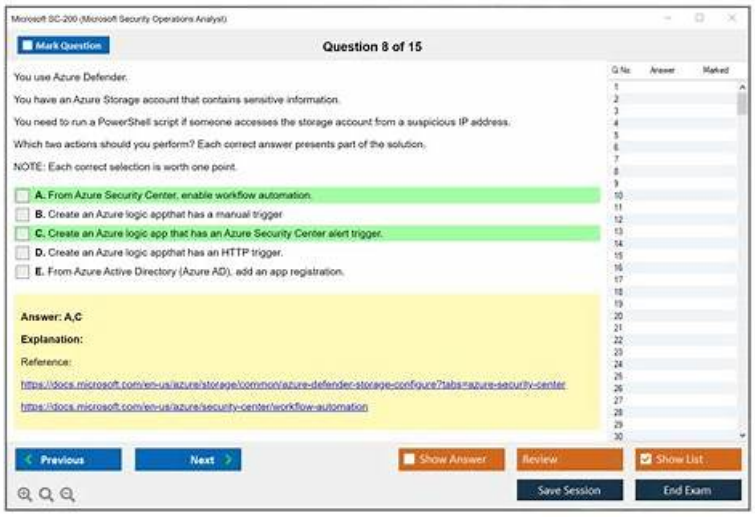
New SC-200 Real Exam - Reliable SC-200 Exam Pdf



What's more, part of that BraindumpQuiz SC-200 dumps now are free: https://drive.google.com/open?id=11A5NUOhDFW_lgZ9PKpYiaoj240kzduWU

We all know that Microsoft Security Operations Analyst (SC-200) exam dumps are an important section of the Microsoft Security Operations Analyst (SC-200) exam that is purely based on your skills, expertise, and knowledge. So, we must find quality SC-200 Questions drafted by industry experts who have complete knowledge regarding the Microsoft Security Operations Analyst (SC-200) certification exam and can share the same with those who want to clear the SC-200 exam. The best approach to finding Microsoft Security Operations Analyst (SC-200) exam dumps is to check the BraindumpQuiz that is offering the Microsoft Security Operations Analyst (SC-200) practice questions.

A brief introduction of Microsoft SC-200 Exam

Microsoft Security Operations Analyst Certification, often referred to as Microsoft SC-200 Exam is one of the most important courses among other courses provided by Microsoft. The course focuses on Security Analysis and Design, which is a very important factor in Network Administration. This helps us to create a secure environment for our organization. This certification provides you with the skills necessary to plan, deploy and monitor security solutions in an enterprise environment and also the skills required to administer and manage the computer security infrastructure. It gives you an edge over other candidates in terms of skill set and makes you more competitive in the job market of today's time. The course helps you understand how to plan, deploy and monitor security solutions in an enterprise environment and also how to administer and manage the computer security infrastructure. **SC-200 Dumps** is designed to make your Microsoft SC-200 certification preparation easy and fast.

It gives you an edge over other candidates in terms of skill-set and makes you more competitive in the job market of today's time. SC-200 Exam validates your ability to design, deploy, manage and monitor a security infrastructure for a private or public organization. The exam measures your knowledge of risk management; incident response; compliance with privacy laws; data protection; cryptography, access control; business continuity planning; auditing & monitoring; intrusion detection & prevention systems (IDS/IPS); web application firewall.

To earn the Microsoft SC-200 certification, candidates must pass one exam, which consists of around 40-60 multiple-choice questions. SC-200 exam duration is 150 minutes, and the passing score is 700 out of 1000 points. Candidates can take the exam either in-person or online, depending on their preference. Microsoft Security Operations Analyst certification is valid for two years and can be renewed by passing a renewal exam or by earning a higher-level certification.

>> New SC-200 Real Exam <<

Reliable SC-200 Exam Pdf, SC-200 Guaranteed Passing

Now you can think of obtaining any Microsoft certification to enhance your professional career. BraindumpQuiz's SC-200 study guides are your best ally to get a definite success in SC-200 exam. The guides contain excellent information, exam-oriented questions and answers format on all topics of the certification syllabus. If you just make sure learning of the content in the guide,

there is no reason of losing the SC-200 Exam.

