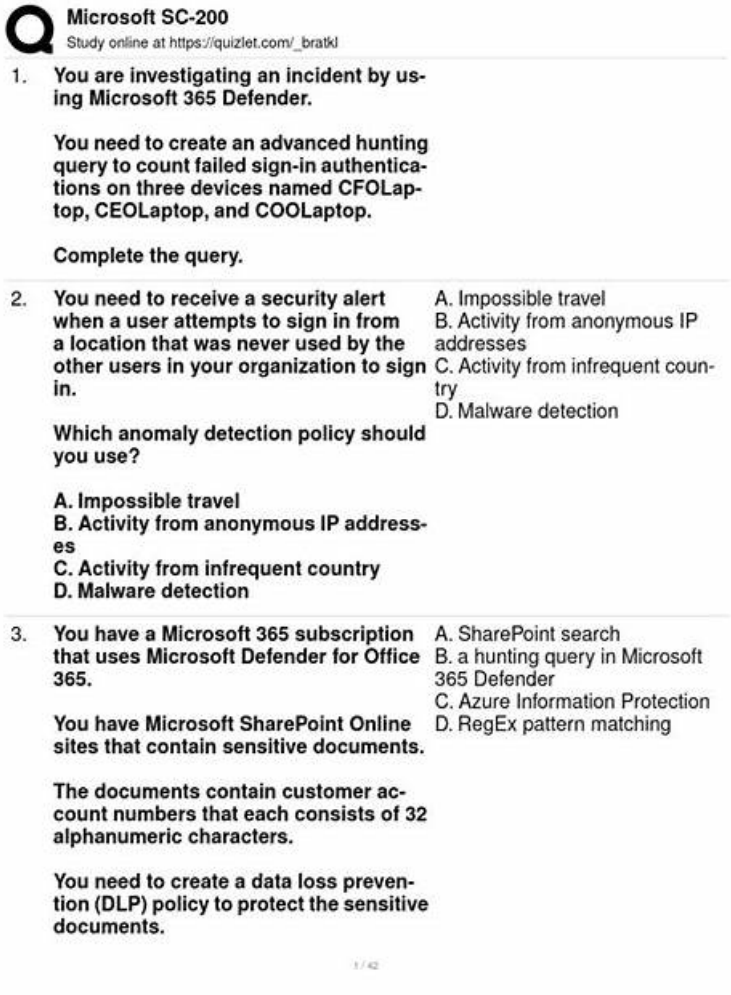
Your Ultimate Resource Actual of Microsoft SC-200 Questions



Microsoft SC-200
Study online at https://quizlet.com/_bratkl

1. **You are investigating an incident by using Microsoft 365 Defender.**

   You need to create an advanced hunting query to count failed sign-in authentications on three devices named CFOLaptop, CEOLaptop, and COOLaptop.

   Complete the query.

2. **You need to receive a security alert when a user attempts to sign in from a location that was never used by the other users in your organization to sign in.**

   Which anomaly detection policy should you use?

   A. Impossible travel
   B. Activity from anonymous IP addresses
   C. Activity from infrequent country
   D. Malware detection

   A. Impossible travel
   B. Activity from anonymous IP addresses
   C. Activity from infrequent country
   D. Malware detection

3. **You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.**

   You have Microsoft SharePoint Online sites that contain sensitive documents.

   The documents contain customer account numbers that each consists of 32 alphanumeric characters.

   You need to create a data loss prevention (DLP) policy to protect the sensitive documents.

   A. SharePoint search
   B. a hunting query in Microsoft 365 Defender
   C. Azure Information Protection
   D. RegEx pattern matching

1 / 42

2026 Latest ValidTorrent SC-200 PDF Dumps and SC-200 Exam Engine Free Share: https://drive.google.com/open?id=1Fn-pVeQOMtRk-chb6UCjJ3wwGtCsBQHN

To ensure your 100% satisfaction, SC-200 free demo are available for the certification exam you're going to take before you purchased. All our SC-200 dumps collection is quite effectively by millions of people that passed SC-200 Real Exam and become professionals in IT filed. You will never regret choosing our SC-200 test answers as your practice materials because we will show you the most authoritative study guide.

