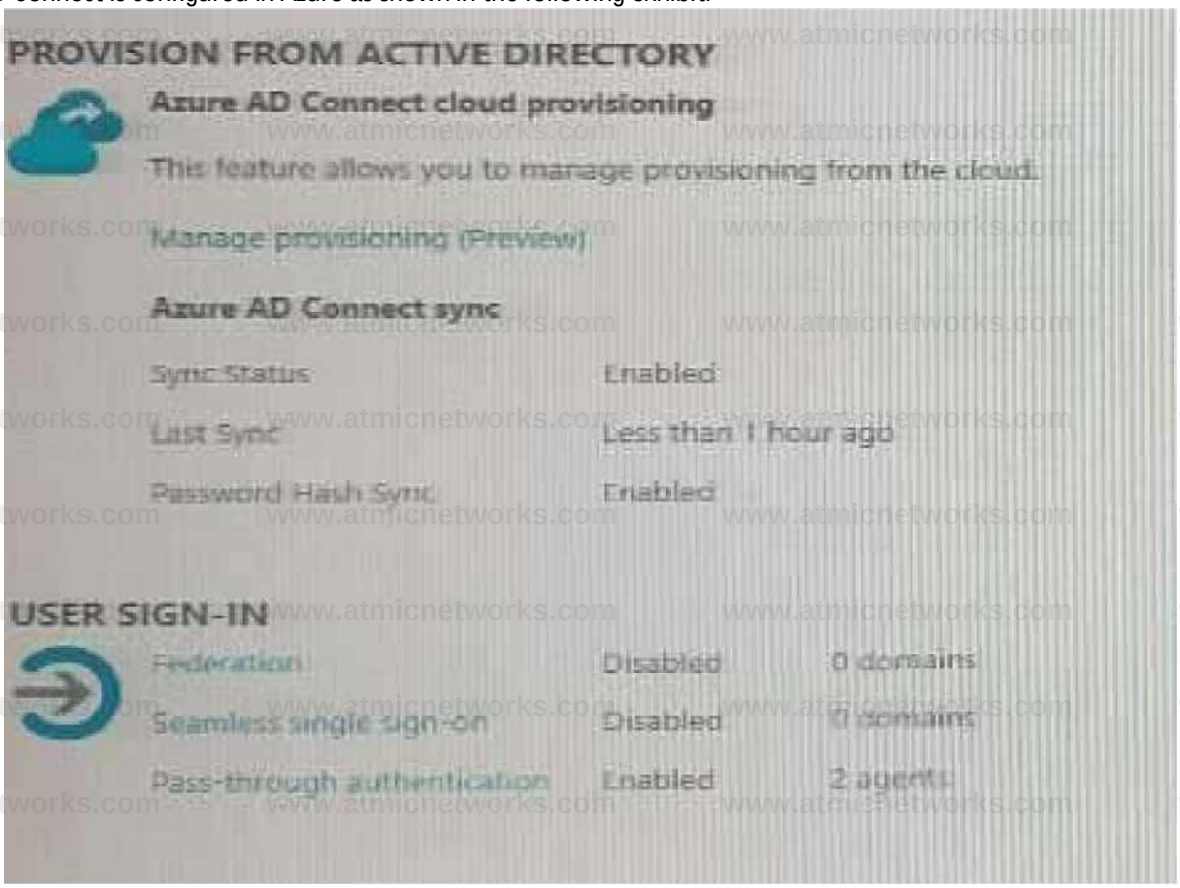
Explanation:

Question: 58

Your network contains an on-premises Active Directory domain that sync to an Azure Active Directory (Azure AD) tenant. The tenant contains the shown in the following table.

Name	Type	Directory synced
User1	User	No
User2	User	Yes
User3	Guest	No

All the users work remotely.
Azure AD Connect is configured in Azure as shown in the following exhibit.



Connectivity from the on-premises domain to the internet is lost.
Which user can sign in to Azure AD?

A. User1 only
B. User1 and User 3 only
C. User1, and User2 only
D. User1, User2, and User3

Answer: B

Explanation:

Question: 59

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

You need to ensure that Azure AD External Identities pricing is based on monthly active users (MAU). What should you configure?

A. an access review
B. the terms or use
C. a linked subscription
D. a user flow

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/external-identities- pricing

Question: 60

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

- A device named Device1
- Users named User1, User2, User3, User4, and User5
- Five groups named Group1, Group2, Group3, Ciroup4, and Group5

The groups are configured as shown in the following table.

Name			Members
Gioupl	Security	Assigned	Used. User3, Group/. Gioup4
Group?	Security	Dynamic User	Uset2
Groups	Security	Dynamic Device	Devree 1
Grnup4	Microsoft 365	Assigned	Groups
GioupS	Microsoft 3&>	Assigned	User5

How many licenses are used if you assign the Microsoft Office 365 Enterprise E5 license to Group1?

A. 0
B. 2
C. 3
D. 4

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced

Question: 61

DRAG DROP

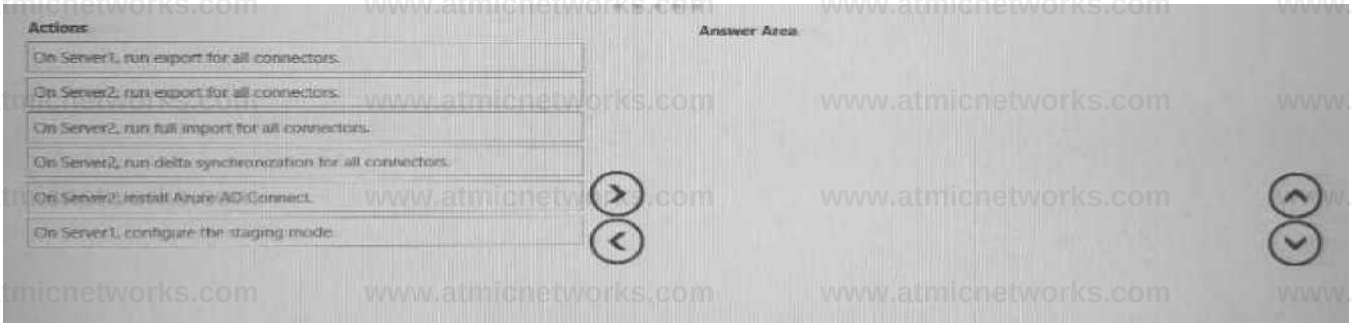
Your network contains an Active Directory forest named contoso.com that is linked to an Azure Active Directory (Azure AD) tenant named contoso.com by using Azure AD Connect.

Attire AD Connect is installed on a server named Server 1.

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

You need to implement a failover server for Azure AD Connect. The solution must minimize how long it takes to fail over if Server1 fails.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:

Explanation:

Answer:

Question: 62

You have a Microsoft Exchange organization that uses an SMTP' address space of contoso.com.

Several users use their contoso.com email address for self-service sign up to Azure Active Directory (Azure AD).

You gain global administrator privileges to the Azure AD tenant that contains the self-signed users. You need to prevent the users from creating user accounts in the contoso.com Azure AD tenant for self-service sign-up to Microsoft 365 services.

Which PowerShell cmdlet should you run?

A. Set-MsolCompanySettings
B. Set-MsolDomainFederationSettings
C. Update-MsolfederatedDomain
D. Set-MsolDomain

Answer: C

Explanation:

https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/directory-self-service- signup

Question: 63

HOTSPOT

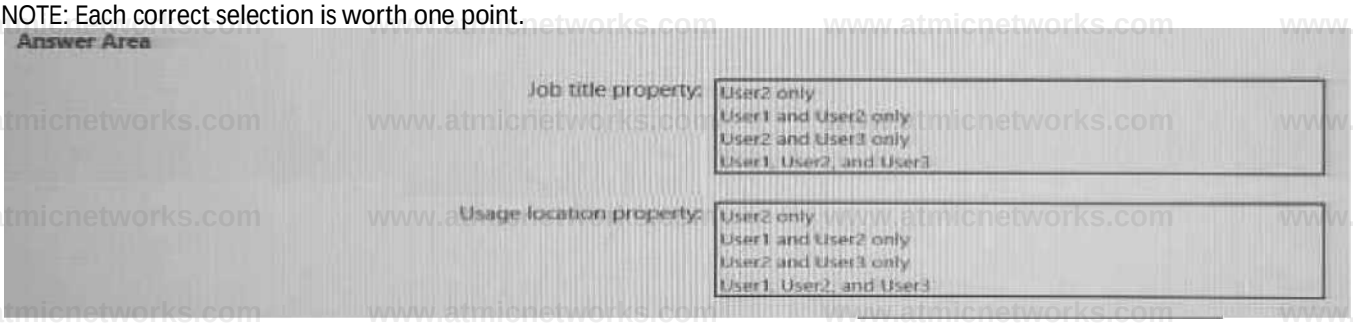
You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Type	Directory synced
User1	Member	Yes
User2	Member	No
User3	Guest	No

For which users can you configure the Job title property and the Usage location property in Azure AD?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Explanation:

Answer:

User1, User2, and User3

User2 only

Question: 64

HOTSPOT

Name	Type	Membership type
Group1	Security	Assigned
Group2	Security	Dynamic User
Group3	Security	Dynamic Device
Group4	Microsoft 365	Assigned

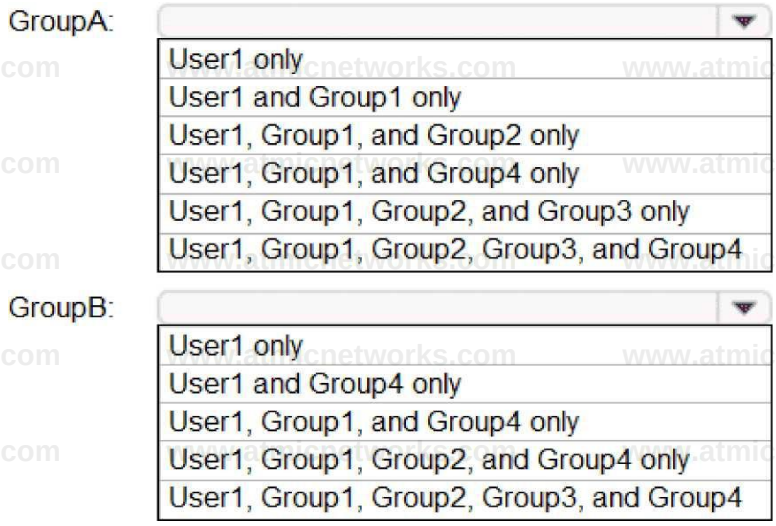
You have an Azure Active Directory (Azure AD) tenant that contains a user named User1 and the groups shown in the following table.

In the tenant, you create the groups shown in the following table.

Name	Type	Membership type
GroupA	Security	Assigned
GroupB	Microsoft 365	Assigned

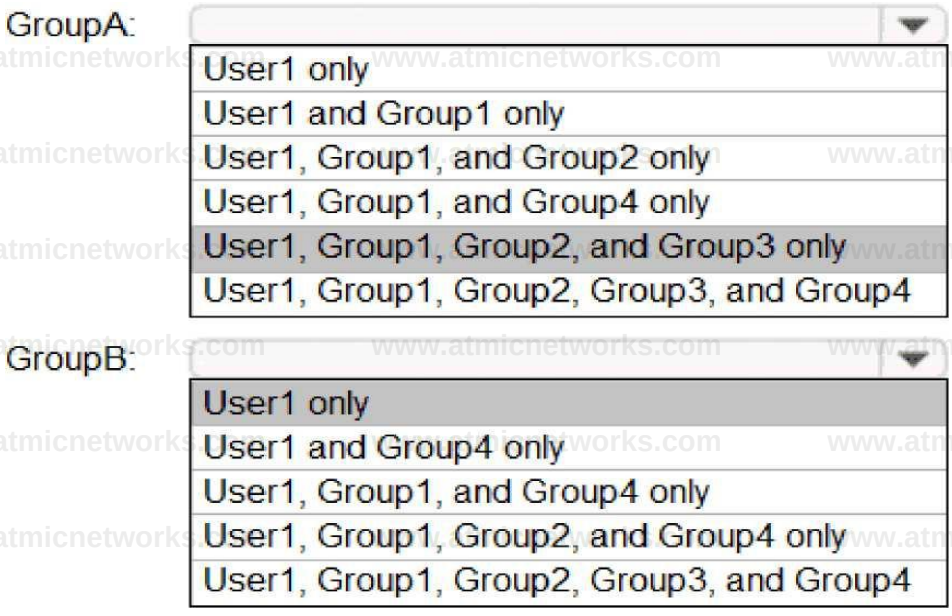
Which members can you add to GroupA and GroupB? To answer, select the appropriate options in the answer area.

NOTE:Each correct selection is worth one point.



Answer:

Explanation:



Reference:
https://bitsizedbytes.wordpress.com/2018/12/10/distribution-security-and-office-365-groups- nesting/

Question: 65

Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant
Users sign in to computers that run Windows 10 and are joined to the domain.
You plan to implement Azure AD Seamless Single Sign-On (Azure AD Seamless SSO).
You need to configure the computers for Azure AD Seamless SSO.
What should you do?

A. Enable Enterprise State Roaming.
B. Configure Sign-in options.
C. Install the Azure AD Connect Authentication Agent.
D. Modify the Intranet Zone settings.

Answer: D

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-quick-start

Question: 66

DRAG DROP

You have a new Microsoft 365 tenant that uses a domain name of contoso.onmicrosoft.com.

You register the name contoso.com with a domain registrar.

You need to use contoso.com as the default domain name for new Microsoft 365 users.

Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
Delete the contoso.onmicrosoft.com domain.	
Register a custom domain name of contoso.com.	
Set the domain to primary.	
Create a new TXT record in DNS.	
Verify the domain name.	

Answer:

Explanation:

Register a custom domain name of contoso.com.

Create a new TXT record in DNS.

Verify the domain name.

Set the domain to primary.

Reference:
https://practical365.com/configure-a-custom-domain-in-office-365/

Question: 67

You use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.

Yon receive more than 100 email alerts each day for tailed Azure Al) user sign-in attempts.
You need to ensure that a new security administrator receives the alerts instead of you. Solution: From

Azure AD, you create an assignment for the Insights at administrator role. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Question: 68

You use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.
Yon receive more than 100 email alerts each day for tailed Azure Al) user sign-in attempts.
You need to ensure that a new security administrator receives the alerts instead of you.
Solution: From Azure monitor, you modify the action group.
Does this meet the goal?

A. Yes
C. No

Answer: B

Explanation:

Question: 69

You use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.
Yon receive more than 100 email alerts each day for tailed Azure Al) user sign-in attempts.
You need to ensure that a new security administrator receives the alerts instead of you.
Solution: From Azure monitor, you create a data collection rule.
Does this meet the goal?

A. Yes
D. No

Answer: B

Explanation:

Question: 70

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 Block/unblock users settings for multi-factor authentication (MFA).

Does this meet the goal?

A. Yes

E. No

Answer: B

Explanation:

You need to configure the fraud alert settings.

Reference:

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

Question: 71

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 Account lockout settings for multi-factor authentication (MFA).

Does this meet the goal?

A. Yes

F. No

Answer: B

Explanation:

You need to configure the fraud alert settings.

Reference:

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

Question: 72

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

Answer: A

Explanation:

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:

Automatically block users who report fraud.

Code to report fraud during initial greeting.

Reference:

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

Question: 73

You have an Azure Active Directory (Azure AD) tenant that contains the following objects:

A device named Device1

Users named User1, User2, User3, User4, and User5

Groups named Group1, Group2, Group3, Group4, and Group5

The groups are configured as shown in the following table.

Name	Type	Membership type	Members
Groupl	Security	Assigned	Useri User3, Group? Group3
Group?	Security	Dynamic User	User?
Group3	Security	Dynamic Device	Devicel
Group4	Microsoft 365	Assigned	User4
Group5	Microsoft 365	Dynamic User	User5

To which groups can you assign a Microsoft Office 365 Enterprise E5 license directly?

A. Group1 and Group4 only
B. Group1, Group2, Group3, Group4, and Group5
C. Group1 and Group2 only
D. Group1 only
E. Group1, Group2, Group4, and Group5 only

Answer: C

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced

Question: 75

You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users.
From the Groups blade in the Azure Active Directory admin center, you assign Microsoft 365 Enterprise E5 licenses to the users.
You need to remove the Office 365 Enterprise E3 licenses from the users by using the least amount of administrative effort.
What should you use?

A. the Identity Governance blade in the Azure Active Directory admin center
B. the Set-AzureAdUser cmdlet
C. the Licenses blade in the Azure Active Directory admin center
D. the Set-WindowsProductKey cmdlet

Answer: B

Explanation:

Box 1: Yes

Invitations can only be sent to outlook.com. Therefore, User1 can accept the invitation and access the application.

Box 2. Yes

Invitations can only be sent to outlook.com. However, User2 has already received and accepted an invitation so User2 can access the application.

Box 3. No

Invitations can only be sent to outlook.com. Therefore, User3 will not receive an invitation.

Question: 77

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: A,B

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/external-identities/tutorial-bulk-invite

Question: 78

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

Name	Type	Directly assigned license
Useri	User	*None*
User2	User	Microsoft Office 365 Enterprise E5
Group 1	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:

Reference:
https://bitsizedbytes.wordpress.com/2018/12/10/distribution-security-and-office-365-groups- nesting/

Question: 79

DRAG DROP

You have an on-premises Microsoft Exchange organization that uses an SMTP address space of contoso.com.

You discover that users use their email address for self-service sign-up to Microsoft 365 services.

You need to gain global administrator privileges to the Azure Active Directory (Azure AD) tenant that contains the self-signed users.

Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Sign in to the Microsoft 365 admin center.

Create a seif-signed user account in the Azure AD tenant.

From the Microsoft 365 admin center, add the domain name.

Respond to the Become the admin message.

From the Microsoft 365 admin center, remove the domain name.

Create a TXT record in the contoso.com DNS zone

Answer Area

Answer:

Explanation:

Create a self-signed user account in the Azure AD tenant.

Sign in to the Microsoft 365 admin center.

Respond to the Become the admin message.

Create a TXT record in the contoso.com DNS zone.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/domains-admin-takeover

Question: 80

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 password writeback.

Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

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

Question: 81

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

Question: 82

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 conditional access policies.

Does this meet the goal?

A. Yes
B. No

Answer: B

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

Question: 83

HOTSPOT

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 theUserstab.)

Dashboard > ContosoAiureAD > Department! Administrative Unit

. Departmentl Administrative Unit | Users (Preview)

ContcsoArureAD Acute Active Directory

■ Add member : I ~ Bulk operations v Q Refresh == Columns 0 Preview features \2 Got feedback?

Q This page incudes previews ava ao'-e for your evaluation. View previews "♦

P Search users †V Add filters

2 users found

Name	T User principal name	u User type	Directory synced
Q ^ User!	UserI@m365x629615.onmicrosoft.com	Member	No
□ ^ User2	User2@m365x629615.onmicrosoft.com	Member	No

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

Dashboard > ContosoAzureAD > Department1 Administrative Unit

Department1 Administrative Unit | Groups

ContosoAzureAD - Azure Active Directory

» + Add | Remove | Refresh | Columns | Preview features | Got feedback?

Search groups | Add filters

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 theAssignmentstab.)

Dashboard > ContosoAzureAD > Identity Governance > Privileged Identity Management > ContosoAzureAD

User Administrator | Assignments

Privileged Identity Management | Amie AD roles

+ Add assignments @ Settings 0 Refresh ^ Export 9? Got feedback?

Eligible assignments Active assignments Expired assignments

P Search by member name or principal name

Name	Principal name	Type	Scope	
User Administration				
Adminl	Adminl@m365x629615.onmicrosoft.com	User	trfaiim, l tl - l [1] •' ■	(Administrative unit)
Admin2	Admin2@m365x629615.onmicrosoft.com	User	Directory	

The members of Group2 are shown in the Group2 exhibit. (Click theGroup2tab.)

Dashboard > ContosoAzureAD Groups > Group2

• Group2 | Members

Group

Add members Q Refresh Pi Bulk operations v Columns Ei Preview features Got feedback?

Q This page includes previews available for your evaluation. View previews ~*.

Direct members

Name	User type
	Member
[1]| User3	Member
0 0 User4	

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

NOTE:Each correct selection is worth one point.

Statements	Yes	No
Adminl can reset the passwords of User3 and User4.	O	O
Adminl can add Useri to Group 2	0	0
Admin 2 can reset the password of Useri.	O	O

Answer:

Explanation:

Statements	Yes	No
Adminl can reset the passwords of User3 and User4.	O	O
Adminl can add Useri to Group 2	0	0
Admin 2 can reset the password of Useri.	O	O

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units

Question: 84

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 nonadministrative 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: C

Explanation:

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

Question: 85

You configure Azure Active Directory (Azure AD) Password Protection as shown in the exhibit. (Click theExhibittab.)

Custom smart lockout

Lockout threshold	5
Lockout duration in seconds Q	3600

Custom banned passwords

Enforce custom list 0	[(Yes No
Custom banned password list 0	Contoso v* Litware Tailwind project Zettabyte Ma in Street

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory Q I|^^^^B No

ModeO Enforced

You are evaluating the following passwords:

Pr0jectlitw@re
T@ilw1nd
C0nt0s0

Which passwords will be blocked?

A. Pr0jectlitw@re and T@ilw1nd only
B. C0nt0s0 only
C. C0nt0s0, Pr0jectlitw@re, and T@ilw1nd
D. C0nt0s0 and T@ilw1nd only
E. C0nt0s0 and Pr0jectlitw@re only

Answer: C

Explanation:
Reference:
https://blog.enablingtechcorp.com/azure-ad-password-protection-password-evaluation

Question: 86

You have a Microsoft 365 tenant.
All users have mobile phones and laptops.
The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity.
While working from the remote locations, the users connect their laptop to a wired network that has internet access.
You plan to implement multi-factor authentication (MFA).
Which MFA authentication method can the users use from the remote location?

A. a notification through the Microsoft Authenticator app
B. security questions
C. voice
D. an app password

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication- authenticator-app#verification-code-from-mobile-app

Question: 87

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:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals- security-defaults

Question: 88

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:

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

Question: 89

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:

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy- authentication

Question: 90

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:

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

Question: 91

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:

Reference:
https://docs.microsoft.com/en-us/cloud-app-security/proxy-intro-aad

Question: 92

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

Answer: C

Explanation:

Question: 93

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:

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

Question: 94

HOTSPOT

You have a Microsoft 365 tenant.

Sometimes, users use external, third-party applications that require limited access to the Microsoft 365 data of the respective user. The users register the applications in Azure Active Directory (Azure AD).

You need to receive an alert if a registered application gains read and write access to the users' email.

What should you do? To answer, select the appropriate options in the answer area.

NOTE:Each correct selection is worth one point.

Tool to use: I▼

Azure AD Identity Protection

Identity Governance

Microsoft Cloud App Security Microsoft Endpoint Manager

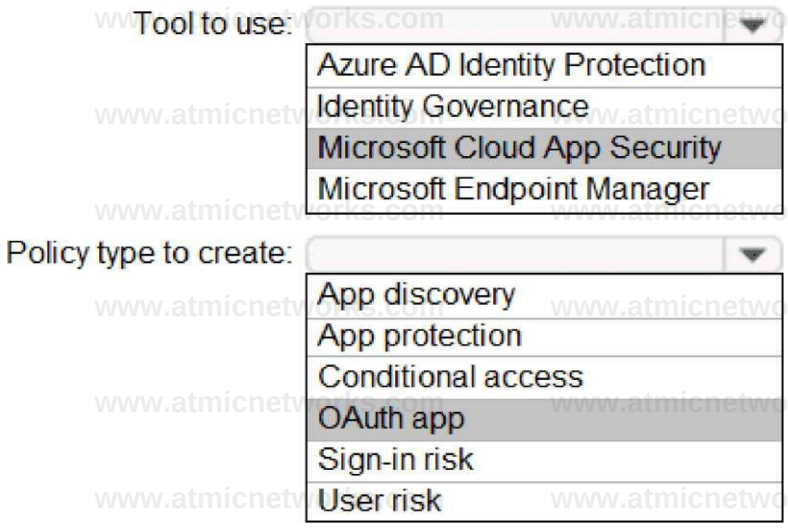
Policy type to create:

App discovery App protection Conditional access

OAuth app Sign-in risk User risk

Answer:

Explanation:



Reference:
https://docs.microsoft.com/en-us/cloud-app-security/app-permission-policy

Question: 95

You have a Microsoft 365 tenant.

The Azure Active Directory (Azure AD) tenant syncs to an on-premises Active Directory domain.

Users connect to the internet by using a hardware firewall at your company. The users authenticate to the firewall by using their Active Directory credentials.

You plan to manage access to external applications by using Azure AD.

You need to use the firewall logs to create a list of unmanaged external applications and the users who access them.

What should you use to gather the information?

A. Application Insights in Azure Monitor
B. access reviews in Azure AD
C. Cloud App Discovery in Microsoft Cloud App Security
D. enterprise applications in Azure AD

Answer: C

Explanation:

Reference:

https://docs.microsoft.com/en-us/cloud-app-security/create-snapshot-cloud-discovery-reports#using-traffic-logs-for-cloud-discovery

Question: 96

HOTSPOT

You have an on-premises datacenter that contains the hosts shown in the following table.

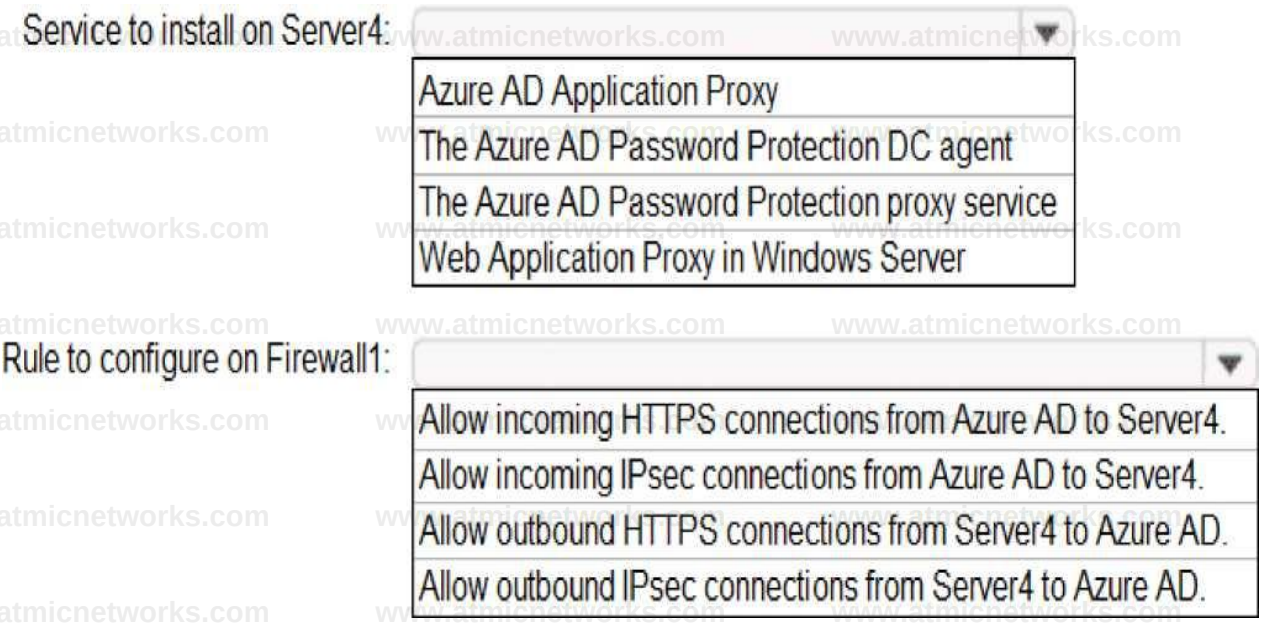
Name	Description
Serveri	Domain controller that runs Windows Server 2019
Server2	Server that runs Windows Server 2019 and has Azure AD Connect deployed
Server3	Server that runs Windows Server 2019 and has a Microsoft ASP.NET application named App1 installed
Server4	Unassigned server that runs Windows Server 2019
Firewall 1	Hardware firewall connected to the internet that blocks all traffic unless explicitly allowed

You have an Azure Active Directory (Azure AD) tenant that syncs to the Active Directory forest. Multifactor authentication (MFA) is enforced for Azure AD.

You need to ensure that you can publish App1 to Azure AD users.

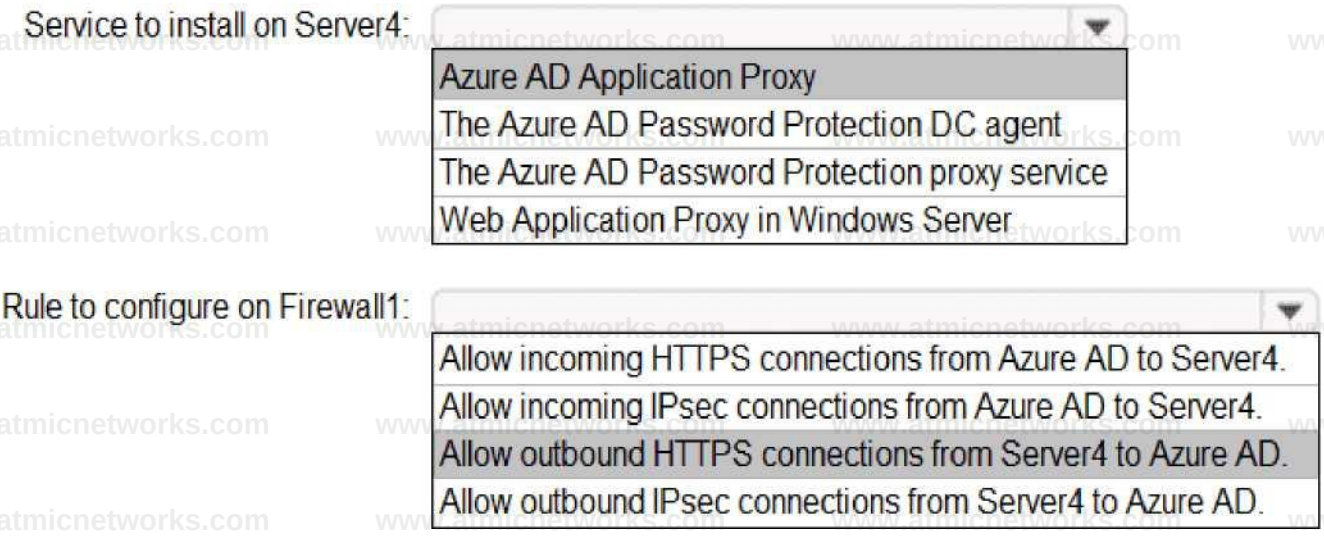
What should you configure on Server and Firewall1? To answer, select the appropriate options in the answer area.

NOTE:Each correct selection is worth one point.



Answer:

Explanation:



Reference:

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy

Question: 97
HOTSPOT

You have an Azure Active Directory (Azure AD) tenant that has the default App registrations settings.
The tenant contains the users shown in the following table.

Name	Role
Adminl	Application administrator
Admin2	Application developer
Admin3	C oud application administrator
Useri	User

You purchase two cloud apps named App1 and App2. The global administrator registers App1 in Azure AD.

You need to identify who can assign users to App1, and who can register App2 in Azure AD.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE:Each correct selection is worth one point.

Can assign users to App 1: ▼

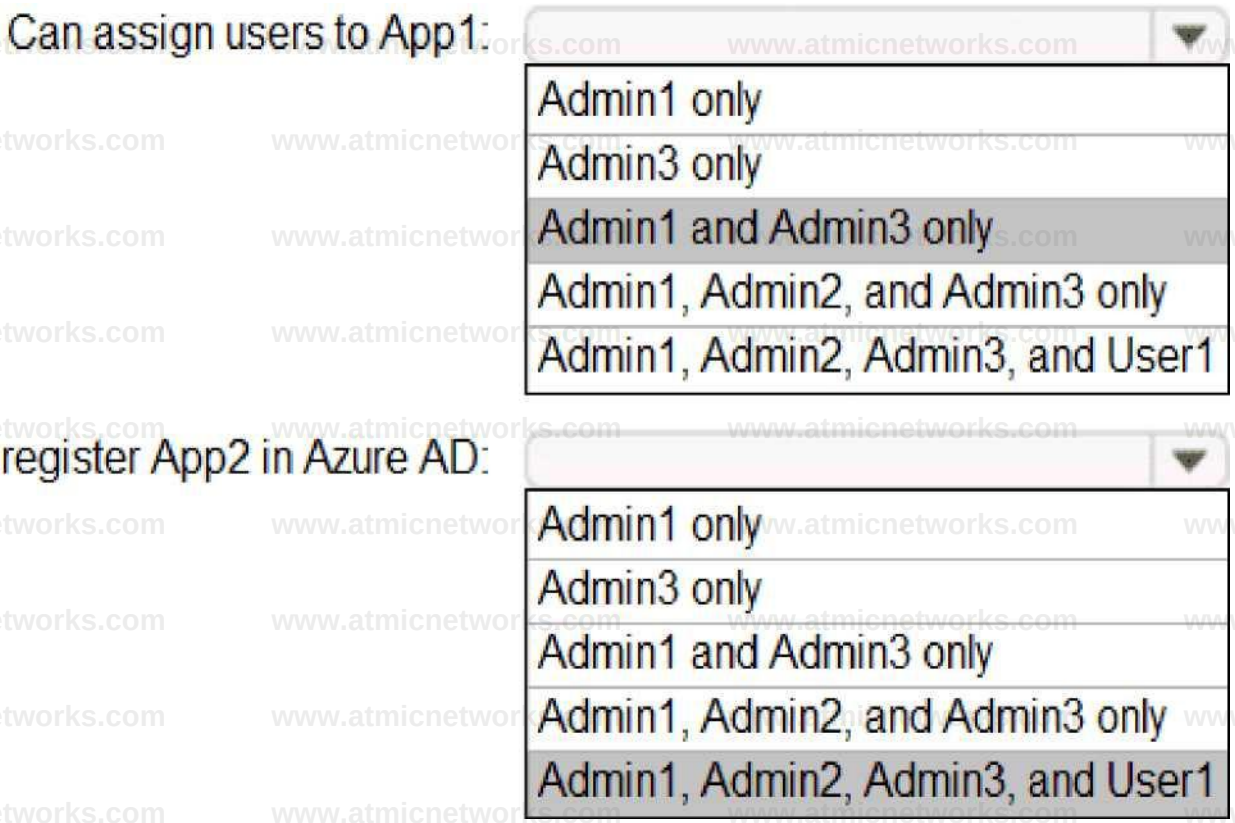
- Adminl only
- Admin3 only
- Adminl and Admin3 only
- Adminl, Admin2, and Admin3 only
- Adminl, Admin2, Admin3, and Useri

Can register App2 in Azure AD: ▼

- Adminl only
- Admin3 only
- Adminl and Admin3 only
- Adminl, Admin2, and Admin3 only
- Adminl, Admin2, Admin3, and Useri

Answer:

Explanation:



Reference:

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal- assign-users

https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how- applications-are-added

Question: 98

You have a Microsoft 365 tenant.

The Azure Active Directory (Azure AD) tenant syncs to an on-premises Active Directory domain.

You plan to create an emergency-access administrative account named Emergency1. Emergency1 will be assigned the Global administrator role in Azure AD. Emergency1 will be used in the event of Azure AD functionality failures and on-premises infrastructure failures.

You need to reduce the likelihood that Emergency1 will be prevented from signing in during an emergency.

What should you do?

A. Configure Azure Monitor to generate an alert if Emergency1 is modified or signs in.
B. Require Azure AD Privileged Identity Management (PIM) activation of the Global administrator role forEmergency1.
C. Configure a conditional access policy to restrict sign-in locations for Emergency1 to only the corporatenetwork.
D. Configure a conditional access policy to require multi-factor authentication (MFA) for Emergency1.

Answer: A

Explanation:

Question: 99

You have a Microsoft 365 tenant.

In Azure Active Directory (Azure AD), you configure the terms of use.