Microsoft Security Operations Analyst Sample Questions (Q209-Q214):

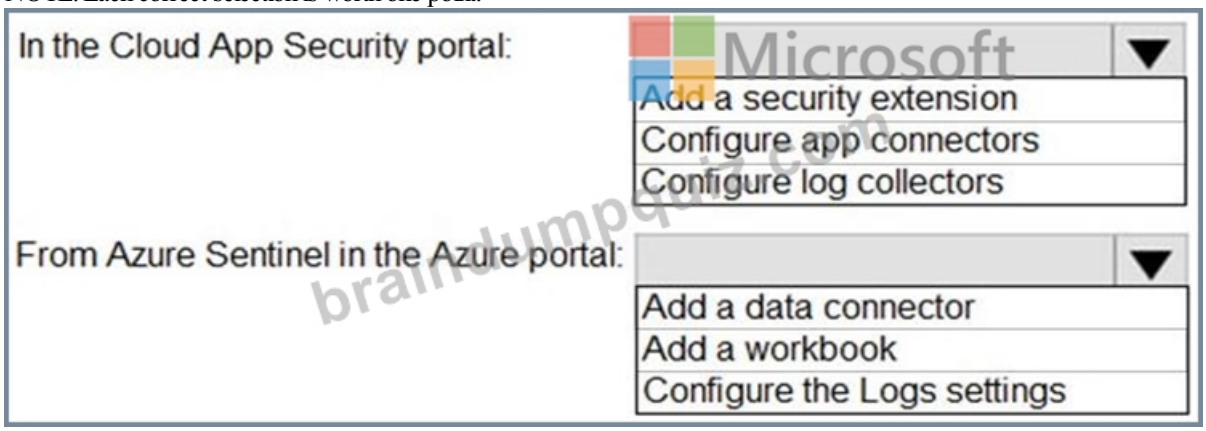
NEW QUESTION # 209
You have two Azure subscriptions that use Microsoft Defender for Cloud.
You need to ensure that specific Defender for Cloud security alerts are suppressed at the root management group level. The solution must minimize administrative effort.
What should you do in the Azure portal?

- A. Modify the alert settings in Defender for Cloud.
- B. Modify the Workload protections settings in Defender for Cloud.
- C. Create an alert rule in Azure Monitor.
- D. Create an Azure Policy assignment.

Answer: D

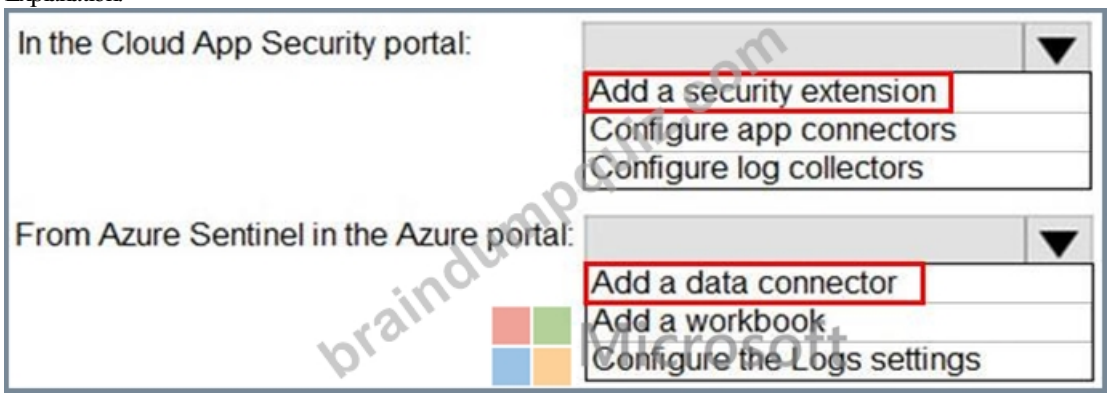
Explanation:
To suppress alerts at the management group level, use Azure Policy.
Reference:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-suppression-rules#create-a- suppression-rule

NEW QUESTION # 210
You need to configure the Azure Sentinel integration to meet the Azure Sentinel requirements.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