Microsoft SC-200 exam covers a wide range of topics, including threat protection, vulnerability management, incident response, and compliance. Microsoft Security Operations Analyst certification exam is designed to test a candidate's ability to identify, assess, and respond to security threats in real-time. SC-200 exam consists of multiple-choice questions that test a candidate's knowledge and skills in various areas of cybersecurity. SC-200 exam duration is 180 minutes, and the candidate must score at least 700 out of 1000 to pass the exam.

Microsoft SC-200 (Microsoft Security Operations Analyst) Exam is a certification exam that tests the skills and knowledge needed to identify, investigate, and respond to security incidents in a Microsoft environment. SC-200 exam is intended for security professionals who have experience in security operations and are looking to validate their skills with a recognized certification. SC-200 exam covers various topics related to security operations, including threat detection, incident response, cloud security, and compliance.

>> SC-200 Trustworthy Source <<

Pass Your SC-200 Microsoft Security Operations Analyst Exam on the First Try with ValidTorrent

In order to ensure the quality of SC-200 actual exam, we have made a lot of efforts. Our company spent a great deal of money on hiring hundreds of experts and they formed a team to write the work. The qualifications of these experts are very high. They have rich knowledge and rich experience on SC-200 study guide. These experts spent a lot of time before the SC-200 Study Materials officially met with everyone. And we have made scientific arrangements for the content of the SC-200 actual exam. You will be able to pass the SC-200 exam with our excellent SC-200 exam questions.

Microsoft Security Operations Analyst Sample Questions (Q139-Q144):

NEW QUESTION # 139
You provision Azure Sentinel for a new Azure subscription. You are configuring the Security Events connector.
While creating a new rule from a template in the connector, you decide to generate a new alert for every event. You create the following rule query.

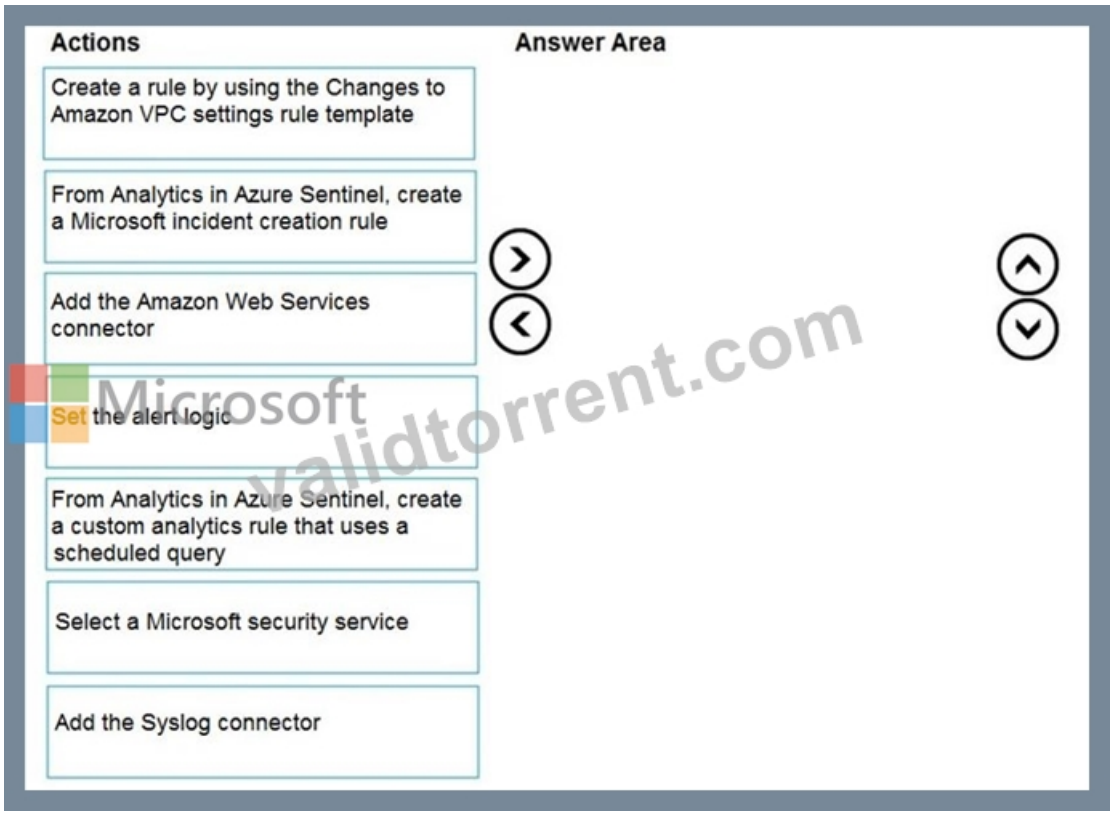
```
let timeframe = 1d;
SecurityEvent
| where TimeGenerated >= ago(timeframe)
| where EventID == 1102 and EventSourceName == "Microsoft-Windows-Eventlog"
| summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated),
EventCount = count() by
Computer, Account, EventID, Activity
| extend timestamp = StartTimeUtc, AccountCustomEntity = Account,
HostCustomEntity = Computer
```

