

# SC-200題庫更新 & SC-200考題

## SC-200 Microsoft Security Operations Analyst



BONUS!!! 免費下載Fast2test SC-200考試題庫的完整版: <https://drive.google.com/open?id=12gMGfml71fO3JPCkAMWGXWH848oE2aXa>

來吧，讓暴風雨來得更猛烈些吧！那些想通過IT認證的考生面臨那些考前準備將束手無策，但是又不得不準備，從而形成了那種急躁不安的心理狀態。不過，自從有了Fast2test Microsoft的SC-200考試認證培訓資料，那種心態將消失的無蹤無影，因為有了Fast2test Microsoft的SC-200考試認證培訓資料，他們可以信心百倍，不用擔心任何考不過的風險，當然也可以輕鬆自如的面對考試了，這不僅是心理上的幫助，更重要的是通過考試獲得認證，幫助他們拼一個美好的明天。

SC-200考試測試候選人配置和管理安全解決方案、應用威脅情報以及調查和回應安全事件的能力。該考試還涵蓋身份和訪問管理、數據保護、網絡安全和雲安全等主題。此認證非常適合想要增強安全操作技能和專業知識的安全分析師、安全管理員和其他安全專業人士。通過獲得SC-200認證，候選人可以證明他們在管理安全操作方面的能力，展示他們在網絡安全領域發展事業的承諾。

Microsoft SC-200認證考試對於想要展示其在Microsoft安全技術和技巧方面的專業知識的安全專業人士來說是一項有價值的認證。該認證考試涵蓋與安全操作有關的廣泛主題，包括威脅管理、漏洞管理、事件響應和合規性。通過考試，候選人可以展示其保護組織IT環境免受各種安全威脅的能力。

>> SC-200題庫更新 <<

## 最真實的SC-200認證考古題

要想一次性通過Microsoft SC-200 認證考試您必須得有一個好的準備和一個完整的知識結構。Fast2test為你提供的資源正好可以完全滿足你的需求。

微軟 SC-200 認證考試是安全專業人員在網絡安全領域發展職業生涯的絕佳選擇。它涵蓋了與安全操作相關的廣泛主題，並評估了候選人使用微軟安全技術保護其組織 IT 環境的能力。通過獲得這項認證，個人可以展示他們的技術技能和知識，並在就業市場上獲得優勢。

## 最新的 Microsoft Certified: Security Operations Analyst Associate SC-200 免費考試真題 (Q256-Q261):

### 問題 #256

You have a Microsoft 365 subscription.

You have 1,000 Windows devices that have a third-party antivirus product installed and Microsoft Defender Antivirus in passive mode. You need to ensure that the devices are protected from malicious artifacts that were undetected by the third-party antivirus product Solution: You enable automated investigation and response (AIR).

Does this meet the goal?

- A. No
- B. Yes

答案: A

**問題 #257**

Hotspot Question

You have a Microsoft 365 E5 subscription that uses Microsoft Defender 365.

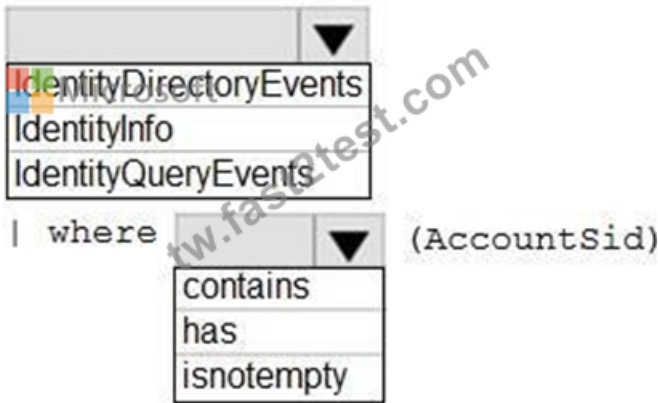
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD.

You need to identify LDAP requests by AD DS users to enumerate AD DS objects.

How should you complete the KQL query? To answer, select the appropriate options in the answer area.

