SC-200問題集無料、SC-200日本語版復習資料

P.S.Fast2testがGoogle Driveで共有している無料の2026 Microsoft SC-200ダンプ：https://drive.google.com/open?id=1HW3OTKUbMcQuCkN031x--CTwlRZWoPiy

Fast2testのSC-200 PDF学習試験のガイダンスのもとで、認定資格を簡単に取得できる可能性が高いことはよく知られています。 しかし、証明書を取得した後の利点を知っている人はほとんどいないと思います。 基本的に、MicrosoftのSC-200模擬テストを使用した認定の利点は、3つの側面に分類できます。 まず、認定資格を取得すると、大企業にアクセスでき、中小企業では得られない雇用機会を増やすことができます。 次に、SC-200準備資料を使用して、SC-200証明書と高給を取得できます。

Microsoft Security Operations Analyst（SC-200）認定試験は、Microsoft環境でのセキュリティインシデントの監視と対応を担当するセキュリティ専門家向けに設計されています。この試験では、脅威管理、脆弱性管理、インシデント対応、コンプライアンスなどのさまざまな分野での候補者の知識とスキルをテストします。 SC-200試験に合格すると、候補者がサイバー脅威からMicrosoft環境を保護するために必要な専門知識を持っていることが示されています。

>> SC-200問題集無料 <<

Microsoft SC-200日本語版復習資料 & SC-200認定テキスト

弊社のSC-200問題集はIT業界で有名で、ブランドになっています。SC-200問題集はすごく人気がある商品で、どこでも広告を掲載する必要がないです。従って、多くの受験者は弊社のSC-200問題集を選びました。なぜ彼らがSC-200問題集を選ぶかというと、弊社のSC-200問題集は高品質で、便利で、勉強しやすいからです。弊社のSC-200問題集を買う人は全部SC-200試験にいい成績で合格しました。

Microsoft SC-200（Microsoft Security Operations Analyst）試験は、セキュリティオペレーションの専門家のスキルと知識を検証するMicrosoftによって提供される認定試験です。この試験は、セキュリティデータの分析、脅威の検出、セキュリティインシデントへの対応の経験を持つ個人を対象としています。この認定試験は、脅威インテ

リジェンス、セキュリティオペレーションセンター（SOC）のオペレーション、インシデント対応、コンプライアンスなど、様々なトピックをカバーしています。

Microsoft Security Operations Analyst 認定 SC-200 試験問題 (Q368-Q373):

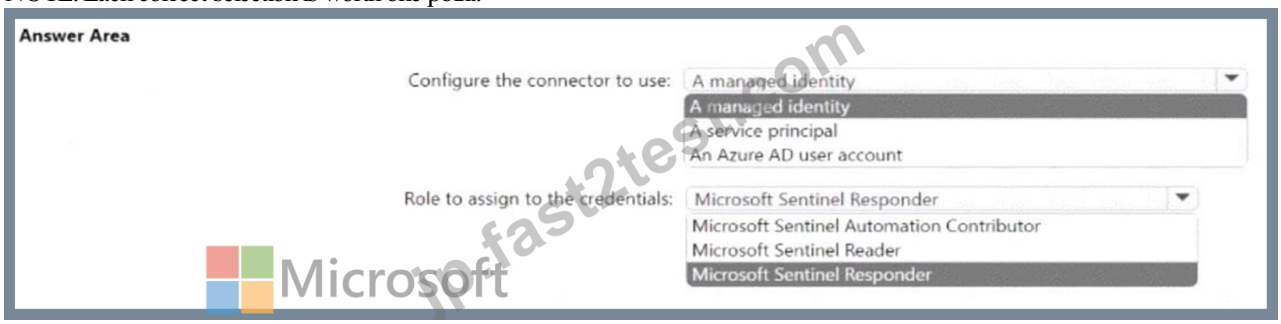
質問 # 368
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you 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 are configuring Azure Sentinel.
You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.
Solution: You create a Microsoft incident creation rule for a data connector.
Does this meet the goal?