By which two components can you group alerts into incidents? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

- A. resource group
- B. IP address
- C. computer
- D. user

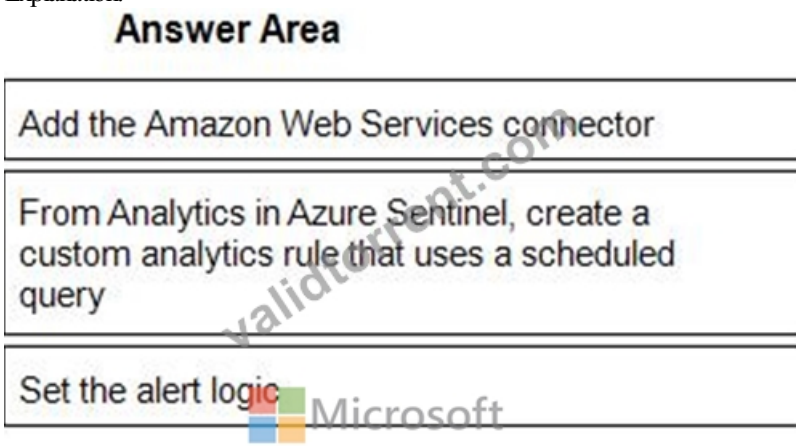
Answer: B,C

NEW QUESTION # 140
You need to use an Azure Sentinel analytics rule to search for specific criteria in Amazon Web Services (AWS) logs and to generate incidents.
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.
a Microsoft 365 E5



