

Question: 174

CertyIQ

HOTSPOT

-

Case Study

-

Overview

-

ADatum Corporation is a consulting company in Montreal.

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

Existing Environment. ADatum Environment

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

ADatum 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.

ADatum 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.

Name	Role
User1	None

•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.

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

Feature:

An authentication method policy
A Conditional Access policy
An MFA registration policy
The Multi-Factor Authentication Server settings

Grace period:

7 days
14 days
28 days

Question: 175

DRAG DROP

-

Case Study

-

Overview

-

ADatum Corporation is a consulting company in Montreal.

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

Existing Environment. ADatum Environment

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

ADatum 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.

ADatum 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.

Name	Role
User1	None
User2	None
User3	User administrator

- 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.

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 policy

Answer Area

Leaked credentials:

A sign-in from a suspicious browser:

Resources accessed from an anonymous IP address:

Question: 182

CertyIQ

HOTSPOT

-

You have an Azure subscription.

From Entitlement management, you plan to create a catalog named Catalog1 that will contain a custom extension.

What should you create first, and what should you use to distribute Catalog1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

First create:

▼

A managed account

An Azure Automation account

An Azure logic app

Distribute Catalog1 by using:

▼

A playbook

A workflow

An access package

Question: 188

CertyIQ

HOTSPOT

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

Name	Type
User1	User
User2	User
Vault1	Azure Key Vault

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

User1:

▼

Key Vault Certificates Officer
Key Vault Crypto Officer
Key Vault Secrets Officer

User2:

▼

Key Vault Certificates Officer
Key Vault Crypto Officer
Key Vault Secrets Officer

Question: 190

DRAG DROP

-

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

Admin1 uses the Require password change for high-risk users 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

Options**Answer Area**Include: Exclude:

Question: 194

CertyIQ

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.

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

The users have the devices shown in the following table.

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.

Statements	Yes	No
User1 can access Site1 from Device1.	☐	☐
User2 can access Site1 from Device2.	☐	☐
User3 can access Site1 from Device3.	☐	☐

Question: 197

DRAG DROP

You have an Azure subscription that is linked to an Azure AD tenant named contoso.com. The subscription contains a group named Group1 and a virtual machine named VM1.

You need to meet the following requirements:

- Enable a system-assigned managed identity for VM1.
- Add VM1 to Group1.

How should you complete the PowerShell script? To answer, drag the appropriate cmdlets to the correct targets.

Each cmdlet 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.

Cmdlets

Get-AzADGroup

Get-AzADServicePrincipal

Get-AzVM

Update-AzADServicePrincipal

Update-AzVM

Answer Area

```
$vm = [Cmdlet] -ResourceGroupName myResourceGroup -Name vm1
Update-AzVM -ResourceGroupName myResourceGroup -VM $vm -IdentityType SystemAssigned
$displayname = [Cmdlet] -displayname "vm1"
$group = Get-AzADGroup -searchstring "group1"
Add-AzureADGroupMember -ObjectId $group.id -RefObjectId $displayname.id
```

Question: 199**CertyIQ**

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 Active Directory admin center, you configure the Block/unblock users settings for multi-factor authentication (MFA).

Does this meet the goal?

A.Yes

B.No

Question: 202

Cert

HOTSPOT

-

You have a Microsoft Entra tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

You have a user risk policy that has the following settings:

•Assignments:

oInclude: Group1

oExclude: Group2

•Sign-in risk: Medium and above

•Access controls:

oGrant 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
User1	High
User2	Medium
User3	High

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
User1 must change their password during sign in.	☐	☐
User2 must change their password during sign in.	☐	☐
User3 must change their password during sign in.	☐	☐