- A. No
- B. Yes

正解：B

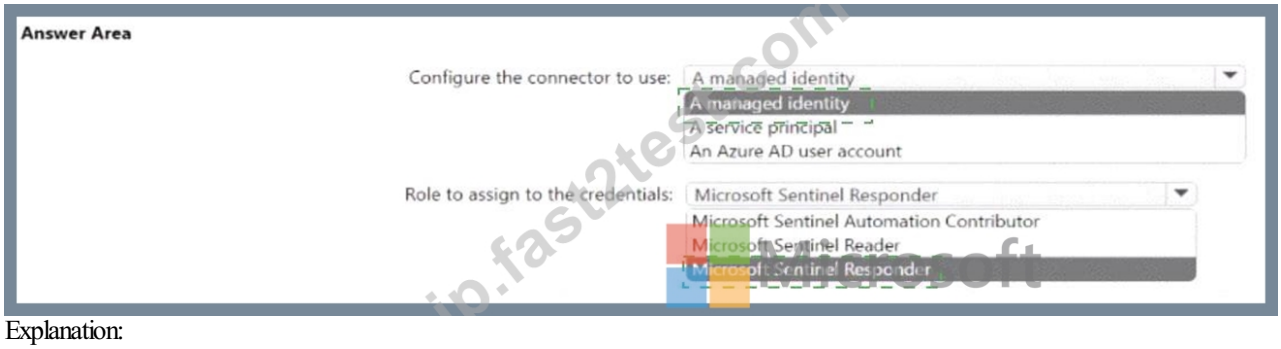
解説：
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

質問 # 369
You have a Microsoft Sentinel workspace named sws1.
You plan to create an Azure logic app that will raise an incident in an on-premises IT service management system when an incident is generated in sws1.
You need to configure the Microsoft Sentinel connector credentials for the logic app. The solution must meet the following requirements:
* Minimize administrative effort.
* Use the principle of least privilege.
How should you configure the credentials? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