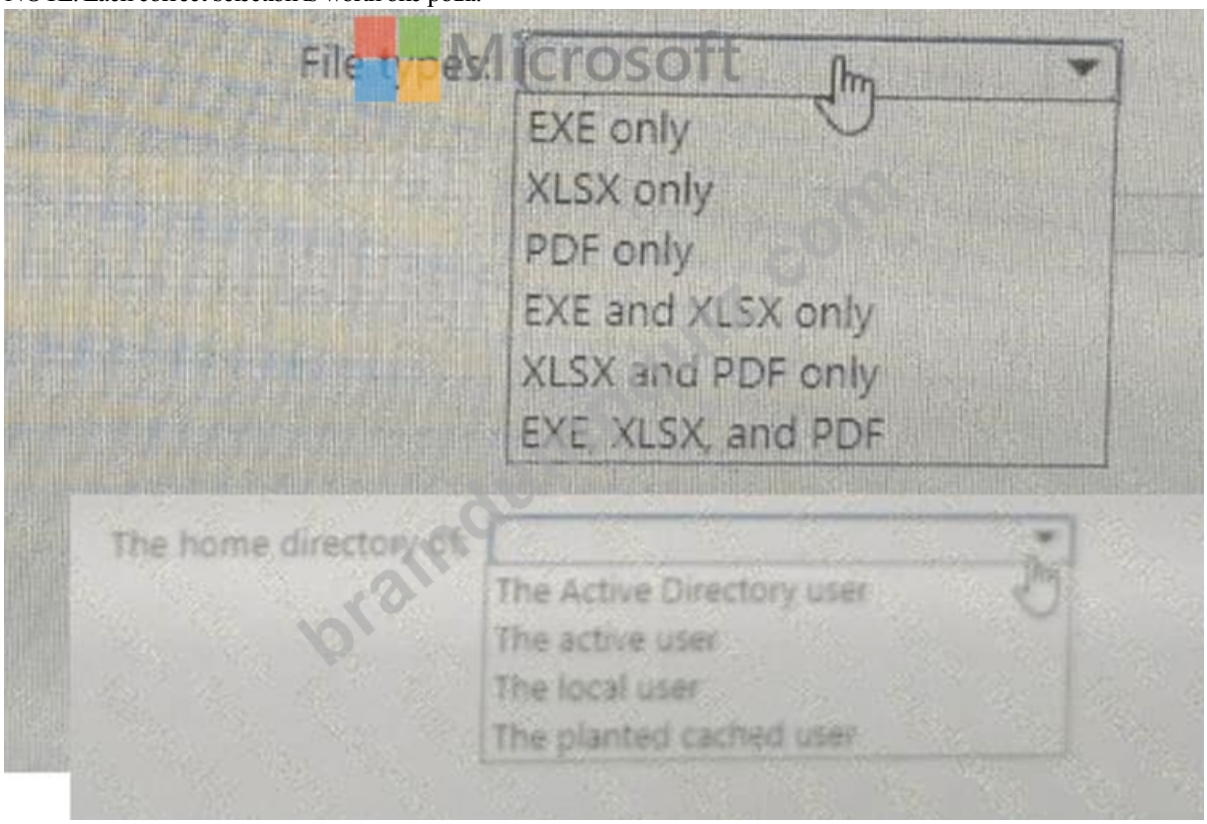
Answer:

Explanation:



