DUMPSGATE

Microsoft

SC-300

Microsoft Identity and Access Administrator (beta)

QUESTION & ANSWERS

QUESTION 1

Case Study	Number of Questions	Total Question
Case Study: 1	9	1 – 9
Case Study: 2	9	10 – 18
Case Study: 3	82	19 - 100
	Total	100

Case Study: 1

Litware, Inc

Overview

Identity Environment

Cloud Environment

Authentication Requirements

Access Requirements

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 guest 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 :

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.

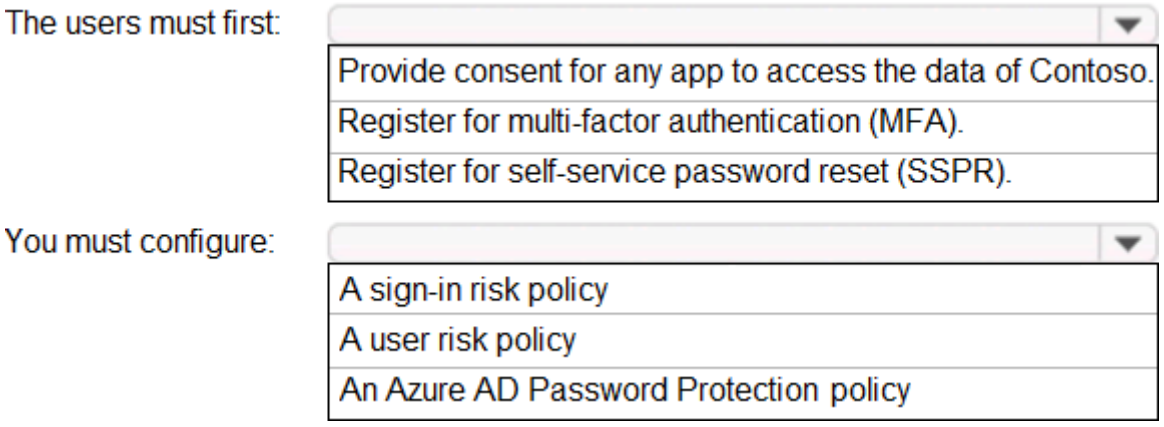
Correct Answer: C

Explanation/Reference:

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

QUESTION 2

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.



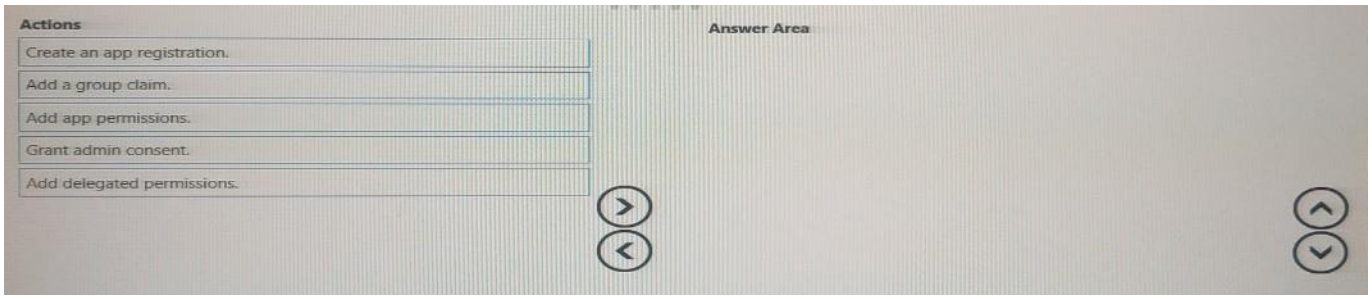
Correct Answer:

Explanation/Reference:

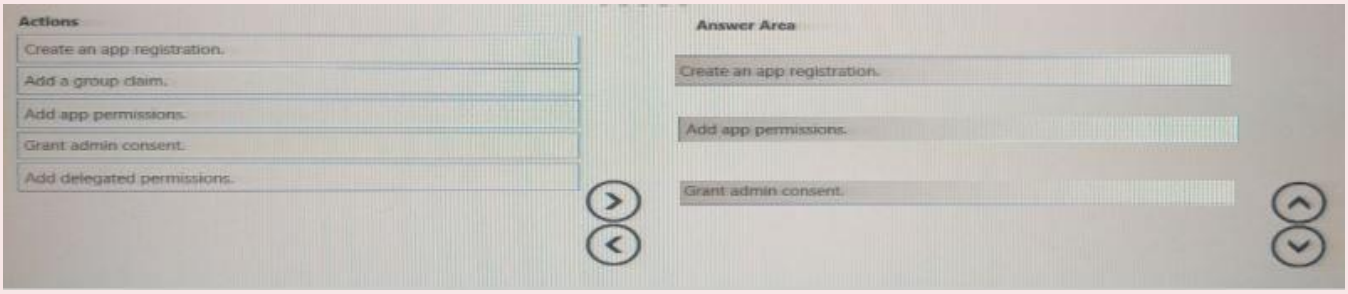
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies

QUESTION 3

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.



Correct Answer:



QUESTION 4

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.

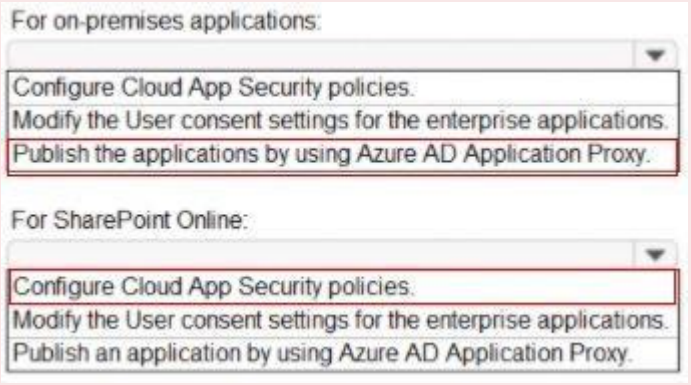
For on-premises applications:

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.

Correct Answer:



QUESTION 5

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.

Correct Answer: A

QUESTION 6

Case Study: 2

Contoso, Ltd

Overview

Problem Statements

Planned Changes

Technical Requirements

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 :

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.

Correct Answer: A

Explanation/Reference:

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

QUESTION 7

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

Correct Answer: C

QUESTION 8

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 (Ml A) registration policy1.
D. Configure password protection for Windows Server Active Directory.

Correct Answer: B

QUESTION 9

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

Name	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:
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

Correct Answer: B