正解：

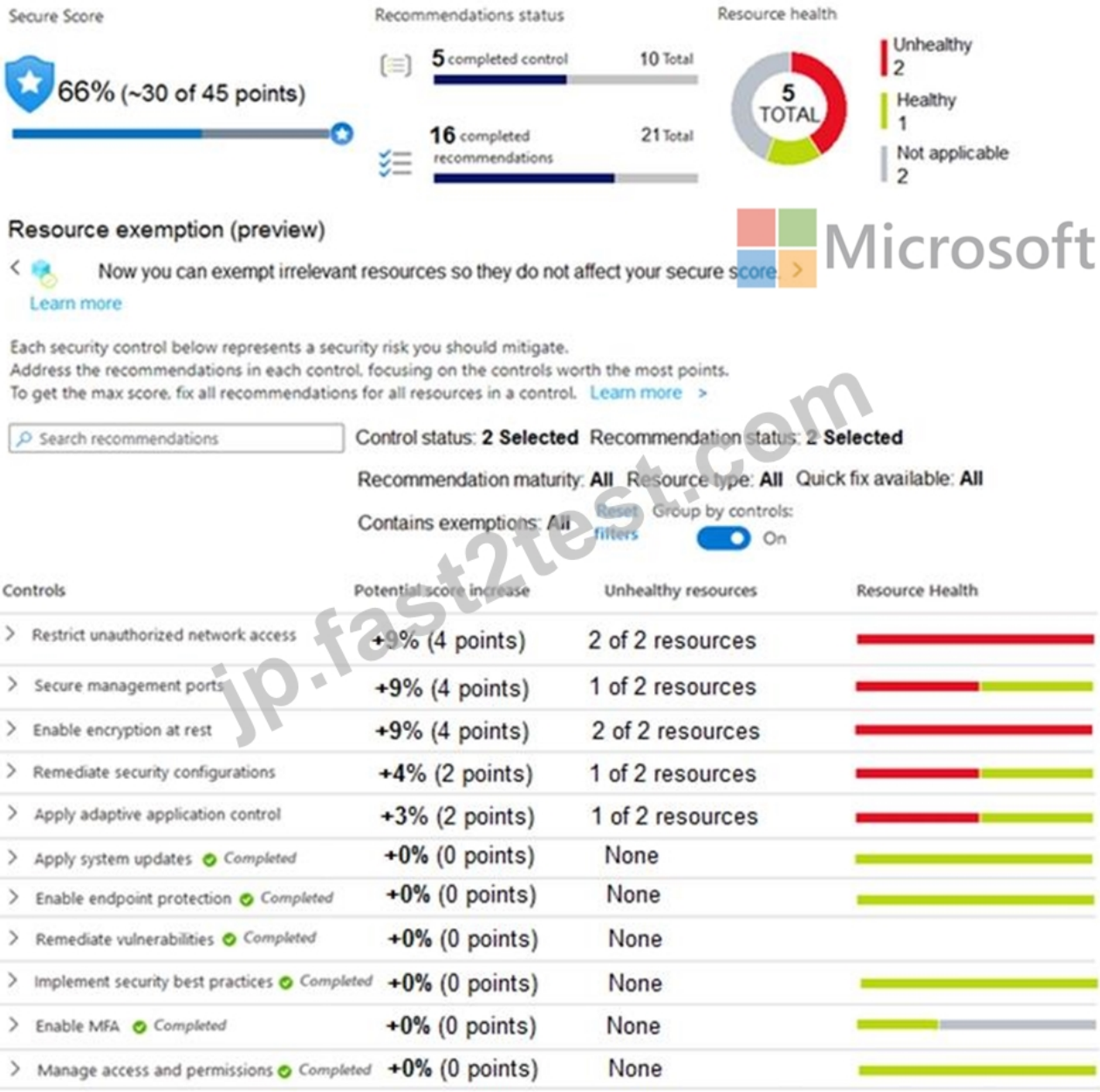
解説：



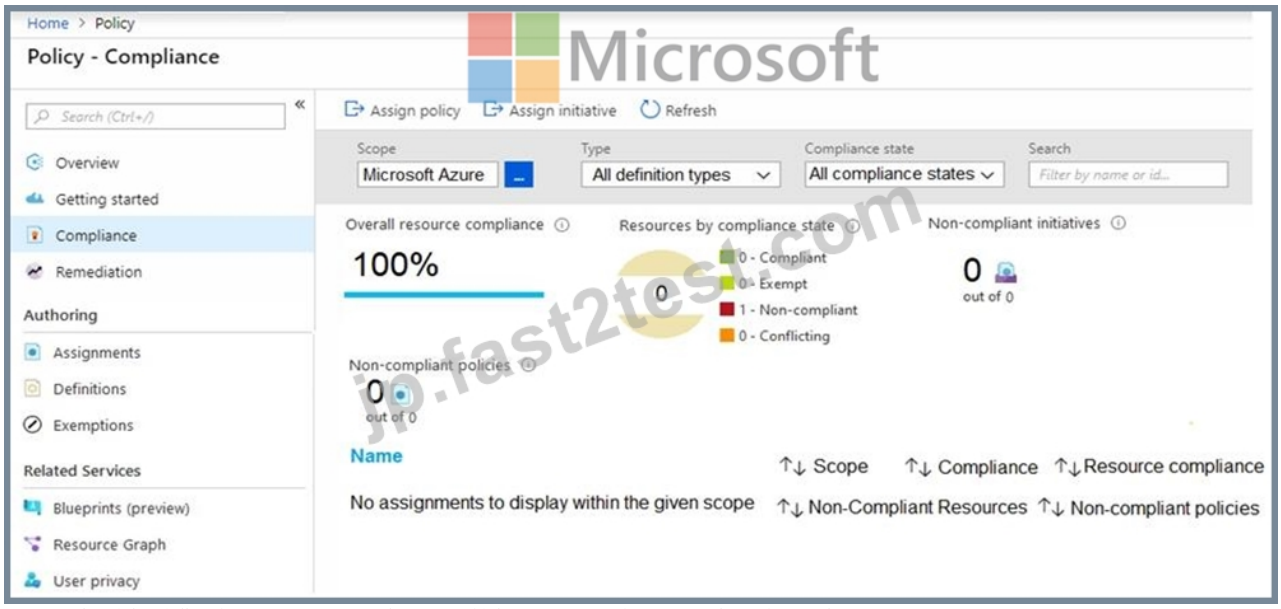
Explanation:

質問 # 370

You manage the security posture of an Azure subscription that contains two virtual machines name vm1 and vm2.
The secure score in Azure Security Center is shown in the Security Center exhibit. (Click the Security Center tab.)



Azure Policy assignments are configured as shown in the Policies exhibit. (Click the Policies 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

Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	○	○
Both virtual machines have management ports exposed directly to the internet.	○	○
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point	○	○

