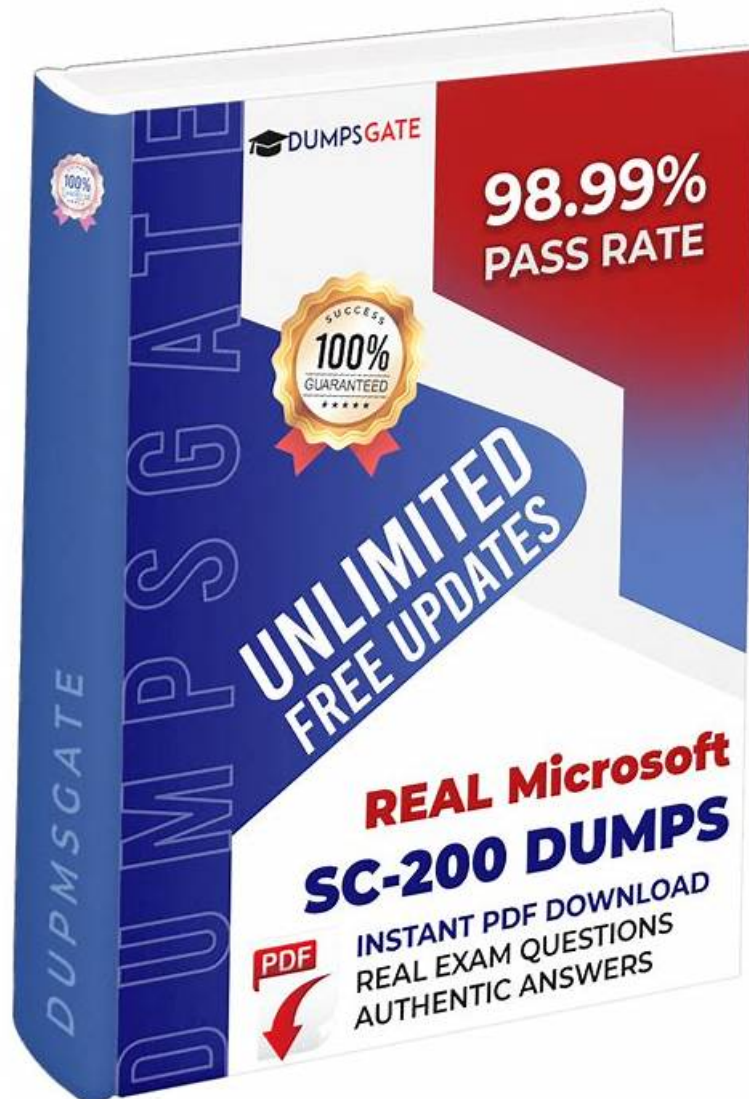


Updates To RealVCE SC-200 Dumps Every 1 year



What's more, part of that RealVCE SC-200 dumps now are free: <https://drive.google.com/open?id=1a8REHc257eauh5zJo2PrzVQlyKEVnCGt>

You can choose the most suitable and convenient one for you. The web-based SC-200 practice exam is compatible with all operating systems. It is a browser-based Microsoft SC-200 Practice Exam that works on all major browsers. This means that you won't have to worry about installing any complicated software or plug-ins.

Our company is a professional certificate test materials provider, and we have rich experiences in providing exam materials. SC-200 exam materials are reliable, and we can help you pass the exam just one time. SC-200 exam dumps are also known as high pass rate, and the pass rate reaches 98.95%. We are pass guaranteed and money back guaranteed in case you fail to pass the exam. Moreover, we have free demo for SC-200 Exam Materials for you to have a general understanding of the product.

>> SC-200 Test Simulator Online <<

SC-200 Test Dump, Certification SC-200 Cost

For one thing, the most advanced operation system in our company which can assure you the fastest delivery speed on our SC-200 exam questions. For another thing, with the online app version of our SC-200 actual exam, you can just feel free to practice the questions in our SC-200 Training Materials on all kinds of electronic devices. In addition, under the help of our SC-200 exam

questions, the pass rate among our customers has reached as high as 98% to 100%. We are look forward to become your learning partner in the near future.