You need to ensure that only users who accept the terms of use can access the resources in the tenant. Other users must be denied access.

What should you configure?

A. an access policy in Microsoft Cloud App Security.
B. Terms and conditions in Microsoft Endpoint Manager.
C. a conditional access policy in Azure AD
D. a compliance policy in Microsoft Endpoint Manager

Answer: C

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use

Question: 100

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

Name	> Type	Membership type
Group!	Security	Assigned
Group2	Security	Dynamic User
Group3	Security	Dynamic Device
Group4	Microsoft 365	Assigned
Group5	Microsoft 365	Dynamic User

For which groups can you create an access review?

A. Group1 only
B. Group1 and Group4 only
C. Group1 and Group2 only
D. Group1, Group2, Group4, and Group5 only
E. Group1, Group2, Group3, Group4 and Group5

Answer: D

Explanation:

You cannot create access reviews for device groups.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

Question: 101

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

Name	Type	Member of
Useri	Member	Groupl
User2	Member	Groupl
User3	Guest	Groupl

User1 is the owner of Group1.

You create an access review that has the following settings:

Users to review: Members of a group

Scope: Everyone

Group: Group1

Reviewers: Members (self)

Which users can perform access reviews for User3?

A. User1, User2, and User3
B. User3 only
C. User1 only
D. User1 and User2 only

Answer: B

Explanation:

Question: 102

HOTSPOT

You have an Azure Active Directory (Azure AD) tenant that contains Azure AD Privileged Identity Management (PIM) role settings for the User administrator role as shown in the following exhibit.

... ContosoAzureAD Identity Governance Privileged Identity Management ContosoAzureAD User Administrator

Role setting details - User Administrator

Privileged Identity Management | Azure AD roles

X* Edit

Activation

SETTING	STATE
Activation maximum duration (hours)	8 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	Yes
Approvers	None

Assignment

SETTING	STATE
Allow permanent eligible assignment	No
Expire eligible assignments after	15day(s)
Allow permanent active assignment	No
Expire active assignments after	1 month(s)
Require Azure Multi-Factor Authentication on active assignment	No
Require justification on active assignment	No

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE:Each correct selection is worth one point.

A user who requires access to the User administration role must perform multi-factor authentication (MFA) every **[answer choice]**.

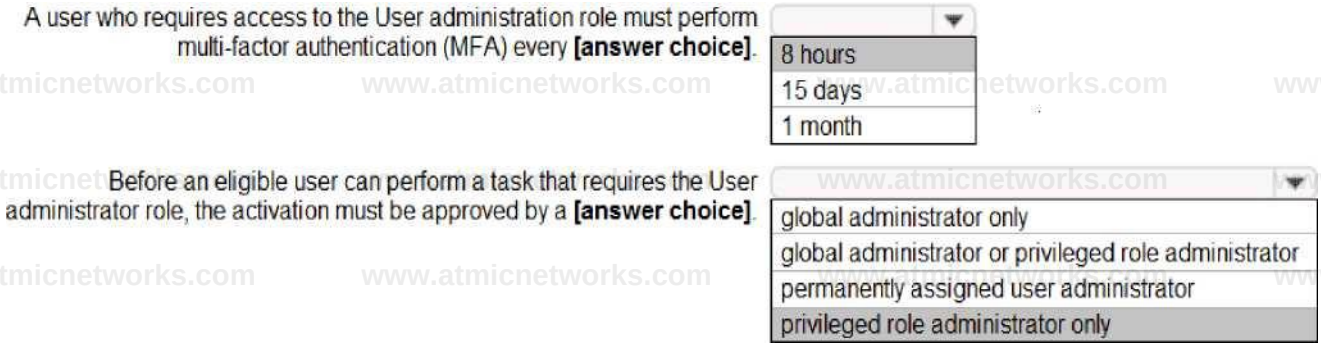
- 8 hours
- 15 days
- 1 month

Before an eligible user can perform a task that requires the User administrator role, the activation must be approved by a **[answer choice]**.

- global administrator only
- global administrator or privileged role administrator
- permanently assigned user administrator
- privileged role administrator only

Answer:

Explanation:



Reference:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim- configure

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim- deployment-plan

Question: 103

HOTSPOT

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1.

User1 has the devices shown in the following table.

Name	Platform	Registered in contoso.com
Devicel	Windows 10	Yes
Device?	Windows 10	No
Device3	iOS	Yes

On November 5, 2020, you create and enforce terms of use in contoso.com that has the following settings:

Name: Terms1

Display name: Contoso terms of use

Require users to expand the terms of use: On

Require users to consent on every device: On

Expire consents: On

Expire starting on: December 10, 2020

Frequency: Monthly

On November 15, 2020, User1 accepts Terms1 on Device3.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
On November 20,2020, Useri can accept Termsl on Devicel.	0	0
On December 11,2020, Useri can accept Termsl on Device2.	0	0
On December?, 2020, Useri can acceptTermsl on Devices.	0	O

Answer:

Explanation:

Statements	Yes	No
On November20,2020, Useri can accept Termsl on Devicel.	O	0
On December 11,2020, Useri can accept Termsl on Device2.	O	0
On December 7,2020, Useri can acceptTermsl on Devices.	0	0

Question: 104

Your company recently implemented Azure Active Directory (Azure AD) Privileged Identity Management (PIM).

While you review the roles in PIM, you discover that all 15 users in the IT department at the company have permanent security administrator rights.

You need to ensure that the IT department users only have access to the Security administrator role when required.

What should you configure for the Security administrator role assignment?

A. Expire eligible assignments after from the Role settings details
B. Expire active assignments after from the Role settings details
C. Assignment type to Active
D. Assignment type to Eligible

Answer: D

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim- configure

Question: 105

You have a Microsoft 365 tenant.

The Sign-ins activity report shows that an external contractor signed in to the Exchange admin center. You need to review access to the Exchange admin center at the end of each month and block sign-ins if required.

What should you create?

A. an access package that targets users outside your directory
B. an access package that targets users in your directory
C. a group-based access review that targets guest users
D. an application-based access review that targets guest users

Answer: C

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

Question: 106

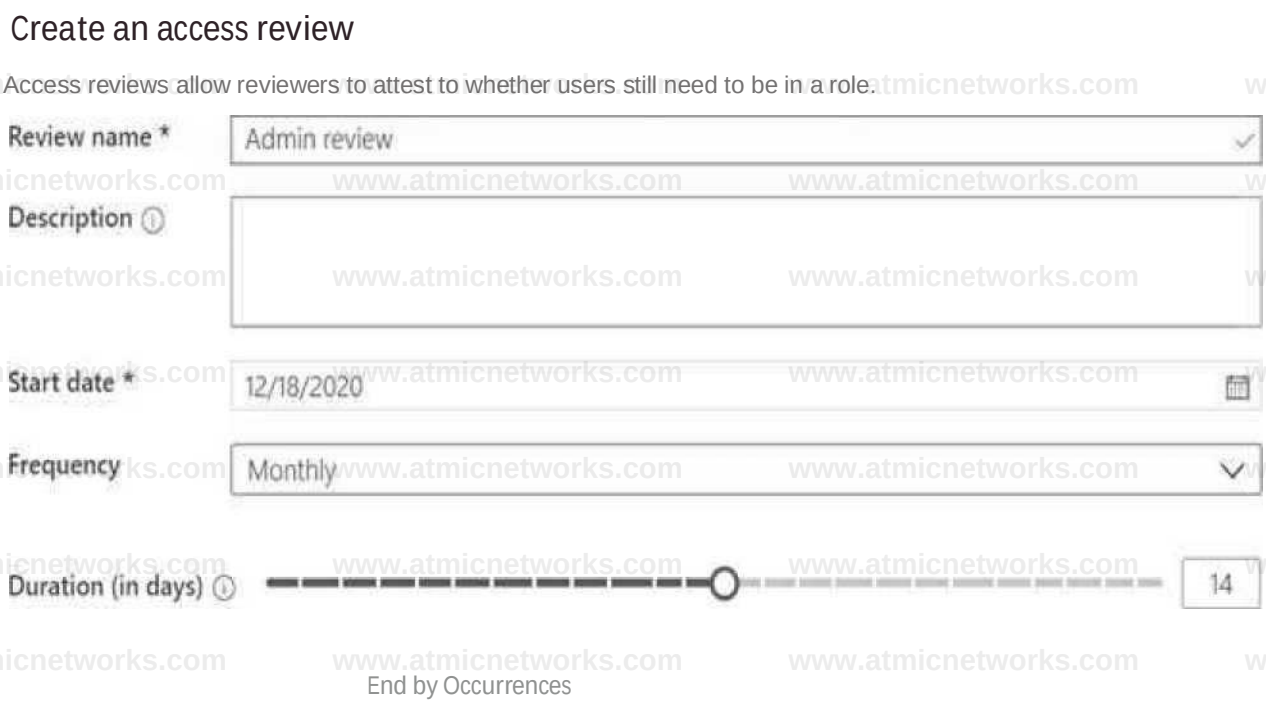
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 a Microsoft 365 tenant.

You have 100 IT administrators who are organized into 10 departments.

You create the access review shown in the exhibit. (Click theExhibittab.)



You discover that all access review requests are received by Megan Bowen.

You need to ensure that the manager of each department receives the access reviews of their respective department.

Solution: You create a separate access review for each role.

Does this meet the goal?

A. Yes

B. NoD18912E1457D5D1DDCBD40AB3BF70D5D

Answer: B

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

Question: 107

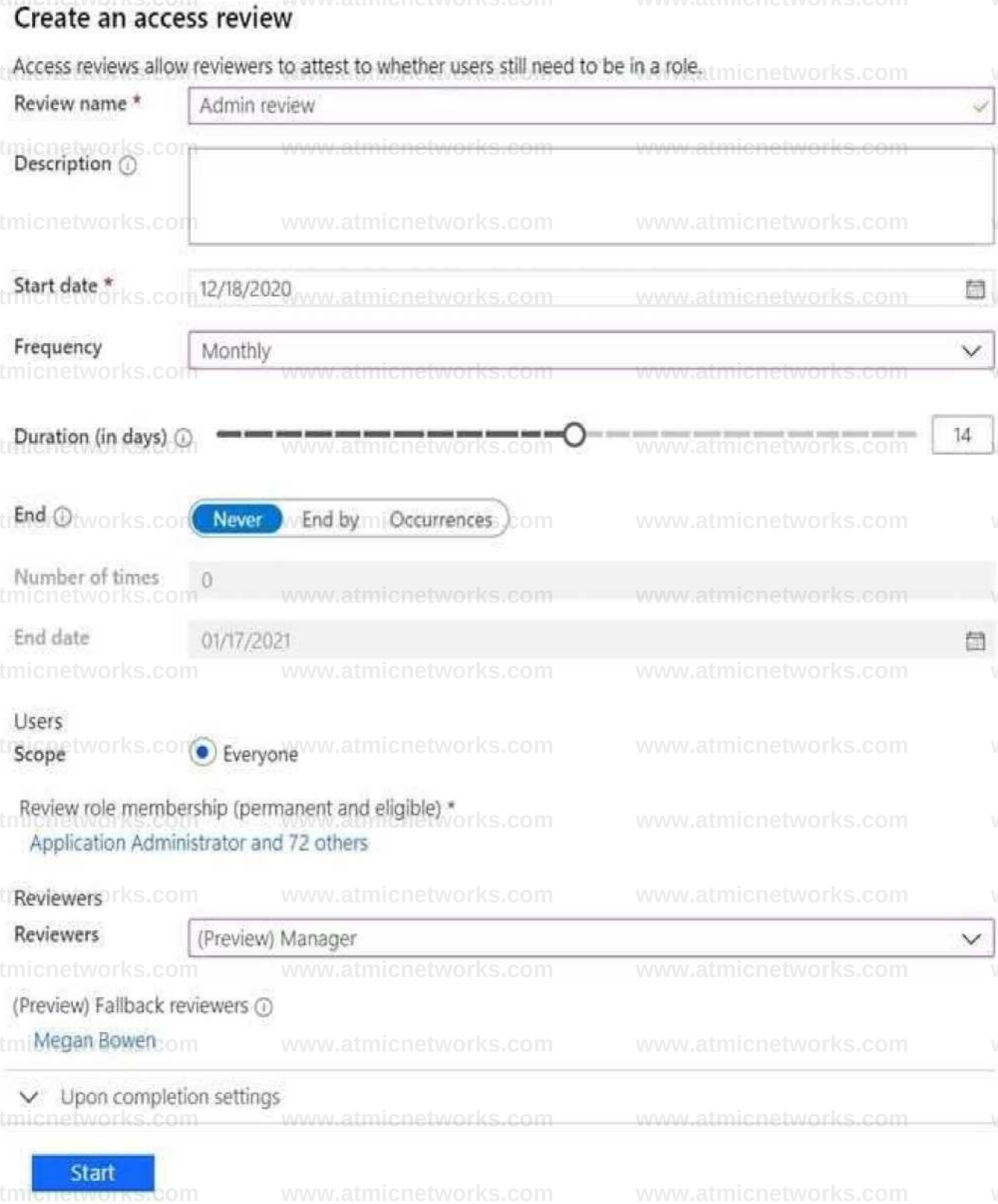
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 a Microsoft 365 tenant.

You have 100 IT administrators who are organized into 10 departments.

You create the access review shown in the exhibit. (Click theExhibittab.)



You discover that all access review requests are received by Megan Bowen.

You need to ensure that the manager of each department receives the access reviews of their respective department.

Solution: You modify the properties of the IT administrator user accounts.

Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:

Reference:
D18912E1457D5D1DDCBD40AB3BF70D5D
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

Question: 108

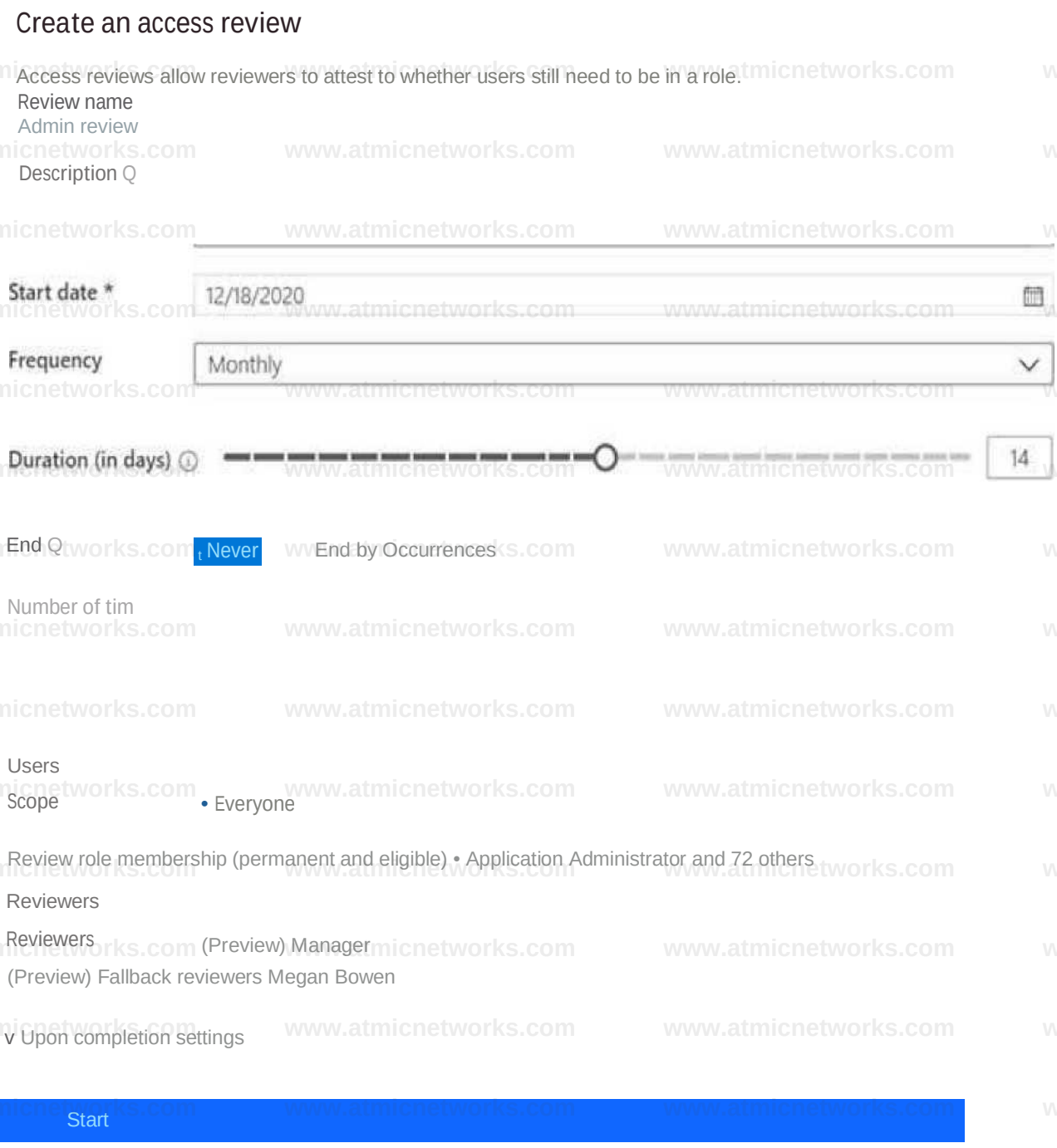
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 a Microsoft 365 tenant.

You have 100 IT administrators who are organized into 10 departments.

You create the access review shown in the exhibit. (Click theExhibittab.)



You discover that all access review requests are received by Megan Bowen.

You need to ensure that the manager of each department receives the access reviews of their respective department.

Solution: You set Reviewers toMember (self).

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Question: 109

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains an Azure AD enterprise application named App1.

A contractor uses the credentials of user1@outlook.com.

You need to ensure that you can provide the contractor with access to App1. The contractor must be able to authenticate as user1@outlook.com.

What should you do?

A. Run the New-AzADUser cmdlet.
B. Configure the External collaboration settings.
C. Add a WS-Fed identity provider.
D. Create a guest user account in contoso.com.

Answer: D

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-usersportal

Question: 110

Your network contains an Active Directory forest named contoso.com that is linked to an Azure Active Directory (Azure AD) tenant named contoso.com by using Azure AD Connect.

You need to prevent the synchronization of users who have the extensionAttribute15 attribute set to NoSync.

What should you do in Azure AD Connect?

A. Create an inbound synchronization rule for the Windows Azure Active Directory connector.
B. Configure a Full Import run profile.
C. Create an inbound synchronization rule for the Active Directory Domain Services connector.
D. Configure an Export run profile.

Answer: C

Explanation:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the- configuration

Question: 111

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

Name	Type	Directory synced
Useri	User	No
User2	User	Yes
User3	Guest	No

All the users work remotely.

Azure AD Connect is configured in Azure AD as shown in the following exhibit.

PROVISION FROM ACTIVE DIRECTORY

1- Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

Manage provisioning (Preview)

Azure AD Connect sync

Sync Status	Enabled
Last Sync	Less than 1 hour ago
	Password Hash Sync Enabled

USER SIGN IN

Federation	Disabled	0 domains
Seamless single sign-on	Disabled	0 domains
Pass-through authentication	Enabled	2 agents

Connectivity from the on-premises domain to the internet is lost.

Which users can sign in to Azure AD?

A. User1 and User3 only
B. User1 only
C. User1, User2, and User3
D. User1 and User2 only

Answer: A

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-current- limitations

Question: 112

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:

Question: 113

HOTSPOT

You have a Microsoft 365 tenant and an Active Directory domain named adatum.com.

You deploy Azure AD Connect by using the Express Settings.

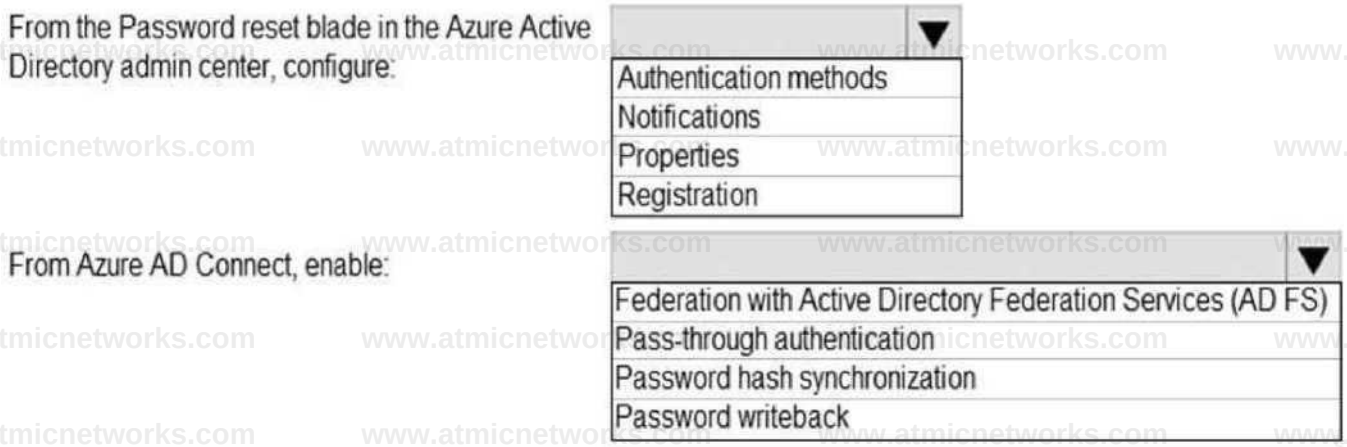
You need to configure self-service password reset (SSPR) to meet the following requirements:

When users reset their password, they must be prompted to respond to a mobile app notification or answer three predefined security questions.

Passwords must be synced between the tenant and the domain regardless of where the password was reset.

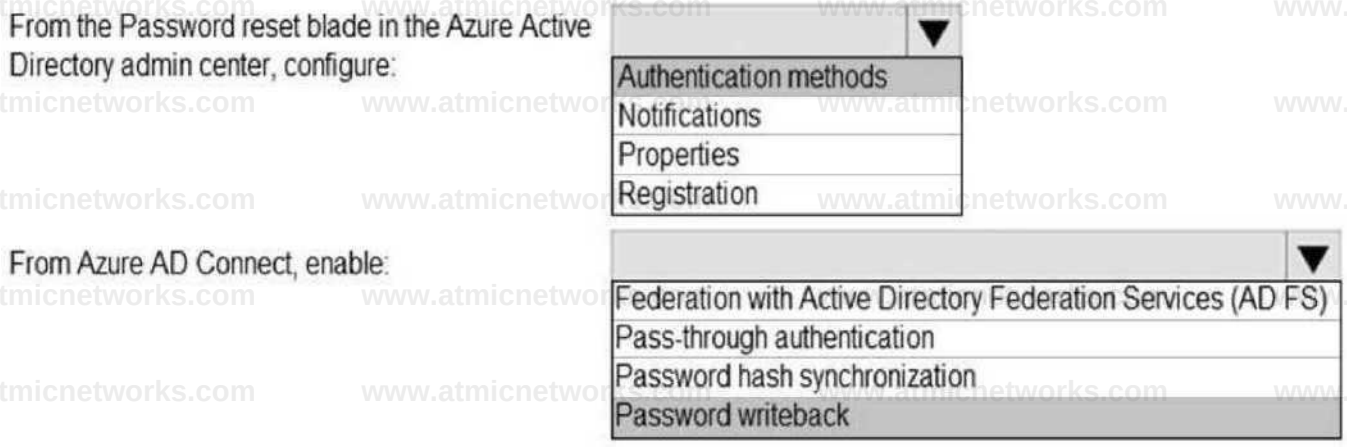
What should you do? To answer, select the appropriate options in the answer area.

NOTE:Each correct selection is worth one point.



Answer:

Explanation:



Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment

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

Question: 114

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

You implement entitlement management to provide resource access to users at a company named Fabrikam, Inc.

Fabrikam uses a domain named fabrikam.com.

Fabrikam users must be removed automatically from the tenant when access is no longer required.

You need to configure the following settings:

Block external user from signing in to this directory: No

Remove external user: Yes

Number of days before removing external user from this directory: 90

What should you configure on the Identity Governance blade?

A. Access packages
B. Entitlement management settings
C. Terms of use
D. Access reviews setting

Answer: B

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management- external-users

Question: 115

You have an Azure Active Directory (Azure AD) tenant.
You need to review the Azure AD sign-in logs to investigate sign-ins that occurred in the past.
For how long does Azure AD store events in the sign-in logs?

A. 14 days
B. 30 days
C. 90 days
D. 365 days

Answer: B

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-reports- dataretention#how-long-does-azure-ad-store-the-data

Question: 116

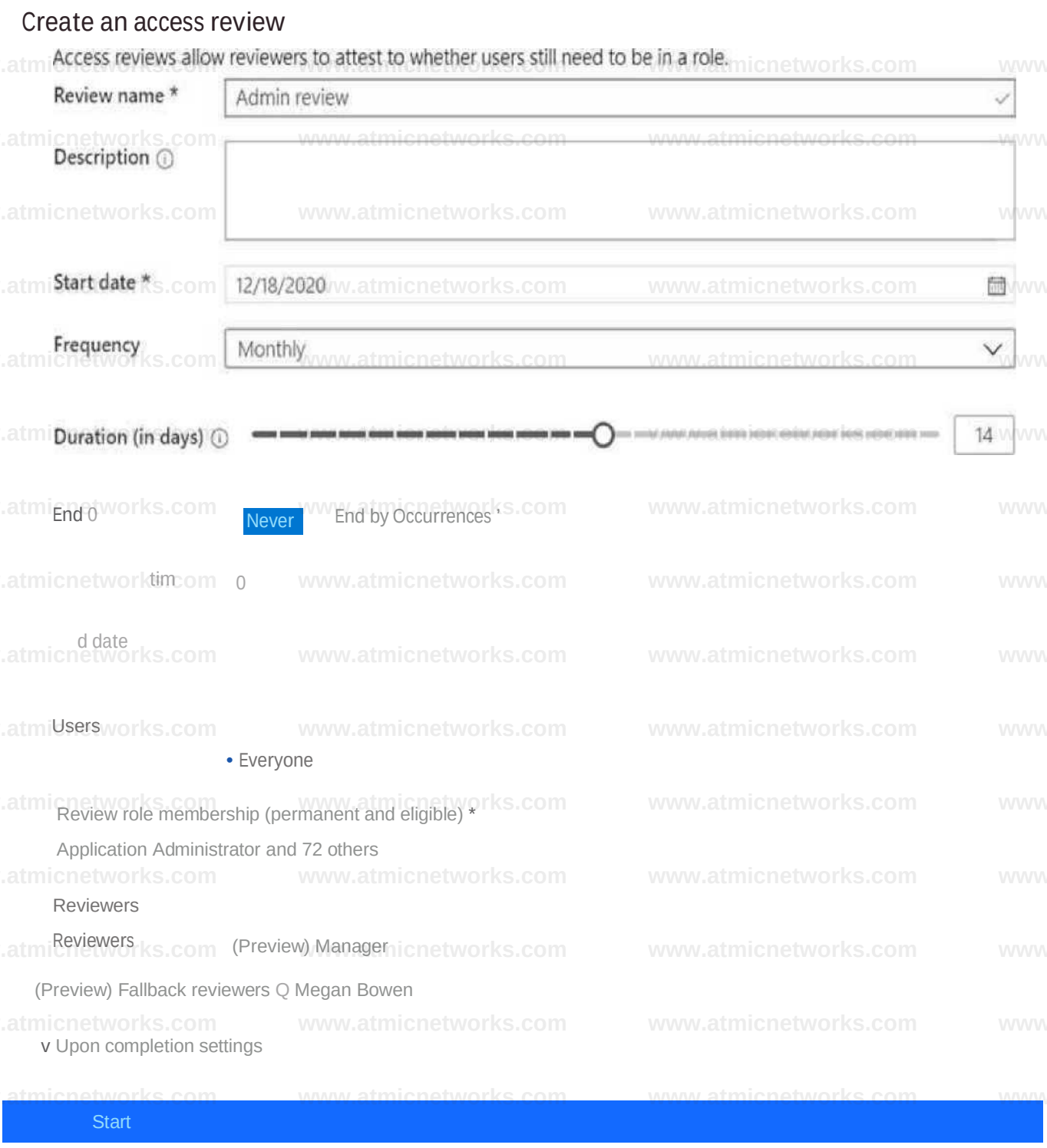
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 a Microsoft 365 tenant.

You have 100 IT administrators who are organized into 10 departments.

You create the access review shown in the exhibit. (Click theExhibittab.)



You discover that all access review requests are received by Megan Bowen.

You need to ensure that the manager of each department receives the access reviews of their respective department.

Solution: You add each manager as a fallback reviewer.

Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

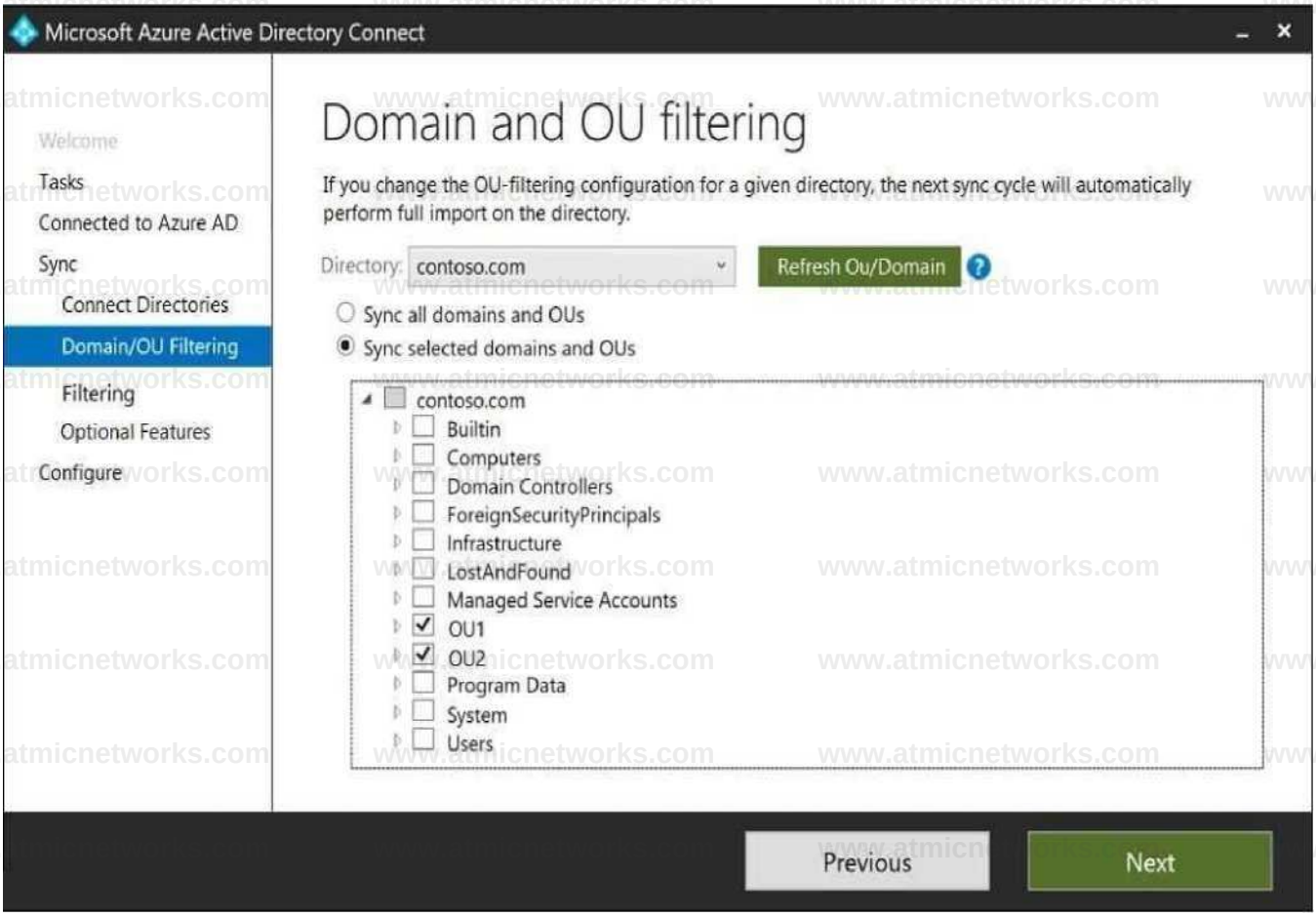
Question: 117

HOTSPOT

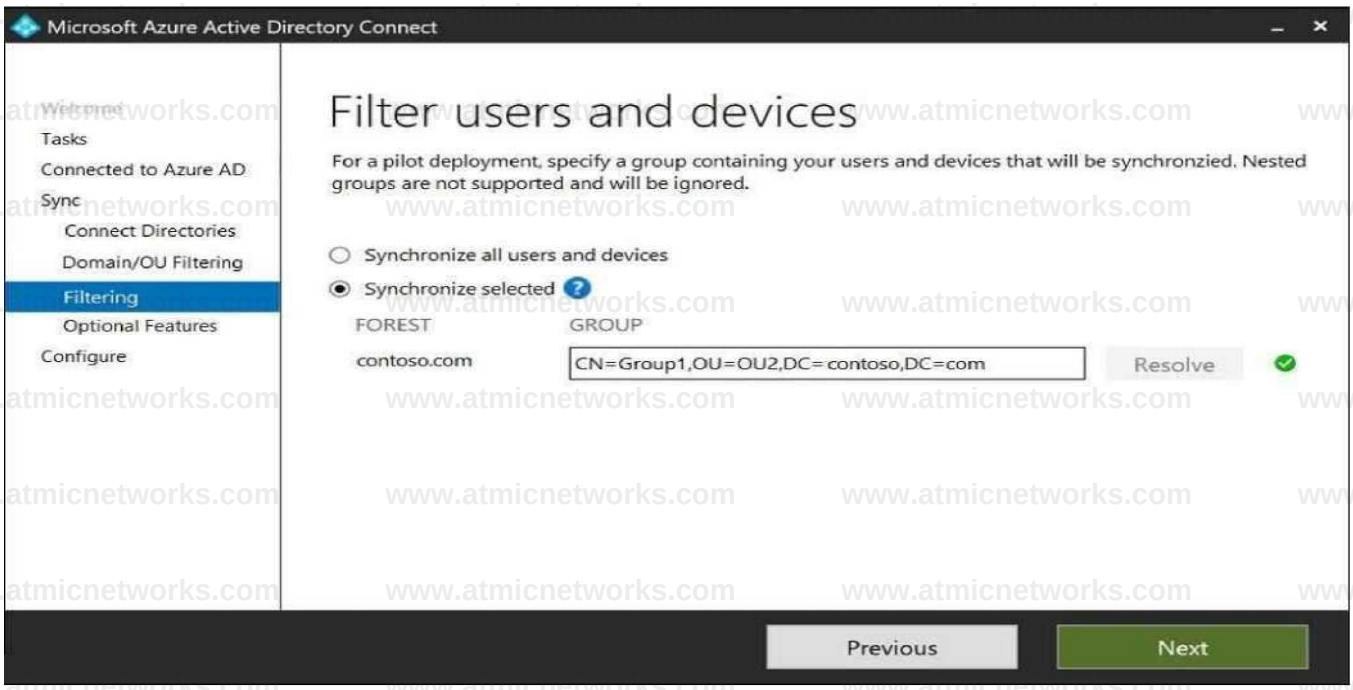
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the objects shown in the following table.

Name	Type	In organizational unit (OU)	Description
Useri	User	OU1	Useri is a member of Groupl
User2	User	OU1	User2 is not a member of any groups.
Groupl	Security group	OU2	Useri and Group2 are members of Groupl.
Group2	Security group	OU1	Group2 is a member of Groupl.

You install Azure AD Connect. You configure the Domain and OU filtering settings as shown in the Domain and OU Filtering exhibit. (Click theDomain and OU Filteringtab.)



You configure the Filter users and devices settings as shown in the Filter Users and Devices exhibit. (Click theFilter Users and Devicestab.)