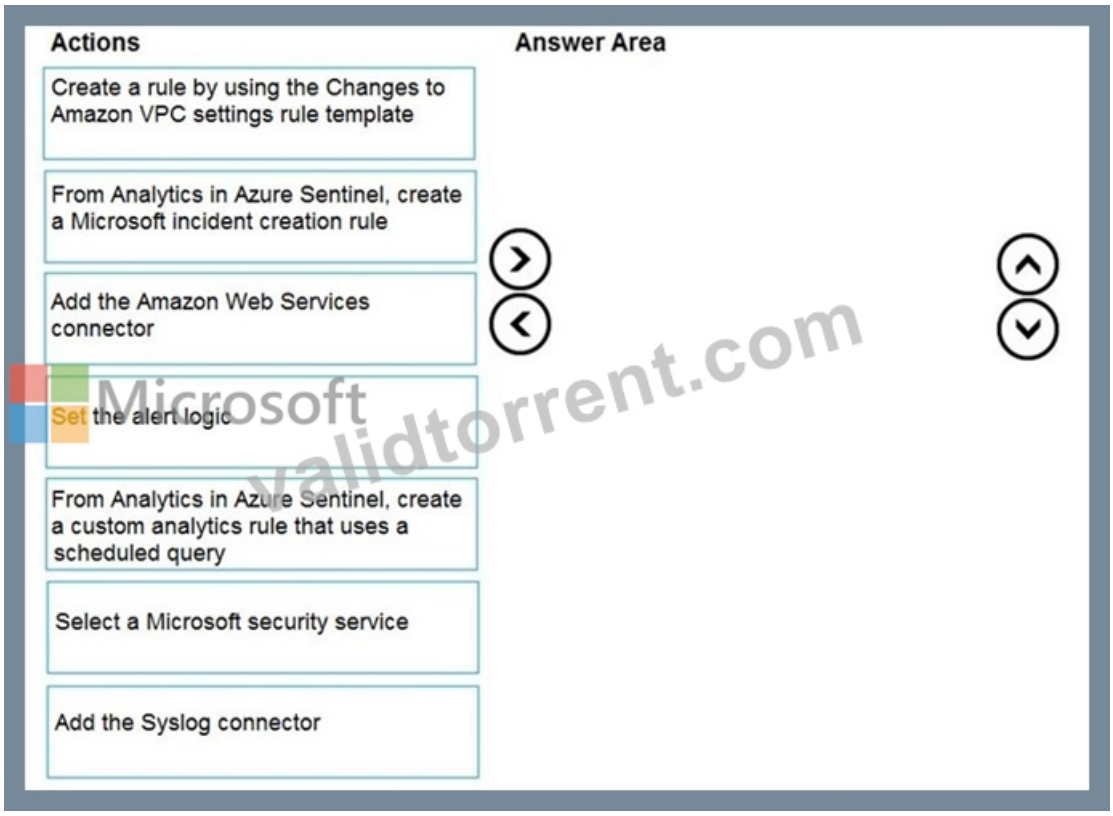
Answer:

Explanation:



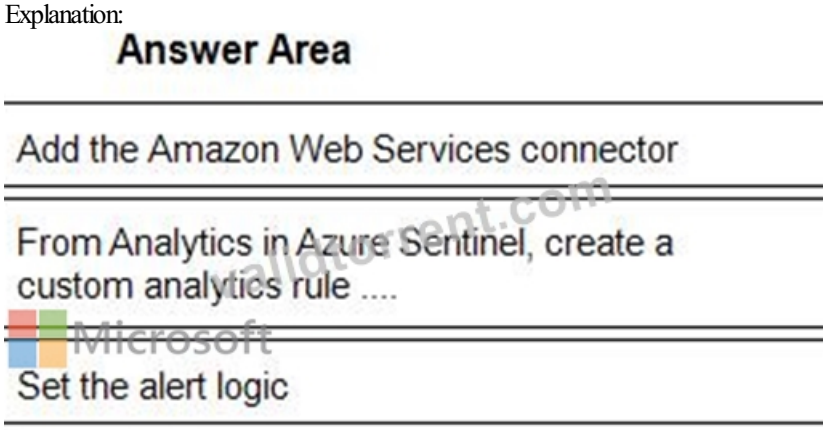
1 - Add the Amazon Web Services connector
2 - From Analytics in Azure Sentinel, create a custom analytics rule that uses a scheduled query
3 - Set the alert logic
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom

NEW QUESTION # 141
You need to use an Azure Sentinel analytics rule to search for specific criteria in Amazon Web Services (AWS) logs and to generate incidents.
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.



Answer:

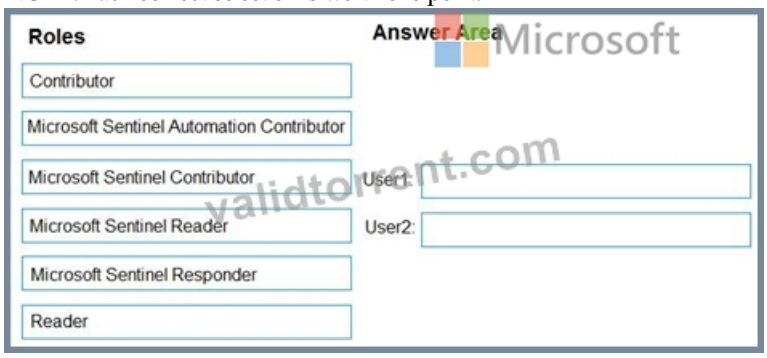
Explanation:



1 - Add the Amazon Web Services connector
2 - From Analytics in Azure Sentinel, create a custom analytics rule ....
3 - Set the alert logic
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom

NEW QUESTION # 142
Drag and Drop Question
You have an Azure subscription that contains two users named User1 and User2 and a Microsoft Sentinel workspace named workspace1.
You need to ensure that the users can perform the following tasks in workspace1:
- User1 must be able to dismiss incidents and assign incidents to users.
- User2 must be able to modify analytics rules.
The solution must use the principle of least privilege.
Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role 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.



Answer:

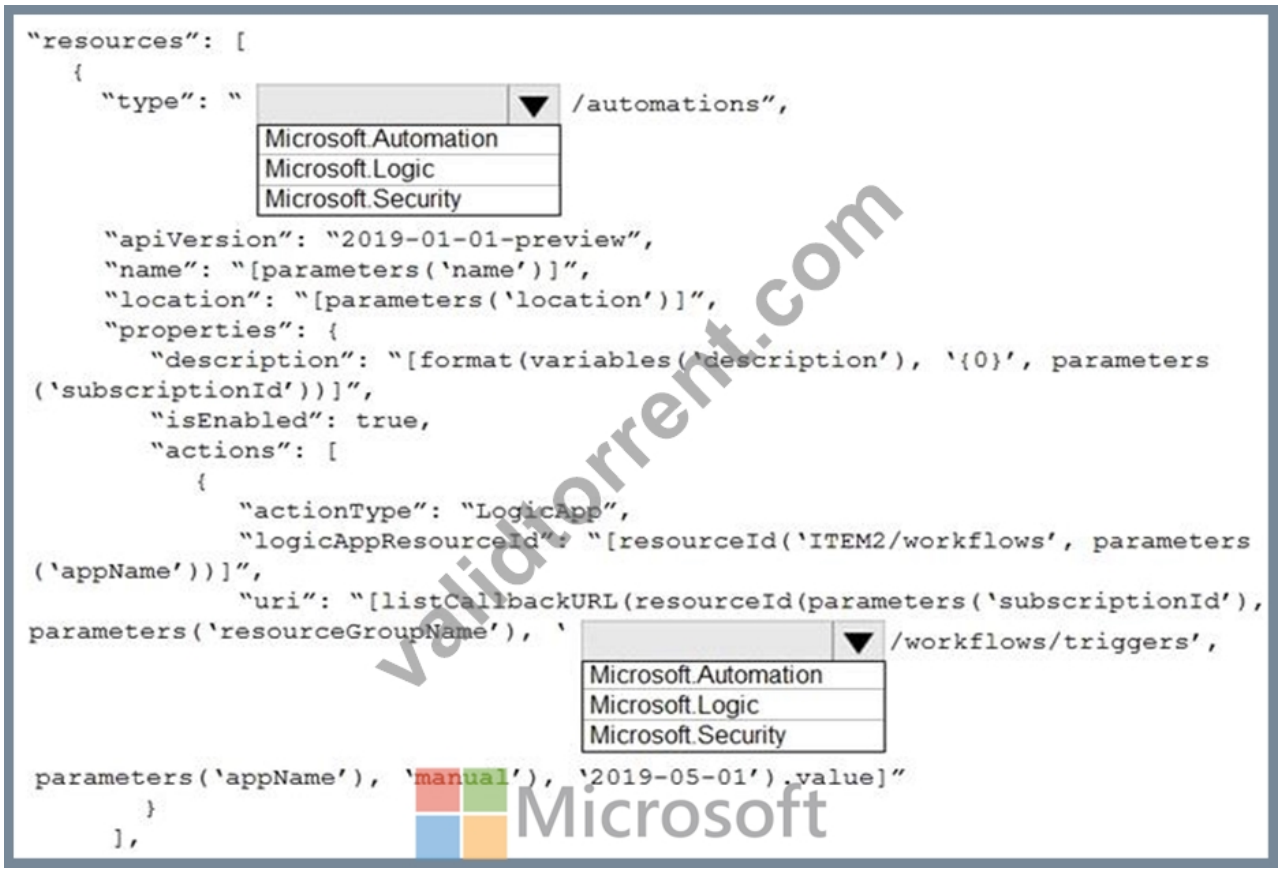
Explanation:

NEW QUESTION # 143

You need to use an Azure Resource Manager template to create a workflow automation that will trigger an automatic remediation when specific security alerts are received by Azure Security Center.