正解：

解説：

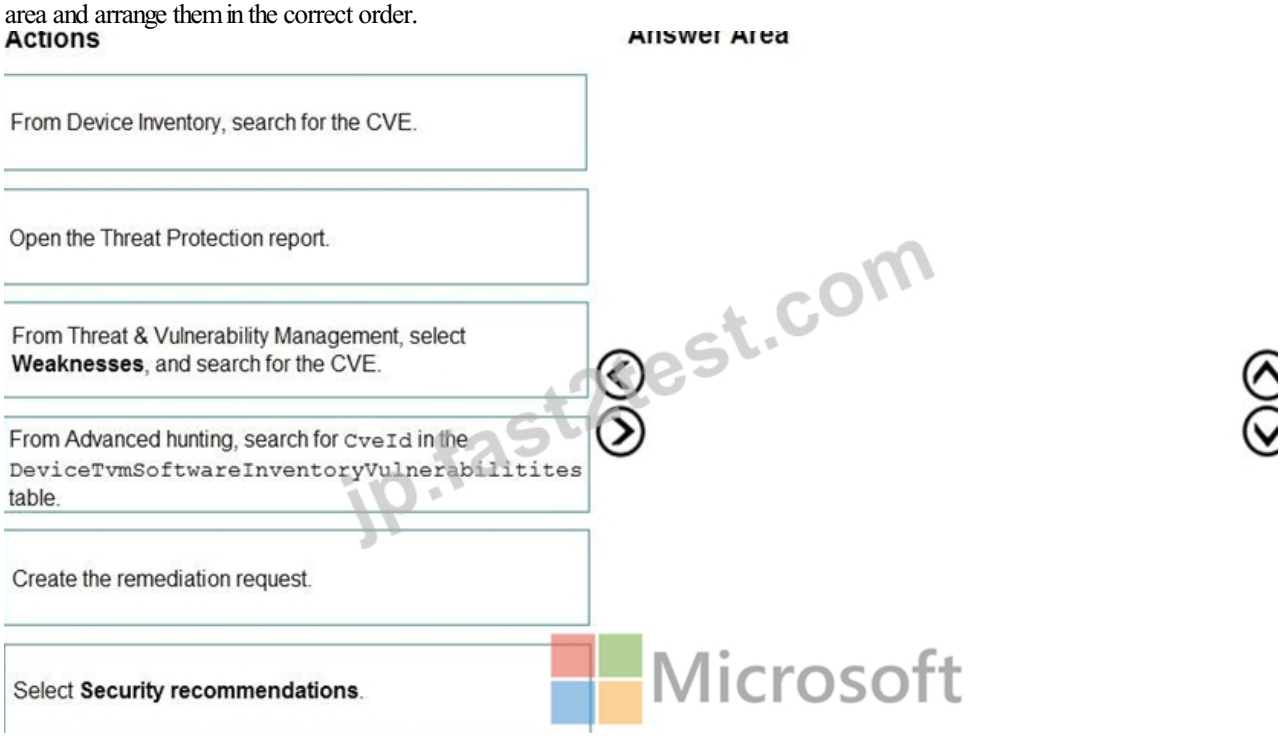
Answer Area

Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	○	○
Both virtual machines have management ports exposed directly to the internet.	○	○
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	○	○

Reference:
https://techcommunity.microsoft.com/t5/azure-security-center/security-control-restrict-unauthorized-network-access/ba-p/1593833
https://techcommunity.microsoft.com/t5/azure-security-center/security-control-secure-management-ports/ba-p/1505770

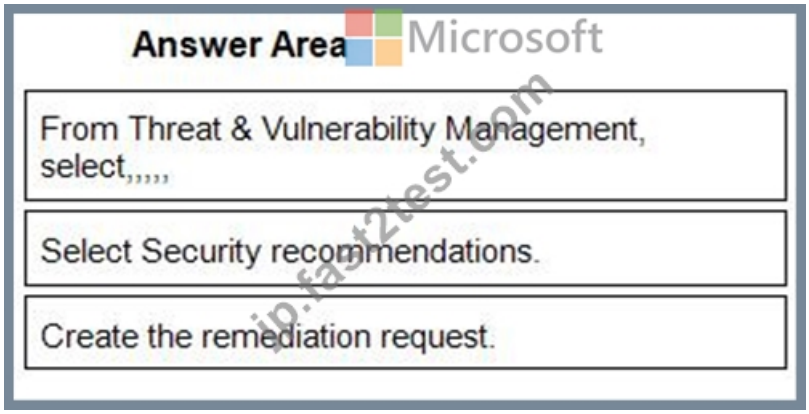
質問 # 371
You are informed of a new common vulnerabilities and exposures (CVE) vulnerability that affects your environment.

You need to use Microsoft Defender Security Center to request remediation from the team responsible for the affected systems if there is a documented active exploit available.
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.