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

Statements	Yes	No
Used syncs to Azure AD.	0	0
User2 syncs to Azure AD.	O	0
Group2 syncs to Azure AD	o	0

Answer:

Explanation:

Statements	Yes	No
User1 syncs to Azure AD.	O	O
User2 syncs to Azure AD.	O	O
Group2 syncs to Azure AD.	O	O

Only direct members of Group1 are synced. Group2 will sync as it is a direct member of Group1 but the members of Group2 will not sync.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom

Question: 118

You have a Microsoft 365 tenant.

All users have mobile phones and laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptop to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

A. a notification through the Microsoft Authenticator app
B. an app password
C. Windows Hello for Business
D. SMS

Answer: C

Explanation:

In Windows 10, Windows Hello for Business replaces passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN.
After an initial two-step verification of the user during enrollment, Windows Hello is set up on the user's device and Windows asks the user to set a gesture, which can be a biometric, such as a fingerprint, or a PIN. The user provides the gesture to verify their identity. Windows then uses Windows Hello to authenticate users.

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

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

Question: 119

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 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 Notifications settings for multi-factor authentication (MFA).

Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

You need to configure the fraud alert settings.

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

Question: 120

HOTSPOT

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

Name	Role
Useri	Conditional Access administrator
User2	Authentication administrator
User3 \	Security administrator
User4	Security operator

You plan to implement Azure AD Identity Protection.

Which users can configure the user risk policy, and which users can view the risky users report? To answer, select the appropriate options in the answer area.

NOTE:Each correct selection is worth one point.

Configure the user risk policy:

- User3 only
- User3 and User4 only
- User1, User2, and User3 only
- User1, User3, and User4 only
- User1, User2, User3, and User4

View the risky users report:

- User3 only
- User3 and User4 only
- User1, User2, and User3 only
- User1, User3, and User4 only
- User1, User2, User3, and User4

Answer:

Explanation:

Configure the user risk policy:

- User3 only
- **User3 and User4 only**
- User1, User2, and User3 only
- User1, User3, and User4 only
- User1, User2, User3, and User4

View the risky users report:

- **User3 only**
- User3 and User4 only
- User1, User2, and User3 only
- User1, User3, and User4 only
- User1, User2, User3, and User4

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

Question: 121

HOTSPOT

Your company has a Microsoft 365 tenant.

All users have computers that run Windows 10 and are joined to the Azure Active Directory (Azure AD) tenant.

The company subscribes to a third-party cloud service named Service1. Service1 supports Azure AD authentication and authorization based on OAuth. Service1 is published to the Azure AD gallery.

You need to recommend a solution to ensure that the users can connect to Service1 without being prompted for authentication. The solution must ensure that the users can access Service1 only from Azure AD-joined computers. The solution must minimize administrative effort.

What should you recommend for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Ensure that the users can connect to Servicel without being prompted for authentication:

An app registration in Azure AD Azure AD Application Proxy
An enterprise application in Azure AD A managed identity in Azure AD

Ensure that the users can access Servicel only from the Azure AD-joi ned computers: _____

Azure AD Application Proxy
A compliance policy
A conditional access policy
An OAuth policy

Answer:

Explanation:

Ensure that the users can connect to Servicel without being prompted for authentication:

An app registration in Azure AD

Azure AD Application Proxy
An enterprise application in Azure AD
A managed identity in Azure AD

Ensure that the users can access Servicel only from the Azure AD-joined computers:

Azure AD Application Proxy
A compliance policy
A conditional access policy
An OAuth policy

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how- applications-are-added

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/require-managed- devices

Question: 123

You have an Azure Active Directory (Azure AD) tenant named contoso.com that has Azure AD Identity Protection policies enforced.

You create an Azure Sentinel instance and configure the Azure Active Directory connector.

You need to ensure that Azure Sentinel can generate incidents based on the risk alerts raised by Azure AD Identity Protection.

What should you do first?

A. Add an Azure Sentinel data connector.
B. Configure the Notify settings in Azure AD Identity Protection.
C. Create an Azure Sentinel playbook.
D. Modify the Diagnostics settings in Azure AD.

Answer: A

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-ad-identity-protection

You have the Device Settings shown in the following exhibit.

Question: 125

You have a Microsoft 365 tenant.

All users have mobile phones and laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptop to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

A. a notification through the Microsoft Authenticator app
B. email
C. security questions
D. a verification code from the Microsoft Authenticator app

Answer: D

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication- authenticator-app#verification-code-from-mobile-app

Question: 126

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 use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.

You receive more than 100 email alerts each day for failed Azure AD user sign-in attempts.

You need to ensure that a new security administrator receives the alerts instead of you.

Solution: From Azure AD, you modify the Diagnostics settings.

Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:

Question: 127

DRAG DROP

You have a Microsoft 365 E5 subscription that contains three users named User1, User2, and User3.

You need to configure the users as shown in the following table.

User	Configuration
Useri	• User administrator role • Device Administrators role • Identity Governance Administrator role
User2	• Records Management role • Quarantine Administrator role group
User3	• Endpoint Security Manager role • Intune Role Administrator role

Which portal should you use to configure each user? To answer, drag the appropriate portals to the correct users. Each portal may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE:Each correct selection is worth one point.

Portals	Answer Area
Azure Active Directory admin center	
Exchange admin center	Useri
Microsoft 365 compliance center	User2
Microsoft Endpoint Manager admin center	User3:
SharePoint admin center	

Answer:

Explanation

User1:Azure Active Directory admin center

User2: Exchange admin center

User3: Microsoft Endpoint Manager admin center

Question: 128

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains an Azure AD enterprise application named App1.

A contractor uses the credentials of user1@outlook.com.

You need to ensure that you can provide the contractor with access to App1. The contractor must be able to authenticate as user1@outlook.com.

What should you do?

A. Run theNew-AzureADMSInvitationcmdlet.
B. Configure the External collaboration settings.
C. Add a WS-Fed identity provider.
D. Implement Azure AD Connect.

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add- guest-users-portal

https://docs.microsoft.com/en-us/powershell/module/azuread/new-azureadmsinvitation?view=azureadps-2.0

Question: 129

You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users.

From the Groups blade in the Azure Active Directory admin center, you assign Microsoft 365 Enterprise E5 licenses to the users.

You need to remove the Office 365 Enterprise E3 licenses from the users by using the least amount of administrative effort.

What should you use?

A. the Set -KindohsProductKcy cmdlct
B. the Update-MgGroup cmdlet
C. the Set-HgUserLicense cmdlet
D. the Update-MgUser cmdlet

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/powershell/module/msonline/set-msoluserlicense?view=azureadps-1.0

Question: 130

HOTSPOT

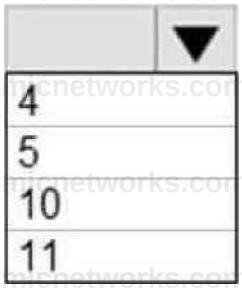
A user named User1 attempts to sign in to the tenant by entering the following incorrect passwords:

Pa55w0rd12
Pa55w0rd12
Pa55w0rd12
Pa55w.rd12
Pa55w.rd123
Pa55w.rd123
Pa55w.rd123
Pa55word12
Pa55word12
Pa55word12
Pa55w.rd12

You need to identify how many sign-in attempts were tracked for User1, and how User1 can unlock her account before the 300-second lockout duration expires.What should identify? To answer, select the appropriate

NOTE:Each correct selection is worth one point.

Tracked sign-in attempts:

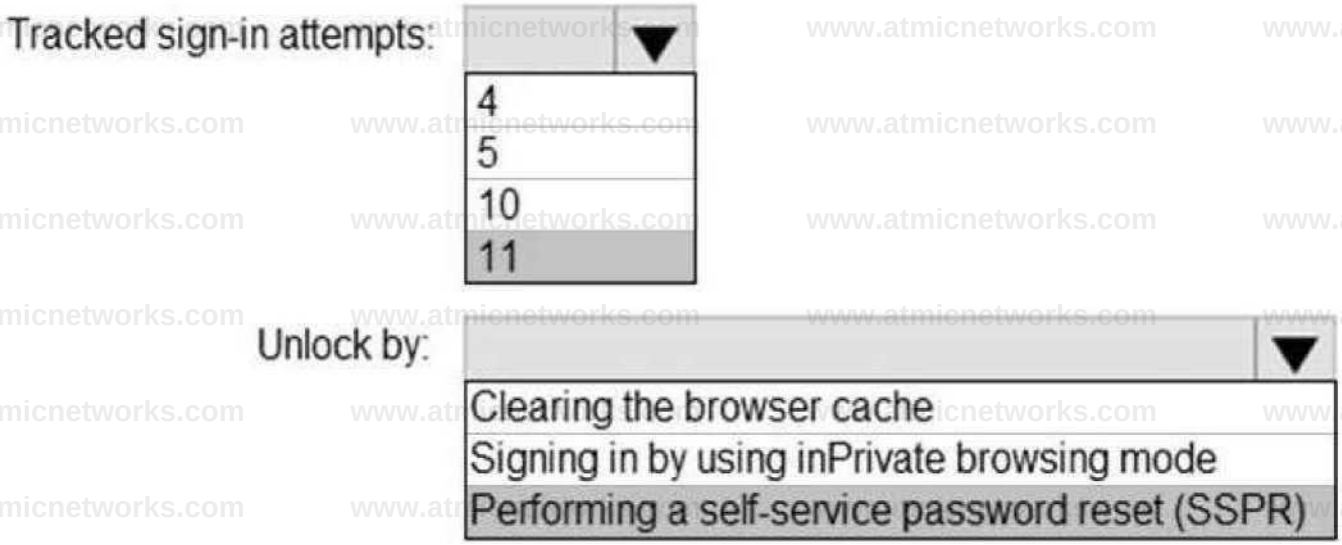


Unlock by:

Clearing the browser cache
Signing in by using inPrivate browsing mode
Performing a self-service password reset (SSPR)

Answer:

Explanation:



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

Question: 131

You have an Azure Active Directory (Azure AD) tenant that contains cloud-based enterprise apps.

You need to group related apps into categories in the My Apps portal.

What should you create?

A. tags
B. collections

C. naming policies
D. dynamic groups

Answer: B

Explanation:
Reference:
https://support.microsoft.com/en-us/account-billing/customize-app-collections-in-the-my-apps- portal-2dae6b8a-d8b0-4a16-9a5d-71ed4d6a6c1d

Question: 132

You have an Azure Active Directory Premium P2 tenant.

You create a Log Analytics workspace.

You need to ensure that you can view Azure Active Directory (Azure AD) audit log information by using Azure Monitor.

What should you do first?

A. Run theSet-AzureADTenantDetailcmdlet.
B. Create an Azure AD workbook.
C. Modify the Diagnostics settings for Azure AD.
D. Run theGet-AzureADAuditDirectoryLogscmdlet.

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-integrate- activity-logs-with-log-analytics

Question: 133

HOTSPOT

You have an Azure subscription.

You need to create two custom roles named Role1 and Role2. The solution must meet the following requirements:

- Users that are assigned Role1 can create or delete instances of Azure Container Apps.
- Users that are assigned Role2 can enforce adaptive network hardening rules.

Which resource provider permissions are required for each role? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Rolel:

MicrosofLApp
MicrosoftCompute
Microsoft Management
MicrosoftSecunty

Role2:

MicrosoftAp p _____
MicrosoftCompute
MicrosoftNetwork
MicrosoftSecunty

Answer:

Explanation:

Answer Area

Rolel: MicrosoftCompute

Role2; Microsoft Security

Question: 134

DRAG DROP

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2.
You need to ensure that User1 can create access reviews for groups, and that User2 can review the history report for all the completed access reviews. The solution must use the principle of least privilege.
Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content
NOTE: Each correct selection is worth one point.

Answer:

Explanation:

Question: 136

HOTSPOT

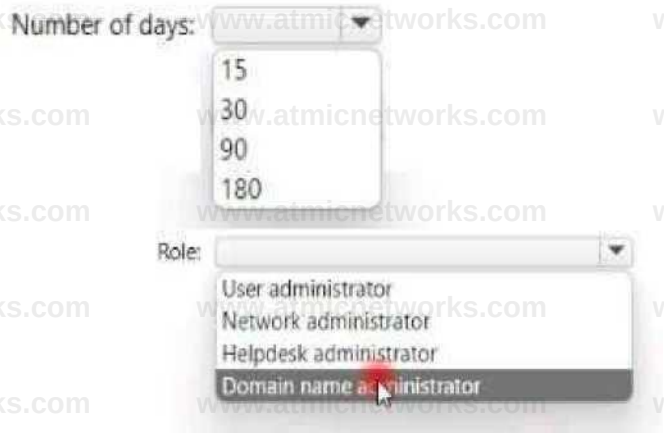
You have an Azure Active Directory (Azure AD) tenant that contains a user named User1. An administrator deletes User1.

You need to identity the following:

- How many days after the account of User1 is deleted can you restore the account?
- Which is the least privileged role that can be used to restore User1?

What should you identify? To answer, select the appropriate options in the answer are a. NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Number of days: 30

Role. User administrator

Question: 137

You have a Microsoft 365 E5 subscription.

You need to create a Microsoft Defender for Cloud Apps session policy.

What should you do first?

A. From the Microsoft Defender for Cloud Apps portal, select User monitoring.
B. From the Microsoft Defender for Cloud Apps portal, select App onboarding/maintenance
C. From the Azure Active Directory admin center, create a Conditional Access policy.
D. From the Microsoft Defender for Cloud Apps portal, create a continuous report.

Answer: C

Question: 141

You have an Azure subscription that contains the custom roles shown in the following table.

Name	Type
Role1	Azure Active Directory (Azure AD) role
Role2	Azure subscription role

You need to create a custom Azure subscription role named Role3 by using the Azure portal. Role3 will use the baseline permissions of an existing role. Which roles can you clone to create Role3?

A. Role2 only
B. built-in Azure subscription roles only
C. built-in Azure subscription roles and Role2 only
D. built-in Azure subscription roles and built-in Azure AD roles only
E. Role1, Role2 built-in Azure subscription roles, and built-in Azure AD roles

Answer: C

Explanation:

Question: 142

You have a Microsoft 365 tenant.

You have an Active Directory domain that syncs to the Azure Active Directory {Azure AD) tenant. Users connect to the internet by using a hardware firewall at your company. The users authenticate to the firewall by using their Active Directory credentials.

You plan to manage access to external applications by using Azure AD.

You need to use the firewall logs to create a list of unmanaged external applications and the users who access them. What should you use to gather the information?

A. Cloud App Discovery in Microsoft Defender for Cloud Apps
B. enterprise applications in Azure AD
C. access reviews in Azure AD
D. Application Insights in Azure Monitor

Answer: A

Explanation:

Question: 143

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1.

You need to ensure that User1 can create new catalogs and add resources to the catalogs they own. What should you do?

A. From the Roles and administrators blade, modify the Service support administrator role.
B. From the identity Governance blade, modify the Entitlement management settings.
C. From the Identity Governance blade, modify the roles and administrators for the General catalog
D. From the Roles and administrators blade, modify the Groups administrator role.

Answer: B

Explanation:

Question: 144

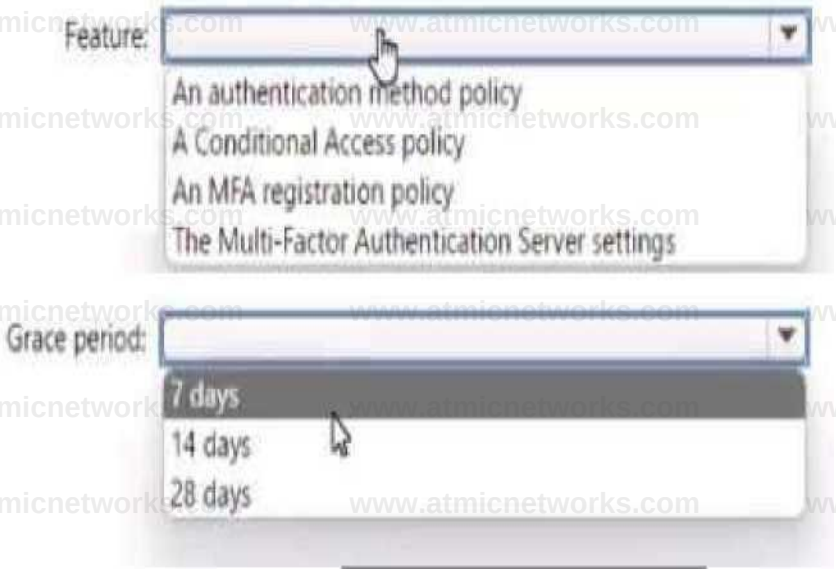
HOTSPOT

You need to support the planned changes and meet the technical requirements for MFA.

Which feature should you use, and how long before the users must complete the registration? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer Area

Feature A Conditional Access policy

Grace period: 14 days

Question: 145

DRAG DROP

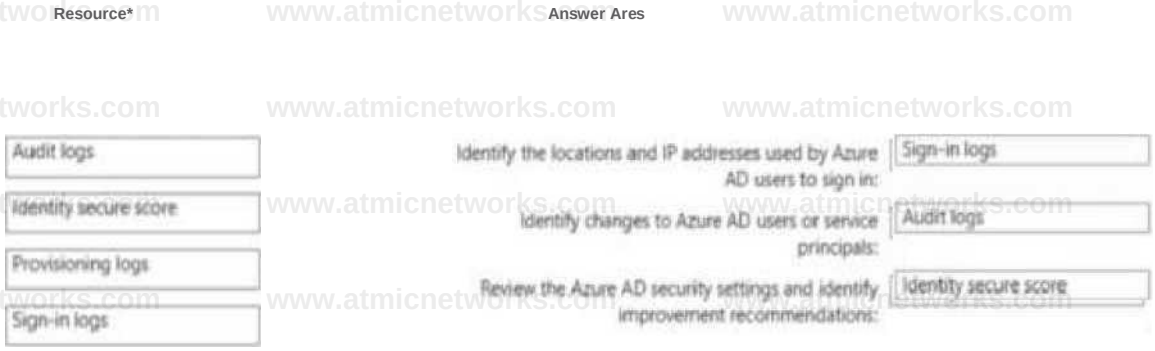
You have a Microsoft 365 E5 subscription. You need to perform the following tasks:

- Identify the locations and IP addresses used by Azure AD users to sign in
- Review the Azure AD security settings and identify improvement recommendations.
- Identify changes to Azure AD users or service principle.

What should you use for each task? To answer, drag the appropriate resources to the correct requirements. Each resource may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

Answer:

Explanation:



Question: 146

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

- Create a group named Group 1.
- Add User1 and User 2 to Group1.
- 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: Dynamic User
B. Group type: Security Membership type: Dynamic Device
C. Group type Security Membership type: Dynamic User
D. Group type Security Membership type: Assigned
E. Group type: Microsoft 365 Membership type: Assigned

Answer: D,E

Explanation:

Question: 147

DRAG DROP

You have a Microsoft 365 E5 subscription and an Azure subscription. You need to meet the following requirements:

- Ensure that users can sign in to Azure virtual machines by using their Microsoft 365 credentials.
- Delegate the ability to create new virtual machines.

What should you use for each requirement? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

Answer:

Explanation:

Question: 148

You have a Microsoft 365 E5 subscription.

Users authorize third-party cloud apps to access their data.

You need to configure an alert that will be triggered when an app requires high permissions and is authorized by more than 20 users.

Which type of policy should you create in the Microsoft Defender for Cloud Apps portal?

A. anomaly detection policy
B. OAuth app policy
C. access policy
D. activity policy

Answer: D

Explanation:

Question: 149

Your company has an Azure AD tenant that contains the users shown in the following table.

Name	Role
User1	Application administrator
User2	None
User3	Exchange administrator
User4	Cloud application administrator

You have the app registrations shown in the following table.

App name	Used by	Microsoft Graph permission
App1	User1	Calendars.Read of type Delegated
App2	User2	Calendars.Read of type Delegated Calendars.ReadWrite of type Application
App3	User3, User4	Calendars.Read of type Application

A company policy prevents changes to user permissions.

Which user can create appointments in the calendar of each user at the company?

A. User1

B. User2
C. User3
D. User4

Answer: B

Explanation:

Question: 150

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site!. Site! hosts PDF files
You need to prevent users from printing the files directly from Sitel.
Which type of policy should you create in the Microsoft Defender for Cloud Apps portal?

A. activity policy
B. file policy
C. access policy
D. session policy

Answer: D

Explanation:

Question: 152

HOTSPOT
You have an Azure AD tenant that contains the groups shown in the following table.

Name	Owner	Number of internal users	Number of guest users
Group1	User1	500	25
Group2	User2	295	100

You create an access review for Group1 as shown in the following table.

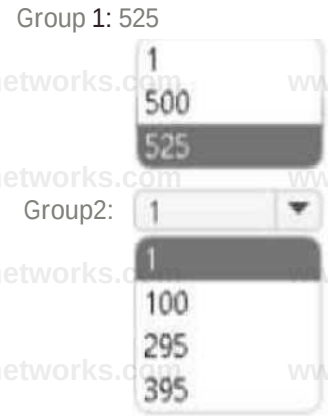
Setting	Value
Review type	Teams + Groups
Review scope	All users
Reviewers	Users review own access

You create an access review for Group2 as shown in the following table.

Setting	Value
Review type	Teams + Groups
Review scope	Guest users only
Reviewers	Group owner

What is the minimum number of Azure AD Premium P2 licenses required for each group? To answer, select the appropriate options in the answer are a. NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Question: 153

You have an Azure AD tenant
You open the risk detections report.
Which risk detection type is classified as a user risk?

A. password spray
B. anonymous IP address
C. unfamiliar sign-in properties
D. Azure AD threat intelligence

Answer: A

Explanation:

Question: 154

You create a conditional access policy that blocks access when a user triggers a high-seventy 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 AD
C. access reviews in Azure AD
D. the activity logs in Microsoft Defender for Cloud Apps

Answer: A

Explanation:

Question: 155

You create a new Microsoft 365 E5 tenant.

You need to ensure that when users connect to the Microsoft 365 portal from an anonymous IP address, they are prompted to use multi-factor authentication (MFA).

What should you configure?

A. a sign-in risk policy
B. a user risk policy
C. an MFA registration policy

Answer: A

Explanation:

Question: 156

You have a Microsoft 36S subscription. The subscription contains users that use Microsoft Outlook 2016 and Outlook 2013 clients. You need to implement tenant restrictions. The solution must minimize administrative effort. What should you do first?

A. Upgrade the Outlook 2013 clients to Outlook 2016.
B. Configure the Outlook 2013 clients to use modem authentication.
C. Upgrade all the Outlook clients to Outlook 2019.

D. From the Exchange admin center, configure Organization Sharing.

Answer: A

Explanation:

Question: 157

You have an Azure AD tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

The tenant has the authentication methods shown in the following table.

Method	Target	Enabled
FIDO?	Group?	Yes
Microsoft Authenticator app	Groupl	Yes
SMS	Groups	Yes

Which users will sign in to cloud apps by matching a number shown in the app with a number shown on their phone?

A. User1 only
B. User2 only
C. User3 only
D. User1 and User2 only
E. User2 and User3 only

Answer: A

Explanation

Question: 159

You have an Azure subscription that contains a user named User1. You need to meet the following requirements:

- Prevent User1 from being added as an owner of newly registered apps.
- Ensure that User1 can manage the application proxy settings.
- Ensure that User2 can register apps.
- Use the principle of least privilege.

Which role should you assign to User1?

A. Application developer
B. Cloud application administrator
C. Service support administrator
D. Application administrator

Answer: D

Explanation:

Question: 160

You have an Azure AD tenant that contains the users shown in the following table.

Name	Role
User1	None
User2	None
Admin1	Application administrator
Admin2	Authentication administrator

The User settings for enterprise applications have the following configuration.

- Users can consent to apps accessing company data on their behalf:
- Users can consent to apps accessing company data for the groups they
- Users can request admin consent to apps they are unable to consent to: Yes

• Who can review admin consent requests: Admin2, User2

User1 attempts to add an app that requires consent to access company data. Which user can provide consent?

A. User1
B. User2
C. Admin1
D. Admin2

Answer: C

Explanation:

Question: 161

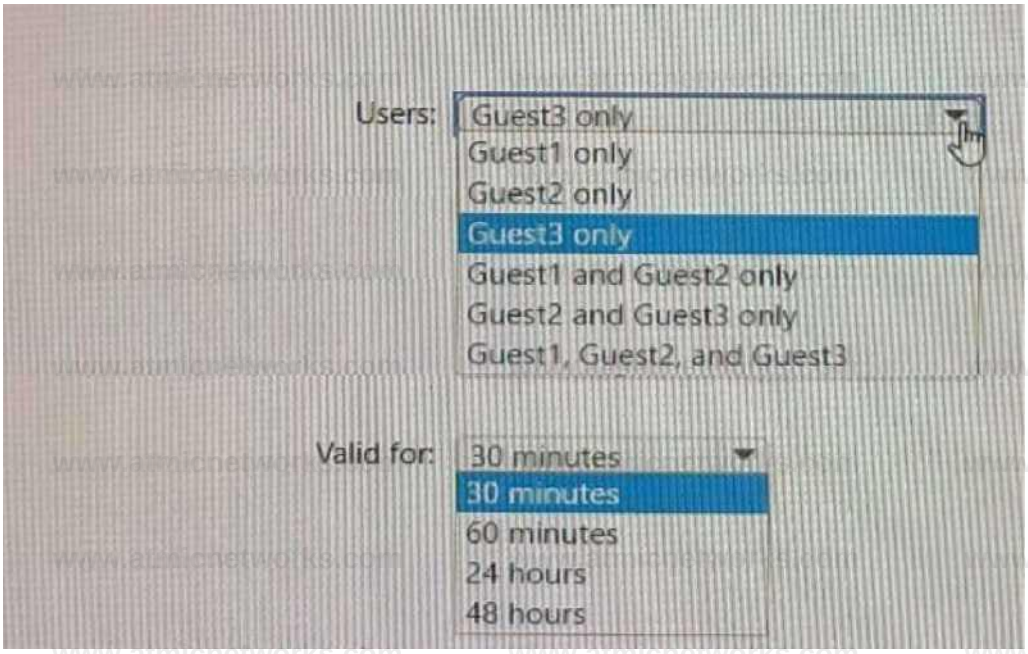
HOTSPOT

You have an Azure AD tenant named contoso.com that has Email one-time passcode for guests set to Yes.
You invite the guest users shown in the following table.

Name	Email domain	Account type
Guest1	adatum.com	Azure AD account
Guest2	outlook.com	Microsoft account
Guest3	gmail.com	Personal Google account

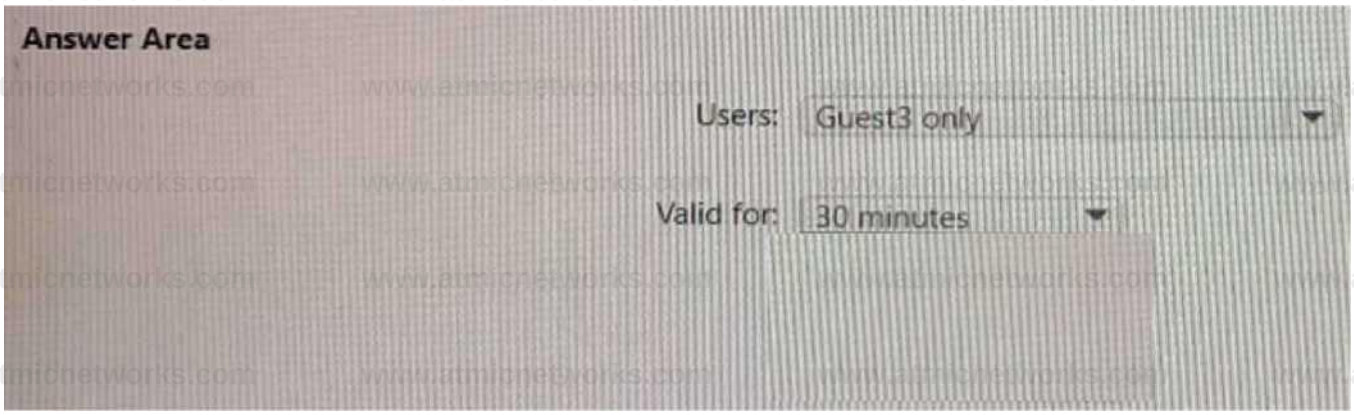
Which users will receive a one-time passcode, and how long will the passcode be valid? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:



Question: 162

HOTSPOT

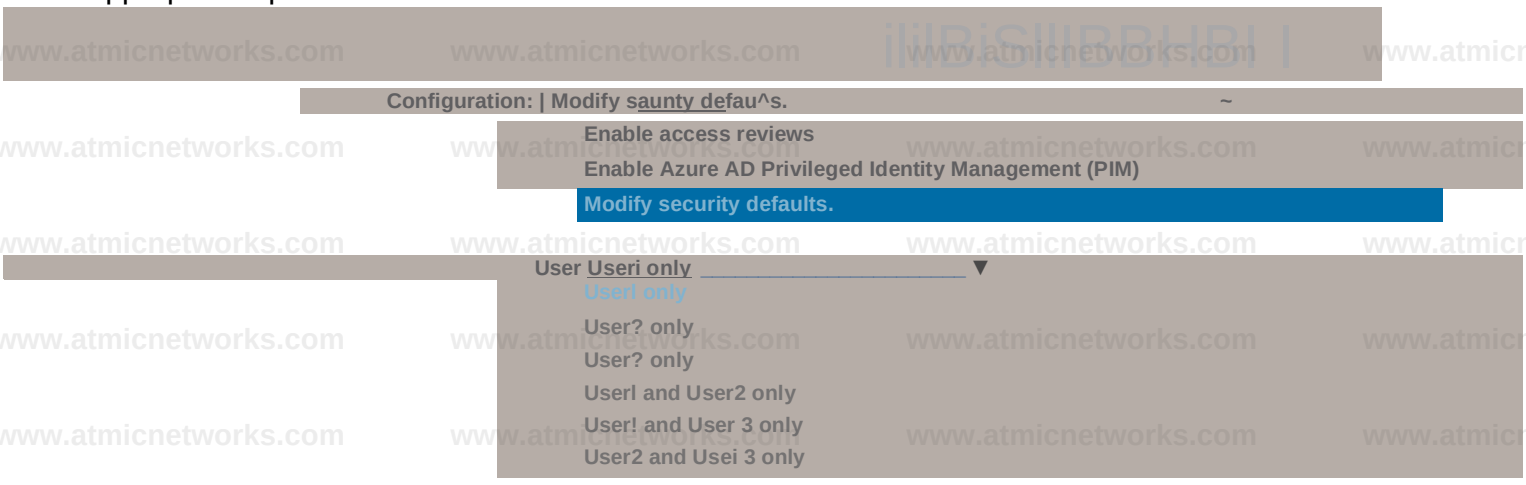
You have an Azure AD tenant that contains the users shown in the following table.

Name	Role
User1	Security administrator
User2	Privileged authentication administrator
User3	Service support administrator

User2 reports that he can only configure multi-factor authenticating (MFA) to use the Microsoft Authenticator app.

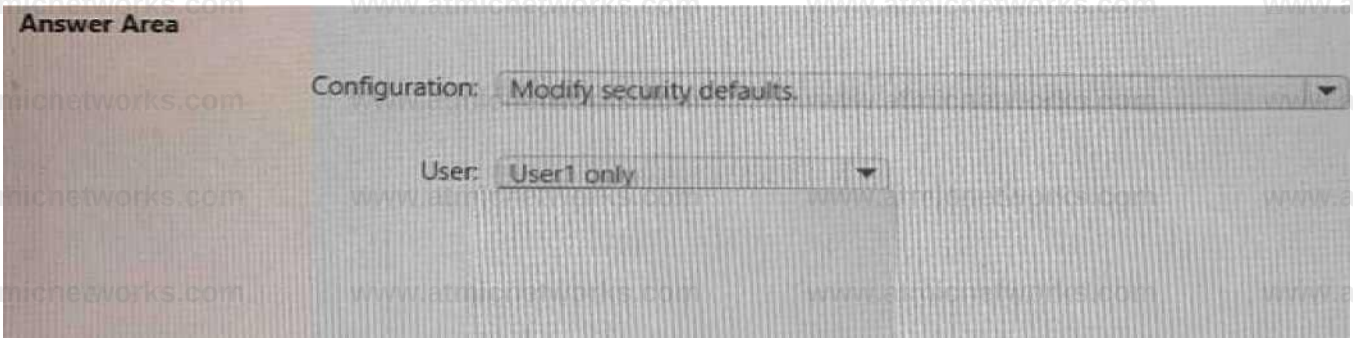
You need to ensure that User2 can configure alternate MFA methods.

Which configuration is required, and which user should perform the configuration? To answer, select the appropriate options in the answer area.



Answer:

Explanation:



Question: 163

Your network contains an on-premises Active Directory domain that syncs to an Azure AD tenant.
Users sign in to computers that run Windows 10 and are joined to the domain.
You plan to implement Azure AD Seamless Single Sign-On (Azure AD Seamless SSO).
You need to configure the Windows 10 computers to support Azure AD Seamless SSO.
What should you do?

A. Modify the Local intranet zone settings
B. Configure Sign-in options from the Settings app.
C. Enable Enterprise State Roaming.
D. Install the Azure AD Connect Authentication Agent.

Answer: B

Explanation:

Question: 164

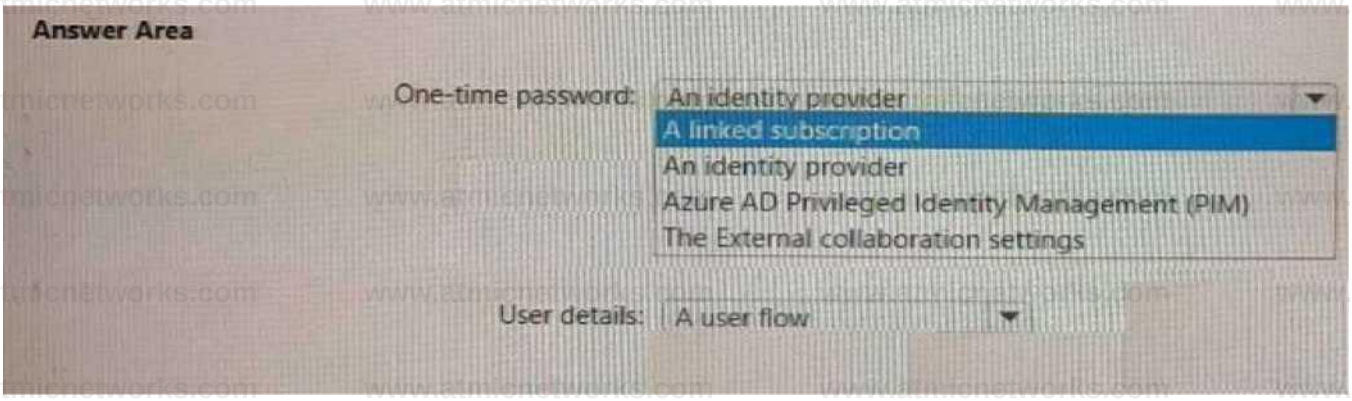
HOTSPOT

You have an Azure AD tenant and an Azure web app named App1.

You need to provide guest users with self-service sign-up for App1. The solution must meet the following requirements:

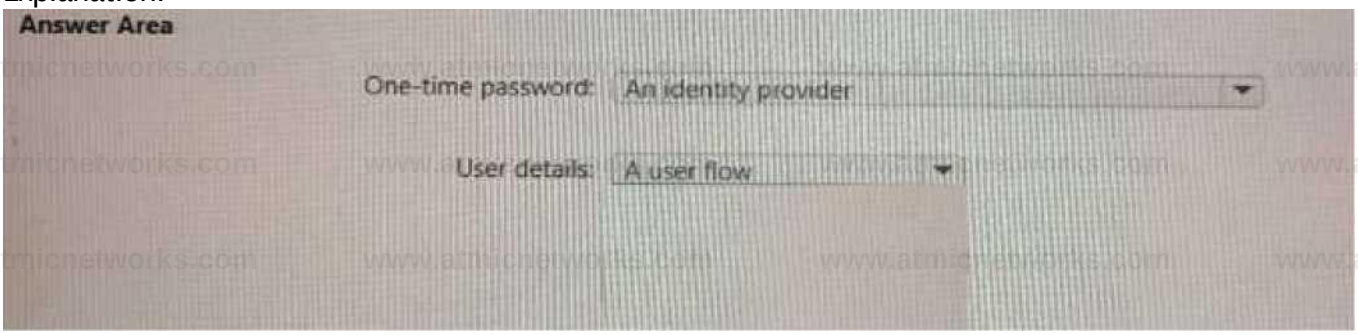
- Guest users must be able to sign up by using a one-time password.
- The users must provide their first name, last name, city, and email address during the sign-up process.