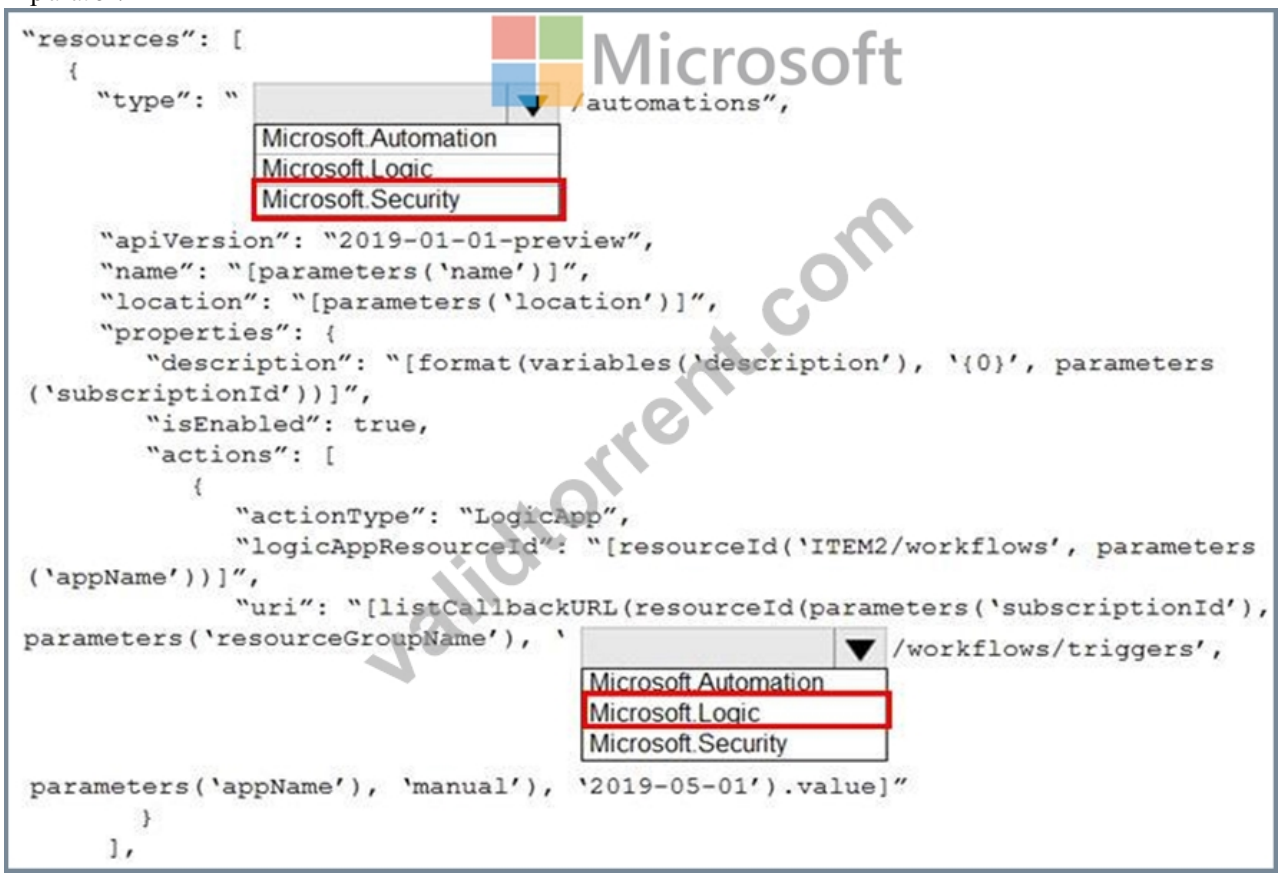
How should you complete the portion of the template that will provision the required Azure resources? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Reference:
https://docs.microsoft.com/en-us/azure/security-center/quickstart-automation-alert

NEW QUESTION # 144
.....