正解：

解説：



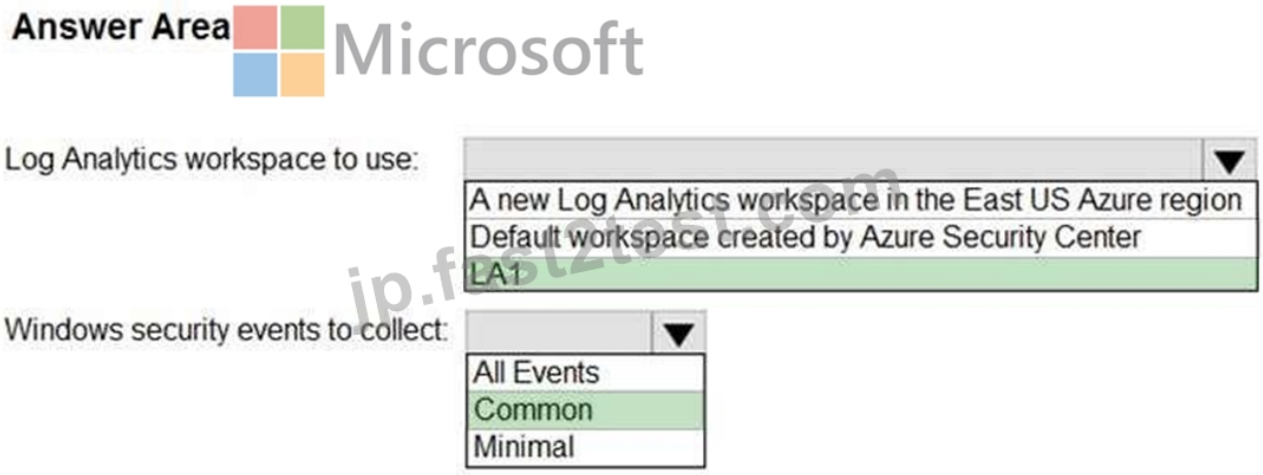
1 - From Threat & Vulnerability Management, select,,,,,
2 - Select Security recommendations.
3 - Create the remediation request.
Reference:
https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-remediate-apps-using-mem/ba-p/1599271

質問 # 372
HOTSPOT
You need to implement Azure Defender to meet the Azure Defender requirements and the business 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.
Hot Area:

Answer Area

正解：

解説：



Section: [none]
Explanation/Reference:
Testlet 2
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
A company named Contoso Ltd. has a main office and five branch offices located throughout North America.
The main office is in Seattle. The branch offices are in Toronto, Miami, Houston, Los Angeles, and Vancouver.
Contoso has a subsidiary named Fabrikam, Ltd. that has offices in New York and San Francisco.
Existing Environment
End-User Environment
All users at Contoso use Windows 10 devices. Each user is licensed for Microsoft 365. In addition, iOS devices are distributed to the members of the sales team at Contoso.
Cloud and Hybrid Infrastructure
All Contoso applications are deployed to Azure.
You enable Microsoft Cloud App Security.

Contoso and Fabrikam have different Azure Active Directory (Azure AD) tenants. Fabrikam recently purchased an Azure subscription and enabled Azure Defender for all supported resource types.
Current Problems
The security team at Contoso receives a large number of cybersecurity alerts. The security team spends too much time identifying which cybersecurity alerts are legitimate threats, and which are not.
The Contoso sales team uses only iOS devices. The sales team members exchange files with customers by using a variety of third-party tools. In the past, the sales team experienced various attacks on their devices.
The marketing team at Contoso has several Microsoft SharePoint Online sites for collaborating with external vendors. The marketing team has had several incidents in which vendors uploaded files that contain malware.
The executive team at Contoso suspects a security breach. The executive team requests that you identify which files had more than five activities during the past 48 hours, including data access, download, or deletion for Microsoft Cloud App Security-protected applications.
Requirements
Planned Changes
Contoso plans to integrate the security operations of both companies and manage all security operations centrally.
Technical Requirements
Contoso identifies the following technical requirements:
* Receive alerts if an Azure virtual machine is under brute force attack.
* Use Azure Sentinel to reduce organizational risk by rapidly remediating active attacks on the environment.
* Implement Azure Sentinel queries that correlate data across the Azure AD tenants of Contoso and Fabrikam.
* Develop a procedure to remediate Azure Defender for Key Vault alerts for Contoso in case of external and internal threats. The solution must minimize the impact on legitimate attempts to access the key vault content.
* Identify all cases of users who failed to sign in to an Azure resource for the first time from a given country. A junior security administrator provides you with the following incomplete query.
BehaviorAnalytics
| where ActivityType == "FailedLogOn"
| where _____ == True

質問 # 373
.....

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, jesseptal725319.vigilwiki.com, sahillmvg168810.bcbloggers.com, tayaqdlt992790.wikiannouncement.com, mentor.khai.edu, socialfactories.com, Disposable vapes

2026年Fast2testの最新SC-200 PDFダンプおよびSC-200試験エンジンの無料共有：https://drive.google.com/open?id=1HW3OTKUbMcQuCkN031x--CTwlRZWoPiy