What should you configure in the Azure Active Directory admin center for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Question: 165

You have an Azure AD tenant that uses Azure AD Identity Protection and contains the resources shown in the following table.

Name	Type	Configuration
Risk1	User risk policy	Users that have a high severity risk must reset their password upon next sign-in.
User1	User	*Not applicable*

Azure Multi-Factor Authentication (MFA) is enabled for all users.

User1 triggers a medium severity alert that requires additional investigation.

You need to force User1 to reset his password the next time he signs in. the solution must minimize administrative effort.

What should you do?

A. Configure a sign-in risk policy.
B. Mark User1 as compromised.
C. Reconfigure the user risk policy to trigger on medium or low severity.
D. Reset the Azure MFA registration for User1.

Answer: B

Explanation:

Question: 167

You have an Azure AD tenant that contains a user named User1 and the conditional access policies shown in the following table.

Name	Status	Conditional access requirement
CAPolicy1	On	Users connect from a trusted IP address.
CAPolicy2	On	Users' devices are marked as compliant.
CAPolicy3	Report-only	The sign-in risk of users is low.

You need to evaluate which policies will be applied User1 when User1 attempts to sign-in from various IP addresses.
Which feature should you use?

A. Access reviews
B. Identity Secure Score
C. The What If tool
D. the Microsoft 365 network connectivity test tool

Answer: C

Explanation:

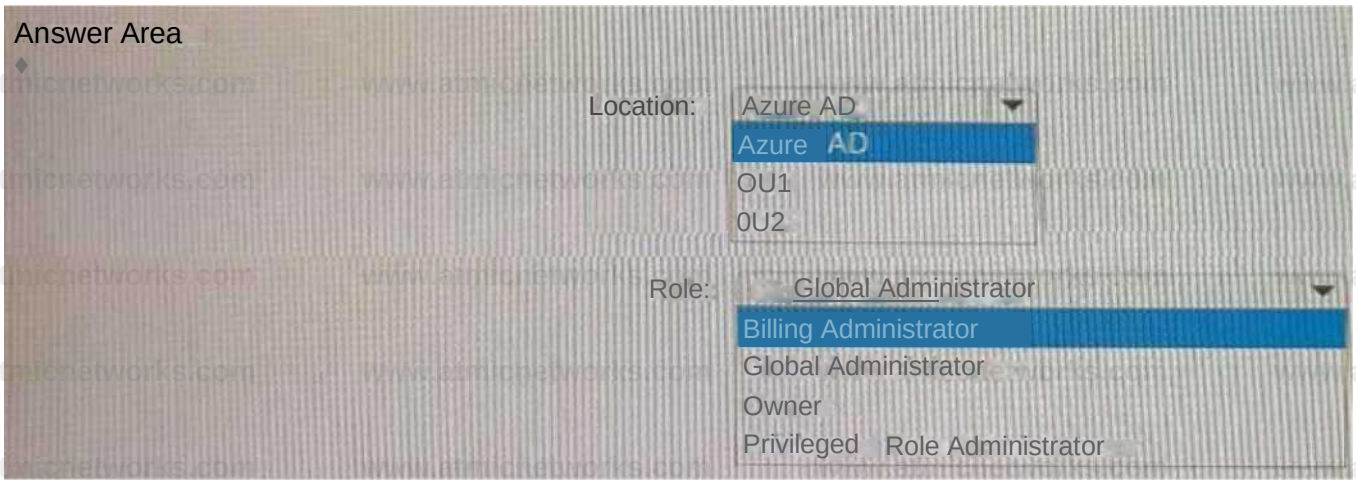
Question: 168

HOTSPOT
Your network contains an on-premises Active Directory Domain services (AD DS) domain that syncs with an Azure AD tenant. The AD DS domain contains the organizational units (OUs) shown in the following table.

Name	Description
OU1	Syncs with Azure AD
OU2	Does **NOT** sync with Azure AD

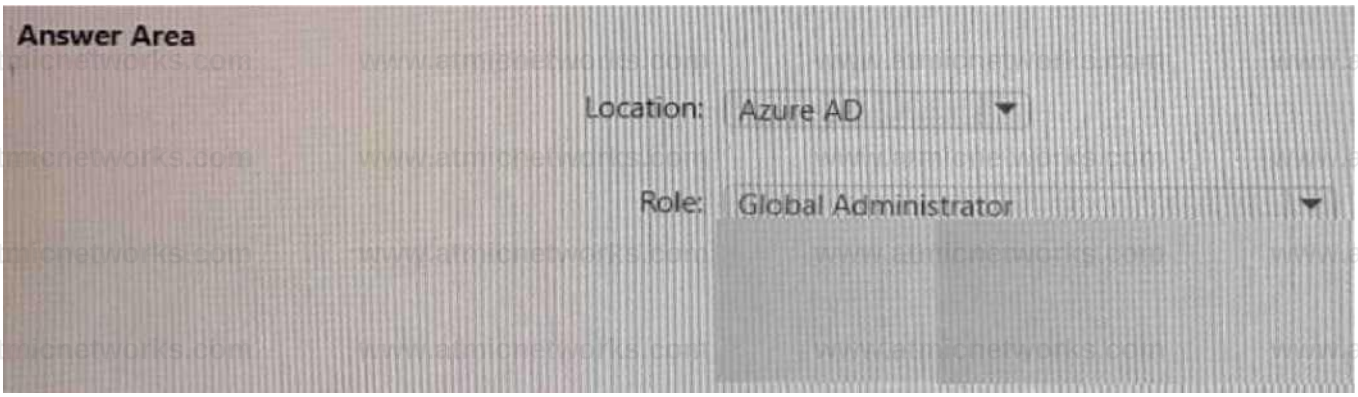
You need to create a break-glass account named BreakGlass.
Where should you create BreakGlass, and which role should you assign to BreakGlass? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Question: 169

You have a Microsoft 365 E5 subscription that contains a web app named App1.

Guest users are regularly granted access to App1.

You need to ensure that the guest users that have NOT accessed App1 during the past 30 days have their access removed the solution must minimize administrative effort.

What should you configure?

A. a compliance policy
B. an access review for application access
C. a guest access review
D. a Conditional Access policy

Answer: B

Explanation:

Question: 170

You have an Azure AD tenant named Contoso that contains a terms of use (ToU) named Terms1 and an access package. Contoso users collaborate with an external organization named Fabrikam.

Fabrikam users must accept Terms1 before being allowed to use the access package.

You need to identify which users accepted or declined Terms1.
What should you use?

A. provisioning logs
B. the Usage and Insights report
C. sign-in logs
D. audit logs

Answer: D

Explanation:

Question: 171

You have an Azure AD tenant that contains a user named User1 and a registered app named App1. User1 deletes the app registration of Appl.
You need to restore the app registration.
What is the maximum number of days you have to restore the app registration from when it was deleted?

A. 14
B. 30
C. 60
D. 180

Answer: B

Explanation:

Question: 172

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.
You need to ensure that users can request access to Site. the solution must meet the following requirements.

- Automatically approve requests from users based on their group membership.
- Automatically remove the access after 30 days

What should you do?

A. Create a Conditional Access policy.

B. Create an access package.
C. Configure Role settings in Azure AD Privileged Identity Management.
D. Create a Microsoft Defender for Cloud Apps access policy.

Answer: B

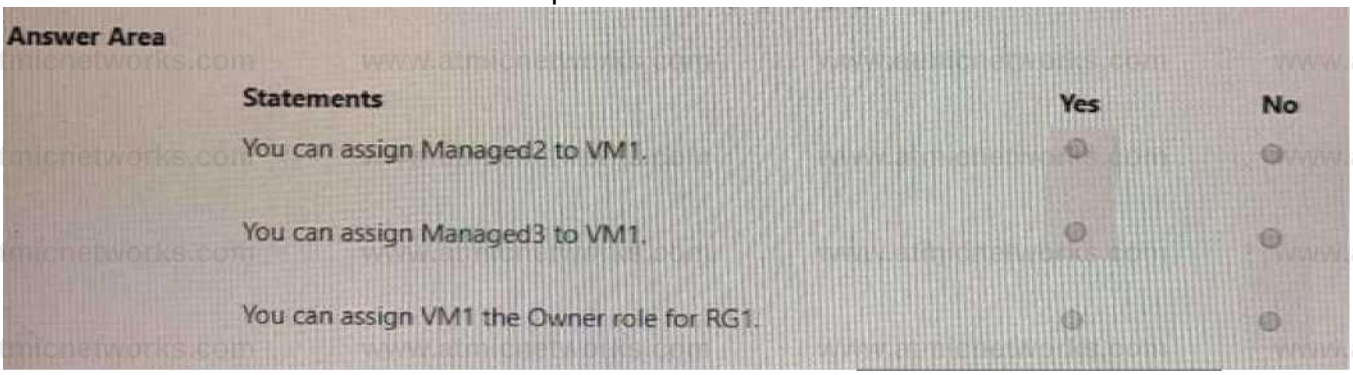
Explanation:

Question: 173

HOTSPOT
You have an Azure subscription that contains the following virtual machine
Name: VM1
Azure region: East US
System-assigned managed identity: Disabled
You create the managed identities shown in the following table.

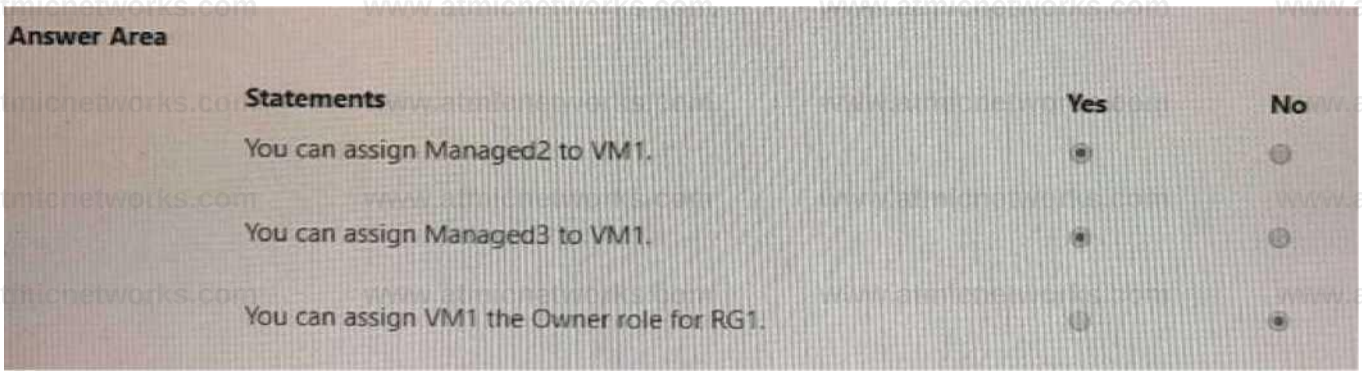
Name	Location
Managed1	East US
Managed2	East US
Managed3	West US

You perform the following actions:
• Assign Managed1 to VM1.
• Create a resource group named RG1 in the West US region.
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:

Explanation:



Question: 174

HOTSPOT

You have an Azure subscription that contains the key vaults shown in the following table.

Name	In resource group	Number of days to Purge protection retain deleted il ! W^ vaults	
KeyVaultl	RG1	15	Enabled
KeyVault2	RG1	10	Disabled

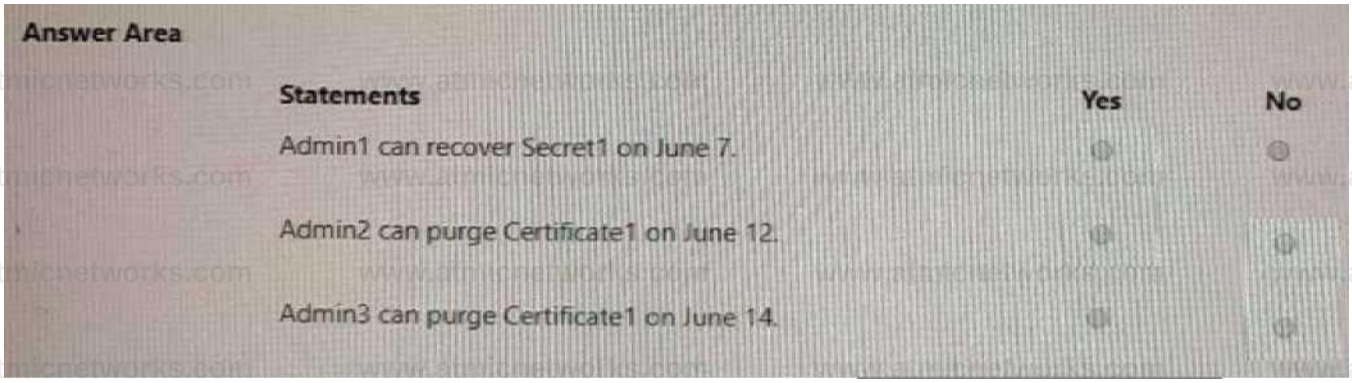
The subscription contains the users shown in the following table.

Name	Role
Admin1	Key Vault Administrator
Admin2	Key Vault Contributor
Admin3	Key Vault Certificates Officer
Admin4	Owner

On June1, Admin4 performs the following actions:

- Deletes a certificate named Certificate! from Key Vault1
- Deletes a secret named Secret1 from KeyVault2

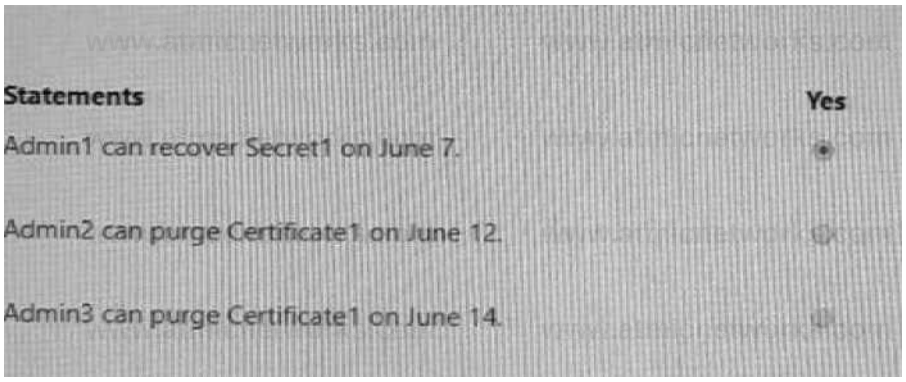
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Answer Area



Question: 175

Your company purchases 2 new Microsoft 365 ES subscription and an app named App.
You need to create a Microsoft Defender for Cloud Apps access policy for App1.
What should you do you first? (Choose Correct Answer based on Microsoft Identity and Access Administrator at microsoft.com)

A. Configure a Token configuration for App1.
B. Add an API permission for App1.
C. Configure a Conditional Access policy to use app-enforced restrictions.
D. Configure a Conditional Access policy to use Conditional Access App Control.

Answer: D

Explanation:

https://learn.microsoft.com/en-us/defender-cloud-apps/access-policy-aad

To create a Microsoft Defender for Cloud Apps access policy for App1, you should configure a Conditional Access policy to use app-enforced restrictions. This will allow you to control access to your cloud apps based on conditions such as user, device, location, and app state. You can also use app-enforced restrictions to control access to your cloud apps based on the state of the app, such as whether it's running on a managed or unmanaged device.

Question: 176

You have an Azure AD tenant named contoso.com that contains the resources shown in the following table.
You create a user named Admin 1.

Name	Description
Au1	Administrative unit
CAPolicy1	Conditional Access policy
Package1	Access package

You need to ensure that Admin can enable Security defaults for contoso.com. What should you do first?

A. Configure Identity Governance.
B. Delete Package1.
C. Delete CAPolicy1.
D. Assign Admin1 the Authentication administrator role for Au1

Answer: D

Explanation:

To enable Security defaults for contoso.com, you should first sign in to the Azure portal as a security administrator, Conditional Access administrator, or global administrator. Then, browse to Azure Active Directory > Properties and select Manage security defaults. Set the Enable security defaults toggle to Yes and select Save.

After that, you can assign Admin1 the Identity Administrator role for Au1 to enable them to manage security defaults for the tenant.

https://practical365.com/what-are-azure-ad-security-defaults-and-should-you-use-them/

Question: 179

HOTSPOT

You have an AzureAD tenant that contains the users shown in the following table.

Name	Member of	Multi-factor authentication (MFA)
Uwrl	Grcupl	D^bted
l Uwr2	G^jp?	Ertbrad

You have the locations shown in the following table.

Name	Private address space	Public NAT addns f pace
Location 1	1Q10JOW16	
LoujjCft2	13iWaCV16	mi; 17 0.2J

The tenantcontainsa named location that Das the following configurations:

- Name: location1
- Mark as trusted location: Enabled
- IPv4 range: 10.10.0.0/16

MFA has a trusted iPad dress range of 193.17.17.0/24.

You have a Conditional Access policy that has the following settings:

- Name: CAPolicy1

- Assignments

o Users or workload identities: Group 1

o Cloud apps or actions: All cloud apps

- Conditions

* Locations All trusted locations

- Access controls

o Gant

- Grant access: Require multi-factor authentication

© Session: 0 controls selected

- Enable policy: On

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 Ares

Statements	Yes	No
ft U«r1 connects to the tenant from IP adores* 10.10.0.150. the user wh be prompted for MFA		
ft Useri connects to the tenant from IP address 10101.160 the user mH be prompted tor MFA		
If Useri connects to the tenant from IP address 192 168120. the user ml be prompted for MFA		

Answer:

Explanation:

Answer Area

Statements	Yes	No
if Used connects to the tenant from IP address 10.10.0.150. the user will be prompted for MFA if Useri connects to the tenant from IP address 10,10.1,160. the user will be prompted for MFA		•
If Useri connects 1o the tenant from IP address 192.168120. the user mH be prompted for MFA	•	

Question: 180

You have an Azure AD tenant

You configure User consent settings to allow users to provide consent to apps from verified publishers.

You need to ensure that the users can only provide consent to apps that require low impact permissions.

What should you do?

A. Create an access package.

B. Configure permission classifications.

C. Create an enterprise application collection.

D. Create an access review.

Answer: C

Explanation:

Question: 181

You havean Azure AD tenant that contains the users shown in the following table.

Name	Sotr
Ac ■nir.'	?2u2 J piics: on Ecrri-! snarer
AdmlflZ	AppJ .at ci; administrate'
AcminB	Sea.-ity ■■ mm'Orator
User!	tow

You add an enterprise application named App1 to Azure AD and set User1 as the owner of App1 requires admin consent to access Azure AD before the app can be used.

You configure the Admin consent requests strong as shown in the following exhibit.

Admin consent requests.

Vwi (Art request Admin content to Appt they a«e unable to consent to J

Ha

Who can 'Witw *dn*m consent request!

Reviewer type

RfMeWHS

Utm

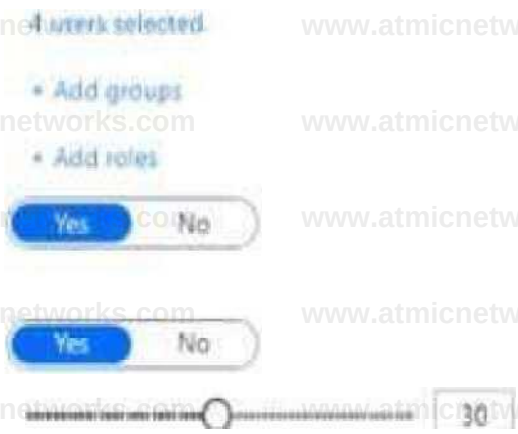
Gttxipi |Ptev<#Al

RoWt (Preview)

Selected uteri w«l1 receive em*" no th cations for requests

Seiected uwrs will recede request eipumon reminders O

Consent request expies after '.days' •[1]



AdminI AdnmnZ AdrmB, end UieH are added as reviewer,

Which users can review and appeove the adnun consent requests'

A. Admm1 only
B. Admm1 and Admin2 only
C. Admm1 Admm2 and Admin3 only
D. Admln1, Admin2. and User1 only
E. Admm1 Admm2. Admm3, and User1

Answer: B

Explanation:

Question: 182

You have a Microsoft 365 subscription that contains a user named User1.
You need to ensure that User1 can create access reviews for Azure AD roles. The solution must use the principal of least privilege.
Which role should you assign to User1?

A. Privileged role administrator
B. Identify Governance administrator
C. User administrator
D. User Access Administrate

Answer: C

Explanation:

Question: 183

You have a Microsoft 365 ES subscription that contains a user named User1. User1 is eligible for the Application administrator role.
User1 needs to configure a new connector group for an application proxy.
What should you to activate the role for User1?

A. the Microsoft Defender for Cloud Apps portal
B. the Microsoft 365 admin center
C. the Azure Active Directory admin center
D. the Microsoft 365 Defender portal

Answer: C

Explanation:

Question: 184

You have a Microsoft 365 ES subscription that user Microsoft Defender for Cloud Apps and Yammer.
You need prevent users from signing in to Yammer from high-risk locations.
What should you do in the Microsoft Defender for Cloud Apps portal?

A. Create an access Policy.

B. Create an activity policy.
C. Unsanction Yammer.
D. Create an anomaly detection policy.

Answer: A

Explanation:

Question: 185

You have an Azure Ad tenant that contains the users show in the following table.

Name	Usage location	Department	Job title
U$er1	Um tec States	Sales	Associate
U«f2	Finland	Sales	Sales Rep
User 3	Austr o ia	Sales	Manager

You create a dynamic user group and configure the following rule syntax.

```
user.usageLocation -in ["US","AU"] -and (user.department -eq "Sales") -and -not (user.jobTitle -eq "Manager") -or (user.jobTitle -eq "SalesRep")
```

Which users will be added to the group?

A. User1 only
B. User2 only
C. User3 only
D. User1 and User2 only
E. User1 and User3 only
F. User1, User2, and User3

Answer: D

Explanation:

Question: 186

You have the Azure resources show in the following table.

Name	Description
Useri	User account
Group!	5ecu'it> group rhr ^es the Dynamic user membership type
VM1	Virtual ma^nr e with a system-assured menaced L'e.ti-y
Appl	Enterprise application
RG1	Resource group

To Which identities can you assign the Contributor role for RG1?

A. User1 only
B. User1 and Group1 only
C. User1 and VW1 only
D. User1, VM1, and App1 only
E. User1, Group1, Vm1, and App1

Answer: E

Explanation:

Question: 187

You have an Azure subscription that contains an Azure SQL database named db1.

You deploy an Azure App Service web app named App1 that provide product information to users that connect to App1 anonymously.

You need to provide App1 with Access to db1. The solution must meet the following requirements:

* Credentials must only be available to App1.
* Administrative effort must be minimized.

Which type of credentials should you use?

A. a user-assigned managed identity
B. an Azure AD user account
C. A SQL Server account
D. a system-assigned managed identity

Answer: D

Explanation:

Question: 188

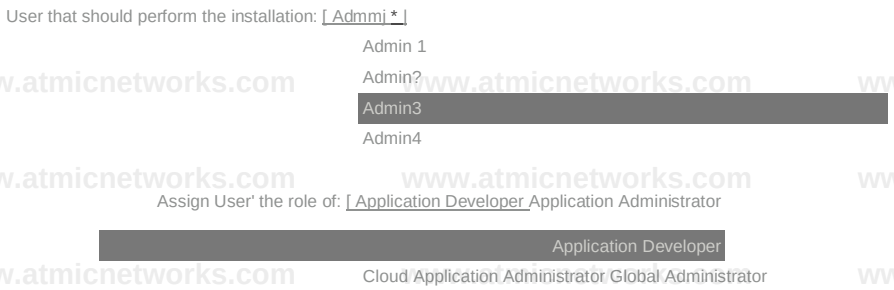
HOTSPOT

You have a hybrid Microsoft 365 subscription that contains the users show in the following table.

Name	Role
Adminl	. otal Administrator
Admin?	Application Administrator
Admm3	Cloud Application Administrator
AdimiM	Application Developer
U^fl	Nonf

You plan to deploy an on-premises app1. App1 will be registered in Azure AD and will use Azure AD Application Proxy.
You need to delegate the installation of the Application Proxy connector and ensure that User1 can register App1 in Azure AD. The solution must use the principle of least privilege.
Which user should perform the installation, and which role should you assign to Users1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

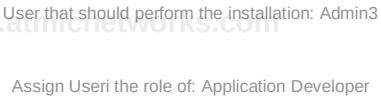
Answer Area



Answer:

Explanation:

Answer Area



Question: 189

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 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 SharePoint Administrator role to User1
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Question: 190

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 a Microsoft 365 ES 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 Exchange Administrator role to User1.

A. Yes
B. No

Answer: A

Explanation:

Question: 191

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 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

Answer: B

Explanation:

Question: 192

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 a Microsoft 365 ES subscription.

You create a user namedUser1.

You need to ensure that User1 can update the status of identity Secure Score improvement actions. Solution: You assign the Security Operator role User1.

Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Question: 193

You have an Azure subscription that uses Azure AD Privileged Identity Management (PIM).
You need to identify users that are eligible for the Cloud Application Administrator role.
Which blade in the Privileged Identity Management settings should you use?

A. Azure resources
B. Privileged access groups
C. Review access
D. Azure AD roles

Answer: B

Explanation:

Question: 194

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1. You need to be notified if a user downloads more than 50 files in one minute from Site1.
Which type of policy should you create in the Microsoft Defender for Cloud Apps portal?

A. session policy
B. anomaly detection policy
C. activity policy

D. file policy

Answer: C

Explanation:

Question: 195

You have an Azure AD tenant.
You need to bulk create 25 new user accounts by uploading a template file.
Which properties are required in the template file?

A accovntEnp&ltd^ gi[1] rnFlamrj tUrritiM) Aid u^grP^i n^j pp i'i#rr

B. atcountfnibledj displayNwiH, uierPrincipilMflne^ and pass trordP ref lie

C dtsp^byMew^ Identity Bluer, ypagelocation. and 115 er Type

D. Kcwnt^nebledj pe^wordProfile* uHfeLDCftivn, and uterPrincipal'iane

A. Option A B. Option B C. Option C D. Option D

Answer: B

Explanation:

Question: 196

HOTSPOT

You have an Azure AD tenant contains the users shown in the following table.

Name	Role
Useri	Now
UserS	Privileged Authentication Administrator
ser-	nh.i| A i^ nirra-T

In Azure AD Privileged Identity Management (PIM), you configure the Global Administrator role as shown in the following exhibit.

Setting	State
Activation maximum duration (hours)	1 hour(s)
Requite justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	No
Approvers	None

Assignment

Setting	State
Allow permanent eligible assignment	Yes
Expire eligible assignments after	•
Allow permanent active assignment	Yes
Expire active assignments after	•
Require Azure Multi- Factor Authentication on active assignment	No
Require justification on active assignment	Yes

User 1 is eligible for the Global Administrator role.

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
Useri requires Azure Multi-Factor Authentication (MFA) to activate the Global Administrator role.		
U$er2 can approve all activation requests for the Global Administrator role.	O	O
User2 and Users can edit the Global Administrator role assignment	O	C

Answer:

Explanation:

Answer Area

Statements	Yes	No
Useri requires Azure Multi-Factor Authentication (MFA) to activate the Global Administrator role.	»	0
User2 can approve all activation requests for the Global Administrator role.	O	*
User2 and User J can edit the Global Administrator role assignment	O	•

Question: 197

HOTSPOT

You have a Microsoft 365 E5 subscription that contains three users named User1, User2, and User3.

You have two Azure AD roles that have the Activation settings shown in the following table.

Name	Required justification on activation	Require approval to activate	Approvers
Rolel	No	Yes	Useri
Role2	Yes	No	None

The Azure AD roles have the Assignment settings shown in the following table.

Role	Allow permanent eligible assignment	Allow Permanent activate assignment	Require justification on active assignment
Rolel	Yes	Yes	Yes
Role2	No	Yes	Yes

The Azure AD roles have the eligible users shown in the following table.

Role	Eligible Assignment
Roiel	useri, users
Rnlei	User3

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	Ye*	No
If Useri requests Rolel, the request will be approved automatically.	O	C
Useri can approve the request of UserS for Role2.		
Useri must provide justification to approve the request of User2 for Rolel.		

Answer:

Explanation:

Answer Area

Statements	Yes	No
If User 1 requests Rolel, the request will be approved automatically.	«	
Useri can approve the request of User3 for Role2.		●
User! must provide justification to approve the request of User2 for Rolel		

Question: 198

A user named User1 receives an error message when attempting to access the Microsoft Defender for Cloud Apps portal.
You need to identify the cause of the error. The solution must minimize administrative effort.
What should you use?

A. Log Analytics
B. sign-in logs
C. audit logs
D. provisioning logs

Answer: B

Explanation:

Question: 199

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of administrative unit
User!	AU1
UserZ	Alli
User3	AU1
Usert	AUZ
User	Vi - member of an ■ Jn'insiicOUr .n t

The users are assigned the roles shown in the following table.

User	Role	Role scope
Used	Password Admmistratoi	Organization
UseiZ	Global Reader	Organization
U«r3	Atom	*Not appL^.iC*
User4	Password Administrator	AUI
UserS	Now	tor *vpphw&c*

For which users can User1 and User4 reset passwords? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User!: User3 only

User 3 only

I User2 and Users only Users and UserS only Useri Users and U$er5 only ! User User4 and Users only . User! User3, User-1, and User5

User* | U$er3 only ᵀ]

User3 only

User2 and User? only

User3 and UserS only

User! User?, and User? only

Answer:

Explanation:

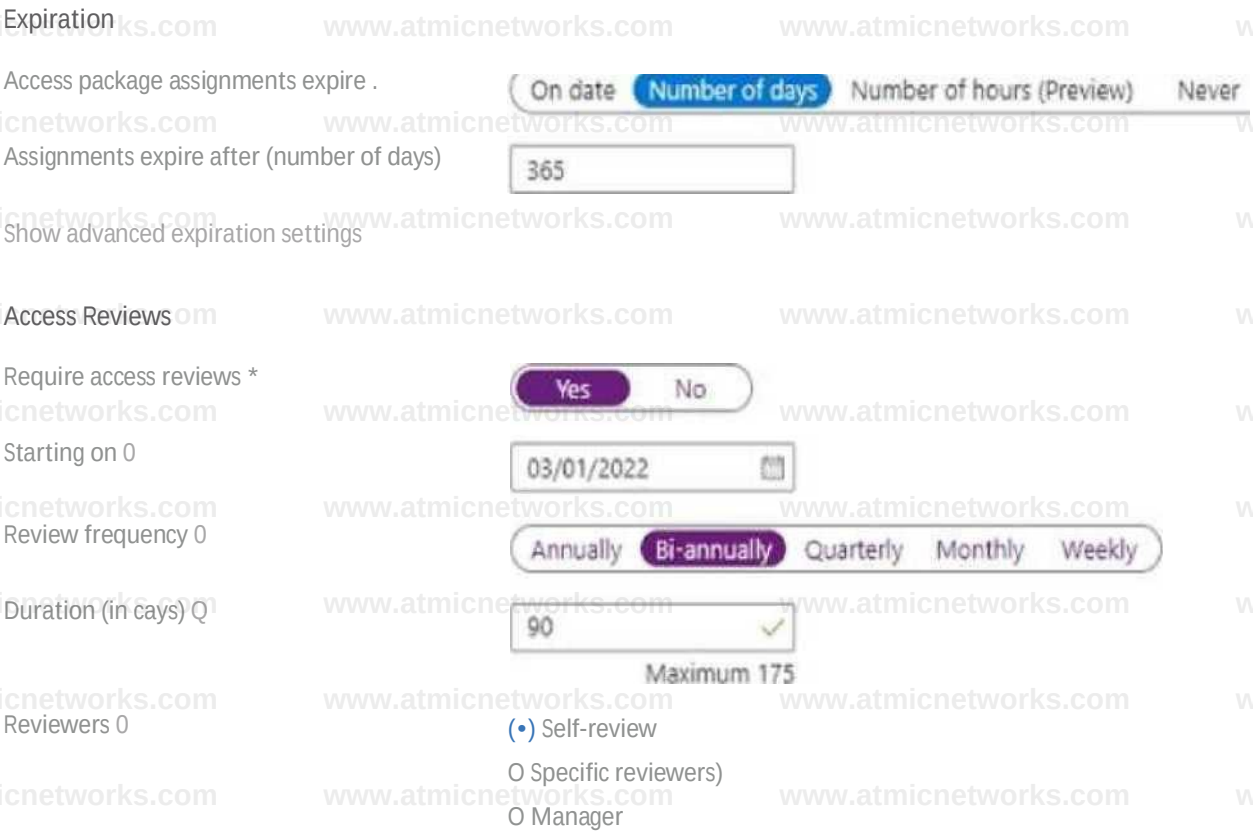
Answer Area

Useri: UserB only

User4: UserS only

Question: 200

You have an Azure AD tenant that contains an access package named Package1 and a user named User1. Package1 is configured as shown in the following exhibit.



You need to ensure that User1 can modify the review frequency of Package1. The solution must use the principle of least privilege.
Which role should you assign to User1?

A. Privileged role administrator
B. User administrator
C. External Identity Provider administrator
D. Security administrator

Answer: B

Explanation:

Question: 201

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.

You need to identify which users access Facebook from their devices and browsers. The solution must minimize administrative effort.

What should you do first?

A. From the Microsoft Defender for Cloud Apps portal, unsanctioned Facebook.
B. Create an app configuration policy in Microsoft Endpoint Manager.
C. Create a Defender for Cloud Apps access policy.
D. Create a Conditional Access policy.

Answer: A

Explanation:

Question: 202

HOTSPOT

You have a Microsoft 365 E5 subscription.

You need to create a dynamic user group that will include all the users that do NOT have a department defined in their user profile.

How should you complete the membership rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Are

Answer:

Explanation:

Question: 204

You have an Azure AD tenant that contains the users shown in The following table.

Name	Role
User1	User Administrator
User2	Password Administrator
User3	Security Reader
User4	User

You enable self-service password reset (SSPR) for all the users and configure SSPR to require security questions as the only authentication method.

Which users must use security questions when resetting their password?