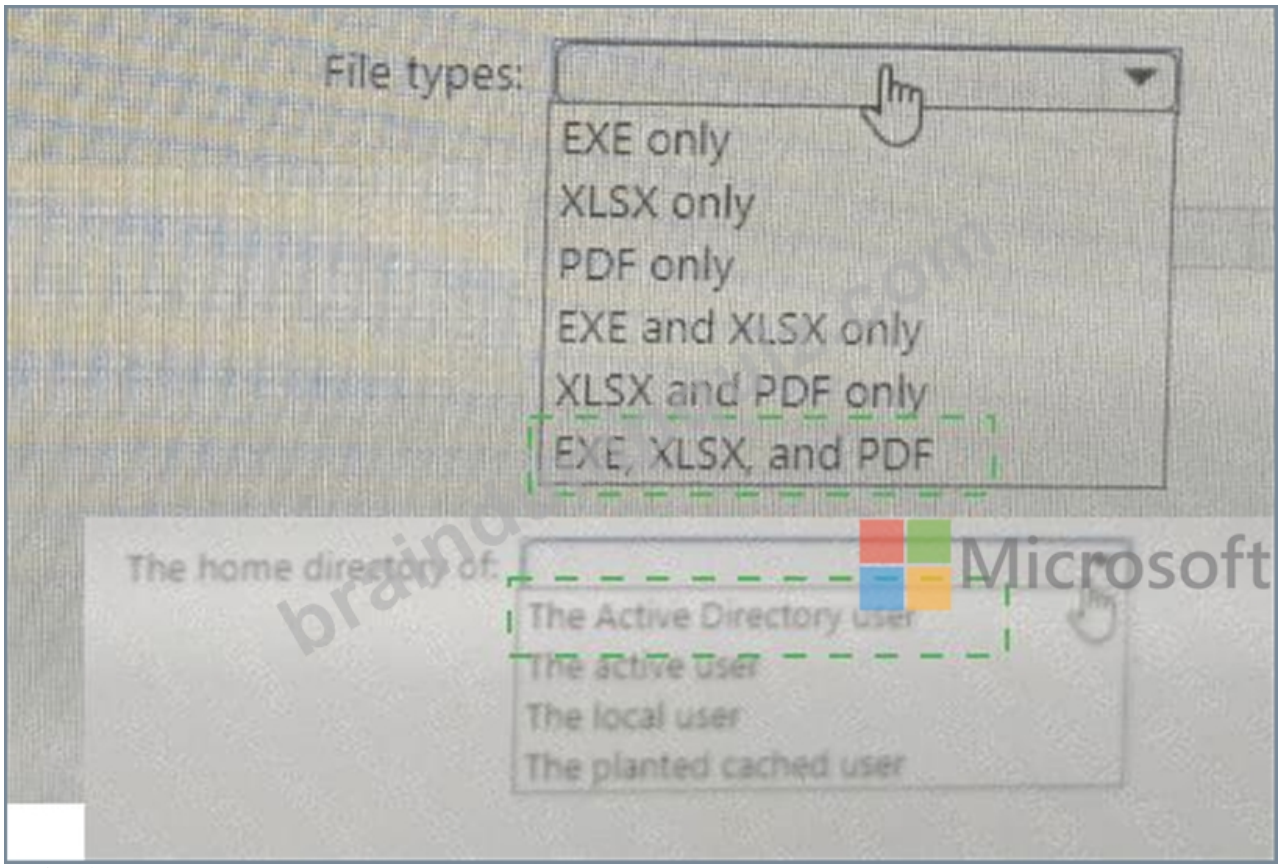
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/siem-sentinel

NEW QUESTION # 211
You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR.
You are implementing a deception rule.
You need to provide a custom lure file.
For the custom lure, you set Planting path to HOME.
Which types of files can you use for the custom lure, and in which home directory should the file be located on a device? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Explanation:
You're configuring a Deception rule in Microsoft Defender XDR and need to provide a custom lure file .
* You set the Planting path to HOME , which means the file will be deployed into user home directories.
You must determine:
* Which file types are supported for custom lure files.
* Which home directory the file should reside in.
1. File types that can be used for a custom lure # Verified Answer = EXE, XLSX, and PDF As per Microsoft Defender for Endpoint Deception documentation:
"Custom lure files can be created using EXE, XLSX, or PDF file types. These file types are supported for deception scenarios and can trigger alerts when accessed or executed by an attacker." The platform uses these file types because they are commonly interacted with by adversaries during lateral movement or reconnaissance.
* EXE : Simulates executables that appear valuable or tempting.
* XLSX / PDF : Represent business-related or sensitive document lures.
Therefore, you can upload EXE, XLSX, and PDF lure files simultaneously or select one of them.
Correct selection: EXE, XLSX, and PDF
2. Home directory the file should be located in # Verified Answer = The active user When you set the Planting path = HOME , Defender plants the deception artifact (lure file) under the active user's home directory .
This ensures that the lure file is visible and accessible within the context of the currently logged-in user- precisely where attackers are most likely to browse or exfiltrate files.
According to Microsoft's deception feature reference:
"When the planting path is set to HOME, the deception files are placed in the home directory of the active user on the device. This ensures that the files are visible during an interactive session and accessible to adversaries using that account." Other options such as "Active Directory user," "Local user," or "Planted cached user" are not used for standard HOME planting. The deception system targets the context of the active session to maximize effectiveness and reduce false positives.
Correct selection: The active user
Final Verified Answers: Configuration Aspect
Correct Option
File types:
EXE, XLSX, and PDF
Home directory of:
The active user
Summary:
When creating a custom lure file in Microsoft Defender XDR Deception with the planting path set to HOME , you should:
* Use EXE, XLSX, and PDF file types.