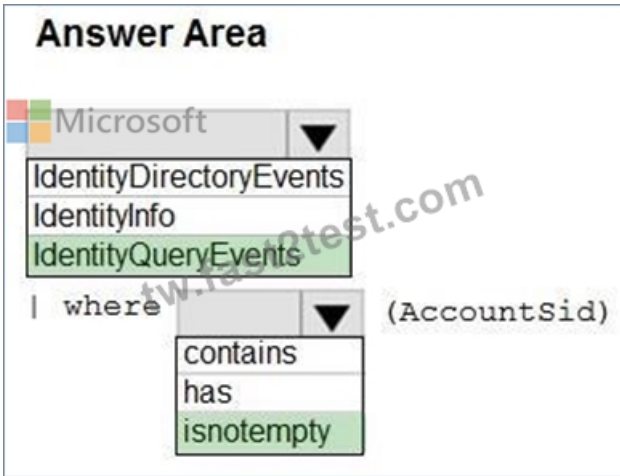
NOTE: Each correct selection is worth one point.

**Answer Area**



答案:

解題說明:



Explanation:

Box 1: IdentityQueryEvents

When considering a table with AccountSid and it's about the LDAP request, it is

"IdentityQueryEvents."

Box 2: isnotempty

For determining whether there is a value in the AccountSid, it is "isnotempty."

**問題 #258**

You have a Microsoft Sentinel workspace that contains the following Advanced Security Information Model (ASIM) parsers:

\* Im ProcessCreate

\* InProcessCreate

You create a new source-specific parser named vimProcessCreate.

You need to modify the parsers to meet the following requirements:

\* Call all the ProcessCreate parsers.

\* Standardize fields to the Process schema.

Which parser should you modify to meet each requirement? To answer, drag the appropriate parsers to the correct requirements.

Each parser 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.

答案:

解題說明:

Explanation:

### 問題 #259

You have a Microsoft 365 E5 subscription that uses Microsoft Purview and contains a user named User1.

User1 shares a Microsoft Power BI report file from the Microsoft OneDrive folder of your company to an external user by using Microsoft Teams.

You need to identify which Power BI report file was shared.

How should you configure the search? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

#### Answer Area

答案:

解題說明:

Answer Area



Activities: Shared Power BI report  
Copied file  
Downloaded files to computer  
Share file, folder, or site  
Shared Power BI report

Record type: Shared Power BI report  
Microsoft Teams  
OneDrive  
PowerBI Audit  
Shared Power BI report

Workload: Microsoft Teams  
Microsoft Teams  
OneDrive  
PowerBI  
SharePoint

Explanation:

To identify which Power BI report file was shared by User1, you should configure the search with the following parameters:

- \* Activities: Shared Power BI report
- \* Record Type: PowerBI Audit
- \* Workload: PowerBI

These parameters will filter the search results to show only the events where a Power BI report was shared by a user in your organization. You can then look for the event that has User1 as the user ID and an external user as the recipient. The event details will show the name and URL of the Power BI report file that was shared.

For more information, see Search the audit log for events in Power BI and Search for content in the Microsoft Purview compliance portal.

### 問題 #260

You have an Azure subscription that uses Azure Defender.

You plan to use Azure Security Center workflow automation to respond to Azure Defender threat alerts.

You need to create an Azure policy that will perform threat remediation automatically.

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.

Set available effects to:

Append  
DeployIfNotExists  
EnforceRegoPolicy

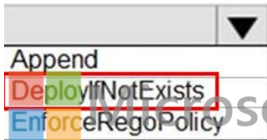
To perform remediation use:

An Azure Automation runbook that has a webhook  
An Azure Logic Apps app that has the trigger set to When an Azure Security Center Alert is created or triggered  
An Azure Logic Apps app that has the trigger set to When a response to an Azure Security Center alert is triggered

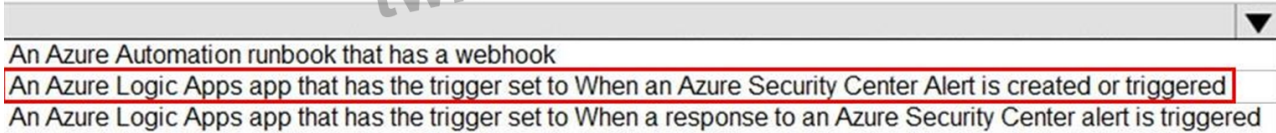
答案:

解題說明:

Set available effects to:



To perform remediation use:



Reference:

- <https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects>
- <https://docs.microsoft.com/en-us/azure/security-center/workflow-automation>

## 問題 #261

.....