A. User4 only
B. User3and User4only
C. User1 and User4only
D. User1, User3, and User4 only
E. User1, User2, User3. and User4

Answer: B

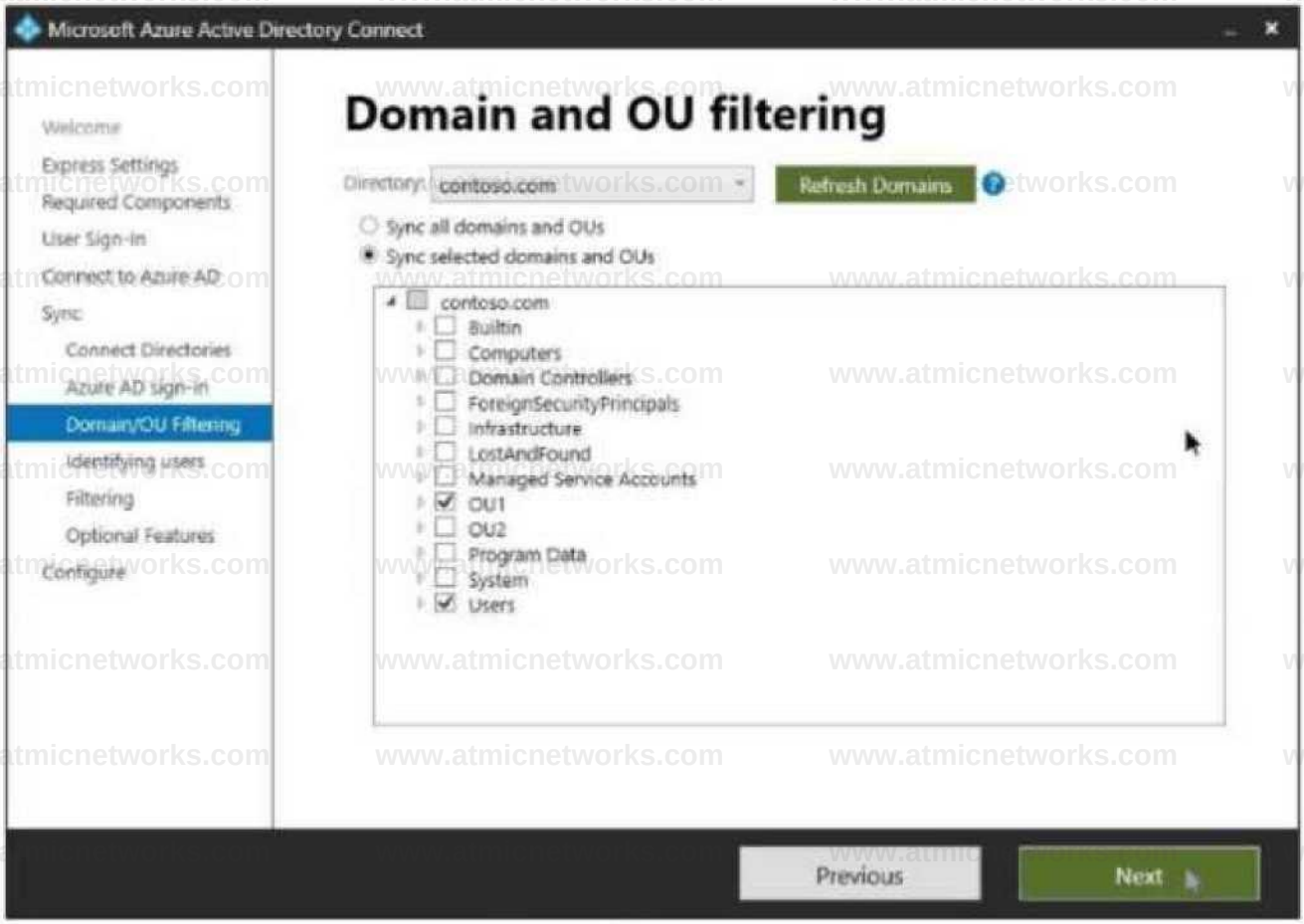
Question: 206

HOTSPOT

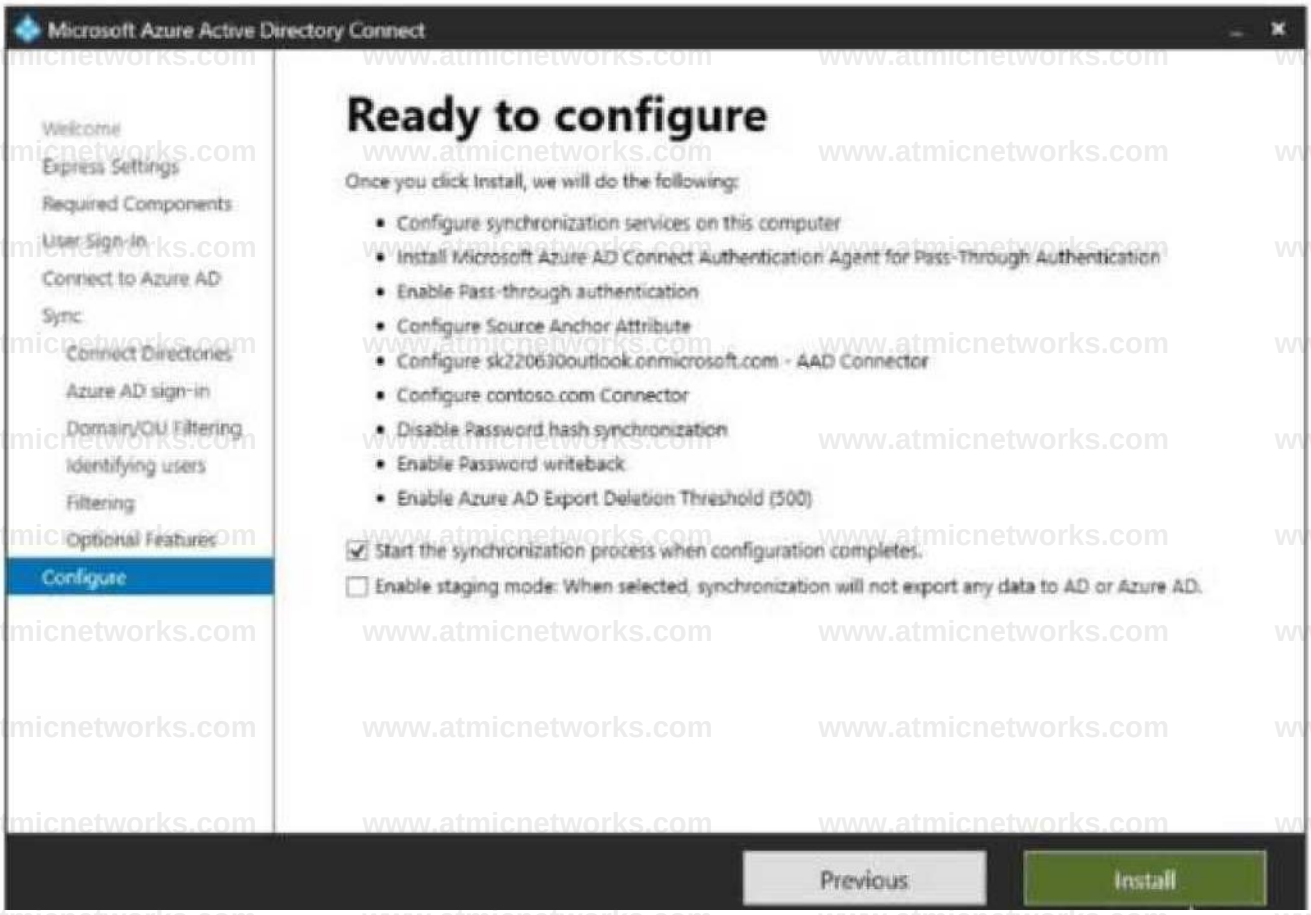
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD and contains the users shown in the following table.

Name	Organizational unit (OU) 1
Userl	OU1
User2	pOU2

In Azure AD Connect. Domain/OU Filtering is configured as shown in the following exhibit.



Azure AD Connect is configured as shown in the following exhibit.



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
Useri can use self-service password reset (SSPR) to reset his password.		O
If Useri accesses Microsoft Exchange Online, he will be authenticated by an on-prerrises domain controller.		
Useri can be added to a Microsoft SharePoint Online site as a member.		

Answer:

Explanation:

Answer Area

Statements	Yes	No
Useri can use self-service password reset (SSPR) to reset his password.	•	O
If Useri accesses Microsoft Exchange Online, he will be authenticated by an on-premises domain controller.	C	•
Useri can be added to a Microsoft SharePoint Online site as a member.	•	O

Question: 207

HOTSPOT
You have an Azure subscription that contains the resources shown in the following table.
You need to configure access to Vault1. The solution must meet the following requirements:

- Ensure that User1 can manage and create keys in Vault1.
- Ensure that User2 can access a certificate stored in Vault1.
- Use the principle of least privilege.

Which role should you assign to each user? To answer select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

Answer Area

U$er1; Ke, Vault Ceil'' ales Officer

User2: Key Vault Certificates Officer

Question: 208

You have a Microsoft 365 E5 subscription.

You purchase the app governance add-on license.

You need to enable app governance integration. Which portal should you use?

A. the Microsoft Defender for Cloud Apps portal
B. the Microsoft 365 admin center
C. Microsoft 365 Defender
D. the Azure Active Directory admin center
E. the Microsoft Purview compliance portal

Answer: A

Explanation:

Question: 209

You have an Azure AD tenant that contains a user named User1

User1 needs to manage license assignments and reset user passwords.

Which role should you assign to User1?

A. License administrator
B. Helpdesk administrator
C. Billing administrator
D. User administrator

Answer: D

Explanation:

Question: 210

You have an Azure AD tenant that has multi-factor authentication (MFA) enforced and self-service password reset (SSPR) enabled.

You enable combined registration in interrupt mode.

You create a new user named User1.

Which two authentication methods can User1 use to complete the combined registration process?

Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. a FID02 security key
B. a hardware token
C. a one-time passcode email
D. Windows Hello for Business
E. the Microsoft Authenticator app

Answer: A,E

Explanation:

Question: 211

DRAG DROP

You have an Azure AD tenant that contains a user named Admin1.

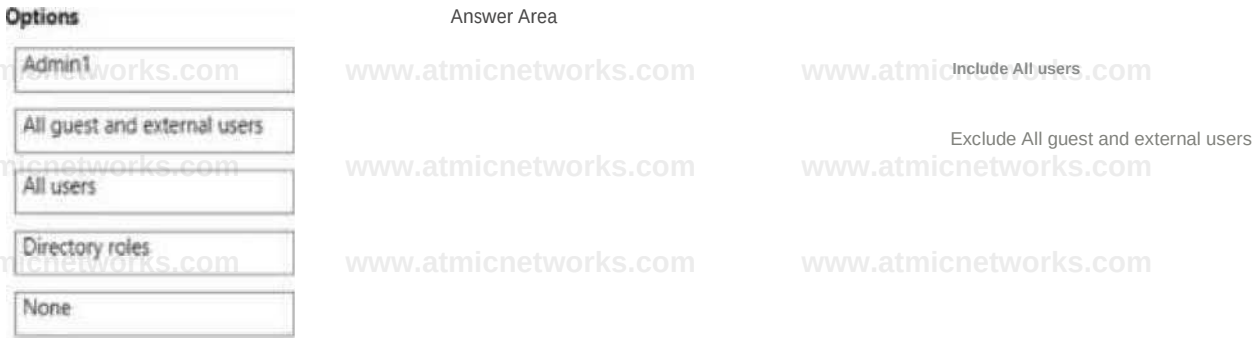
Admin1 uses the Require password change for high-risk user's policy template to create a new Conditional Access policy.

Who is included and excluded by default in the policy assignment? To answer, drag the appropriate options to the correct target. Each option may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Answer:

Explanation:



Question: 212

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps and Conditional Access policies. You need to block access to cloud apps when a user is assessed as high risk.
Which type of policy should you create in the Microsoft Defender for Cloud Apps?

A. OAuth app policy
B. anomaly detection polio
C. access policy
D. activity policy

Answer: C

Explanation:

Question: 213

You plan to deploy a new Azure AD tenant.
Which multifactor authentication (MFA) method will be enabled by default for the tenant?

A. Microsoft Authenticator
B. SMS
C. voice call

D. email OTP

Answer: B

Explanation:

Question: 214

You have an Azure AD tenant that contains the users shown in the following table.

Name	Role
As~ n[J]	User Administrator
Admin2	Password Administrator
Admin3	Application Administrator

You need to compare the role permissions of each user. The solution must minimize administrative effort.
What should you use?

A. the Microsoft 365 Defender portal
B. the Microsoft 365 admin center
C. the Microsoft Entra admin center
D. the Microsoft Purview compliance portal

Answer: D

Explanation:

Question: 215

HOTSPOT
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and the users shown in the following table.

The users have the devices shown in the following table.

You create the following two Conditional Access policies:

- Name: CAPolicy1
- Assignments
  - o Users or workload identities: Group 1
  - o Cloud apps or actions: Office 365 SharePoint Online
  - o Conditions

- Filter for devices: Exclude filtered devices from the policy
- Rule syntax: device.displayName -starts With "Device*"

o Access controls
- Grant: Block access
- Session: 0 controls selected

o Enable policy: On
- Name: CAPolicy2
- Assignments

o Users or workload identities: Group2
o Cloud apps or actions: Office 365 SharePoint Online
o Conditions: 0 conditions selected
- Access controls

o Grant: Grant access
- Require multifactor authentication

o Session:
0 controls selected
- Enable policy: On

All users confirm that they can successfully authenticate using MFA.
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
Userl can access Site! from Device 1.	0	0
User2 can access Sitel from Device2.	O	O
User} can access Sitel from Devices.	O	0

Answer

Explanation:

Answer Area

Statements	Yes	No
Userl can access Sitel from Device!.		
User2 can access Site! from Device2.		
UserS can access Site! from Devices.		

Question: 216

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 Amazon Web Services (AWS) account, a Google Workspace subscription, and a GitHub account.
You deploy an Azure subscription and enable Microsoft 365 Defender.

You need to ensure that you can monitor OAuth authentication requests by using Microsoft Defender for Cloud Apps.
Solution: From the Microsoft 365 Defender portal, you add the Google Workspace app connector. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Question: 217

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 Amazon Web Services (AWS) account, a Google Workspace subscription, and a GitHub account.
You deploy an Azure subscription and enable Microsoft 365 Defender

You need to ensure that you can monitor OAuth authentication requests by using Microsoft Defender for Cloud Apps.
Solution: From the Microsoft 365 Defender portal, you add the Microsoft Azure app connector.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Question: 218

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 Amazon Web Services (AWS) account, a Google Workspace subscription, and a GitHub account.
You deploy an Azure subscription and enable Microsoft 365 Defender.

You need to ensure that you can monitor OAuth authentication requests by using Microsoft Defender for Cloud Apps.
Solution: From the Microsoft 365 Defender portal, you add the Amazon Web Services app connector.
Does this meet the goal?

A. Yes

C. No

Answer: A

Explanation:

Question: 219

You have an Azure AD tenant.
You deploy a new enterprise application named App1.
When users attempt to provide App1 with access to the tenant, the attempt fails.
You need to ensure that the users can request admin consent for App1. The solution must follow the principle of least privilege.
What should you do first?

A. Enable admin consent requests for the tenant.
B. Designate a reviewer of admin consent requests for the tenant.
C. From the Permissions settings of App1, grant App1 admin consent for the tenant
D. Create a Conditional Access policy for Appl.

Answer: A

Explanation:

Question: 220

You have an Azure subscription that contains the users shown in the following table.

Name	Role
Admin1	Account Administrator
Admin2	Service Administrator
Admin3	SharePoint Administrator

You need to implement Azure AD Privileged Identity Management (PIM). Which users can use PIM to activate their role permissions?

A. Admin! only
B. Admin2 only
C. Admin3 only
D. Admin1 and Admin2 only
E. Admin2 and Admin3 only
F. Admin1, Admin2, and Admin3

Answer: D

Explanation:

Question: 221

HOTSPOT

You have an Azure AD tenant.

You perform the tasks shown in the following table.

Date	Task
March 1	Register four enterprise applications named App1, App2, App3, and App4.
March 15	From the tenant, update the following settings for App1: App roles, Users and groups, Client secret and Self-service.
March 20	From the tenant, update the following settings for App2: App roles, Users and groups, Client secret, and Self-service.
March 25	From the tenant, update the following settings for App3: App roles, Users and groups, Client secret, and Self-service.
March 30	From the tenant, update the following settings for App4: App roles, Users and groups, Client secret and Self-service

On April 5, an administrator deletes App1, App2, App3, and App4.

You need to restore the apps and the settings.

Which apps can you restore on April 16, and which settings can you restore for App4 on April 16? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

.

Apps [App J and App4 only

No apps

App4 only

App2, App?. and App4 only

App 1, AppZ App3. and App4

App4 settings | App roles, Users and groups, Client secret and Self-service *]

No settings

Self service only

App roles and Client secret only

Users and groups and Self-service only

App roles, Users and groups, Client secret, and Self-service

Answer:

Explanation:

Answer Area

.

Appt App 3 and App4 only *

App4 settings App roles. Users and groups. Client secret, and Self-service

Question: 222

HOTSPOT

You have an Azure AD tenant named contoso.com that contains a group named All Company and has the following Identity Governance settings:

- Block external users from signing in to this directory: Yes
- Remove external user Yes
- Number of days before removing external user from this directory: 30

On March 1, 2022, you create an access package named Package1 that has the following settings:

- Resource roles

o Name: All Company
o Type: Group and Team
o Role: Member

Name	Email address
Guest!	guest 1 fi[1] out iook com
Guest?	gue$t2@outlook com

On March 2, 2022, you assign the Reports reader role to Guest1.
On April 1(2022, you invite a guest user named Guest3 to contoso.com.
On April 4, 2022, you add Guest3 to the All Company group.
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
On May 5, 2022. the Guest! account is in contoso.com.		
On May 5, 2022. the Guest2 account is in contoso com		
On May 5, 2022. the Guest3 account is in contoso.com.		

Answer:

Explanation:

Answer Area Statements	Yes	No
On May 5,2022, the Guest! account is in contoso com.	O	•

* Lifecycle

o Access package assignment expire: On date
o Assignment expiration date: April 1, 2022

On March 1, 2022, you assign Package1 to the guest users shown in the following table.

On May 5.2022 the Guest2 account is in contoso com O $

On May 5, 2022. the Guest3 account is in contoso com.

Question: 223

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 Amazon Web Services (AWS) account a Google Workspace subscription, and a GitHub account

You deploy an Azure subscription and enable Microsoft 365 Defender.

You need to ensure that you can monitor OAuth authentication requests by using Microsoft Defender for Cloud Apps.

Solution: From the Microsoft 365 Defender portal, you add the GitHub app connector Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Question: 224

You have a Microsoft 365 subscription that contains a Microsoft SharePoint Online site named Site1 and a Microsoft 365 group named Group1. You need to ensure that the members of Group1 can access Site1 for 90 days. The solution must minimize administrative effort. What should you use?

A. an access review
B. a lifecycle workflow
C. an access package
D. a Conditional Access policy

Answer: C

Explanation:

Question: 226

You have an Azure subscription that contains an Azure Automation account named Automation1 and an Azure key vault named Vault1. Vault1 contains a secret named Secret 1.

You enable a system-assigned managed identity for Automation1.

You need to ensure that Automation! can read the contents of Secret1. The solution must meet the following requirements:

- Prevent Automation1 from accessing other secrets stored in Vault1.
- Follow the principle of least privilege.

What should you do?

A. From Vault1, configure the Access control (1AM) settings.
B. From Automation1, configure the Identity settings.
C. From Secret1, configure the Access control (1AM) settings
D. From Automation1, configure the Run as accounts settings.

Answer: A

Explanation:

Question: 227

You have an Azure subscription that contains a resource group named RG1 and four users named User1, User2, User3, and User4. You plan to assign the users the following roles for RG1:

- User1: Reader
- User2: Contributor
- User3: Storage Blob Data Reader
- User4: Virtual Machine Contributor

You are evaluating the use of attribute-based access control (ABAC). Which user's role will support the use of ABAC?

A. User1
B. User2
C. User3
D. User4

Answer: C

Explanation:

Question: 228

You have an Azure subscription named Sub1 that contains a virtual machine named VM1.
You need to enable Microsoft Entra login for VM1 and configure VM1 to access the resources in Sub1.
Which type of identity should you assign to VM1?

A. system-assigned managed identity
B. Azure Automation account
C. Microsoft Entra user account
D. user-assigned managed identity

Answer: A

Explanation:

Question: 229

You have a Microsoft 365 subscription.
You plan to deploy an app named App1 that will have the following configurations:

- Will be registered in Microsoft Entra
- Will run as a service without user interaction
- Will collect audit logs associated with user sign-ins
- Will access resources by using the Microsoft Graph API

You need to ensure that App1 can access Microsoft Graph.
What should you use?

A. application permissions
B. delegated permissions
C. a custom role-based access control (RBAC) role
D. a built-in role-based access control (RBAC) role

Answer: B

Explanation:

Question: 230

You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Role
Useri	Global Administrator
User2	User Administrator
UserS	Grciip; Administrator
User4	Mme

From the tenan1, you configure a naming policy for groups. Which users are affected by the naming policy?

A. User2 only
B. User3only
C. User2 and User3 only
D. User3 and User4 only
E. User1, User2, and User3 only
F. User1, User2, User3, and User4

Answer: D

Explanation:

Question: 234

You have an Azure subscription named Sub1 that contains a user named User1.
You need to ensure that User1 can purchase a Microsoft Entra Permissions Management license for Sub1. The solution must follow the principle of least privilege.
Which role should you assign to User1?

A. User Access Administrator
B. Permissions Management Administrator
C. Billing Administrator
D. Global Administrator

Answer: C

Explanation:

Question: 235

You have three Azure subscriptions that are linked to a single Microsoft Entra tenant.
You need to evaluate and remediate the risks associated with highly privileged accounts. The solution must minimize administrative effort.
What should you use?

A. Microsoft Entra Verified ID
B. Privileged Identify Management (PIM)
C. Global Secure Access
D. Microsoft Entra Permissions Management

Answer: B

Explanation:

Question: 236

You have accounts for the following cloud platforms:

- Azure
- Alibaba Cloud
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)

You configure an A2ure subscription to use Microsoft Entra Permissions Management to manage the permissions in Azure only.
Which additional cloud platforms can be managed by using Permissions Management?

A. AWS only
B. Alibaba Cloud and AWS only
C. Alibaba Cloud and GCP only
D. AWS and GCP only
E. Alibaba Cloud, AWS, and GCP

Answer: D

Explanation:

Question: 237

You have a Microsoft Entra tenant that has a Microsoft Entra ID P1 license.

You need to review the Microsoft Entra ID sign-in logs to investigate sign-ins that occurred in the past.

For how long does Microsoft Entra ID store events in the sign-in logs?

A. 14 days
B. 30 days
C. 90days
D. 365 days

Answer: B

Explanation:

Let's break this down step by step based on Microsoft Entra's sign-in log retention policies as outlined in Microsoft Identity and Access Administrator documentation.

Understanding Microsoft Entra Sign-In Logs and Licensing:

Microsoft Entra ID (formerly Azure Active Directory) provides sign-in logs as part of its auditing and reporting capabilities. These logs track user and application sign-in activities, which are critical for security monitoring and compliance.

The question specifies that the tenant has a Microsoft Entra ID P1 license. Licensing is a key factor in determining the retention period for sign-in logs in Microsoft Entra.

Retention Period Based on License Tier:

Microsoft Entra ID has different editions: Free, P1, and P2. Each edition offers different capabilities and retention periods for audit and sign-in logs.

Free Tier:The Free edition of Microsoft Entra ID retains sign-in logs for7 days.

P1 Tier:With a Microsoft Entra ID P1 license (as mentioned in the question), sign-in logs are retained for30 days. This is a standard feature of the P1 license, which provides enhanced security and monitoring capabilities compared to the Free tier.

P2 Tier:The P2 license also retains sign-in logs for30 days, but it includes additional features like riskbased conditional access and identity protection, which are not relevant to the retention period. Analysis of the Options:

A. 14 days:This is incorrect. Microsoft Entra ID does not have a 14-day retention period for sign-in logs under any license tier. This might be confused with other types of logs or services, but it does not apply here.

B. 30 days:This is correct. As stated, with a P1 license, Microsoft Entra retains sign-in logs for 30 days. C. 90 days:This is incorrect. Microsoft Entra ID does not retain sign-in logs for 90 days, even with a P1 or P2 license. To retain logs for longer periods (e.g., 90 days or more), you would need to export the logs to a storage solution like Azure Monitor Logs or a SIEM system (e.g., Microsoft Sentinel), which allows for custom retention periods.

D. 365 days:This is incorrect for the same reason as option C. Microsoft Entra ID's default retention for sign-in logs is 30 days with a P1 or P2 license. Achieving a 365-day retention would require exporting logs to an external storage solution.

Additional Considerations:

If the tenant integrates Microsoft Entra logs with Azure Monitor or Microsoft Sentinel, the retention period can be extended based on the configuration of those services. However, the question specifically asks about Microsoft Entra's default retention, not an extended retention through integration.

The retention period for audit logs (which track changes to the directory, like user or group modifications) also follows the same

pattern: 7 days for Free, 30 days for P1/P2. However, this question is about sign-in logs, not audit logs.

Conclusion:Given that the tenant has a Microsoft Entra ID P1 license, the sign-in logs are retained for 30 days. Therefore, the correct answer isB.

Reference:

Microsoft Entra ID documentation: "Audit and sign-in logs retention" (Microsoft Learn:https://learn.microsoft.com/en-us/entra/identity/monitoring-health/concept-audit-sign-in- logs#how-long-are-logs-retained)

Microsoft Entra ID P1 and P2 feature comparison: "Editions of Microsoft Entra ID" (Microsoft Learn:https://learn.microsoft.com/en-us/entra/fundamentals/licensing)

Microsoft Identity and Access Administrator (SC-300) exam study guide, which covers monitoring and reporting capabilities, including log retention periods.

Question: 238

HOTSPOT

You have an Azure subscription named Sub1 ilia1 contains a storage account named storage1. You need to deploy two apps named App1 and App2 that will have the following configurations:

- App1 will be deployed as a registered app in Sub1.
- App1 will access storage1 by using Microsoft Entra authentication.
- App2 will access storage1 by using a single Microsoft Entra identity.
- App2 be hosted on two new virtual machines named VM1 and VM2.

The solution must minimize administrative effort.

Which type of identity will each app use to access storage1? To answer, select the appropriate options in the answer area.

Answer Area

Answer:

Explanation:

Answer Are#

Appl: [Service principal

App2: User-assigned managed identity

Question: 239

HOTSPOT

You have a Microsoft Entra tenant that contains the users shown in the following table.

Name	Member of
Ui?r1	Group 1
Use r2	Groups
UMF3	Groups Groups

You have a user risk policy that has the following settings:

- Assignments:

o Include: Group1

o Exclude: Group2

- Sign-in risk Medium and above
- Access controls:

o Grant access: Require password change

When the users attempt to sign in. user risk levels are detected as shown in the following table.

User	Risk level
Userl	High
User^	Medium
User]	High

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

Answer Area Statements	Yes	No
Userl must change their password during sign in		
User? must change their password during sign in. User3 must change their password during sign in.		

o Q

Answer:

Explanation:

Answer Area Statements	Yes	No
Userl must change their password during sign in.	®	
User? must change their password during sign in.	O	*
User} must change their password during sign in.	O	*

Question: 240

You have a Microsoft Entra tenant that contains the groups shown in the following table.

Name	Type	Membership type
Groupl	Security	Assigned
Group 2	Security	Dynamic
Group]	IMkr "sofl 365	Assigned
Groups	Microsoft 335	Dynamic

You need to implement Privileged Identity Management (PIM) for the groups. Which groups can be managed by using PIM?

A. Group1 only
B. Group1 and Group2 only
C. Group1 and Group3 only
D. Group3 and Group4 only
E. Group1. Group2. Group3. and Group4

Answer: C

Explanation:

Question: 241

You have an Azure subscription named Sub1 that contains a resource group named RG1. RG1 contains an Azure Cosmos DB database named DB1 and an Azure Kubernetes Service (AKS) cluster named AKS1. AKS1 uses a managed identity.
You need to ensure that AKS1 can access DB1. The solution must meet the following requirements: • Ensure that AKS1 uses the managed identity to access DB1.
• Follow the principle of least privilege.
Which role should you assign to the managed identity of AKS1.

A. For R61, assign the Azure Cosmos DB Data Reader Role role.
B. For Sub1. assign the Owner role.
C. For RG1, assign the Reader role.
D. For DB1, assign the Azure Cosmos DB Account Reader Role role.

Answer: A

Explanation:

Question: 242

You have an Azure subscription that containes a registered app named App1.
You need to review the sign-in activity for App1. The solution must meet the following requirements:

- Identify the number of failed sign-ins.
- Identify the success rate of sign-ins.

- Minimize administrative effort.

What should you use?

A. Audit logs
B. Usage & insights
C. Access reviews
D. Sign-in logs

Answer: D

Explanation:

Question: 243

You have an Azure subscription that contains a user named User1. The subscription is onboarded to Microsoft Entra Permissions Management. You need to provide User! with access to Permissions Management. The solution must meet the following requirements:

- Follow the principle of least privilege.
- Minimize administrative effort.

What should you do first?

A. From the Microsoft Entra admin center, create a security group.
B. From the Role/Policy Template subtab of Permissions Management, create a template.
C. From the Microsoft Entra admin center, assign a role to User1.
D. From the My Requests subtab of Permissions Management, create a new request.

Answer: C

Explanation:

Question: 244

You have an Azure subscription named Sub1 that uses Microsoft Entra Permissions Management.
Sub1 contains a user named User1. User1 is granted multiple permissions across Sub1.
You need to replace all the permissions granted to User1 with read-only permissions. The solution must minimize administrative effort.
What should you do on the Remediation tab in Permissions Management?

A. From the Roles/Policies subtab. create a role.
B. From the My Requests subtab, create a new request.
C. From the Permissions subtab, use a quick action.
D. From the Role/Policy Template subtab. create a template.

Answer: A

Explanation:

Question: 245

HOTSPOT

You have an Azure subscription named Sub1 that contains two resource groups named RG1 and RG2.

Sub1 contains the users shown in the following table.

Name	Member of
Useri	G'cupl, Group?
User®	Group?
Usei 3	Giaup3

Sub1 contains the resources shown in the following table.

Name	Type	In resource group
VM1	Virtual machine	RG1
Vault!	Azure- Key Vault	RG1
Vaults	Azuie Key Vault	RG2

You create the role-based access control (RBAC) role assignments shown in the following table.

Role	Member of	Scope
Readei	GrOdpl	5ubi
Key Vbult Secrets Usei	Group?	RG2
Ownei	Groups	RG1

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
User 1 can read the contents of the secrets stored in Vault!		
User? can read the contents of the secrets stored in Vault?		
Used can update the configuration of VM1.		

Answer:

Explanation:

Answer Area

Statements	Yes	No
Useri can read the contents of the secrets stored in Vault!		
User? can lead the contents of the secrets stored in Vault? 8		
Used can update the configuration of VM1.		®

Question: 246

HOTSPOT

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Location
RG1	Resource group	East US
Mari aged 1	Managed ident iy	East US
Managed?	M.mnyrd (:►■— ty	West US

The subscription contains the virtual machines shown in the following table.

Name	Location	Identity
VM1	East US	System-assigned
VM2	West US	System-assigned
VMS	East US	Managed!
VM4	West US	Wte _____

Which identities can be assigned the Owner role for RG1, and to which virtual machines can you assign Managed2? To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point.

Answer Area

Identities with Owner role:

- Managedl only
- Managedl, VM1, and VM3 only
- Managedl, Managed?, and VM1 only
- Managedl, Managed?, VM1, and VM? only
- Managedl, Managed?, VM1, VM?, and VM3 only

Virtual machines assigned to Managed?:

- VM4 only
- VM? and VM4 only
- VM1, VM?, and VM4 only
- VM1, VM?, VM3, and VM4

Answer:

Explanation:

Box1:Managed1, Managed2, VM1, and VM2 VM3

Box2: VM1, VM2, VM3, VM4 This article confirms that managed identities can be used across geos: https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/managed- identities-faq

Question: 247

You have an Azure subscription. The subscription contains 50 virtual machines that run Windows Server.
You enable Microsoft Entra login for the virtual machines.
Users report that they cannot sign in to the virtual machines by using their Microsoft Entra credentials.
You need to ensure that the users can sign in to the virtual machines.
What should you do first?

A. Ensure that the virtual machines can access https://enterpriseregistration.windows.net.
B. Revoke the primary refresh token.
C. From the Microsoft Entra admin center, delete the device registrations of the virtual machines.
D. Enable SSH client support for OpenSSH.

Answer: A

Explanation:

Question: 248

DRAG DROP
Your network contains an on-premises Active Directory domain named contoso.com that syncs with a Microsoft Entra tenant by using Microsoft Entra Connect. The domain contains the users shown in the following table.

Name	User principal name (UPN)	Proxy address
U$er1	u$er1@contQSO.com	smtp: user1@contoso.com smtp: sales@contoso.com
User2	user2@contoso.com	smtp: user2@contoso.com smtp: user.2@contoso.com smtp: service@contoso.com

From Active Directory Users and Computers, you add the following user

- Name: User3
- UPN: user3@contoso.com
- Proxy addresses: smtp: user3@contoso.com, smtp: sales@contoso.com

From Active Directory Users and Computers, you update the proxyAddresses attribute for each user as shown in the following table.

Name	Proxy address
Userl	smtp: adrrin@contoso.com
User2	Smtp: sales@contoso.com

You trigger a manual synchronization.

Which sync status will Microsoft Entra Connect sync return for each user? To answer, drag the appropriate status to the correct users. Each status may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Answer:

Explanation:

Statuses	Answer Area
AttributsValueHustBetInique error occurs	User1@contoso.com AttributeValueMustBellnique error occurs
InvalidSoftMatch error occurs	User2@contoso.com InvalidSoftMatch error occurs.
Ob jectTypeMismatch error occurs.	User3@contoso.com Successfully synced
Successfully synced	

Question: 249

DRAG DROP

You have a Microsoft Entra tenant named contoso.com that contains an administrative unit named AU1 and two users named User1 and User2. User1 is a member of AU1.

You need to perform the following role assignments:

- User1: Security Administrator
- User2: User Administrator

For which scopes can each user be assigned the role? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Used AU 1 and contoso.coni
AU1 only contoso.com only
AU1 and contoso.com

AU1 and contoso.com
UserZ: AU1 only contoso.com only
AU1 and contoso.com

Answer:

Explanation:

Answer Area

Used AUIandcontoso.com

User? AU1andcontoso.com

Question: 250

You have an Azure subscription, a Google Cloud Platform (GCP) account, and an Amazon Web Services (AWS) account.

You need to recommend a solution to assess the risks associated with privilege assignments across all the platforms. The solution must minimize administrative effort

What should you include in the recommendation?

A. Microsoft Sentinel
B. Microsoft Defender for Cloud Apps
C. Microsoft Entra ID Protection
D. Microsoft Entra Permissions Management

Answer: D

Explanation:

Question: 251

You have an Azure subscription.
You are evaluating enterprise software as a service (SaaS) apps.
You need to ensure that the apps support automatic provisioning of Microsoft Entra users.
Which specification should the apps support?

A. WS-Fed
B. SCIM 2.0
C. LDAP3
D. OAuth 2.0

Answer: B

Explanation:

Question: 252

You have an Azure subscription that contains a storage account named storage1 and a web app named WebApp1. WebApp1 uses a system-assigned managed identity.
You need to ensure that WebApp1 can read and write files to storage1 by using the system-assigned managed identity.
What should you configure for storage1 in the Azure portal?

A. the File share settings
B. the Access control (1AM) settings
C. a shared access signature (SAS)
D. data protection
E. access keys

Answer: B

Explanation:

Question: 253

You have a Microsoft Entra tenant.
You need to ensure that only users from specific external domains can be invited as guests to the tenant.
Which settings should you configure?

A. Cross-tenant access settings
B. External collaboration settings
C. Linked subscriptions
D. All identity providers

Answer: B

Explanation:

Question: 254

You have an Azure subscription that contains a user named User! and two resource groups named RG1 and RG2.
You need to ensure that User1 can perform the following tasks:

- View all resources.
- Restart virtual machines.
- Create virtual machines in RG1 only.
- Create storage accounts in RG1 only.

What is the minimum number of role-based access control (RBAC) role assignment* required?

A. 1
B. 2
C. 3
D. 4

Answer: B

Explanation:

Question: 255

You have a Microsoft Entra tenant that contains a terms of use (ToU) named Terms1. You create a Conditional Access policy named Policy1 to deploy Terms1. You need to configure Policy1 to require users to accept Terms1. Which settings should you configure for Policy1?

A. Conditions
B. Session
C. Grant
D. Target resources

Answer: A

Explanation:

Question: 256

Your on-premises network contains an Active Directory Domain Services (AD DS) domain and a certification authority (CA) named CAT.
You have a Microsoft Entra tenant.
You need to implement Microsoft Entra certificate-based authentication. The solution must ensure that users can sign in by using certificates issued by CAT What should you do first?