In order to protect the vital interests of each IT certification exams candidate, ValidTorrent provides high-quality Microsoft SC-200 Exam Training materials. This exam material is specially developed according to the needs of the candidates. It is researched by the IT experts of ValidTorrent. Their struggle is not just to help you pass the exam, but also in order to let you have a better tomorrow.

SC-200 New Braindumps Book: https://www.validtorrent.com/SC-200-valid-exam-torrent.html

- Free PDF Microsoft - SC-200 - Microsoft Security Operations Analyst Pass-Sure Trustworthy Source □ Simply search for ➠ SC-200 □ for free download on ☀ www.verifieddumps.com □☀□ □SC-200 Exam Question
- Latest SC-200 Exam Fee □ SC-200 Exam Consultant □ Regualer SC-200 Update □ Search for 「 SC-200 」 and download exam materials for free through ➤ www.pdfvce.com □ □SC-200 Trustworthy Exam Content
- Quiz 2026 High Pass-Rate Microsoft SC-200: Microsoft Security Operations Analyst Trustworthy Source □ Search for 「 SC-200 」 and download exam materials for free through （ www.verifieddumps.com ） □SC-200 Exam Consultant
- Updated Microsoft SC-200 Exam Questions For Accurately Prepare [2026] □ Enter 【 www.pdfvce.com 】 and search for ✔ SC-200 □✔□ to download for free □Exam SC-200 Dump
- Quiz Reliable SC-200 - Microsoft Security Operations Analyst Trustworthy Source □ Copy URL ➥ www.dumpsquestion.com □ open and search for ▹ SC-200 ◃ to download for free □Free SC-200 Vce Dumps
- Free PDF Efficient SC-200 - Microsoft Security Operations Analyst Trustworthy Source □ Easily obtain free download of （ SC-200 ） by searching on ☀ www.pdfvce.com □☀□ ⤴SC-200 Valid Exam Objectives
- SC-200 Online Test □ SC-200 Online Test □ SC-200 Valid Test Tutorial □ Immediately open ✔ www.practicevce.com □✔□ and search for ➡ SC-200 □□□ to obtain a free download □Real SC-200 Braindumps
- SC-200 Reliable Dumps Free □ SC-200 Exam Question □ SC-200 Learning Engine □ Easily obtain " SC-200 " for free download through ➽ www.pdfvce.com □ □Free SC-200 Vce Dumps
- SC-200 Trustworthy Source - 100% Pass Quiz 2026 SC-200: First-grade Microsoft Security Operations Analyst New Braindumps Book □ Download ▹ SC-200 ◃ for free by simply searching on □ www.practicevce.com □ □SC-200 Valid Test Tutorial
- Latest SC-200 Exam Fee □ New SC-200 Test Topics □ Exam SC-200 Dump □ Go to website □ www.pdfvce.com □ open and search for " SC-200 " to download for free □SC-200 Reliable Dumps Free
- New SC-200 Test Test □ Brain Dump SC-200 Free □ Free SC-200 Vce Dumps □ ➥ www.prepawaypdf.com □ is best website to obtain ➠ SC-200 □ for free download □SC-200 Valid Exam Objectives
- haseebzkxb851609.vidublog.com, honeyabwi370497.losblogos.com, gregorybnpw411108.levitra-wiki.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, barbaramvwa865803.wikitelevisions.com, sachinwoqh923727.gigswiki.com, bookmarksea.com, majahxpc552923.techionblog.com, anandurja.in, louiseyimb967099.blogsuperapp.com, Disposable vapes

What's more, part of that ValidTorrent SC-200 dumps now are free: https://drive.google.com/open?id=1Fn-pVeQOMtRk-chb6UCjJ3wwGtCsBQHN