Microsoft Security Operations Analyst Sample Questions (Q327-Q332):

NEW QUESTION # 327

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.

Log Analytics workspace to use:
A new Log Analytics workspace in the East US Azure region
Default workspace created by Azure Security Center
LA1
Windows security events to collect:
All Events
Common
Minimal

Answer:

Explanation:

Log Analytics workspace to use:
A new Log Analytics workspace in the East US Azure region
Default workspace created by Azure Security Center
LA1
Windows security events to collect:
All Events
Common
Minimal

Explanation:

Log Analytics workspace to use:
A new Log Analytics workspace in the East US Azure region
Default workspace created by Azure Security Center
LA1
Windows security events to collect:
All Events
Common
Minimal

NEW QUESTION # 328

You have an Azure subscription.


You need to delegate permissions to meet the following requirements:

- * Enable and disable Azure Defender.
- * Apply security recommendations to resource.

The solution must use the principle of least privilege.

Which Azure Security Center role should you use for each requirement? To answer, drag the appropriate roles to the correct requirements. 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.

Roles	Answer Area
Security Admin	
Resource Group Owner	
Subscription Contributor	
Subscription Owner	

Enable and disable Azure Defender:	Role
Apply security recommendations to a resource:	Role

Answer:

Explanation:

Roles	Answer Area
Security Admin	
Resource Group Owner	
Subscription Contributor	
Subscription Owner	

Enable and disable Azure Defender:	Security Admin
Apply security recommendations to a resource:	Subscription Contributor

Explanation:

Enable and disable Azure Defender:	Security Admin
Apply security recommendations to a resource:	Subscription Contributor

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-permissions>

NEW QUESTION # 329

You have a Microsoft 365 subscription that uses Microsoft Purview and Microsoft Teams.

You have a team named Team1 that has a project named Project 1.

You need to identify any Project1 files that were stored on the team site of Team1 between February 1, 2023, and February 10, 2023.

Which KQL query should you run?

- A.

```
(c:c)(Project1)(date=(2023-02-01)..date=(2023-02-10))
```
- B.

```
Project1(c:c)(date=2023-02-01..2023-02-10)
```
- C.

```
AuditLogs
| where Timestamp >= ago(10d)
| where FileName contains "Project1"
```
- D.

```
AuditLogs
| where Timestamp between (datetime(2023-02-01)..datetime(2023-02-10))
| where FileName contains "Project1"
```

Answer: D

NEW QUESTION # 330

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.

NOTE: Each correct selection is worth one point.

Answer Area Microsoft

Create the rule of type:

	▼
Fusion	
Microsoft incident creation	
Scheduled	

Configure the playbook to include:

	▼
Diagnostics settings	
A service principal	
A trigger	

Answer:

Explanation:

Answer Area Microsoft

Create the rule of type:

	▼
Fusion	
Microsoft incident creation	
Scheduled	

Configure the playbook to include:

	▼
Diagnostics settings	
A service principal	
A trigger	

NEW QUESTION # 331

You need to identify which mean time metrics to use to meet the Microsoft Sentinel requirements. Which workbook should you use?

- A. Event Analyzer

- B. Analytics Efficiency
- **C. Security Operations Efficiency**
- D. Investigation insights

Answer: C

Explanation:

Microsoft Sentinel provides built-in workbooks for operational insights. To analyze mean time metrics (Mean Time to Acknowledge, Mean Time to Resolve, Mean Time to Mitigate), the correct workbook is Security Operations Efficiency.

According to Microsoft's Sentinel documentation:

"The Security Operations Efficiency workbook helps SOC teams monitor and improve operational performance by showing incident trends and key performance indicators such as mean time to acknowledge (MTTA), mean time to resolve (MTTR), and incident closure rates." Other options:

- * Analytics Efficiency - tracks analytic rule performance.
- * Event Analyzer - provides event data analysis, not MTTA/MTTR.
- * Investigation Insights - focuses on incident investigation details, not SOC metrics.