SC-200考題: <https://tw.fast2test.com/SC-200-premium-file.html>

- 更正的SC-200題庫更新 | 第一次嘗試輕鬆學習並通過考試和高通過率的Microsoft Microsoft Security Operations Analyst  進入▶ [www.newdumpspdf.com](http://www.newdumpspdf.com)  搜尋▶ SC-200  免費下載SC-200考古題分享
- SC-200套裝  SC-200題庫  SC-200題庫下載  在《 [www.newdumpspdf.com](http://www.newdumpspdf.com) 》網站上查找▶ SC-200 ◀ 的最新題庫SC-200套裝
- 可靠的SC-200題庫更新擁有模擬真實考試環境與場境的軟件VCE版本 & 可依賴的SC-200考題  在▶ [www.vcesoft.com](http://www.vcesoft.com)  網站下載免費✱ SC-200  ✱  題庫收集SC-200考古題分享
- SC-200題庫  SC-200考題套裝  SC-200熱門認證  在⇒ [www.newdumpspdf.com](http://www.newdumpspdf.com) ◀ 搜索最新的《 SC-200 》題庫SC-200考古題分享
- 更正的SC-200題庫更新 | 第一次嘗試輕鬆學習並通過考試和高通過率的Microsoft Microsoft Security Operations Analyst  透過{ [www.vcesoft.com](http://www.vcesoft.com) } 搜索▶ SC-200 ◀ 免費下載考試資料SC-200考試內容
- SC-200考試大綱  SC-200考試題庫  SC-200認證題庫  “ [www.newdumpspdf.com](http://www.newdumpspdf.com) ” 網站搜索⇒ SC-200 ◀ 並免費下載最新SC-200題庫
- 更正的SC-200題庫更新 | 第一次嘗試輕鬆學習並通過考試和高通過率的Microsoft Microsoft Security Operations Analyst  在▶ [www.newdumpspdf.com](http://www.newdumpspdf.com) ◀ 網站下載免費▶ SC-200  題庫收集SC-200最新考古題
- SC-200題庫下載  SC-200題庫  SC-200考題免費下載  進入▶ [www.newdumpspdf.com](http://www.newdumpspdf.com) ◀ 搜尋▶ SC-200  免費下載SC-200考試大綱
- SC-200最新考古題  SC-200認證題庫  SC-200考試題庫  在⇒ [www.vcesoft.com](http://www.vcesoft.com) ◀ 網站下載免費【 SC-200 】【 題庫收集SC-200考題套裝
- SC-200題庫  SC-200考題寶典  SC-200考題免費下載  在⇒ [www.newdumpspdf.com](http://www.newdumpspdf.com) ◀ 搜索最新的✓ SC-200  ✓  題庫SC-200考試內容
- SC-200考試題庫  SC-200考題寶典  SC-200考試題庫  { [www.newdumpspdf.com](http://www.newdumpspdf.com) } 上的免費下載  SC-200  頁面立即打開SC-200套裝
- [bookmarkja.com](http://bookmarkja.com), [webnowmedia.com](http://webnowmedia.com), [keiranxazz843558.dailyblogz.com](http://keiranxazz843558.dailyblogz.com), [anitakhgz566391.bloggip.com](http://anitakhgz566391.bloggip.com), [georgiamduy463697.blog-kids.com](http://georgiamduy463697.blog-kids.com), [phoebegfte247923.buyoutblog.com](http://phoebegfte247923.buyoutblog.com), [peakbookmarks.com](http://peakbookmarks.com), [myarziu286201.mdkblog.com](http://myarziu286201.mdkblog.com), [kobihkjo379883.blogaritma.com](http://kobihkjo379883.blogaritma.com), [dz.b.mii.in](http://dz.b.mii.in), Disposable vapes

此外，這些Fast2test SC-200考試題庫的部分內容現在是免費的：<https://drive.google.com/open?id=12gMGfml71fO3JPckAMWGXWH848oE2aXa>