A. Enable auto-enrollment for CAT.

B. Deploy an Azure key vault.
C. Add CA1 as a Certificate Authority to the Microsoft Entra tenant.
D. Deploy Windows Hello for Business.

Answer: C

Explanation:

Question: 257

You have an Azure subscription that contains a virtual machine named VM1 and an Azure key vault named Vault1. VM1 has a system-assigned managed identity. You need to ensure that VM1 can retrieve the values of secrets stored in Vault 1. The solution must minimize administrative effort. What should you do first?

A. Configure the Resource access settings for Vault1.
B. Configure the permissions model for Vault1
C. Add a user-assigned managed identity to VM1.
D. Assign an Azure role to VM1.

Answer: D

Explanation:

Question: 258

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.

You plan to increase app security for the subscription.

You need to identify which apps do NOT require user authentication What should you do in the Microsoft 365 Defender portal?

A. Create a discovered app query.
B. Create a snapshot Cloud Discovery report.
C. Create an OAuth policy and review alerts.
D. Review the cloud app catalog.

Answer: A

Explanation:

Question: 259

HOTSPOT

You have a Microsoft Entra tenant that contains the users shown in the following table.

Name	Member of
Adminl	Groupl

Admin2	Group?
Admm3	Groupl, Group?

You add the following assignment for the User Administrator role:

- Scope type: Directory
- Selected members: Group1
- Assignment type: Active
- Assignments starts August 15. 2022
- Assignment ends: December 15, 2022

You add the following assignment for the Exchange Administrator role:

- Scope type: Directory
- Selected members: Group2
- Assignment type: Eligible
- Assignments starts: October 15, 2022
- Assignment ends: January 15. 2023

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
On November 15,2022. Adminl can reset the password of Admin2		
On October 15, 2022. Admin2 signs in and can administer Exchange Online.		
On September 1.2022. Admin3 can reset the password of Adminl.	O	O

Answer:

Explanation:

Answer Area

Statements	Yes	No
On November 15,2022 Admml can reset the password of Admm2		
On October 15. 2022, Admin2 signs in and can administer Exchange Online.	*	
On September 1. 2022. AdminS can reset the password of Admin!		

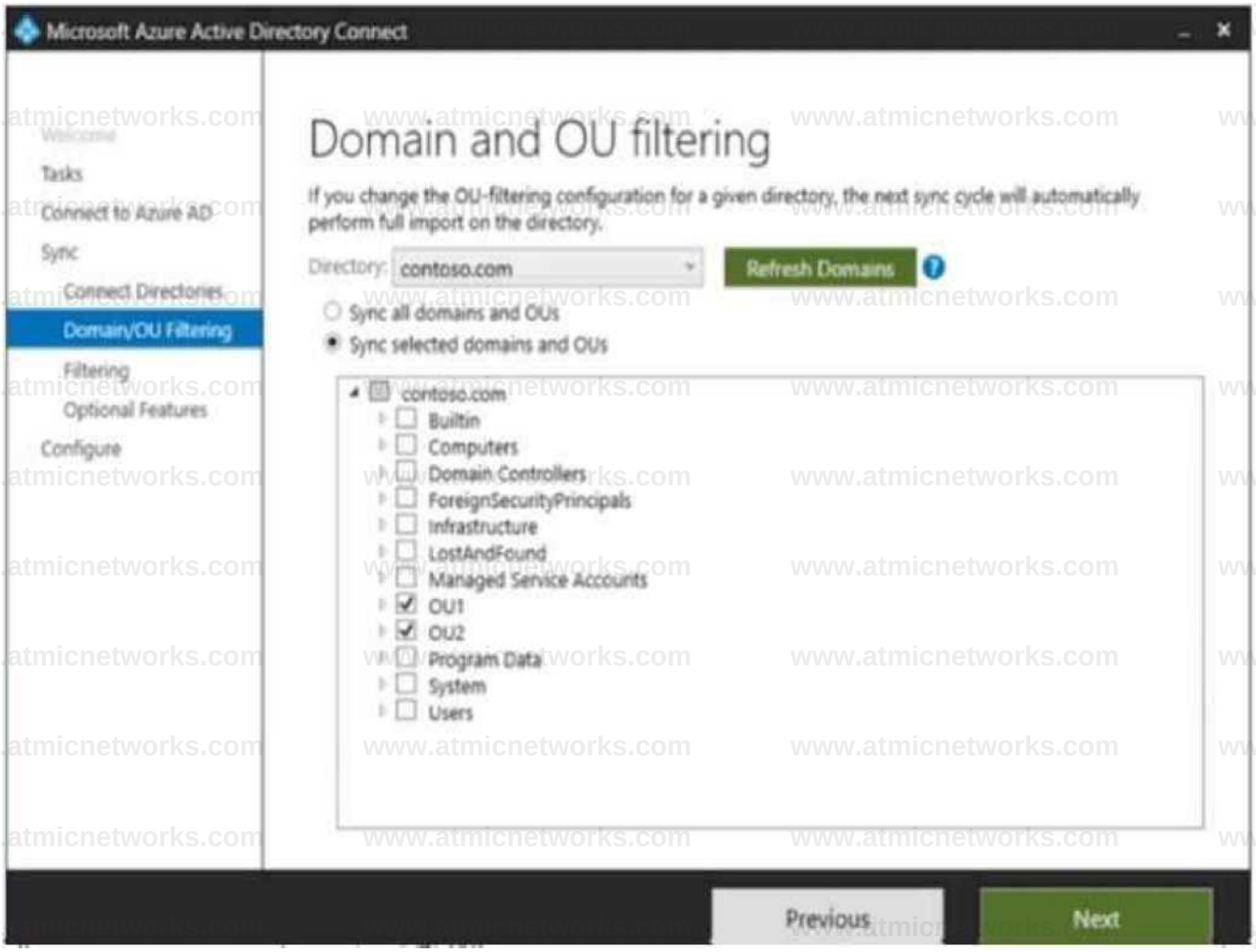
Question: 260

HOTSPOT

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the objects shown in the following table.

Name	Type	In organizational unit (OU)	Description
User!	User	OU1	Useri Is a member of Groupl.
User?		OU1	User? is not a member of any groups
Groupl	Security group	OU?	Used and Group2 are members of Group],
Group?	Security group	OU1	Group? is a member of Groupl.

You install Microsoft Entra Connect. You configure the Domain and OU filtering settings as shown in the Domain and OU Filtering exhibit. (Click the Domain and OU Filtering tab.)



You configure the Filter users and devices settings as shown in the Filter Users and Devices exhibit.
(Click the Filter Users and Devices tab.)
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 0

Statements	Yes	No
Userl syncs to the Microsoft Entra tenant		
User2 syncs to the Microsoft Entra tenant		
Group2 syncs to the Microsoft Entra tenant		

Answer:

Explanation:

Answer Area 5

Statements	Yes	No
User! syncs to the Microsoft Entra tenant	#	0
User2 syncs to the Microsoft Entra tenant	O	®
Group2 syncs to the Microsoft Entra tenant	®	

Question: 261

You have a Microsoft Entra tenant.

You need to query risky user activity for the tenant.

How long will the logs of risky user activity be retained?

A. 30 days
B. 60 days
C. 90 days
D. 180 days

Answer: A

Explanation:

Question: 262

You have a Microsoft Entra tenant.

You need to configure continuous access evaluation for app sign-ins and assign the configuration to users that are assigned the Application Administrator role.

What should you configure?

A. a Conditional Access policy
B. the Admin consent settings
C. a sign-in risk policy
D. an access review

Answer: D

Explanation:

Question: 263

You have a Microsoft Entra tenant that uses Microsoft Entra ID Premium licenses.

You plan to configure a terms of use (ToU) for the tenant.

You need to upload the ToU document.

Which format should you use for the document?

A. HTML
B. RTF
C. PDF
D. DOCX

Answer: C

Explanation:

Question: 264

You have an Azure subscription that contains a user-assigned managed identity named Managed1 in the East US Azure region. The subscription contains the resources shown in the following table.

Name	Type	Location
VM1	Virtual machine	West US
siwagel	Storage account	East US
WebApp1	Azure App Service app	East US

Which resources can use Managed 1 as their identity?

A. WebApp1 only
B. storage1 and WebApp1 only
C. VM1 and WebApp1 only
D. VM1, storage1, and WebApp1

Answer: D

Explanation:

Question: 265

You have a Microsoft Entra tenant.
You need to create a Conditional Access policy to manage administrative access to the tenant. The solution must ensure that administrators are authenticated by using a phishing-resistant multi-factor authentication (MFA) method.
Which three authentication methods should you include in the solution? Each correct answer presents a complete solution.

A. Windows Hello for Business
B. an FID02 security key
C. certificate-based authentication (multi-factor)
D. voice call
E. SMS
F. email OTP
G. certificate-based authentication (single-factor)
H. Microsoft Authenticator

Answer: A,B,C

Explanation:

Question: 266

You have an Azure subscription.
You need to use Microsoft Entra Permissions Management to automatically monitor permissions and create and implement right-size roles. The solution must follow the principle of least privilege.
Which role should you assign to the service principal of Permissions Management?

A. Reader
B. Contributor
C. Owner
D. User Access Administrator

Answer: D

Explanation:

Question: 267

You have a Microsoft 365 E5 subscription.
You need to ensure that users are prompted to accept a custom terms of use (Toll) agreement when they sign in to the subscription.
What should you configure?

A. an access package
B. a Conditional Access policy
C. a lifecycle workflow
D. an authentication method

Answer: B

Explanation:

Question: 268

You have a Microsoft 365 E5 subscription.
You need to be able to create a Microsoft Defender for Cloud Apps session policy. What should you do first?

A. From the Microsoft Defender portal, select User monitoring.
B. From the Microsoft Entra admin center, create a Conditional Access policy.
C. From the Microsoft Defender portal, select App onboarding/maintenance
D. From the Microsoft Defender portal, create a continuous report.

Answer: A

Explanation:

Question: 272

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 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 Microsoft Entra admin center, you configure the Notifications settings for multifactor authentication (MFA).

Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Question: 273

You have a Microsoft Entra tenant that contains the users shown in the following table.

Namt	Group
Used	Groupl
User2	Group!
UserB	Groupi
UseM	Group?
Useri	*None*

You have an administrative unit named Au1.Group1, User2, and User3are members of Au1.

User5 is assigned the User Administrator role for Au1.

For which users can User5 reset passwords?

A. User1 and User2 only
B. User2 and User3 only
C. User3 and User4 only
D. User1, User2, and User3

Answer: B

Explanation:

Question: 274

You have an Azure subscription that contains the resources shown in the following table.

Name	Type
VM1	Virtual machine
App1	Azure App Semite
Vaui:1	Azure key Vault
Storage 1	Storage account

You need to grant permissions to the resources by using attribute-based access control (ABAC). To which resource can you grant permissions?

A. Vault1
B. VM1
C. App1
D. storage 1

Answer: D

Explanation:

Question: 275

Your company has a Microsoft Entra tenant that contains a user named User 1.

The company has two departments named marketing and finance.

You need to grant permissions to User1 to manage only the users in the marketing department. What should you create first?

A. an administrative unit B. a Microsoft 365 group C. a management group D. a resource group

Answer: A

Explanation:

Question: 276

HOTSPOT

You have a Microsoft Entra tenant that contains two groups named Group! and Group2 and the users shown in the following table.

Name	Type	Member of	Description
Useri	Member	Gmupl	Atone
user 2	Guest	Groupl	Atone
Usei?	Member	None	Assigned the Owner role for Groupl
User4	Member	Group2	Assigned the Owner role for Group2
Llser5	Guest	Groups	Atone

Group2 is a member of Group1.

You configure an access review that has the following settings:

- Name: Review 1
- Select what to review: Teams + Groups
- Review scope: Select Teams + groups
- Group: Group1
- Scope: Guest users only
- Select reviewers: Group owners(s)

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
User3 can perform an access review of Useri.	○	○
User3 can perform an access review of UseM		
Usefl can perform an access review of User5,		

Answer:

Explanation:

Answer Area

Statements	Yes	No
User3 can perform an access review of Useri.		●
User3 can perform an access review of User4.	0	●
UserZ can perform an access review of User5.		

Question: 278

You have an Azure subscription named Sub1.

You purchase a Microsoft Entra Permissions Management license.

You need to onboard Permissions Management.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE; Each correct selection is worth one point.

A. Implement a Microsoft Entra application proxy.
B. From Microsoft Entra Permissions Management, configure data collection.
C. Create a role assignment for Sub1.
D. From the Microsoft Entra admin center, configure the Diagnostic settings.
E. From the Microsoft Entra admin center, create an app registration.
F. From the Azure portal, create a data collection rule (DCR).

Answer: B,E

Question: 279

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 a Microsoft Entra tenant.

You discover that when a user account is disabled in Active Directory, the disabled user can still authenticate to Microsoft Entra 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 Microsoft Entra.

Solution: You configure Microsoft Entra Password Protection.

Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Question: 280

HOTSPOT

You have a Microsoft Entra tenant that contains the users shown in the following table.

Name	Microsoft Entra rale
Used	Global Administrator
User2	□ute Definition Administrator
User3	Secur ty Administrator

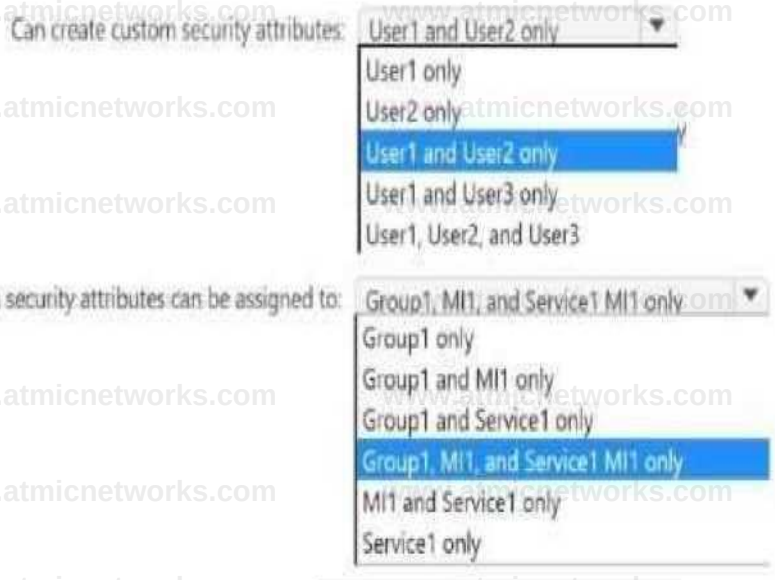
The tenant contains the identities shown in the following table.

Name	Type
Group1	Security group
Service1	Service principal
MI1	Managed identity

Which users can create custom security attributes, and to which identities can the attributes be assigned? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Question: 281

You have a Microsoft Entra tenant that has a Microsoft Entta ID P2 license. You create a Log Analytics workspace. You need to ensure that you can view Microsoft Entra ID audit log information by using Azure Monitor. What should you do first?

A. Create an Microsoft Entra ID workbook.
B. Modify the Diagnostics settings for Microsoft Entra ID.
C. Runtheupdate-ngoomaincmdlet.
D. Run the update-Mgorganization cmdlet

Answer: B

Question: 282

You have a Microsoft 365 tenant.
In Microsoft Entra ID, you configure the terms of use.
You need to ensure that only users who accept the terms of use can access the resources in the tenant Other users must be denied access.
What should you configure?

A. an access policy in Microsoft Defender for Cloud Apps
B. a compliance policy in Microsoft Intune
C. Terms and conditions in Microsoft Intune
D. a conditional access policy in Microsoft Entra ID

Question: 284

You have a Microsoft Entra tenant.
You discover that a large number of new apps were added to the tenant.
You need to implement an approval process for new enterprise applications. What should you do?

A. From the Microsoft Defender portal, create a Cloud Discovery anomaly detection policy.
B. From the Microsoft Entra admin center, configure the Admin consent settings.
C. From the Microsoft Defender portal, configure an app connector.
D. From the Microsoft Entra admin center, configure an access review.

Answer: B

Explanation:

Question: 285

You have an Azure subscription that contains a virtual machine named VM1. VM1 has the following configurations:

- Private IP address: 172.16.1.5
- Public IP address 10fl.143.16U5
- System-assigned managed identity status: On

You install an app named App1 on VM1.
You need to configure App1 to request a managed identity app-only access token. Which IP address should App1 use for the request?

A. 108.143.161.25
B. 127.0.0.1
C. 169.254.169.254
D. 172.1615

Answer: C

Explanation:

Question: 286

You have an Azure subscription that is linked to a Microsoft Entra tenant. The tenant contains a registered app named App1. You have a partner organization that has a Microsoft Entra tenant. The tenant contains a registered app named App2. You need to ensure that App1 can access App2. Which two types of credentials can App1 use? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. certificate

B. managed identity
C. secret
D. user account
E. one-time password

Answer: A,C

Explanation:

Question: 287

HOTSPOT
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with a Microsoft Entra tenant. You need to ensure that user authentication always occurs by validating passwords against the AD DS domain. What should you configure, and what should you use? To answer, select the appropriate options in the answer are a. NOTE: Each coned selection is worth one point.

Answer Area

Configure: Pass-through authentication* Microsoft Entra
Password protection Cross-tenant synchronization

| Password hash synchronization

Use

Microsoft Identity Managei (MIM)
The Microsoft Entra admin center
The Microsoft Purview compliance portal

Answer:

Explanation:

Answer Area

Configure: Pass-through authentication

Use Microsoft Entra Connect

Question: 288

You have two Microsoft Entra tenants named contoso.com and fabrikam.com. Contoso.com contains the identities shown in the following table.

Name	Type
User! Uwi	
GHM^H	Security group
Group?	Microsoft 365 group

You configure cross-tenant synchronization from contoso.com to fabrikam.com. Which identities will sync with fabrikam.com?

A. User1 only
B. User1 and Group1 only
C. User 1 and Gtoup2 only
D. User1, Group1, and Group2

Answer: A

Explanation:

Question: 289

You work for a company named Contoso, Ltd. that has a Microsoft Entra tenant named contoso.com. Contoso is working on a project with the following two partner companies:

• A company named
A. Datum Corporation that has a Microsoft Entra tenant named adatum.com
• A company named Fabrikam, Inc. that has a Microsoft Entra tenant named fabtikam.com

When you attempt to invite a new guest user from adatum.com to contoso.com, you receive an error message. You can successfully invite a new guest user from fabiikam.com to contoso.com. You need to be able to invite new guest users from adatum.com to contoso.com. What should you configure? A. Verifiable credentials

B. Named locations
C. Guest invite settings
D. Collaboration restrictions

Answer: D

Explanation:

Question: 290

You have a Microsoft Entra tenant named contoso.com that contains an enterprise application named Appl.
A contractor uses the credentials of user1@outlook.com.
You need to ensure that you can provide the contractor with access to App1. The contractor must be able to authenticate as user1 @outlook.com.
What should you do?

A. Run the New-Mguser cmdlet
B. Run the New-MgInvitation cmdlet
C. Configure the External collaboration settings
D. Implement Microsoft Entra Connect sync.

Answer: B

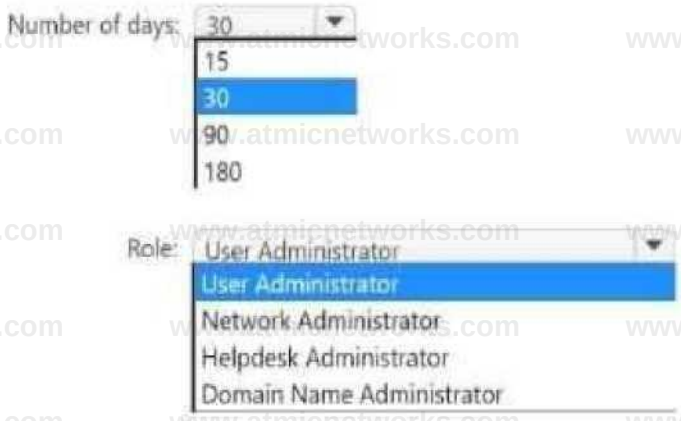
Explanation:

Question: 291

HOTSPOT
You have a Microsoft Entra tenant that contains a user named User1.
An administrator deletes User1. You need to identify the following:
- What is the maximum number of days for which you have the option to restore the User1 account?
- Which is the least privileged role that can be used to restore User1?

To answer, select the appropriate options in the answer are
a. NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Number of days' 30 ^

Role User Administrator

Question: 292

DRAG DROP

You have a Microsoft 365 E5 subscription. The subscription contains 500 devices that run Windows

You deploy the Global Secure Access client to the devices.

You need to prevent users from accessing httpsy/contoso.com from the devices

Which three actions should you perform in sequence? To answer move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

- Create an app protection policy.
- Create a Conditional Access policy.
- Create a remote network.
- Create a web content filtering policy.
- Configure a security profile.

Answer Area

Answer:

Explanation:

Actions

- Create an app protection policy.
- Create a Conditional Access policy.

Answer Area

1. Create a remote network.
2. Create a web content filtering policy.
3. Configure a security profile.

Question: 293

You have an on-premises app named Appl. You have a Microsoft Entra tenant

You plan to publish App1 by using Microsoft Entra Private Access. You need to enable the Private access profile. Which blade should you use in the Microsoft Entra admin center?

A. Remote networks B. Traffic forwarding C. Security profiles

D. Connectors

Answer: C

Explanation:

Question: 294

HOTSPOT

You have a Microsoft Entra tenant that contains the identities shown in the following table.

Name	Typ®	Member of
Useri	User	Groupl
Managed^	Managed identity	Groupl
Us	User	Groups
User4	User	None

Group1 has the following configurations:

- Owners: User1, User4
- Members: User1, Managed2, Gioup2

You create an access review that has the following settings:

- Name: Review1
- Review scope: Select Teams + Groups
- Group: Group1
- Scope: All users
- Select reviewers: Group owner(s)

The Fallback reviewers: setting is NOT configured.

Answer Area

Statements	Yes	No
Used can perform an access review for Used		
User 1 can petform an access review for Managed?.		
Used can perform an access review for User?		

Answer:

Explanation:

Answer Area

Statements	Yes	No
User 1 can perform an access review for User!.	®	O
User 1 can perform an access review for Managed?.	®	
Useri can perform an access review for User?		*

Question: 295

HOTSPOT

You have an Azure subscription named Sub1 that contains three users named User1. User2, and User3. Sub1 has a storage account named storage1 that contains the resources shown in the following table.

Hamfl	Type	Contents
cotul	Container	Fikl
shaiei	1 e sha'e	Filei

Sub1 contains the users shown in the following table.

Name	Role	Scope
User!	Reader	Sub1
Useri	Reader	Su bl
User?	Storage Blob Data Reader	forage 1
User 3	Storage Contributor	storagel

Which users can read File1, and which users can read File2? To answer, select the appropriate options in the answer are

a. NOTE; Each correct selection is worth one point.

Answer Area

Filet
- User 1, User2, and User 3
- User2 only
- User 3 only
- Used and UserZ only
- User? and User 3 only
- Used, User?, and User 3

File?:
- Used, User? and Used
- User 2 only
- User 3 only
- Used and User? only
- User2 and Used only
- Used. User? and User3

Answer:

Explanation:

Answer Area

Filel: User 1. User2, and User J

File2: Useri, User2 and UserB

Question: 296

You have a Microsoft Entra tenant that contains the users shown in the following table:

Name	User type	Member of
User1	Member	Group1
User2	Member	Group1
User3	Guest	Group1

User1 is the owner of Group1.
You create an access review that has the following settings:
What to review: Teams + Groups
Scope: All users
Group: Group1
Reviewers: Users review their own access
Which users can perform access reviews for User3?

A. User1 only
B. User3 only
C. User1 and User2 only
D. User1, User2, and User3

Answer: B

Explanation:

Comprehensive and Detailed In-Depth
Let's break this down step by step based on the Microsoft Entra access review settings and the

principles outlined in Microsoft Identity and Access Administrator documentation.

Understanding the Access Review Settings:

What to review: Teams + GroupsThis indicates that the access review is evaluating memberships in Teams and Groups within the Microsoft Entra tenant. Since the group specified is Group1, the review focuses on Group1 membership.
Scope: All usersThe scope defines who is being reviewed. "All users" in this

Question: 297

DRAG DROP

You have a Microsoft 365 E5 tenant.
You purchase a cloud app named App1.

You need to enable real-time session-level monitoring of App1 by using Microsoft Defender for Cloud Apps.
In which order should you perform the actions? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actons **Answer Area**

:: Register Appt in Microsoft Entra ID.

„ From Microsoft Defender for Cloud Apps modify the Connected " apps settings for App 1

|:: From Microsoft Defender for Cloud Apps create a session policy

.. Create a conditional access policy that has session controls
" configured.

Answer:

Explanation:

Register App1 in Microsoft Entra ID.
Create a conditional access policy that has session controls configured.
From Microsoft Defender for Cloud Apps, modify the Connected apps settings for App1.
From Microsoft Defender for Cloud Apps, create a session policy.

Let's break this down step by step based on Microsoft Defender for Cloud Apps (MDCA) and Microsoft Entra ID integration for enabling real-time session-level monitoring, as outlined in Microsoft Identity and Access Administrator documentation.
Understanding the Goal: Real-Time Session-Level Monitoring with Microsoft Defender for Cloud Apps:
Microsoft Defender for Cloud Apps (MDCA) is a Cloud Access Security Broker (CASB) solution that provides visibility, control, and threat protection for cloud applications.
Real-time session-level monitoring allows MDCA to inspect and control user activities within a cloud app (App1 in this case) during active sessions. This requires integration with Microsoft Entra ID and the use of Conditional Access policies to route sessions through MDCA for monitoring.

The Microsoft 365 E5 tenant includes licenses for Microsoft Entra ID P2 and Microsoft Defender for Cloud Apps, which are necessary for this functionality.
Step-by-Step Analysis of the Actions:To enable real-time session-level monitoring, the actions must be performed in a logical order that aligns with Microsoft's recommended workflow for integrating a cloud app with MDCA.
Step 1: Register App1 in Microsoft Entra ID.

Before App1 can be monitored by MDCA, it must be registered as an application in Microsoft Entra ID. This step involves adding App1 to the tenant's enterprise applications, which allows Microsoft Entra ID to manage authentication and authorization for the app.

Registering the app in Microsoft Entra ID enables single sign-on (SSO) and allows the app to be governed by Conditional Access policies, which is a prerequisite for session-level monitoring. This is the first step because none of the other actions can proceed without App1 being recognized by Microsoft Entra ID.

Step 2: Create a conditional access policy that has session controls configured.

Microsoft Defender for Cloud Apps integrates with Microsoft Entra ID Conditional Access to enforce session-level monitoring. A Conditional Access policy must be created to target App1 and include session controls that route user sessions through MDCA.

In the Conditional Access policy, under "Session" controls, you enable the option "Use Conditional Access App Control," which integrates with MDC

A. This allows MDCA to monitor and control the session in real time.

This step must come after registering the app in Microsoft Entra ID because the Conditional Access policy needs to target an existing app. It must also precede the MDCA-specific steps because the session control integration sets up the connection between Microsoft Entra ID and MDCA. Step 3: From Microsoft Defender for Cloud Apps, modify the Connected apps settings for App1. After the Conditional Access policy routes sessions to MDCA, you need to configure App1 within MDCA by modifying its Connected apps settings. This step involves ensuring that App1 is properly connected to MDCA, which may include configuring API connectors or verifying that MDCA can monitor the app's activities.

This step is necessary to ensure MDCA has the necessary permissions and configurations to monitor App1. It comes after the Conditional Access policy because the policy enables the integration, and now MDCA needs to be set up to handle the app.

Step 4: From Microsoft Defender for Cloud Apps, create a session policy.

Finally, you create a session policy in MDCA to define the real-time monitoring and control rules for App1. A session policy in MDCA allows you to monitor user activities (e.g., file downloads, data sharing) and apply actions (e.g., block, notify) based on predefined conditions.

This step is the last because it relies on the previous steps: the app must be registered, the Conditional Access policy must route sessions to MDCA, and the Connected apps settings must be configured for MDCA to recognize App1. Only then can you define session policies to enforce real-time monitoring.

Why This Order?

The order ensures a logical flow:

Registering the app in Microsoft Entra ID establishes the app's identity in the tenant.

The Conditional Access policy enables the integration with MDCA by routing sessions through it. Modifying the Connected apps settings in MDCA ensures the app is properly set up for monitoring. Creating a session policy in MDCA defines the specific monitoring and control rules for real-time session-level monitoring.

Deviating from this order would result in errors. For example, creating a session policy in MDCA before registering the app in Microsoft Entra ID would fail because MDCA wouldn't recognize the app.

Additional Considerations:

The Microsoft 365 E5 license includes Microsoft Entra ID P2 and Microsoft Defender for Cloud Apps, so no additional licensing is required for this scenario.

If App1 is not a supported app for MDCA's app connectors, additional steps (e.g., using a custom app connector) might be needed, but the question implies App1 can be monitored with the standard process.

Session policies in MDCA can include actions like blocking downloads or requiring step-up authentication, which are applied in real time during the user's session.

Conclusion:The correct order to enable real-time session-level monitoring of App1 using Microsoft Defender for Cloud Apps is:

Register App1 in Microsoft Entra ID.

Create a conditional access policy that has session controls configured.
From Microsoft Defender for Cloud Apps, modify the Connected apps settings for App1.
From Microsoft Defender for Cloud Apps, create a session policy.
Reference:
Microsoft Defender for Cloud Apps documentation: "Session control with Microsoft Defender for Cloud Apps" (Microsoft Learn:https://learn.microsoft.com/en-us/defender-cloud-apps/session- policy)
Microsoft Entra ID Conditional Access documentation: "Session controls in Conditional Access" (Microsoft Learn:https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept- conditional-access-session)
Microsoft Identity and Access Administrator (SC-300) exam study guide, which covers integrating Microsoft Defender for Cloud Apps with Microsoft Entra ID for session-level monitoring.

Question: 298

HOTSPOT

You have a Microsoft Entra tenant that contains a group named Group1 and two users named User1 and User2. User1 is a member of Group1.
You register an enterprise application named App1.
You enable self-service application access for App1 and configure the following settings:
Allow users to request access to this application: Yes
To which group should assigned users be added: Group1
Require approval before granting access to this application: Yes
Who is allowed to approve access to this application: User2
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Statements	Yes	No
User! must request access to App1 before they can use the app	0	O
If UserZ requests access to Appl, they will be added to Groupl automatically	O	O
User2 can approve Appl requests by using the Microsoft Entra admin center	0	O

Answer:

Explanation:

User1 must request access to App1 before they can use the app: No
If User2 requests access to App1, they will be added to Group1 automatically: Yes
User2 can approve App1 requests by using the Microsoft Entra admin center: Yes

Let's break this down step by step based on Microsoft Entra ID self-service application access and the configured settings, as outlined in Microsoft Identity and Access Administrator documentation.
Understanding Self-Service Application Access in Microsoft Entra ID:
Self-service application access in Microsoft Entra ID allows users to request access to applications without needing an administrator to manually assign them. This is configured on a per-application basis.
The settings for App1 are:
Allow users to request access to this application: Yes– Users can request access to App1.
To which group should assigned users be added: Group1– Users who are granted access will be added to Group1, which provides the necessary permissions to use App1.

Require approval before granting access to this application: Yes– Access requests must be approved before the user is added to Group1.

Who is allowed to approve access to this application: User2– User2 is the designated approver for access requests to App1.

Statement 1: User1 must request access to App1 before they can use the app.

Analysis:

User1 is already a member of Group1, as stated in the question.

The self-service settings specify that users who are granted access to App1 will be added to Group1.

This implies that membership in Group1 is what grants access to App1.

Since User1 is already a member of Group1, they already have access to App1. In Microsoft Entra ID, if a user is already assigned to an application (either directly or via group membership), they do not need to request access through the self-service process—they can simply use the app.

The self-service access request process is for users who are not yet assigned to the app (i.e., not in Group1). Since User1 is already in Group1, they do not need to request access.

Conclusion:This statement isNo. User1 does not need to request access because they are already a member of Group1 and can use App1 immediately.

Statement 2: If User2 requests access to App1, they will be added to Group1 automatically.

Analysis:

User2 is not a member of Group1 (the question does not state that User2 is in Group1).

The self-service settings allow users to request access to App1, and the setting "To which group should assigned users be added: Group1" means that users who are granted access will be added to Group1.

However, the setting "Require approval before granting access to this application: Yes" means that User2's request must be approved before they are added to Group1. The approver for App1 requests is User2 themselves, which introduces a potential conflict.

In Microsoft Entra ID, if a user is both the requester and the approver, the system typically allows them to approve their own request (unless additional policies prevent this, which is not specified in the question). Therefore, User2 can request access and approve their own request.

Once the request is approved, User2 will be added to Group1 automatically as per the self-service settings. The term "automatically" in the statement refers to the process after approval—once approved, the addition to Group1 happens without further manual intervention.

Conclusion:This statement isYes. If User2 requests access to App1 and approves their own request, they will be added to Group1 automatically.

Statement 3: User2 can approve App1 requests by using the Microsoft Entra admin center.

Analysis:

The self-service settings specify that User2 is the designated approver for access requests to App1.

In Microsoft Entra ID, approvers can manage access requests through the Microsoft Entra admin center (via the "My Access" portal or the "Access Requests" section, depending on their role and permissions).

User2, as the designated approver, will receive a notification (via email or the My Access portal) when a request is made. They can then log into the Microsoft Entra admin center, navigate to the access requests section, and approve or deny the request.

Even though User2 is not explicitly an admin, the fact that they are designated as the approver for App1 requests grants them the ability to approve requests through the Microsoft Entra admin center. Conclusion:This statement isYes. User2 can approve App1 requests using the Microsoft Entra admin center.

Additional Considerations:

If User2 were not allowed to approve their own request (e.g., due to a separation of duties policy), Statement 2 might be affected. However, Microsoft Entra ID does not enforce such a restriction by default, and the question does not specify any additional policies.

The Microsoft Entra admin center is the primary interface for managing access requests, but users can also approve

requests via email links or the My Access portal. The statement specifically mentions the admin center, which is a valid method.

Conclusion:

Statement 1:No– User1 does not need to request access since they are already in Group1.

Statement 2:Yes– User2 will be added to Group1 automatically after their request is approved (by themselves).

Statement 3:Yes– User2 can approve requests using the Microsoft Entra admin center.

Reference:

Microsoft Entra ID documentation: "Configure self-service application access" (Microsoft Learn:https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/configure-self-service)

Microsoft Entra ID documentation: "Manage access requests" (Microsoft Learn:https://learn.microsoft.com/en-us/entra/identity/governance/access-reviews-overview) Microsoft Identity and Access Administrator (SC-300) exam study guide, which covers self-service application access and approval workflows in Microsoft Entra ID.

Question: 299

You have a Microsoft Entra tenant that contains the users shown in the following table:

Name	Role
Adminl	Global Administrator
Admin2	Conditional Access Administrator
Admin3	Authentication Policy Administrator
Admin4	Global Administrator

Admin4 creates a Conditional Access policy named Policy1 by using the "Require multifactor authentication for Azure management" template.

Which users will be required to use multi-factor authentication (MFA) the next time they sign in?

A. Admin2 and Admin3 only
B. Admin1 and Admin4 only
C. Admin1, Admin2, and Admin3 only
D. Admin1, Admin2, Admin3, and Admin4

Answer: B

Explanation:

Comprehensive and Detailed In-Depth

Let’s break this down step by step based on Microsoft Entra ID Conditional Access policies, the "Require multifactor authentication for Azure management" template, and the roles assigned to the users, as outlined in Microsoft Identity and Access Administrator documentation.

Understanding the "Require multifactor authentication for Azure management" Template:

Microsoft Entra ID Conditional Access policies allow administrators to enforce security controls, such as requiring multi-factor authentication (MFA), based on specific conditions.

The "Require multifactor authentication for Azure management" template is a predefined Conditional Access policy template in Microsoft Entra ID. This template is designed to secure access to Azure management interfaces, such as the Azure portal, Azure PowerShell, Azure CLI, and other Azure management endpoints.

