

QUESTION 7

HOTSPOT

You need to implement Azure Sentinel queries for Contoso and Fabrikam to meet the technical requirements.

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

NOTE: Each correct selection is worth one point.

Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam:

	▼
0	
1	
2	
3	

Query element required to correlate data between tenants:

	▼
extend	
project	
workspace	

Correct Answer:

Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam:

	▼
0	
1	
2	
3	

Query element required to correlate data between tenants:

	▼
extend	
project	
workspace	

QUESTION 8

You need to complete the query for failed sign-ins to meet the technical requirements. Where can you find the column name to complete the where clause?

- A. Security alerts in Azure Security Center
- B. Activity log in Azure
- C. Azure Advisor
- D. the query windows of the Log Analytics workspace

Correct Answer: D

Topic 2, Litware inc.

[Download Full Version SC-200 Exam Dumps\(Updated in Feb/2023\)](#)

Case study

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

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

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

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

Litware Inc. is a renewable company.

Litware has offices in Boston and Seattle. Litware also has remote users located across the United States. To access Litware resources, including cloud resources, the remote users establish a VPN connection to either office.

Existing Environment

Identity Environment

The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.

Microsoft 365 Environment

Litware has a Microsoft 365 E5 subscription linked to the litware.com Azure AD tenant. Microsoft Defender for Endpoint is deployed to all computers that run Windows 10. All Microsoft Cloud App Security built-in anomaly detection policies are enabled.

Azure Environment

Litware has an Azure subscription linked to the litware.com Azure AD tenant. The subscription contains resources in the East US Azure region as shown in the following table.

Name	Type	Description
LA1	Log Analytics workspace	Contains logs and metrics collected from all Azure resources and on-premises servers
VM1	Virtual machine	Server that runs Windows Server 2019
VM2	Virtual machine	Server that runs Ubuntu 18.04 LTS

Network Environment

Each Litware office connects directly to the internet and has a site-to-site VPN connection to the virtual networks in the Azure subscription.

On-premises Environment

[Download Full Version SC-200 Exam Dumps\(Updated in Feb/2023\)](#)

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

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller in litware.com that connects directly to the internet
CLIENT1	Windows 10	Boston	Domain-joined client computer

Current problems

Cloud App Security frequently generates false positive alerts when users connect to both offices simultaneously.

Planned Changes

Litware plans to implement the following changes:

- Create and configure Azure Sentinel in the Azure subscription.
- Validate Azure Sentinel functionality by using Azure AD test user accounts.

Business Requirements

Litware identifies the following business requirements:

- The principle of least privilege must be used whenever possible.
- Costs must be minimized, as long as all other requirements are met.
- Logs collected by Log Analytics must provide a full audit trail of user activities.
- All domain controllers must be protected by using Microsoft Defender for Identity.

Azure Information Protection Requirements

All files that have security labels and are stored on the Windows 10 computers must be available from the Azure Information Protection ?Data discovery dashboard.

Microsoft Defender for Endpoint requirements

All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.

Microsoft Cloud App Security requirements

Cloud App Security must identify whether a user connection is anomalous based on tenant-level data.

Azure Defender Requirements

All servers must send logs to the same Log Analytics workspace.

Azure Sentinel Requirements

Litware must meet the following Azure Sentinel requirements:

- Integrate Azure Sentinel and Cloud App Security.
- Ensure that a user named admin1 can configure Azure Sentinel playbooks.
- Create an Azure Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.
- Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.
- Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

QUESTION 1

You need to assign a role-based access control (RBAC) role to admin1 to meet the Azure Sentinel requirements and the business requirements. Which role should you assign?

[SC-200 Exam Dumps](#) [SC-200 PDF Dumps](#) [SC-200 VCE Dumps](#) [SC-200 Q&As](#)

<https://www.ensurepass.com/SC-200.html>

[Download Full Version SC-200 Exam Dumps\(Updated in Feb/2023\)](#)

- A. Automation Operator
- B. Automation Runbook Operator
- C. Azure Sentinel Contributor
- D. Logic App Contributor

Correct Answer: C

Explanation:

<https://docs.microsoft.com/en-us/azure/sentinel/roles>

QUESTION 2

You need to implement the Azure Information Protection requirements. What should you configure first?

- A. Device health and compliance reports settings in Microsoft Defender Security Center
- B. scanner clusters in Azure Information Protection from the Azure portal
- C. content scan jobs in Azure Information Protection from the Azure portal
- D. Advanced features from Settings in Microsoft Defender Security Center

Correct Answer: D

Explanation:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/information-protection-in-windows-overview>

QUESTION 3

You need to restrict cloud apps running on CLIENT1 to meet the Microsoft Defender for Endpoint requirements.

Which two configurations should you modify? Each correct answer present part of the solution.

NOTE: Each correct selection is worth one point.

- A. the Onboarding settings from Device management in Microsoft Defender Security Center
- B. Cloud App Security anomaly detection policies
- C. Advanced features from Settings in Microsoft Defender Security Center
- D. the Cloud Discovery settings in Cloud App Security

Correct Answer: CD

Explanation:

All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/mde-govern>

QUESTION 4

HOTSPOT

You need to create the analytics rule to meet the Azure Sentinel requirements.

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

[SC-200 Exam Dumps](#) [SC-200 PDF Dumps](#) [SC-200 VCE Dumps](#) [SC-200 Q&As](#)

<https://www.ensurepass.com/SC-200.html>

NOTE: Each correct selection is worth one point.

Answer Area

Create the rule of type:

	▼
Fusion	
Microsoft incident creation	
Scheduled	

Configure the playbook to include:

	▼
Diagnostics settings	
A service principal	
A trigger	

Correct Answer:

Answer Area

Create the rule of type:

	▼
Fusion	
Microsoft incident creation	
Scheduled	

Configure the playbook to include:

	▼
Diagnostics settings	
A service principal	
A trigger	

QUESTION 5

HOTSPOT

You need to configure the Azure Sentinel integration to meet the Azure Sentinel requirements.