* Place them in the active user's home directory on the target device.
These selections align with Microsoft Defender XDR Deception's official documentation and M365 E5 SecOps study material.
Question Part 1: Which types of files can you use for the custom lure?
answer:
EXE, XLSX, and PDF
According to your screenshot (File types drop-down), you can use the following file types for a custom lure in Microsoft Defender XDR deception rules:
* EXE
* XLSX
* PDF
You can select any combination of these, so EXE, XLSX, and PDF are all supported as custom lure file types.
Question Part 2: In which home directory should the file be located on a device?
answer:
The Active Directory user
When you set the Planting path to HOME in a deception rule, the file should be planted in the home directory of a user. According to the available drop-down options and Microsoft documentation, the typical recommended choice for corporate environments (and specifically for most deception scenarios) is " The Active Directory user " . This ensures the lure is placed where the intended target (a domain user) is likely to encounter it.

NEW QUESTION # 212
You have a Microsoft 365 subscription that uses Microsoft Defender XDR.
You have a query that contains the following statements.

You need to configure a custom detection rule that will use the query. The solution must minimize how long it takes to be notified about events that match the query.
Which frequency should you select for the rule?

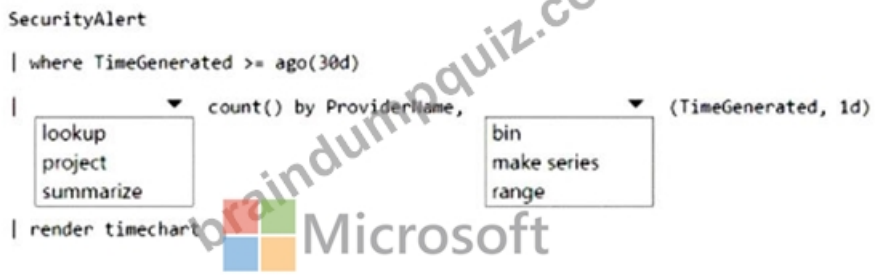
- A. Every hour
- B. Every 12 hours
- C. Every 3 hours
- D. Continuous (NRT)

Answer: D

Explanation:
The query filters on ingestion_time() > ago(1d) , which means it is interested in recently inges ted device telemetry (DeviceEvents and DeviceProcessEvents) within the last 24 hours. To minimize the time between an event ingest and a detection/notification, you want the rule engine to evaluate the query as close to real- time as possible. Microsoft's X DR/Defender detection framework supports continuous (near-real-time, NRT) detection mode, which evaluates incoming telemetry continuously (or at very short intervals) rather than waiting for a scheduled run.
Scheduled analytics/detection rules run on fixed intervals (for example every hour, every 3 hours, etc.), which introduces a guaranteed latency equal to the schedule period. By contrast, a Continuous (NRT) rule processes telemetry as it arrives (or in very short batch windows), dramatically reducing the time-to-alert for matching events. That makes Continuous (NRT) the correct choice when the requirement is to minimize notification latency for device events.
Note the operational trade-offs: continuous rules can generate more frequent evaluations and high er operational overhead (and potentially more noise), so they should be scoped and tuned appropriately (filters, distinct counts, thresholds) to avoid excessive alerts.

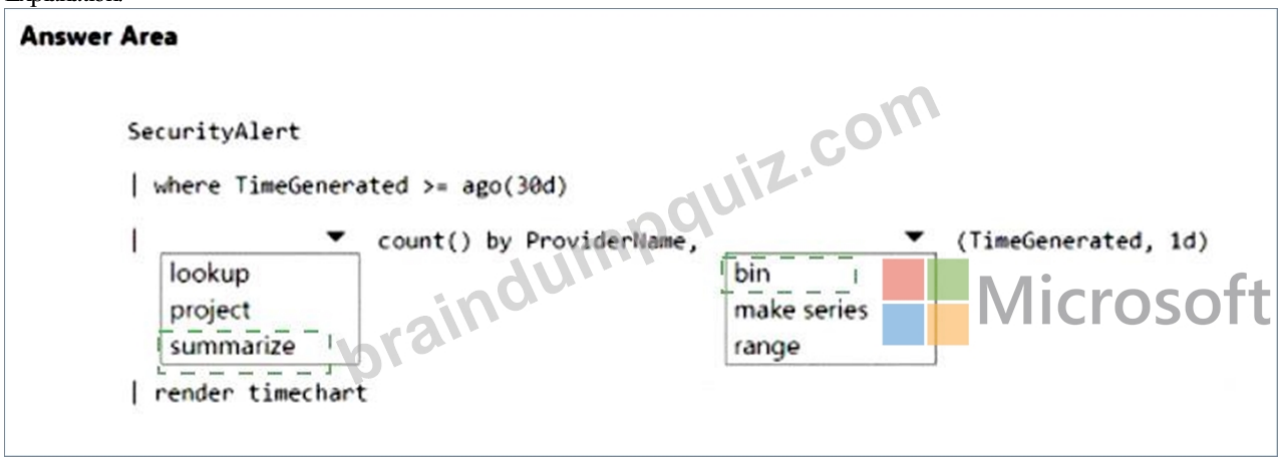
NEW QUESTION # 213
You have a Microsoft Sentinel workspace that contains a custom workbook.
You need to query the number of daily security alerts. The solution must meet the following requirements:
* Identify alerts that occurred during the last 30 days.
* Display the results in a timechart.
How should you complete the query? To answer, select the appropriate options in the answer area. NOTE:
Each correct selection is worth one point.