Key Details of the Template:

Cloud Apps or Actions:The template targets the "Microsoft Azure Management" cloud app. This includes all Azure management interfaces but does not apply to other cloud apps (e.g., Microsoft 365 apps).

Users:By default, the template applies to "All users," but it can be modified to include or exclude specific users or groups. The question does not specify any modifications, so we assume the default "All users" scope.

Conditions:Typically, there are no specific conditions (e.g., device state, location) in this template unless modified.

Grant Controls:The template enforces "Require multi-factor authentication" as the access control. Therefore, this policy will require MFA for any user who attempts to access Azure management interfaces.

Understanding the Roles and Their Interaction with Azure Management:

Let's examine the roles assigned to each user and whether they are likely to interact with Azure management interfaces:

Admin1: Global Administrator

A Global Administrator has full access to all Microsoft Entra ID and Azure resources, including the ability to manage Azure subscriptions, resources, and the Azure portal.

Global Administrators frequently access Azure management interfaces (e.g., the Azure portal) to perform administrative tasks. Therefore, Admin1 will be subject to the Conditional Access policy when they sign in to access Azure management.

Admin2: Conditional Access Administrator

A Conditional Access Administrator can manage Conditional Access policies in Microsoft Entra ID but does not have direct access to Azure management interfaces by default.

This role is focused on Microsoft Entra ID, not Azure resource management. Unless Admin2 has been granted additional Azure roles (e.g., Contributor, Owner), they are unlikely to access Azure management interfaces. The question does not indicate any additional roles for Admin2, so we assume they do not interact with Azure management.

Admin3: Authentication Policy Administrator

An Authentication Policy Administrator can manage authentication methods and policies in Microsoft Entra ID (e.g., MFA settings, passwordless authentication).

Like the Conditional Access Administrator, this role is specific to Microsoft Entra ID and does not grant access to Azure management interfaces by default. Admin3 would not typically access Azure management unless assigned additional Azure roles, which are not specified.

Admin4: Global Administrator

Like Admin1, Admin4 is a Global Administrator and has full access to Azure management interfaces.

Admin4 will be subject to the Conditional Access policy when accessing Azure management.

Applying the Conditional Access Policy:

The policy applies to "All users" (default scope of the template) and targets the "Microsoft Azure Management" cloud app.

The policy requires MFA for any user who accesses Azure management interfaces.

Admin1 and Admin4 (Global Administrators):

As Global Administrators, both Admin1 and Admin4 will access Azure management interfaces (e.g., the Azure portal) as part of their administrative duties.

The next time they sign in to access Azure management, the Conditional Access policy (Policy1) will enforce MFA.

Admin2 (Conditional Access Administrator) and Admin3 (Authentication Policy Administrator): These roles do not inherently grant access to Azure management interfaces. Their responsibilities are limited to Microsoft Entra ID tasks, such as

managing Conditional Access policies or authentication methods.
Unless Admin2 or Admin3 attempts to access Azure management (which they are not authorized to do by default), the policy will not apply to them. The question asks about the "next time they sign in," but the policy only triggers MFA when accessing the targeted cloud app (Microsoft Azure Management). If Admin2 and Admin3 sign in to Microsoft Entra ID or other apps (e.g., Microsoft 365), the policy does not apply.
Analysis of the Options:
A. Admin2 and Admin3 only:
Incorrect. Admin2 and Admin3 are not likely to access Azure management interfaces based on their roles, so the policy will not require MFA for them.
B. Admin1 and Admin4 only:
Correct. Admin1 and Admin4 are Global Administrators who will access Azure management interfaces, triggering the policy to require MFA the next time they sign in to those interfaces.
C. Admin1, Admin2, and Admin3 only:
Incorrect. Admin2 and Admin3 are not subject to the policy for the reasons stated above.
D. Admin1, Admin2, Admin3, and Admin4:
Incorrect. While the policy applies to "All users," only Admin1 and Admin4 (Global Administrators) are likely to access Azure management interfaces, triggering the MFA requirement.
Additional Considerations:
If Admin2 or Admin3 were assigned additional Azure roles (e.g., Contributor, Owner) that grant access to Azure management, they would also be subject to the policy. However, the question does not indicate any such roles.
The phrase "the next time they sign in" can be misleading. The policy only enforces MFA when the user signs in to the targeted cloud app (Microsoft Azure Management). IfAdmin2 or Admin3 signs in to a different app (e.g., Microsoft 365), the policy does not apply.
If the policy were modified to target a different cloud app (e.g., "All apps") or to include specific users, the answer might change. However, the question specifies the default template behavior. Conclusion:The Conditional Access policy (Policy1) created using the "Require multifactor authentication for Azure management" template will require MFA for users who access Azure management interfaces. Based on their roles:
Admin1 and Admin4 (Global Administrators) will be required to use MFA the next time they sign in to Azure management.
Admin2 and Admin3 (Conditional Access Administrator and Authentication Policy Administrator) are not likely to access Azure management, so the policy does not apply to them.Therefore, the correct answer isB.
Reference:
Microsoft Entra ID Conditional Access documentation: "Common Conditional Access policies – Require MFA for Azure management" (Microsoft Learn:https://learn.microsoft.com/en- us/entra/identity/conditional-access/concept-conditional-access-policy-common#require-mfa-for- azure-management)
Microsoft Entra ID role documentation: "Administrator role permissions in Microsoft Entra ID" (Microsoft Learn:https://learn.microsoft.com/en-us/entra/identity/role-based-access- control/permissions-reference)
Microsoft Identity and Access Administrator (SC-300) exam study guide, which covers Conditional Access policies and their application to specific roles and cloud apps.

Question: 300

You have a Microsoft Entra tenant.
You configure self-service password reset (SSPR) with the following settings:
Require users to register when signing in: Yes
Number of methods required to reset: 1
What is a valid authentication method available to users?

A. A smartcard
B. A mobile app code
C. An FIDO2 security token
D. A Windows Hello PIN

Answer: B

Explanation:

Comprehensive and Detailed In-Depth

Let's break this down step by step based on Microsoft Entra ID self-service password reset (SSPR) settings and the available authentication methods, as outlined in Microsoft Identity and Access Administrator documentation.

Understanding Self-Service Password Reset (SSPR) in Microsoft Entra ID:

Self-service password reset (SSPR) allows users to reset their passwords without administrator intervention, improving security and reducing helpdesk workload.

The settings provided are:

Require users to register when signing in: Yes– Users must register their authentication methods (e.g., phone number, email, security questions) the first time they sign in. This ensures they have methods available for SSPR.

Number of methods required to reset: 1– Users must verify their identity using one authentication method to reset their password. This is the minimum number of methods required, meaning users must have at least one method registered, and they will use one method during the reset process. Available Authentication Methods for SSPR:

Microsoft Entra ID SSPR supports a specific set of authentication methods that users can use to verify their identity during a password reset. These methods are configured by the administrator in the Microsoft Entra admin center under "Password reset" settings.

The default authentication methods available for SSPR include:

Email:Users receive a code sent to an alternate email address.

Mobile phone (SMS):Users receive a code via SMS to their registered mobile phone.

Mobile app code:Users use a code generated by the Microsoft Authenticator app (or another compatible authenticator app).

Mobile app notification:Users receive a push notification in the Microsoft Authenticator app to approve the reset.

Security questions:Users answer predefined security questions they set up during registration.

Important Note:Methods like smartcards, FIDO2 security tokens, and Windows Hello are not supported for SSPR. These methods are typically used for authentication during sign-in (e.g., MFA or passwordless sign-in), not for the SSPR process.

Analysis of the Options:

A. A smartcard:

Smartcards are a form of certificate-based authentication often used for sign-in to Windows devices or VPNs. They require a physical card and a reader, and they are typically used for primary authentication, not for SSPR.

Microsoft Entra ID SSPR does not support smartcards as an authentication method for password reset. Smartcards are not listed as an available method in the SSPR configuration settings.

Conclusion:This is incorrect.

B. A mobile app code:

A mobile app code refers to a time-based one-time password (TOTP) generated by an authenticator app, such as the Microsoft Authenticator app.

This is a supported method for SSPR in Microsoft Entra ID. Users can register the Microsoft Authenticator app (or another compatible app) and use the generated code to verify their identity during a password reset.

Since the setting "Number of methods required to reset: 1" means only one method is needed, a mobile app code is a

valid option if the user has registered it.
Conclusion:This is correct.
C. An FIDO2 security token:
FIDO2 security tokens (e.g., YubiKey) are hardware-based security keys that support passwordless authentication in Microsoft Entra ID. They are part of Microsoft's passwordless authentication strategy and can be used for sign-in. However, FIDO2 security tokens are not supported for SSPR. The SSPR process does not allow users to verify their identity using a FIDO2 security key because the reset process is designed to work with simpler, more accessible methods like email, SMS, or app-based codes.
Conclusion:This is incorrect.
D. A Windows Hello PIN:
Windows Hello PIN is a device-specific authentication method used to sign in to Windows devices. It is part of Windows Hello, which also includes biometric authentication (e.g., facial recognition, fingerprint).
Windows Hello PIN is not supported for SSPR in Microsoft Entra ID. The SSPR process occurs in a web-based portal (e.g., aka.ms/sspr) and does not integrate with device-specific authentication methods like Windows Hello. Additionally, Windows Hello PIN is tied to a specific device, whereas SSPR is designed to be device-agnostic.
Conclusion:This is incorrect.
Additional Considerations:
The setting "Require users to register when signing in: Yes" ensures that users have at least one authentication method registered. However, the question does not specify which methods are enabled by the administrator. In Microsoft Entra ID, the default enabled methods for SSPR typically include email, mobile phone (SMS), mobile app code, and mobile app notification. Security questions may also be enabled but are less common due to security concerns.
If the administrator has disabled certain methods (e.g., mobile app code), the answer could change. However, the question does not indicate any such restrictions, so we assume the default methods are available.
The "Number of methods required to reset: 1" setting means users only need to use one method to reset their password, but they may have multiple methods registered. The question asks for a "valid authentication method available to users," so we need to identify a method that SSPR supports.
Conclusion:Based on the SSPR settings and the supported authentication methods in Microsoft Entra ID:
A mobile app code (option B) is a valid authentication method for SSPR, as it is supported by default and aligns with the configuration.
Smartcards, FIDO2 security tokens, and Windows Hello PIN are not supported for SSPR.Therefore, the correct answer isB.
Reference:
Microsoft Entra ID documentation: "Self-service password reset authentication methods" (Microsoft Learn:https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr- howitworks#authentication-methods)
Microsoft Entra ID documentation: "Configure self-service password reset" (Microsoft Learn:https://learn.microsoft.com/en-us/entra/identity/authentication/howto-sspr-deployment) Microsoft Identity and Access Administrator (SC-300) exam study guide, which covers SSPR configuration and supported authentication methods.

Question: 301

You have an Azure subscription that contains a user named User1 and an Azure Key Vault named Vault1.
You need to ensure that User1 can read the metadata of certificates, keys, and secrets stored in Vault1. The solution must follow the principle of least privilege.
Which role should you assign to User1?

A. Key Vault Crypto User

B. Key Vault Crypto Officer
C. Key Vault Reader
D. Key Vault Secrets User

Answer: C

Explanation:

Comprehensive and Detailed In-Depth
Let's break this down step by step based on Azure Key Vault roles, permissions, and the principle of least privilege, as outlined in Microsoft Identity and Access Administrator documentation.
Understanding Azure Key Vault and the Requirement:
Azure Key Vault is a service that securely stores and manages cryptographic keys, secrets, and certificates. It uses role-based access control (RBAC) to manage permissions for users, groups, and applications.
The question requires that User1 canread the metadataof certificates, keys, and secrets in Vault1. In Azure Key Vault, "metadata" refers to the properties of these objects (e.g., name, creation date, expiration date), not the actual content (e.g., the secret value, key value, or certificate private key). The solution must follow theprinciple of least privilege, meaning User1 should be granted the minimum permissions necessary to perform the task, without access to unnecessary actions (e.g., modifying or deleting objects).
Azure Key Vault RBAC Roles and Permissions:
Azure Key Vault supports built-in RBAC roles that define specific permissions for managing keys, secrets, and certificates. Let's examine each role in the options:
Key Vault Crypto User:
This role allows a user to perform cryptographic operations using keys (e.g., encrypt, decrypt, sign, verify) and to read key metadata.
Permissions include: Microsoft.KeyVault/vaults/keys/read (read key metadata) and cryptographic operations like encrypt, decrypt, etc.
However, this role does not grant permissions to read metadata for secrets or certificates, and it includes cryptographic operation permissions, which are not needed for the task.
Key Vault Crypto Officer:
This role is designed for managing keys and performing cryptographic operations. It includes permissions to create, delete, update, and read keys, as well as perform cryptographic operations. Permissions include: Microsoft.KeyVault/vaults/keys/* (full control over keys).
This role does not grant access to secrets or certificates and provides more permissions than needed (e.g., create, delete), violating the principle of least privilege.
Key Vault Reader:
This role provides read-only access to the metadata of all objects in the Key Vault (keys, secrets, and certificates).
Permissions include: Microsoft.KeyVault/vaults/read (read vault properties) and Microsoft.KeyVault/vaults/*/read (read metadata for keys, secrets, and certificates).
Importantly, this role does not allow access to the actual content of the objects (e.g., the secret value, key value, or certificate private key), only the metadata. It also does not allow write operations (e.g., create, update, delete).
This aligns perfectly with the requirement to "read the metadata" and follows the principle of least privilege.
Key Vault Secrets User:
This role allows a user to read the content of secrets (not just metadata) and perform operations like getting the secret value.
Permissions include: Microsoft.KeyVault/vaults/secrets/get (read secret values) and Microsoft.KeyVault/vaults/secrets/read (read secret metadata).

This role does not grant access to keys or certificates, and it provides more access than needed (reading the secret value, not just metadata), violating the principle of least privilege.

Applying the Principle of Least Privilege:

The task requires User1 to read the metadata of certificates, keys, and secrets, but not to access their content or perform any write operations.

Key Vault Readeris the most appropriate role because:

It grants read-only access to the metadata of all objects (keys, secrets, certificates).

It does not allow access to the content of the objects (e.g., secret values), which is not required.

It does not allow write operations (e.g., create, delete), adhering to the principle of least privilege.

The other roles either provide too much access (e.g., Key Vault Crypto Officer, Key Vault Secrets User) or do not cover all required objects (e.g., Key Vault Crypto User, Key Vault Secrets User).

Analysis of the Options:

A. Key Vault Crypto User:

Incorrect. This role only allows reading key metadata and performing cryptographic operations, but it does not provide access to secrets or certificates metadata. It also grants unnecessary cryptographic permissions.

B. Key Vault Crypto Officer:

Incorrect. This role provides full control over keys, which is far more than needed, and does not grant access to secrets or certificates metadata.

C. Key Vault Reader:

Correct. This role provides read-only access to the metadata of keys, secrets, and certificates, exactly matching the requirement while following the principle of least privilege.

D. Key Vault Secrets User:

Incorrect. This role allows reading secret values (not just metadata) and does not provide access to keys or certificates metadata. It grants more access than needed.

Additional Considerations:

If the question had asked for User1 to read the content of secrets (not just metadata), the Key Vault Secrets User role might be considered, but it still wouldn't cover keys and certificates.

Custom RBAC roles could be created to fine-tune permissions, but the question asks for a built-in role, and Key Vault Reader is the best fit.

The question does not specify whether User1 needs to perform other actions (e.g., cryptographic operations, managing the vault). If additional permissions were needed, a combination of roles or a

custom role might be required, but the principle of least privilege guides us to the minimal role. Conclusion:To ensure User1 can read the metadata of certificates, keys, and secrets in Vault1 while following the principle of least privilege, theKey Vault Readerrole should be assigned. This role provides the exact permissions needed without granting unnecessary access. Therefore, the correct answer isC.

Reference:

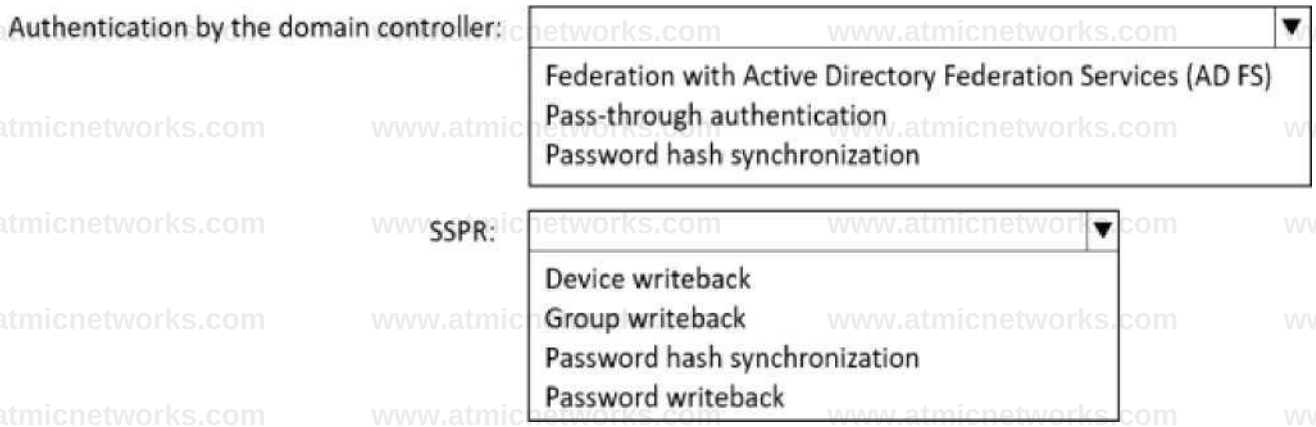
Azure Key Vault documentation: "Azure Key Vault RBAC roles" (Microsoft Learn:https://learn.microsoft.com/en-us/azure/key-vault/general/rbac-guide) Azure Key Vault documentation: "Secure access to a key vault" (Microsoft Learn:https://learn.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault) Microsoft Identity and Access Administrator (SC-300) exam study guide, which covers Azure Key Vault access control and the principle of least privilege.

Question: 302

HOTSPOT

Your on-premises network contains an Active Directory domain that uses Microsoft Entra Connect to sync with a Microsoft Entra tenant.

You need to configure Microsoft Entra Connect to meet the following requirements: Microsoft Entra sign-ins must be authenticated by an Active Directory domain controller. Active Directory domain users must be able to use Microsoft Entra self-service password reset (SSPR).
Minimize administrative effort.
What should you use for each requirement? To answer, select the appropriate options in the answer area.



Answer:

Explanation:

Microsoft Entra sign-ins must be authenticated by an Active Directory domain controller: Passthrough authentication
Active Directory domain users must be able to use Microsoft Entra self-service password reset (SSPR): Password writeback
Let's break this down step by step based on Microsoft Entra Connect, authentication methods, and

SSPR requirements, as outlined in Microsoft Identity and Access Administrator documentation.

Requirement 1: Microsoft Entra sign-ins must be authenticated by an Active Directory domain controller
Understanding the Requirement:
The requirement states that Microsoft Entra sign-ins must be authenticated by an on-premises Active Directory domain controller. This means that the authentication process must occur on-premises rather than in the cloud.
Microsoft Entra Connect supports several authentication methods for hybrid identity:
Password Hash Synchronization (PHS):Password hashes are synchronized to Microsoft Entra ID, and authentication occurs in the cloud. This does not meet the requirement because the domain controller is not involved in the authentication process.
Pass-through Authentication (PTA):Users sign in to Microsoft Entra ID, but the authentication request is passed to an on-premises Active Directory domain controller for validation. This meets the requirement because the domain controller performs the authentication.
Federation with Active Directory Federation Services (AD FS):Users are redirected to an on-premises AD FS server, which authenticates them against the domain controller. This also meets the requirement because the domain controller is involved via AD FS.
Comparing the Options:
Federation with Active Directory Federation Services (AD FS):
AD FS provides federated authentication, where users are redirected to an on-premises AD FS server for authentication. The AD FS server communicates with the domain controller to validate credentials.
This meets the requirement because the domain controller authenticates the user.
However, AD FS requires significant infrastructure (e.g., AD FS servers, Web Application Proxy servers) and ongoing

maintenance, which increases administrative effort.

Pass-through Authentication (PTA):

PTA allows Microsoft Entra ID to pass the authentication request directly to an on-premises domain controller via a lightweight agent installed on a server in the on-premises environment.

This meets the requirement because the domain controller performs the authentication.

PTA is simpler to deploy and manage than AD FS. It requires only the Microsoft Entra Connect server and the PTA agent, with no additional infrastructure like AD FS servers. This aligns with the requirement to "minimize administrative effort."

Minimizing Administrative Effort:

The question emphasizes minimizing administrative effort.

AD FS requires deploying and maintaining a federation infrastructure, including AD FS servers, Web Application Proxy servers, certificates, and load balancers. This involves significant administrative overhead.

PTA, on the other hand, is lightweight. It uses the existing Microsoft Entra Connect server and a small agent, with no additional infrastructure required. It also supports high availability by allowing multiple PTA agents.

Therefore, PTA is the better choice to minimize administrative effort while meeting the requirement.

Conclusion for Requirement 1:

Both options meet the requirement for domain controller authentication, but PTA is the better choice because it minimizes administrative effort.

The correct answer for this requirement isPass-through authentication.

Requirement 2: Active Directory domain users must be able to use Microsoft Entra self-service password reset (SSPR)

Understanding the Requirement:

The requirement states that Active Directory domain users must be able to use Microsoft Entra selfservice password reset (SSPR).

SSPR allows users to reset their passwords via a web portal (e.g., aka.ms/sspr) without contacting an administrator. In a hybrid environment (with Microsoft Entra Connect), SSPR must be configured to work with on-premises Active Directory accounts.

For SSPR to work in a hybrid environment, the password reset must be written back to the onpremises Active Directory so that the user's password is updated in both Microsoft Entra ID and Active Directory.

Understanding the Options:

Device writeback:

Device writeback synchronizes device objects (e.g., for Conditional Access or Windows Hello for Business) between Microsoft Entra ID and Active Directory.

This is unrelated to SSPR or password management.

Group writeback:

Group writeback synchronizes Microsoft 365 groups from Microsoft Entra ID to Active Directory, allowing on-premises applications to use these groups.

This is also unrelated to SSPR or password management.

Password hash synchronization:

Password hash synchronization (PHS) synchronizes the hash of a user's Active Directory password to Microsoft Entra ID, enabling cloud authentication.

While PHS is often used in hybrid environments, it only synchronizes passwords from Active Directory to Microsoft Entra ID (one-way). It does not support writing password changes (e.g., from SSPR) back to Active Directory, which is required for SSPR in a hybrid environment.

Password writeback:

Password writeback is a feature of Microsoft Entra Connect that allows password changes made in Microsoft Entra ID (e.g.,

via SSPR) to be written back to the on-premises Active Directory.
This is specifically designed for SSPR in hybrid environments. When a user resets their password using SSPR, the new password is written back to Active Directory, ensuring the user's credentials are consistent across both environments.
Password writeback requires Microsoft Entra ID P1 or P2 licenses and must be enabled in Microsoft Entra Connect.
SSPR in a Hybrid Environment:
For SSPR to work for Active Directory domain users, password writeback must be enabled. Without password writeback, a password reset in Microsoft Entra ID would not update the on-premises Active Directory, rendering the user unable to sign in to on-premises resources.
Password writeback ensures that when a user resets their password via SSPR, the new password is synchronized to Active Directory, meeting the requirement.
Conclusion for Requirement 2:
The only option that enables SSPR for Active Directory domain users in a hybrid environment isPassword writeback.
The other options (Device writeback, Group writeback, Password hash synchronization) do not support writing password changes back to Active Directory, which is necessary for SSPR.

Final Answer Summary:
Microsoft Entra sign-ins must be authenticated by an Active Directory domain controller:Pass- through authentication (meets the requirement and minimizes administrative effort compared to AD FS).
Active Directory domain users must be able to use Microsoft Entra self-service password reset (SSPR):Password writeback (required for SSPR in a hybrid environment).
Reference:
Microsoft Entra Connect documentation: "Choose the right authentication method" (Microsoft Learn:https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/choose-ad-authn)
Microsoft Entra Connect documentation: "Password writeback for SSPR" (Microsoft Learn:https://learn.microsoft.com/en-us/entra/identity/authentication/howto-sspr-writeback)
Microsoft Identity and Access Administrator (SC-300) exam study guide, which covers Microsoft Entra Connect authentication methods and SSPR configuration in hybrid environments.

Question: 303

You have multiple on-premises devices that run either Windows or Linux.
You have a Microsoft 365 E5 subscription.
You configure Microsoft Entra Internet Access.
You need to ensure that all the on-premises devices route internet traffic through Global Secure Access for security policy evaluation.
What should you do in the Microsoft Entra admin center?

A. Deploy the Global Secure Access client.
B. Create a remote network.
C. Create a named location.
D. Create an access package.

Answer: B

Explanation:

Comprehensive and Detailed In-Depth

Let's break this down step by step based on Microsoft Entra Internet Access, Global Secure Access, and the requirements for routing internet traffic from on-premises devices, as outlined in Microsoft Identity and Access Administrator documentation.

Understanding the Scenario and Requirements:

On-premises devices running Windows or Linux:The devices are located in an on-premises environment (e.g., a corporate office or branch) and run either Windows or Linux operating systems. Microsoft 365 E5 subscription:This subscription includes Microsoft Entra ID P2 and Microsoft Entra Internet Access, which are part of the Global Secure Access suite. This provides the necessary licensing for the solution.

Microsoft Entra Internet Access:This is a Secure Web Gateway (SWG) solution that secures internet and SaaS app access by routing traffic through Microsoft's Security Service Edge (SSE) for policy evaluation (e.g., web content filtering, Conditional Access).

Requirement:All on-premises devices must route their internet traffic through Global Secure Access for security policy evaluation. Global Secure Access is the unified framework for Microsoft Entra Internet Access and Microsoft Entra Private Access, providing a centralized way to manage network traffic security.

How Global Secure Access Routes Internet Traffic:

Global Secure Access can route internet traffic in two primary ways:

Global Secure Access Client:This client is installed on individual devices (e.g., Windows, macOS, Android, iOS) and routes traffic from the device to Microsoft's SSE for policy evaluation. The client is user-aware and integrates with Microsoft Entra ID for identity-based policies.

Remote Network:This method creates an IPsec tunnel between an on-premises network (e.g., a branch office) and Microsoft's SSE. All internet-bound traffic from devices in the network is routed through the tunnel for security policy evaluation, without requiring a client on each device.

The question involvesmultiple on-premises devicesrunning Windows or Linux, which suggests a network-level solution may be more practical than installing a client on each device, especially since Linux support for the Global Secure Access client is limited.

Question: 304

You have a Microsoft 365 E5 subscription.

You deploy a third-party web gateway named Gateway1.

You need to integrate Gateway1 with Microsoft Defender for Cloud Apps. The solution must meet the following requirements:

Ensure that data flows automatically to Defender for Cloud Apps.

Minimize administrative effort.

What should you do first?

A. Add a data source
B. Create an app registration
C. Create a snapshot report
D. Add a log collector

Answer: D

Explanation:

Comprehensive and Detailed In-Depth

Let's break this down step by step based on Microsoft Defender for Cloud Apps (MDCA) integration with third-party web gateways, as outlined in Microsoft Identity and Access Administrator documentation.

Understanding the Scenario and Requirements:

Microsoft 365 E5 subscription:This subscription includes Microsoft Defender for Cloud Apps, which provides the necessary licensing for integrating with third-party web gateways.

Third-party web gateway named Gateway1:A web gateway (e.g., a Secure Web Gateway like Zscaler, Netskope, or Symantec) is deployed to manage and secure internet traffic. The question does not specify the vendor, but the process for integration with MDCA is generally the same for supported gateways.

Requirement:Integrate Gateway1 with Microsoft Defender for Cloud Apps to ensure that data (e.g., traffic logs, events) flows automatically to MDCA for analysis, visibility, and policy enforcement. The solution must also minimize administrative effort.

Microsoft Defender for Cloud Apps supports integration with third-party web gateways to provide visibility into cloud app usage, detect shadow IT, and enforce security policies. This integration typically involves collecting logs from the gateway for analysis in MDCA.

How Microsoft Defender for Cloud Apps Integrates with Third-Party Web Gateways:

MDCA can integrate with third-party web gateways by collecting logs that contain traffic data (e.g., user activity, app usage, IP addresses). This allows MDCA to analyze the data and provide insights into cloud app usage, detect threats, and enforce policies.

The primary method for integrating a third-party web gateway with MDCA is toadd a log collector.

This involves:

Configuring the web gateway to send logs to a log collector (e.g., via Syslog or FTP).

Setting up a log collector in MDCA to receive and process these logs.

Once configured, the log collector automatically pulls logs from the web gateway, ensuring that data flows to MDCA for analysis.

This method supports automatic data flow and minimizes administrative effort because, after the initial setup, the log collection process runs continuously without manual intervention.

Analyzing the Options:

A. Add a data source:

In Microsoft Defender for Cloud Apps, "data sources" typically refer to sources of user activity data, such as Microsoft Entra ID audit logs, Microsoft 365 audit logs, or other Microsoft services. Adding a data source in MDCA is used to import user activity data for correlation with cloud app usage, but it is not the mechanism for integrating a third-party web gateway.

Third-party web gateways are not considered "data sources" in MDCA; instead, they are integrated via log collectors.

Conclusion:This option is incorrect because adding a data source does not facilitate integration with a third-party web gateway like Gateway1.

B. Create an app registration:

Creating an app registration in Microsoft Entra ID is typically used to integrate cloud apps with MDCA for session control (e.g., via Conditional Access App Control) or to enable API-based log collection for supported apps (e.g., Salesforce, Box).

However, a third-party web gateway like Gateway1 is not a cloud app that requires an app registration. Web gateways are network appliances or services that manage traffic, and their integration with MDCA involves log collection, not app registration.

Conclusion:This option is incorrect because creating an app registration is not relevant to integrating a web gateway with MDCA.

C. Create a snapshot report:

A snapshot report in MDCA is a manual process where an administrator uploads a log file (e.g., a CSV or JSON file) from a third-party service to analyze cloud app usage. This is a one-time, manual process used for discovery (e.g., to

identify shadow IT).

The requirement specifies that data must flow "automatically" to Defender for Cloud Apps, and a snapshot report does not meet this requirement because it requires manual uploads each time. It also does not minimize administrative effort due to the ongoing manual intervention.

Conclusion:This option is incorrect because creating a snapshot report does not enable automatic data flow and increases administrative effort.

D. Add a log collector:

Adding a log collector in Microsoft Defender for Cloud Apps is the standard method for integrating third-party web gateways. MDCA supports log collection from many web gateways (e.g., Zscaler, Netskope, Symantec) via Syslog or FTP.

Process:

In the Microsoft Defender for Cloud Apps portal, navigate toSettings > Log collectors.

Add a new log collector, specifying the protocol (e.g., Syslog over TCP/UDP or FTP) and the details of the web gateway (e.g., IP address, port).

Configure Gateway1 to send logs to the log collector (this step is done on the Gateway1 side, typically by the network team).

Once set up, the log collector automatically collects logs from Gateway1 and processes them in MDCA for analysis.

Automatic Data Flow:The log collector ensures that data flows automatically to MDCA, meeting the first requirement.

Minimize Administrative Effort:After the initial setup, the log collector runs continuously without manual intervention, minimizing administrative effort.

Conclusion:This option is correct because adding a log collector is the first step to integrate Gateway1 with MDCA, ensuring automatic data flow and minimizing administrative effort.

Why "Add a log collector" is the First Step:

The question asks for the first step to integrate Gateway1 with Microsoft Defender for Cloud Apps. Adding a log collector is the initial action in MDCA to enable log collection from a third-party web gateway.

Subsequent steps (not asked in the question) would include configuring Gateway1 to send logs to the log collector, but this is done outside MDCA (e.g., in Gateway1's management console). The question focuses on the action in MDCA, making "Add a log collector" the correct first step.

Additional Considerations:

The question does not specify the vendor of Gateway1, but Microsoft Defender for Cloud Apps supports log collection from many third-party web gateways (e.g., Zscaler, Netskope, Symantec, Cisco Umbrella). The process is the same regardless of the vendor, as long as the gateway supports Syslog or FTP log export.

If Gateway1 were not a supported web gateway, additional steps (e.g., custom log parsing) might be required, but the question implies Gateway1 can be integrated using standard methods.

The Microsoft 365 E5 subscription includes Microsoft Defender for Cloud Apps, so no additional licensing is required.

Conclusion:To integrate Gateway1 with Microsoft Defender for Cloud Apps, ensuring that data flows automatically and minimizing administrative effort, the first step is toadd a log collectorin MDCA. This sets up the infrastructure to receive logs from Gateway1, enabling automatic data flow for analysis. Therefore, the correct answer isD.

Reference:

Microsoft Defender for Cloud Apps documentation: "Integrate with a third-party web gateway" (Microsoft Learn:https://learn.microsoft.com/en-us/defender-cloud-apps/connect-third-party- gateway)

Microsoft Defender for Cloud Apps documentation: "Set up a log collector" (Microsoft Learn:https://learn.microsoft.com/en-us/defender-cloud-apps/log-collector)

Microsoft Identity and Access Administrator (SC-300) exam study guide, which covers integrating Microsoft Defender for Cloud Apps with third-party services for cloud app visibility and control.

Question: 305

HOTSPOT

You have a Microsoft Entra tenant that contains an administrative unit named AU1. AU1 is configured for assigned membership.

The tenant contains the users shown in the following table.

Name	Department	Administrative unit
Useri	HR	*None*
User2	IT	AU1

The tenant contains the groups shown in the following table

Name	Members	Administrative unit
HR	Useri	AU1
IT	User2	AU1

For AU1, you update the following configurations:
. Membership type: Dynamic User
· Dynamic membership rule: (user.department -eq "hr")

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

Statements	Yes	No
HR is a member of AU1.	○	○
User1 is a member of AU1.	○	○
User2 is a member of AU1.	○	○

Answer:

Explanation:

HR is a member of AU1: No
User1 is a member of AU1: Yes
User2 is a member of AU1: No

Let's break this down step by step based on Microsoft Entra ID dynamic membership rules, administrative units, and group membership, as outlined in Microsoft Identity and Access Administrator documentation.

Understanding Administrative Units and Dynamic Membership in Microsoft Entra ID:

Administrative Units (AUs):Administrative Units in Microsoft Entra ID are used to delegate administrative tasks to a subset of users, groups, or devices. They allow you to scope administrative roles (e.g., User Administrator) to specific users or groups within the AU.

Membership Types for AUs:

Assigned Membership:Members (users, groups, or devices) are manually added to the AU by an administrator.

Dynamic Membership:Members are automatically added or removed based on a dynamic membership rule, similar to dynamic groups. Dynamic membership for AUs can be applied to users or devices (but not groups directly).

The question states that AU1 is initially configured for assigned membership but is then updated to useDynamic Usermembership with the rule (user.department -eq "HR").

Dynamic Membership Rule:The rule (user.department -eq "HR") means that AU1 will automatically include all users whose department attribute in Microsoft Entra ID is set to "HR". This rule applies to users, not groups or devices, because the membership type is "Dynamic User."

Impact of Changing AU1 to Dynamic Membership:

When AU1's membership type is changed from assigned to dynamic, the existing assigned memberships (e.g., User2, HR group, IT group) are no longer relevant. Thedynamic rule takes over, and AU1's membership is determined solely by the rule (user.department -eq "HR").

Dynamic User Membership:Only users whose attributes match the rule will be members of AU1. Groups (like HR and IT) are not evaluated by this rule because the membership type is "Dynamic User," not "Dynamic Group."

Let's evaluate the users based on the rule:

User1:Department = "HR". The rule (user.department -eq "HR") matches, so User1 will be dynamically added to AU1.

User2:Department = "IT". The rule does not match, so User2 will not be a member of AU1, even though they were previously assigned to AU1 and are a member of the IT group.