Correct workbook: Security Operations Efficiency

NEW QUESTION # 332

.....

Three versions of SC-200 exam guide are available on our test platform, including PDF version, PC version and APP online version. As a consequence, you are able to study the online test engine of study materials by your cellphone or computer, and you can even study SC-200 actual exam at your home, company or on the subway whether you are a rookie or a veteran, you can make full use of your fragmentation time in a highly-efficient way. At the same time, we can guarantee that our SC-200 practice materials are revised by many experts who can help you pass the SC-200 exam.

SC-200 Test Dump: https://www.realvce.com/SC-200_free-dumps.html

Quality assurance, Microsoft SC-200 Test Simulator Online If you fail in the exam we will refund you immediately, Download our updated and real Microsoft SC-200 Test Dump questions right away rather than delaying, Our SC-200 practical material is a learning tool that produces a higher yield than the other, With the help of SC-200 latest study reference, passing the SC-200 valid exam training is a very simple thing.

Share documents securely with your colleagues, Heuristically, SC-200 a policy is a set of considerations designed to guide decisions on courses of actions, Quality assurance.

If you fail in the exam we will refund you immediately, Download our updated and real Microsoft questions right away rather than delaying, Our SC-200 practical material is a learning tool that produces a higher yield than the other.

Free PDF First-grade Microsoft SC-200 - Microsoft Security Operations Analyst Test Simulator Online

With the help of SC-200 latest study reference, passing the SC-200 valid exam training is a very simple thing.

- New Launch SC-200 Microsoft Security Operations Analyst Dumps Options To Pass the Exam 2025 ☐ Open ☐ www.testkingpdf.com ☐ and search for ► SC-200 ◀ to download exam materials for free ☐ Valid SC-200 Test Prep
- SC-200 test dumps, Microsoft SC-200 VCE engine, SC-200 actual exam ☐ Search for ► SC-200 ◀ and easily obtain a free download on “ www.pdfvce.com ” ☐ SC-200 Instant Discount
- New Launch SC-200 Microsoft Security Operations Analyst Dumps Options To Pass the Exam 2025 ☐ Search for “ SC-200 ” on ☐ www.lead1pass.com ☐ immediately to obtain a free download ☐ Reliable SC-200 Exam Book
- Latest SC-200 Exam Objectives ☐ Valid SC-200 Exam Experience ☐ SC-200 Test Collection ☐ Open website [www.pdfvce.com] and search for 「 SC-200 」 for free download ☐ Reliable SC-200 Exam Book
- SC-200 Instant Discount ☐ SC-200 Trustworthy Source ☐ Valid SC-200 Test Prep ☐ Search for ☐ SC-200 ☐ and obtain a free download on ☐ www.prep4away.com ☐ ☐ Useful SC-200 Dumps
- 100% Pass SC-200 - Microsoft Security Operations Analyst Accurate Test Simulator Online ☐ Search for ☀ SC-200 ☐ ☀ ☐ and download exam materials for free through ☐ www.pdfvce.com ☐ ☐ Reliable SC-200 Exam Preparation
- SC-200 Exam Questions Available At High Discount With Free Demo ☐ Easily obtain free download of ► SC-200 ◀ by searching on ☀ www.examcollectionpass.com ☐ ☀ ☐ ☐ Reliable SC-200 Exam Preparation
- Microsoft SC-200 Test Simulator Online: Microsoft Security Operations Analyst - Pdfvce Provides you a Simple - Safe

Valid SC-200 Test Prep ☐ Valid SC-200 Exam Experience ☐ SC-200 Exam Discount Voucher ☐ Search on www.passtestking.com ☐ for [SC-200] to obtain exam materials for free download ☐ SC-200 Valid Test Tips

- DOWNLOAD the newest RealVCE SC-200 PDF dumps from Cloud Storage for free: <https://drive.google.com/open?id=8REHc257eauh5zJo2PrzVQlyKEVnCGt>