Answer Area



Answer:

Explanation:



Explanation:

NEW QUESTION # 214

.....

The software keeps track of the previous Microsoft Security Operations Analyst (SC-200) practice exam attempts and shows the changes of each attempt. You don't need to wait days or weeks to get your performance report. The software displays the result of the Microsoft Security Operations Analyst (SC-200) practice test immediately, which is an excellent way to understand which area needs more attention.

Reliable SC-200 Exam Pdf: https://www.braindumpquiz.com/SC-200-exam-material.html

- Free PDF 2026 Microsoft Reliable SC-200: New Microsoft Security Operations Analyst Real Exam □ Immediately open ✔ www.verifieddumps.com □✔□ and search for ▸ SC-200 ◂ to obtain a free download □SC-200 Latest Test Online
- Free PDF 2026 Microsoft SC-200: Fantastic New Microsoft Security Operations Analyst Real Exam □ Search for □ SC-200 □ and easily obtain a free download on ▸ www.pdfvce.com ◂ □Accurate SC-200 Study Material
- Microsoft Security Operations Analyst Valid Exam Guide - SC-200 Free Pdf Vce - Microsoft Security Operations Analyst Latest Practice Questions □ Search for ⇛ SC-200 ⇚ and easily obtain a free download on ➠ www.troytecdumps.com □ □SC-200 Reliable Exam Syllabus
- Microsoft SC-200 Web-Based Practice Test Questions □ Search on ➥ www.pdfvce.com □ for { SC-200 } to obtain exam materials for free download □SC-200 Latest Test Online
- Top SC-200 Dumps ❤ Hot SC-200 Spot Questions □ SC-200 Download □ Simply search for " SC-200 " for free download on ▹ www.troytecdumps.com ◃ □Top SC-200 Dumps
- SC-200 Reliable Exam Syllabus □ SC-200 Interactive Course □ SC-200 Reliable Test Materials □ Copy URL "

www.pdfvce.com" open and search for □ SC-200 □ to download for free □SC-200 PDF Cram Exam

- Hot SC-200 Spot Questions □ SC-200 PDF Questions □ SC-200 Download □ Go to website ▸ www.validtorrent.com ◂ open and search for ▹ SC-200 ◃ to download for free □SC-200 Latest Test Online
- SC-200 PDF Questions □ SC-200 Authorized Certification □ SC-200 Download □ Easily obtain free download of ▸ SC-200 ◂ by searching on ▸ www.pdfvce.com ◂ □Accurate SC-200 Study Material
- SC-200 Latest Test Online □ SC-200 Valid Exam Sims □ Study SC-200 Tool □ Download ➠ SC-200 □ for free by simply searching on { www.prep4sures.top } □SC-200 Download
- SC-200 Exam Quizzes □ SC-200 Exam Quizzes □ SC-200 Reliable Exam Syllabus □ Search for （ SC-200 ） and download it for free on □ www.pdfvce.com □ website □SC-200 PDF Questions
- The Best New SC-200 Real Exam Offers Candidates Perfect Actual Microsoft Microsoft Security Operations Analyst Exam Products □ Download （ SC-200 ） for free by simply entering ☀ www.easy4engine.com □☀□ website □Latest SC-200 Dumps Sheet
- freshcakesavenue.com, keirancrgw981488.empirewiki.com, aadamsjpu149076.blog-eye.com, hypebookmarking.com, forum-directory.com, ellaelzz357064.azzablog.com, zakariarmzc556023.blazingblog.com, excelmanindia.com, mohamadhcrw301773.blogacep.com, dawudlasz392073.webbuzzfeed.com, Disposable vapes

2026 Latest BraindumpQuiz SC-200 PDF Dumps and SC-200 Exam Engine Free Share: https://drive.google.com/open?id=11A5NUOhDFW_lgZ9PKpYiaoj240kzduWU