Groups (HR and IT):The dynamic membership rule for AU1 applies to users, not groups. Therefore, groups like HR and IT are not directly evaluated by the rule. However, we need to consider whether group membership in AU1 affects the statements.

Statement 1: HR is a member of AU1:

Analysis:

The HR group is listed in the second table with AU1 as its administrative unit, indicating that it was initially assigned to AU1 when AU1 used assigned membership.

However, AU1's membership type has been updated to "Dynamic User" with the rule (user.department -eq "HR"). Dynamic User membership applies to users, not groups.

In Microsoft Entra ID, administrative units with dynamic user membership do not include groups as members unless the AU's membership type is explicitly set to "Dynamic Group" (which is not the case here).

When AU1 was changed to dynamic membership, the HR group would no longer be considered a member of AU1 because the dynamic rule only evaluates users. Groups are not dynamically added to AUs based on user attributes.

Conclusion:The HR group is not a member of AU1 after the change to dynamic membership. Therefore, this statement isNo.

Statement 2: User1 is a member of AU1:

Analysis:

User1 has the department attribute set to "HR" (from the first table).

The dynamic membership rule for AU1 is (user.department -eq "HR"), which matches User1's department.
Therefore, User1 will be automatically added to AU1 as a member based on the dynamic rule.
Additionally, User1 is a member of the HR group, which was initially assigned to AU1. However, since AU1 now uses dynamic membership, the HR group's assignment to AU1 is irrelevant. User1's membership in AU1 is determined solely by the dynamic rule, not their group membership.
Conclusion:User1 is a member of AU1 because their department matches the dynamic rule. Therefore, this statement isYes.
Statement 3: User2 is a member of AU1:
Analysis:
User2 has the department attribute set to "IT" (from the first table).
The dynamic membership rule for AU1 is (user.department -eq "HR"), which does not match User2's department.
User2 was initially assigned to AU1 (as shown in the first table) and is a member of the IT group, which was also assigned to AU1. However, when AU1's membership type was changed to "Dynamic User," the assigned memberships (including User2 and the IT group) are no longer relevant.
The dynamic rule only includes users with the department "HR," so User2 is not added to AU1. Conclusion:User2 is not a member of AU1 because their department does not match the dynamic rule. Therefore, this statement isNo.
Additional Considerations:
If AU1's membership type were "Dynamic Group" instead of "Dynamic User," we would evaluate whether the HR and IT groups match a group-based rule. However, the question specifies "Dynamic User," so the rule applies to user attributes only.
The initial assigned memberships (e.g., User2, HR group, IT group) are overridden by the dynamic membership rule. Microsoft Entra ID does not retain assigned memberships when an AU or group is converted to dynamic membership.
The HR and IT groups being assigned to AU1 initially does not affect the dynamic membership of users, but it might be relevant for administrative scoping (e.g., if an admin role is scoped to AU1). However, the statements are about membership, not administrative roles.
Conclusion:Based on the dynamic membership rule (user.department -eq "HR") for AU1:
HR group:Not a member of AU1 because dynamic user membership does not apply to groups.
User1:A member of AU1 because their department is "HR," matching the rule.
User2:Not a member of AU1 because their department is "IT," which does not match the rule.Therefore, the answers are:
HR is a member of AU1:No
User1 is a member of AU1:Yes
User2 is a member of AU1:No
Reference:
Microsoft Entra ID documentation: "Dynamic membership rules for groups and administrative units" (Microsoft Learn:https://learn.microsoft.com/en-us/entra/identity/users/groups-dynamic- membership)
Microsoft Entra ID documentation: "Manage administrative units" (Microsoft Learn:https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/administrative- units)
Microsoft Identity and Access Administrator (SC-300) exam study guide, which covers dynamic membership rules and administrative units in Microsoft Entra ID.

Question: 306

You have an Azure subscription that contains a storage account named storage1.
You plan to deploy an app named App1 that will be hosted on multiple virtual machines. The virtual machines will authenticate to a Third-party API by using secrets
You need to recommend an authentication solution for the virtual machines The solution must meet the following

requirements

- Securely store secrets.
- Ensure that credentials do NOT need to be stored in the App1 code.
- Ensure that the virtual machines can access Azure resources by using Microsoft Entra authentication.
- Minimize administrative effort.

What should you include in the recommendation?

A. user accounts and Storage Service Encryption
B. user accounts and Azure Key Vault
C. user-assigned managed identities and Azure Key Vault
D. system-assigned managed identities and Storage Service Encryption

Answer: C

Explanation:

Question: 307

HOTSPOT

Your network contains an on premises Active Directory domain named conloso.com. The domain contains the objects shown in the following table.

Name	Type	In organizational unit (OU)	Description
Userl	User	GUI	Used is a membet of Group 1
UMr2	User	QU1	User? *5 r>ot a member of any groups
Gro up '	Security group	OU2	Use> 1 and GroupZ are members of Group 1
Group?	Security group	out	Gtoupi? is a membei of Groupl

You install Microsoft Entra Connect. You configure the Domain and OU filtering settings as shown in the Domain and OU filtering exhibit. (Click the domain and OU Filtering tab.)

You configure the Filter user and devices settings as shown in the Filter Users and Devices exhibit. (Click the filter Users and Devices tab).

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

Anwer Area

Statements	Yes	No
Usa1 syncs to the Microsoft Entta tenant		
User? syncs to the Microsoft Entra tenant	O	O
Groups syncs to the Microsoft Entra tenant	'	O

Answer:

Explanation:

Answer Area Statements	Yes	No
User 1 syncs to the Microsoft Entra tenant,	S	O
User? syncs to the Microsoft Entra tenant	O	^

Question: 308

You have a Microsoft Exchange organization that uses an SMTP address space of contoso.com.
Several users use their contoso.com email address for self-service sign-up to 1 Microsoft Entra.
You gain global administrator privileges to the Microsoft Entra tenant that contains the self-signed users.
You need to prevent the users from creating user accounts in the contoso.com 2 Microsoft Entra tenant for self-service sign-up to Microsoft 365 services.
Which PowerShell cmdlet should you run?

A. Update-MgDomain
B. Update-MgPolicyAuthorizationPolicy
C. Update-MgPolicyPermissionGrantPolicyExclude
D. Update-MgDomainFederationConfiguration

Answer: C

Explanation:

Question: 309

You have an Azure subscription. The subscription contains a virtual machine named VM1 that runs Linux. You need to configure enhanced security for VM1. The solution must meet the following requirements:

- Ensure that users can sign in to VM1 by using their Microsoft Entra credentials
- Ensure That users authenticate by using multi-factor out-of-band
- Prevent users from signing in to VM1 by using passwords.

Which two authentication methods can you include in the solution? Each correct answer presents a complete solution. NOTE: Each correct selection Is worth one point.

A. the Microsoft Authenticator app
B. Windows Hello for Business
C. Passkey(FID02)
D. Temporary Access Pass
E. SMS

Answer: A, D

Explanation:

Question: 310

You have a Microsoft Entra tenant.
You need to implement smart lockout with a lockout threshold of 10 failed sign-ins. What should you configure in the Microsoft Entra admin center?

A. User risk policy

B. Password protection

C. Authentication strengths

D. Sign-in risk policy

Answer: B

Explanation:

Question: 311

HOTSPOT

You have a Microsoft 365 E5 subscription that contains two groups named Group1 and Group2 and the users shown in the following table.

Name	Member of	Role
User 1	Group 1	*None*
User?	Group! Group?	*None*
UserS	Group?	Global Administrator |

The subscription contains a Conditional Access policy that has the following settings:

- Name: Policy1

Target resources

- Include
- All cloud apps
- Access controls
- Grant
- Requite multifactor authentication

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
Useri must use multifnctoi authentication (MFA) when signing in to Microsoft365 apps		
User 2 must use muttrfactor authentication (MFA) when signing in to Microsoft365 apps.	O	
User 3 must use multifactot authentication (MFA) when signing in to Microsoft365 apps	O	

Answer:

Explanation:

Yes, No, Yes

Question: 312

HOTSPOT

You have an azure subscription that contains a resource group named RG1, RG1 contains two virtual machines named VM1 and VM2 that have Microsoft intra ID login enabled.

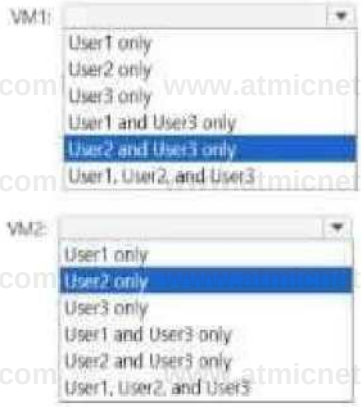
The subscription contains the users shown in the following, table.

Name	Role	Role scope
User1	Virtual Machine User Login	Subscription
User2	Virtual Machine Contributor	RG1
User3	Virtual Machine Administrator Login	VM1

Which users can sign in to VM1. and which users can sign in to VM?? To answer, select the appropriate options in the answer are a. NOTE:
Each correct selection is worth one point.

Which users can sign in to VM1, and which users can sign in to VM2? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

VM1: User1 and User3 only

VM2: User1 only

Question: 313

HOTSPOT

You have a Microsoft Entra tenant that contains two remote networks named RemoteNetworkl and RemoteNetwork2 and the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1
User3	Group2

You have the devices shown in the following table.

Answer Area

Statements	Yes	No
When User! signs in to Microsoft Exchange Online, the user will be prompted for multifactor authentication (MFA).	○	○
When User? signs in to Microsoft SharePoint Online the user will be prompted for multifactor authentication (MFA)	○	○
When User3 signs in to Microsoft Exchange Online the user will be prompted for muftifactor authentication (MFA).	○	○

Answer

Explanation:

Answer Area

Statements	Yes	No
When User! signs in to Microsoft Exchange Online the user will be prompted for multifactor authentication (MFA)	○	○
When User? signs in to Microsoft SharePoint Online, the user will be prompted for multdactor authentication (MFA)	○	○
When User3 signs in to Microsoft Exchange Online the user will be prompted for multifactor authentication (MFA)	○	○

Question: 314

You have a Microsoft 365 subscription.

You need to ensure that users can grant enterprise applications access to their profile. The solution must ensure that the users can consent only to the User. Read and profile delegated permissions. What should you configure first?

A. Security defaults
B. Admin consent settings
C. Permission classifications
D. Identity Protection settings

Answer: B

Explanation:

Question: 315

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

Name	Type
Group 1	Security
Group2	Microsoft 365
Group3	Mail-enabled security
Group4	Distribution

You plan to manage the lifecycles of the groups.

Which groups can be set to expire, and what is the shortest group lifetime you can set? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Question: 316

You have a Microsoft 365 E5 subscription.

You plan to deploy a third-party software as a service (SaaS) app named App1.

You need to onboard App1 to Microsoft Defender for Cloud Apps. The solution must ensure that you can implement session control policies.

What should you do first?

A. From the Microsoft Defender portal, configure Cloud discovery.

B. From the Microsoft Entra admin center, configure a traffic forwarding profile.

C. From the Microsoft Entra admin center, configure single sign-on (SSO) for App1.
D. From the Microsoft Defender portal, create an OAuth app policy.

Answer: A

Explanation:

Question: 317

HOTSPOT
You have a Microsoft 365 subscription that contains three users named User1, User2, and User3 and an enterprise app named Appl. The subscription contains the devices shown in the following table.

Name	Compliance state
Device!	Compliant
Device?	Compliant
Device3	Compliant

The subscription contains the groups shown in the following table.

Name	Members
Group1	User1, User3
Group2	User2, User3
Group3	User1

You create two Conditional Access policies that have the following settings:

- Name: Policy1
- Users:
  - o Include: Group1
  - o Exclude: Group3
- Target resources:
  - o Include: All resources
- Access controls: Block access
- Name: Policy2
- Users:
  - o Include: Group2
- Target resources:
  - o Include: App1
- Access controls:
  - ° Grant access: Require device to be marked as compliant

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
LlserI can sign in to App1 from DeviceI.	u	o
User2 can sign in to App1 from Device?.	0	0
User3 can sign in to App1 from Device3.		

Answer:

Explanation:

Answer Area

Statements	Yes	No
Useri can sign in to Appl from DeviceI.	®	0
User? can sign in to App1 from Device?	®	0
User3 can sign in to Appl from Device3		

Question: 318

HOTSPOT

You have a Microsoft 365 E5 subscription that contains three groups named Groups1, Group2, and Group3, and the users shown in the following table.

Name	Role	Member of
UserI	Global Administrator	Groupl
User?	*None*	Group2
User3	Global Reader	Group2, Group3

You create a Conditional Access policy named CAT that has the following settings:

- Users
  - ° Include
    - Users and groups: Groupl
  - o Exclude
    - Users and groups: Group2
    - Directory roles: Global Administrator
  - o Target resources
    - Include: All cloud apps
  - o Access controls
    - Grant: Require multifactor authentication

You create a Conditional Access policy named CA2 that has the following settings:

- Users
  - ° Include
    - Users and groups: Group2

- Exclude
  - Users and groups: Group3
- Target resources
  - Include: All cloud apps
- Access controls
  - Grant: Block access

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
Userl will be prompted for multifactor authentication (MFA) when the user signs in to Microsoft SharePoint Online		
User? will be prevented from signing in to Microsoft SharePoint Online	0	o
User3 will be prevented from signing in to Microsoft SharePoint Online.	O	O

Answer:

Explanation:

Answer Area

Statements	Yes	No
User! will be prompted for multifactor authentication (MFA) when the user signs in to Microsoft SharePoint Online	O	©
User? will be prevented from signing in to Microsoft SharePoint Online.	©	
User3 will be prevented from signing in to Microsoft SharePoint Online.	O	®

Question: 319

HOTSPOT

You have an on-premises server named Server! that runs Windows Server.

You have a Microsoft Entra tenant that contains an app registration named App1. App1 has Microsoft Graph application permissions.

You need to configure the environment to support App1. The solution must meet the following requirements:

- App1 must be accessible only from the corporate network.
- The credentials for App1 must NOT be stored as plain text.
- Non-interactive scheduled tasks on Server 1 must be able to authenticate to App1.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

In the tenant configure: A Conditional Access policy

An authentication method
A Conditional Access policy
A Microsoft Entra application proxy A
permission classification

Configure scheduled tasks on Serveri to authenticate by using a: Certificate

Certificate
Client secret
System-assigned managed identity
User-assigned managed identity

Answer:

Explanation:

Answer Area

In the tenant configure A Conditional Access policy

Configure scheduled tasks on Serveri to authenticate by using a: Certificate

Question: 320

HOTSPOT

You have an Azure subscription that contains two resource groups named RG1 and RG2, a storage account named storage1.

You assign roles for the subscription as shown in the following table.

User	Role
Useri	Reader
User2	Reader
User3	Reader
User4	Owner

You assign roles for RG1 as shown in the following table.

User	Role
Useri	Reader and Data Access
User2	Contributor

You assign roles for storage1 as shown in the following exhibit.

```
1   1
        "RoleAssignmentId": "9deaS88b-7569-4cfb-b92b-92748cdc550b",
4           "Scope": "/subscriptions/7fefd66e-8694-4b54-beae-
    17fd819d4873/resourceGroups/RG2/providers/Microsoft.Storage/storageAccounts/storage 1",
5           "DisplayName": "User3",
6           "SignInName": "User3gcontoso.com",
7           "RoleDefinitionNaae*: "User Access Administrator",
8           "RoleDefinitionId": "/subscriptions/7fefd66e-8694-4b54-beae-
    17fd819d4873/providers/Hicrosoft.Authorization/roleDefinitions/18d7d88d-d35e-4fb5-a5c3-7773c20a72d9"
9           "ObjectId": "919948b2-bc94-41a0-9562-9399576cc8f0",
10          "ObjectType": "User",
11          "RoleAssignmentQescription": "",
12          "Conditionversion": "",
13          "Condition": ""
M }
15   1
```

Roles are NOT assigned for other Azure resources.

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

Answer Area

Statements	Yes	No
Used can read the data stored in storagel.		
User2 can create a virtual network in RG2.	0	O
UserS can assign roles for storagel,	O	O

Answer:

Explanation:

Answer Area

Statements	Yes	No
Userl can read the data stored in storagel	•	
User2 can create a virtual network in RG2.	•	
User3 can assign roles for storagel.		

Question: 321

You have a Microsoft 365 tenant

You currently allow email clients that use Basic authentication to connect to Microsoft Exchange Online.

You need to ensure that users can connect to Exchange Online only from email clients that use Modern authentication protocols.

What should you implement?

A. a Microsoft Defender for Cloud Apps OAuth policy
B. a Microsoft Intune app protection policy
C. a Microsoft Intune compliance policy
D. a Microsoft Entra conditional access policy

Answer: D

Explanation:

Question: 322

You have a Microsoft Entra tenant.
You have the end-user desktop environments shown in the following table.

Name	Description
Office staff	Contains Windows 11 devices that are Microsoft Entra joined
Contractors	Contains Windows 11 devices that are Microsoft Entra registered
Frontline workers	Contains Windows 11 Enterprise multi session remote desktops that are Microsoft Entra joined
Senior managers	Contains Windows 11 single session hosts that are Microsoft Entra joined
Developers	Contains Windows 365 devices that aie Microsoft fntra joined

You need to deploy Global Secure Access.
In which environments can you install the Global Secure Access client?

A. Developers, Office staff, and Senior managers only
B. Contractors, Developers, Frontline workers. Office staff, and Senior managers
C. Frontline workers and Senior managers only
D. Contractors and Office staff only

Answer: A

Explanation:

Question: 323

You have on-premises Linux devices.
You have a Microsoft 365 E5 subscription.
You plan to configure Global Secure Access Internet Access.
You need to ensure that the devices can connect to Global Secure Access.
What should you do?

A. Deploy a private network connector.
B. Configure the Adaptive Access settings.
C. Install the Azure Connected Machine agent on the devices.
D. Create a remote network.

Answer: A

Explanation:

Question: 324

HOTSPOT
You have an Azure subscription that contains a user named User1. You onboard Microsoft Entra Permissions Management. You need to perform the following tasks:

- Identify all the accounts that are assigned the Global Administrator role permanently.
- Review the Permission Creep Index (PCI) of User1.

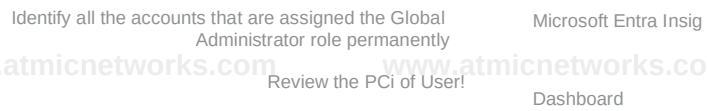
Which tab in Permissions Management should you use for each task? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

Answer Area



Question: 325

You have a Microsoft 365 E5 subscription.

You have an Azure subscription that is linked to a Microsoft Entra tenant. The tenant contains a user named User1.

You plan to deploy Microsoft Entra Permissions Management.

You need to ensure that User1 can onboard the Azure subscription to Permissions Management. The solution must follow the principle of least privilege.

Which Microsoft Entra role should you assign to User1?

A. Security Administrator
B. Application Administrator
C. Permissions Management Administrator
D. Global Administrator

Answer: C

Explanation:

Question: 326

You have a Microsoft 365 E5 subscription.

You create an access review named Review1. Review1 requires that every six months, Microsoft 365 group

owners review guest user access to their groups.

You need to ensure that if the group owners fail to review the membership of Review1, guest users ate removed automatically.

Which settings should you configure for Review1?

A. Reviewers
B. Advanced settings
C. General
D. Upon completion settings

Answer: D

Explanation:

Question: 327

You have a Microsoft 365 subscription that uses Microsoft Defender for Cloud Apps.
You have multiple third-party apps that access the resources in the subscription.
You need to monitor the access of the third-party apps.
What should you create?

A. an OAuth app policy
B. an endpoint protection policy
C. an app permission policy
D. an access policy

Answer: D

Explanation:

Question: 328

Your company purchases a Microsoft 565 ES subscription.

A user named User1 is assigned the Security Administrator role.

You need to ensure that User1 can create Microsoft Defender for Cloud Apps session policies. What should you do first?

A. Create a Conditional Access policy and select Use Conditional Access App Control.
B. Assign the Cloud Application Administrator role to Used.
C. Create a Conditional Access policy and select Require app protection policy.
D. Assign the Cloud App Security Administrator role to User1.

Answer: A

Explanation:

Topic 5, SIMULATIONS and TASK

Question: 329

SIMULATION

Task 1

You need to deploy multi factor authentication (MFA). The solution must meet the following requirements:

- Require MFA registration only for members of the Sg-Finance group.
- Exclude Debra Berger from having to register for MFA.
- Implement the solution without using a Conditional Access policy.

Answer: See the Explanation for the complete step by step solution.

Explanation:

To deploy Multi-Factor Authentication (MFA) for only the members of the Sg-Finance group, excluding Debra Berger, and without using a Conditional Access policy, you can follow these steps: Open the Microsoft Entra admin center:

Sign in as a Security Administrator or Global Administrator.

Navigate to MFA settings:

Go to Users > Active users.

On the Active users page, select Multi-factor authentication.

Manage user settings:

Find and select the Sg-Finance group.

Enable MFA for this group by setting the requirement status to Enabled.

Exclude a user from MFA:

In the Multi-factor authentication page, search for Debra Berger.

Set her MFA status to Disabled to exclude her from MFA registration.

Verify the configuration:

Ensure that all members of the Sg-Finance group have MFA enabled except for Debra Berger.

Communicate the change:

Inform the Sg-Finance group members about the MFA requirement and provide instructions on how to register for MFA.

Monitor the setup:

Check the sign-in logs to confirm that MFA is being prompted for the Sg-Finance group members and not for Debra Berger.

Question: 330

SIMULATION

Task 2

You need to implement a process to review guest users who have access to the Salesforce app. The review must meet the following requirements:

- The reviews must occur monthly.
- The manager of each guest user must review the access.
- If the reviews are NOT completed within five days, access must be removed.
- If the guest user does not have a manager, Megan Bowen must review the access.

Answer: See the Explanation for the complete step by step solution.

Explanation:

To implement a process for reviewing guest users' access to the Salesforce app with the specified requirements, you can use Microsoft Entra's Identity Governance access reviews feature. Here's a step-by-step guide:

Assign the appropriate role:

Ensure you have one of the following roles: Global Administrator, User Administrator, or Identity Governance Administrator1.

Navigate to Identity Governance:

Sign in to the Microsoft Entra admin center.

Go toIdentity governance>Access reviews1.

Create a new access review:

Select New access review.

Choose the Salesforce app to review guest user access1.

Configure the review settings:

Set the frequency of the review to monthly.

Define thedurationof the review period to5 days1.

Determine the reviewers:

Assign the manager of each guest user as the reviewer.

If a guest user does not have a manager, assignMegan Bowenas the reviewer1.

Automate the removal process:

Configure settings toautomatically remove accessif the review is not completed within the specified time frame1.

Monitor and enforce compliance:

Regularly check the access review results to ensure compliance with the review policy1.

Communicate the process:

Inform all stakeholders about the new review process and provide guidance on how to complete the reviews.

By following these steps, you can ensure that guest users' access to the Salesforce app is reviewed monthly, with managers being responsible for the review, and access is removed if the review is not completed in time.

Question: 331

SIMULATION

Task 3

You need to add the LinkedIn application as a resource to the Sales and Marketing access package.

The solution must NOT remove any other resources from the access package.

Answer: See the Explanation for the

complete step by step solution.

Explanation:

To add the LinkedIn application as a resource to the Sales and Marketing access package without removing any other resources, you can follow these steps: Sign in to the Microsoft Entra admin center:

Ensure you have the role of Global Administrator or Identity Governance Administrator.

Navigate to Entitlement Management:

Go to Identity governance > Entitlement management > Access packages1.

Select the Sales and Marketing access package:

Find and select the Sales and Marketing access package to modify it.

Add a new resource:

Within the access package details, select Resources.

Click on + Add resource.

Search for and select the LinkedIn application from the list of available resources.

Configure the resource role:

Assign the appropriate role for the LinkedIn application that users in the Sales and Marketing access package will have.

Review and update the access package:

Ensure that the LinkedIn application has been added as a resource.

Confirm that no other resources have been removed from the access package.

Save the changes:

After reviewing, save the changes to the access package.

Communicate the update:

Notify the relevant users about the addition of the LinkedIn application to their access package.

By following these steps, you will successfully add the LinkedIn application to the Sales and Marketing access package without affecting the other resources.

Question: 332

SIMULATION

Task 4

You need to ensure that all users can consent to apps that require permission to read their user profile. Users must be prevented from consenting to apps that require any other permissions.

Answer: See the Explanation for the complete step by step solution.

Explanation:

To ensure that all users can consent to apps that require permission to read their user profile and prevent them from consenting to apps that require any other permissions, you can configure the user consent settings in the Microsoft Entra admin center. Here's how you can do it: Sign in as a Global Administrator:

Access the Microsoft Entra admin center with Global Administrator privileges.

Navigate to user consent settings:

Go toIdentity>Applications>Enterprise applications>Consent and permissions>User consent settings1.

Configure the consent settings:

Under User consent for applications, select the option that allows users to consent to apps that only require permission to read their user profile.

Ensure that all other permissions are set to require administrator consent, thus preventing users from consenting to apps that require additional permissions1.

Save the settings:

After configuring the consent settings, select Save to apply the changes.

By following these steps, you will have configured the system to allow user consent for apps that need to read the user profile while blocking consent for apps that require additional permissions. This setup helps maintain user autonomy where appropriate while safeguarding against unauthorized access to broader permissions.

Question: 333

SIMULATION

Task 5

You need to assign a Windows 10/11 Enterprise E3 license to the Sg-Retail group.

Answer: See the Explanation for the complete step by step solution.

Explanation:

To assign a Windows 10/11 Enterprise E3 license to the Sg-Retail group, you can follow these steps: Sign in to the Microsoft Entra admin center:

Make sure you have the role of Global Administrator or License Administrator.

Navigate to the licensing page:

Go toBilling>Licenses1.

Find the Windows 10/11 Enterprise E3 license:

Look for the Windows 10/11 Enterprise E3 license in the list of available products.

Assign licenses to the group:

Select the license and then choose Assign licenses.

Search for and select the Sg-Retail group.

Confirm the assignment and make sure that the correct number of licenses is available for the group.

Review and confirm the assignment:

Ensure that the licenses have been properly assigned to the Sg-Retail group without affecting other groups or users.

Monitor the license status:

Check the license usage and status to ensure that the Sg-Retail group members can utilize the Windows 10/11 Enterprise E3 features.

By following these steps, the Sg-Retail group should now have the Windows 10/11 Enterprise E3 licenses assigned to them.

Question: 334
SIMULATION

Task 6
You need to implement additional security checks before the members of the Sg-Executive can access any company apps. The members must meet one of the following conditions:

- Connect by using a device that is marked as compliant by Microsoft Intune.
- Connect by using client apps that are protected by app protection policies.

Answer: See the Explanation for the complete step by step solution.

Explanation:

To implement additional security checks for the Sg-Executive group members before they canaccess any company apps, you can use Conditional Access policies in Microsoft Entr a. Here's a step-by-step guide:

Sign in to the Microsoft Entra admin center:

Ensure you have the role of Global Administrator or Security Administrator.

Navigate to Conditional Access:

Go to Security > Conditional Access.

Create a new policy:

Select + New policy.

Name the policy appropriately, such as "Sg-Executive Security Checks".

Assign the policy to the Sg-Executive group:

Under Assignments, select Users and groups.

Choose Select users and groups and then Groups.

Search for and select the Sg-Executive group.

Define the application control conditions:

Under Cloud apps or actions, select All cloud apps to apply the policy to any company app.

Set the device compliance requirement:

Under Conditions > Device state, configure the policy to include devices marked as compliant by Microsoft Intune.

Set the app protection policy requirement:

Under Conditions > Client apps, configure the policy to include client apps that are protected by app protection policies.

Configure the access controls:

Under Access controls > Grant, select Grant access.

Choose Require device to be marked as compliant and Require approved client app.

Ensure that the option Require one of the selected controls is enabled.

Enable the policy:

Set Enable policy to On.

Review and save the policy:

Review all settings to ensure they meet the requirements.

Click Create to save and implement the policy.

By following these steps, you will ensure that the Sg-Executive group members can only access company apps if

they meet one of the specified conditions, either by using a compliant device or a protected client app. This enhances the security posture of your organization by enforcing stricter access controls for executive-level users.

Question: 335

SIMULATION

Task 7

You need to lock out accounts for five minutes when they have 10 failed sign-in attempts.

Answer: See the Explanation for the complete step by step solution.

Explanation:

To configure the account lockout settings so that accounts are locked out for five minutes after 10 failed sign-in attempts, you can follow these steps:

Open the Microsoft Entra admin center:

Sign in with an account that has the Security Administrator or Global Administrator role.

Navigate to the lockout settings:

Go to Security > Authentication methods > Password protection.

Adjust the Smart Lockout settings:

Set the Lockout threshold to 10 failed sign-in attempts.

Set the Lockout duration (in minutes) to 5.

Please note that by default, smart lockout locks an account from sign-in after 10 failed attempts in Azure Public and Microsoft Azure operated by 21Vianet tenants1. The lockout period is one minute at first, and longer in subsequent attempts.However, you can customize these settings tomeet your organization's requirements if you have Microsoft Entra ID P1 or higher licenses for your users1.

Question: 336

SIMULATION

Task 8

You need to prevent all users from using legacy authentication protocols when authenticating to Microsoft Entra ID.

Answer: See the Explanation for the complete step by step solution.

Explanation:

To prevent all users from using legacy authentication protocols when authenticating to Microsoft Entra ID, you can create a Conditional Access policy that blocks legacy authentication. Here's how to do it:

Sign in to the Microsoft Entra admin center:

Ensure you have the role of Global Administrator or Conditional Access Administrator.

Navigate to Conditional Access:

Go to Security > Conditional Access.

Create a new policy:

Select + New policy.

Give your policy a name that reflects its purpose, like "Block Legacy Auth".

Set users and groups:

Under Assignments, select Users or workload identities.

Under Include, select All users.

Under Exclude, select Users and groups and choose any accounts that must maintain the ability to use legacy authentication.It's recommended to exclude at least one account to prevent lockout1.

Target resources:

Under Cloud apps or actions, select All cloud apps.

Set conditions:

Under Conditions > Client apps, set Configure to Yes.

Check only the boxes for Exchange ActiveSync clients and Other clients.

Configure access controls:

Under Access controls > Grant, select Block access.

Enable policy:

Confirm your settings and set Enable policy to Report-only initially to understand the impact.

After confirming the settings using report-only mode, you can move theEnable policytoggle fromReport-onlytoOn2.

By following these steps, you will block legacy authentication protocols for all users, enhancing the security posture of your organization by requiring modern authentication methods. Remember to monitor the impact of this policy and adjust as necessary to ensure business continuity.

Question: 337

SIMULATION

Task 9

You need to ensure that when users in the Sg-Operations group go to the My Apps portal a tab named Operations appears that contains only the following applications:

- UnkedIn
- Box

Answer: See the Explanation for the complete step by step solution.

Explanation:

To ensure that users in the Sg-Operations group see a tab named "Operations" containing only LinkedIn and Box applications in the My Apps portal, you can create a collection with these specific applications. Here's how to do it:

Sign in to the Microsoft Entra admin center:

Make sure you have one of the following roles: Global Administrator, Cloud Application Administrator, Application Administrator, or owner of the service principal.
Navigate to App launchers:
Go to Identity > Applications > Enterprise applications.
Under Manage, select App launchers.
Create a new collection:
Click on New collection.
Enter “Operations” as the Name for the collection.
Provide a Description if necessary.
Add applications to the collection:
Select the Applications tab within the new collection.
Click on + Add application.
Search for and select LinkedIn and Box applications.
Click Add to include them in the collection.
Assign the collection to the Sg-Operations group:
Select the Users and groups tab.
Click on + Add users and groups.
Search for and select the Sg-Operations group.
Click Select to assign the collection to the group.
Review and create the collection:
Select Review + Create to check the configuration.
If everything is correct, click Create to finalize the collection.
By following these steps, when users in the Sg-Operations group visit the My Apps portal, they will see a new tab named “Operations” that contains only the LinkedIn and Box applications1.
Please note that to create collections on the My Apps portal, you need a Microsoft Entra ID P1 or P2 license1.

Question: 338
SIMULATION
Task 10
You need to create a group named Audit. The solution must ensure that the members of Audit can activate the Security Reader role.

Answer: See the Explanation for the complete step by step solution.

Explanation:

To create a group named “Audit” and ensure that its members can activate the Security Reader role, follow these steps:
Open the Microsoft Entra admin center:
Sign in with an account that has the Security Administrator or Global Administrator role.
Navigate to Groups:
Go toTeams & groups>Active teams and groups1.
Create the security group:
Select Add a security group.
On the Set up the basics page, enter “Audit” as the group name.

Add a description if necessary and chooseNext1.

Edit settings:

On theEdit settingspage, select whether you want Microsoft Entra roles to be assignable to this group and selectNext1.

Assign roles:

After creating the group, go to Roles > All roles.

Find and select the Security Reader role.

Under Assignments, choose Assign.

Select the "Audit" group to assign the role to its members2.

Review and finish:

Review the settings to ensure the "Audit" group is created with the ability for its members to activate the Security Reader role.

Finish the setup and save the changes.

By following these steps, you will have created the "Audit" group and enabled its members to activate the Security Reader role, which allows them to view security-related information without having permissions to change it. Remember to communicate the new group and role assignment to the relevant stakeholders in your organization.

Question: 339

You have a Microsoft Entra tenant that contains the users shown in the following table.

Name	Role
Adminl	Cloud Application Administrator
Adm m2	Application Administrator
Adm m3	Security Administrator
User!	*None*

You add an enterprise application named App1 to Microsoft Entra ID and set User! as the owner of App1. App1 requires admin consent to access Microsoft Entra ID before the app can be used.

You configure the Admin consent requests settings as shown in the following exhibit.

Admin consent requests

Users can request admin consent to apps they are unable to consent to Q

Yes No

Who can review admin consent requests

Reviewer type	Reviewers
Users	4 users sele<
Groups (Preview)	^ Add grou|
Roles (Preview)	* Add roles

Admin1, Admin2. Admin3, and User1 are added as reviewers. Which users can review and approve the admin consent requests?

A. Admin1 only

B. Admin1 and Admin2 only

C. Admin1, Admin2 and Admin3 only

D. Admin1, Admin2, and User1 only

E. Admin1, Admin2, Admin3, and User1

Answer: B

Explanation:

Question: 340

HOTSPOT

You have a Microsoft 365 tenant that contains the administrative units shown in the following table.

Name	Membership type	Restricted management	Dynamic membership rule
AU1	Dynamic user	Disabled	(user.department -eq "Department!")
AU2	Dynamic user	Disabled	(user.department -eq "Department?")

The subscription contains the administrators shown in the following table.

Name	Role	Role assignment scope
Adminl	Password Administrator	AU1
Admin?	Password Administrator	AU2
AdminS	Password Administrator	Global

The subscription contains the users shown in the following table.

Name	Department
Useri	Department!
User?	Department!
User3	Department?

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
Adminl can reset the password of Useri,		
Admin? can reset the password of User2.	)	
Admin3 can reset the password of User3.	Q	

Answer:

Explanation:

Answer Area

Statements	Yes	No
Admin 1 an reset the password of Useri.	®	0
Admin? an reset the password of User?.	O	®
Admin3 an reset the password of User3.	^	O

Question: 341

You have a Microsoft Entra tenant that contains the devices shown in the following table.

Name	Platform	Join type
Device 1	Windows 11	Microsoft Entra registered
Device2	Windows 10	Microsoft Entra joined
Devices	Windows 10	Microsoft Entra registered
Device4	Android	Microsoft Entra registered

You plan to configure Microsoft Entra Private Access. You deploy the Global Secure Access client to compatible devices. From which devices can you use Private Access?

A. Device1 only

B. Device2 only

C. Device2 and Device4 only

D. Device1. Device2. and Device3 only

E. Device1. Device2, Device3, and Device4

Answer: C

Explanation:

Question: 342

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

You configure Microsoft Entra Internet Access. Which users can manage Microsoft Entra Internet Access?

A. User1 only

B. User2only

C. User3only

D. User1 and User2 only

E. User1, User2, and User3

Answer: A

Explanation: