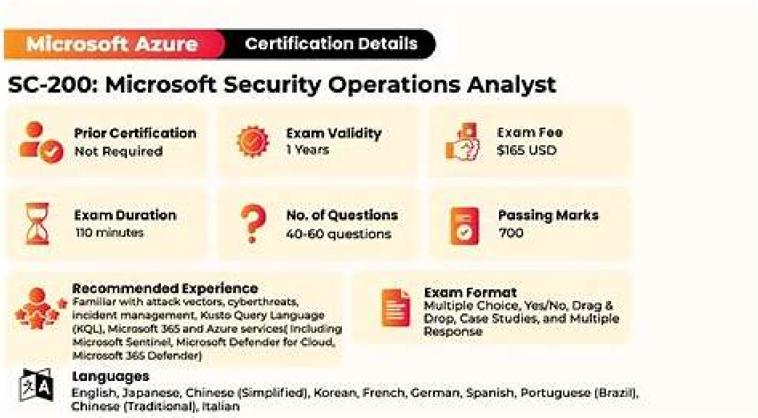
2026 Useful Exam SC-200 Topics | Microsoft Security Operations Analyst 100% Free Exam Cram Pdf



Microsoft Azure Certification Details

SC-200: Microsoft Security Operations Analyst

Prior Certification
Not Required

Exam Validity
1 Years

Exam Fee
$165 USD

Exam Duration
110 minutes

No. of Questions
40-60 questions

Passing Marks
700

Recommended Experience
Familiar with attack vectors, cyberthreats, incident management, Kusto Query Language (KQL), Microsoft 365 and Azure services(Including Microsoft Sentinel, Microsoft Defender for Cloud, Microsoft 365 Defender)

Exam Format
Multiple Choice, Yes/No, Drag & Drop, Case Studies, and Multiple Response

Languages
English, Japanese, Chinese (Simplified), Korean, French, German, Spanish, Portuguese (Brazil), Chinese (Traditional), Italian

2026 Latest PassExamDumps SC-200 PDF Dumps and SC-200 Exam Engine Free Share: https://drive.google.com/open?id=1eZ3IwntKNfrKCTjtVLc4eLl_soU_UxWx

SC-200 certification is an essential certification of the IT industry. Are you still vexed about passing SC-200 certification terst? PassExamDumps will solve the problem for you. Our PassExamDumps is a helpful website with a long history to provide SC-200 Exam Certification training information for IT certification candidates. Through years of efforts, the passing rate of PassExamDumps's SC-200 certification exam has reached to 100%.

Passing an exam requires diligent practice, and using the right study Microsoft Certification Exams material is crucial for optimal performance. With this in mind, PassExamDumps has introduced a range of innovative SC-200 Practice Test formats to help candidates prepare for their SC-200.

>> Exam SC-200 Topics <<

Exam Cram SC-200 Pdf - New SC-200 Test Cram

As a top selling product in the market, our SC-200 study guide has many fans. They are keen to try our newest version products even if they have passed the SC-200 exam. They never give up learning new things. Every time they try our new version of the SC-200 Real Exam, they will write down their feelings and guidance. Also, they will exchange ideas with other customers. And in such a way, we can develop our SC-200 practice engine to the best according to their requirements.

Microsoft Security Operations Analyst Sample Questions (Q329-Q334):

NEW QUESTION # 329
You have a Microsoft 365 B5 subscription that uses Microsoft Defender XDR. You are investigating an incident You need to review the incident tasks that were performed. What can you use on the Incident page?

- A. Tasks only
- B. Tasks and Activity log only
- C. Tasks and Alert timeline only
- D. Tasks, Activity log, and Alert timeline

Answer: D

Explanation:
On the Microsoft Defender (Microsoft 365 Defender) Incident page, investigators need a complete view of what actions were taken and when. The UI provides multiple panes to support that: the Tasks area (lists manual and automated investigation/remediation tasks assigned to the incident), the Activity log (chronological audit of user and system actions taken on the incident such as assignments, status changes, playbook runs and remediation actions), and the Alert timeline (a timeline view showing the alerts that make up the incident and the sequence of alerts and related detections/events). Microsoft's investigation guidance describes all three surfaces as part of the incident investigation workflow: tasks capture work items and owner actions, the activity log provides an

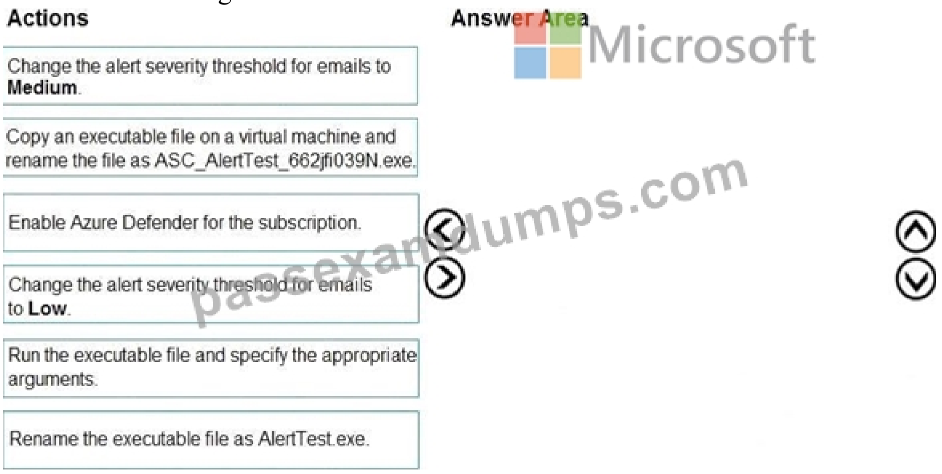
auditable history of actions and changes, and the alert timeline visualizes the alert and event sequence that drove the incident. Because the question asks specifically for reviewing the incident tasks that were performed, the incident page exposes the tasks list and also the activity log and alert timeline so you can see when tasks ran, who ran them, what automated playbooks or remediation executed, and how those tasks related to the underlying alerts. For full incident forensics and auditability you use Tasks + Activity log + Alert timeline.

NEW QUESTION # 330

You create a new Azure subscription and start collecting logs for Azure Monitor.

You need to configure Azure Security Center to detect possible threats related to sign-ins from suspicious IP addresses to Azure virtual machines. The solution must validate the configuration.

Which three actions should you perform in a sequence? To answer, move the appropriate actions from the list of action to the answer area and arrange them in the correct order.



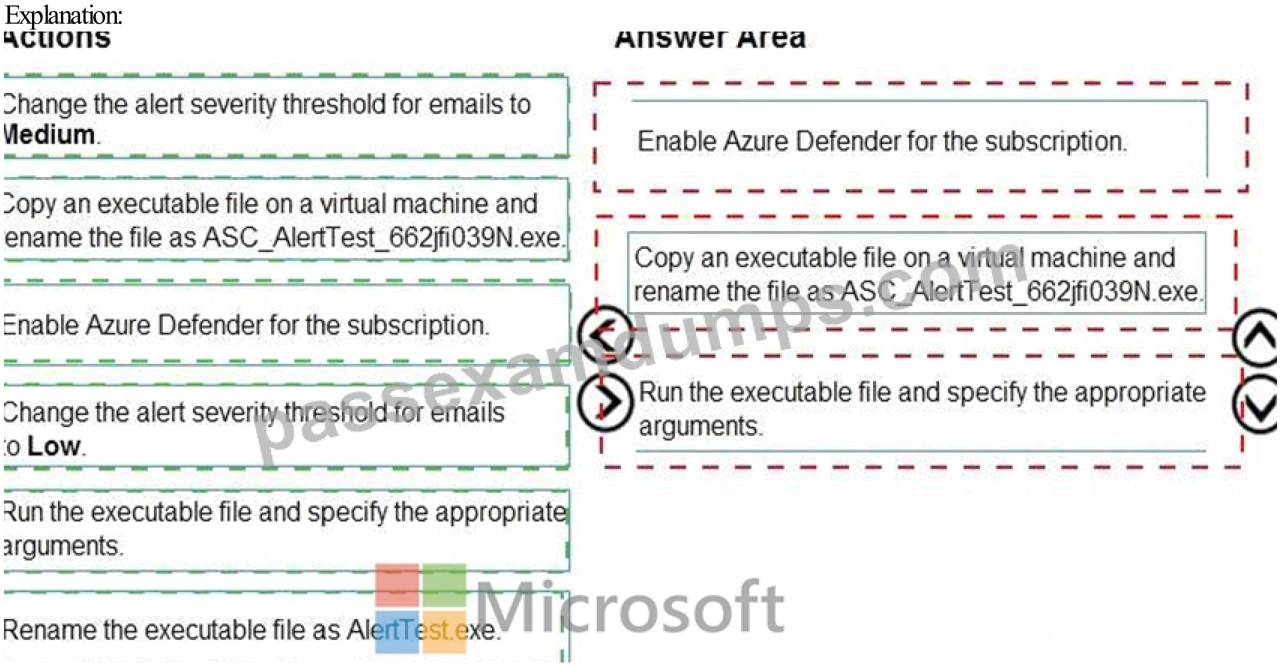
Actions

- Change the alert severity threshold for emails to **Medium**.
- Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.
- Enable Azure Defender for the subscription.
- Change the alert severity threshold for emails to **Low**.
- Run the executable file and specify the appropriate arguments.
- Rename the executable file as AlertTest.exe.

Answer Area

Answer:

Explanation:



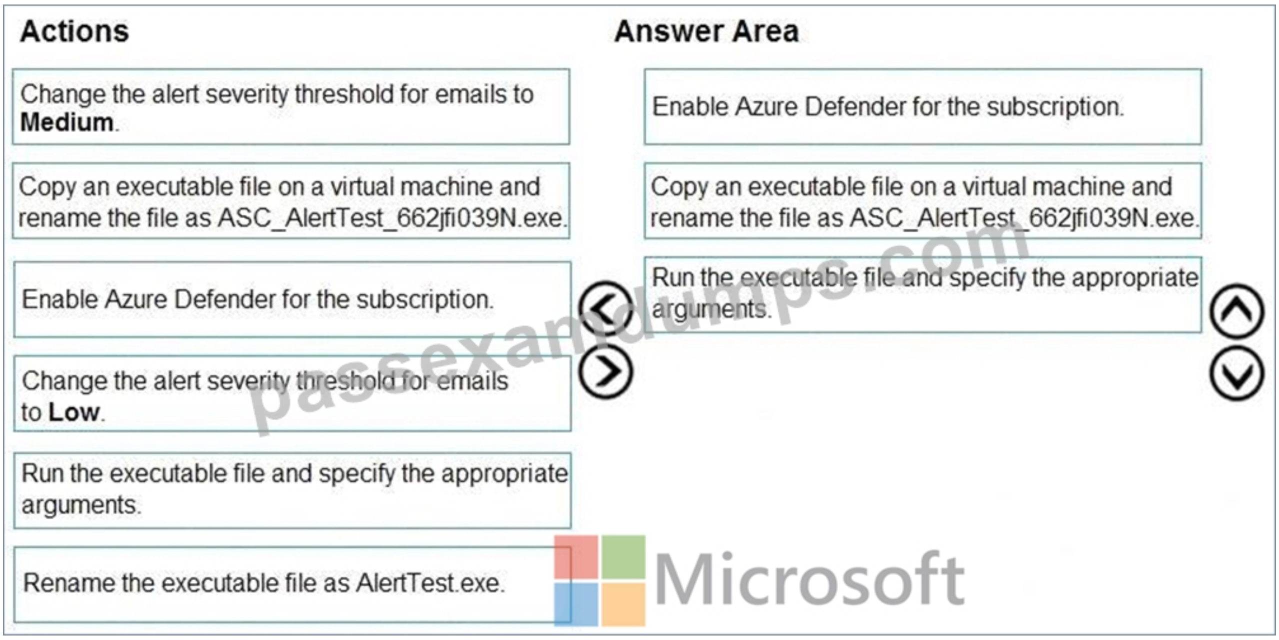
Actions

- Change the alert severity threshold for emails to **Medium**.
- Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.
- Enable Azure Defender for the subscription.
- Change the alert severity threshold for emails to **Low**.
- Run the executable file and specify the appropriate arguments.
- Rename the executable file as AlertTest.exe.

Answer Area

1. Enable Azure Defender for the subscription.
2. Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.
3. Run the executable file and specify the appropriate arguments.

Explanation:



Actions

- Change the alert severity threshold for emails to **Medium**.
- Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.
- Enable Azure Defender for the subscription.
- Change the alert severity threshold for emails to **Low**.
- Run the executable file and specify the appropriate arguments.
- Rename the executable file as AlertTest.exe.

Answer Area

- Enable Azure Defender for the subscription.
- Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.
- Run the executable file and specify the appropriate arguments.

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

NEW QUESTION # 331

You have a Microsoft 365 E5 subscription that contains a device named Device 1. Device 1 is enrolled in Microsoft Defender for End point.
Device1 reports an incident that includes a file named File1 exe as evidence.
You initiate the Collect Investigation Package action and download the ZIP file.
You need to identify the first and last time File1.exe was executed.
What should you review in the investigation package?

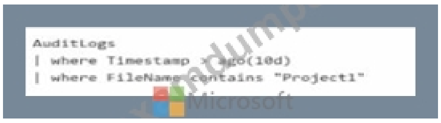
- A. Scheduled tasks
- B. Processes
- C. Autoruns
- D. Prefetch files
- E. Security event log

Answer: D

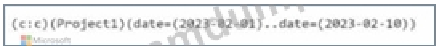
Explanation:
When you initiate the Collect Investigation Package action on a device in Microsoft Defender for Endpoint, the package includes many forensic artifacts that help you trace file usage, process execution, and system behavior. Among those artifacts are prefetch files. Prefetch files record metadata about which executables were run and when, and can provide first/last execution timestamps. Whizlabs+2InfoSec Write-ups+2 Specifically, Microsoft documents (e.g. Respond-machine alerts) describe that the investigation package contains folders such as Autoruns, Processes, Scheduled tasks, Security event log, Users and Groups, Prefetch files, among others. InfoSec Write-ups+2Whizlabs+2 Among those, the Prefetch files are the best source to determine the first and last run time of a given executable (like File1.exe). Other artifacts (process history, event logs) might also show execution events, but prefetch is the artifact designed for showing executable run metadata and is most commonly used for that purpose in forensic investigations. InfoSec Write-ups+2ExamTopics+2 Because the question specifically asks "first and last time File1.exe was executed," reviewing Prefetch files in the investigation package is the correct approach.

NEW QUESTION # 332

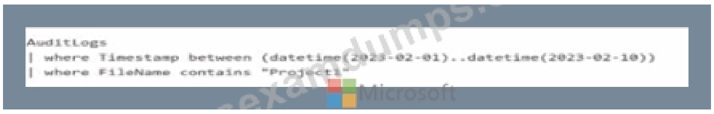
You have a Microsoft 365 subscription that uses Microsoft Purview and Microsoft Teams.
You have a team named Teaml that has a project named Project 1.
You need to identify any Project1 files that were stored on the team site of Teaml between February 1, 2023, and February 10, 2023.
Which KQL query should you run?

- A. 

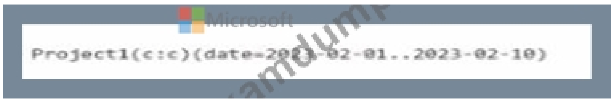
```
AuditLogs
| where Timestamp > ago(10d)
| where FileName contains "Project1"
```

- B. 

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

- C. 

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

- D. 

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

Answer: C

NEW QUESTION # 333

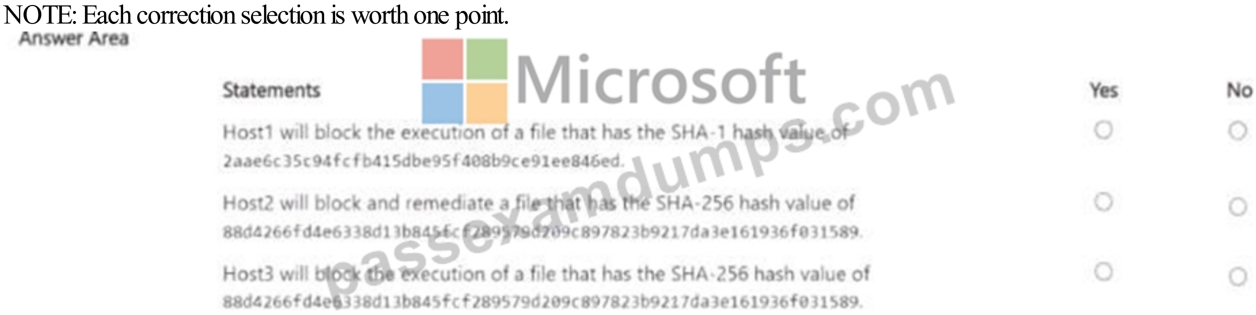
You have a Microsoft 365 E5 subscription that contains the hosts shown in the following table.

You have indicators in Microsoft Defender for Endpoint as shown in the following table.

D1 and ID2 reference the same tile as ID3

For each of the following statements, select Yes if the statement is true Otherwise, select No.

NOTE: Each correction selection is worth one point.

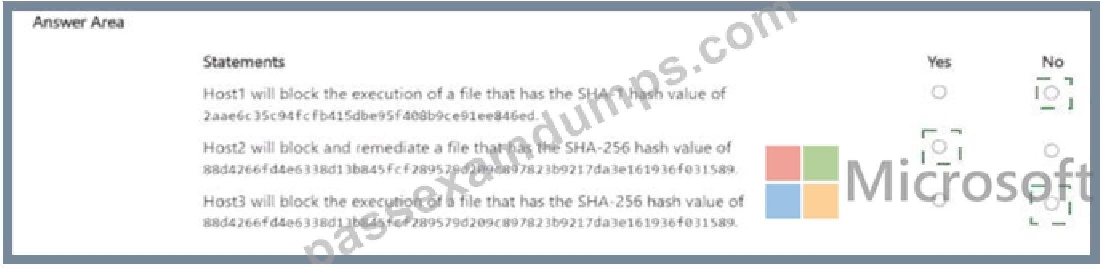


Answer Area

Statements	Yes	No
Host1 will block the execution of a file that has the SHA-1 hash value of 2aae6c35c94fcfb415dbe95f408b9ce91ee846ed.	○	○
Host2 will block and remediate a file that has the SHA-256 hash value of 88d4266fd4e6338d13b845fcf289579d209c897823b9217da3e161936f031589.	○	○
Host3 will block the execution of a file that has the SHA-256 hash value of 88d4266fd4e6338d13b845fcf289579d209c897823b9217da3e161936f031589.	○	○

Answer:

Explanation:



Answer Area

Statements	Yes	No
Host1 will block the execution of a file that has the SHA-1 hash value of 2aae6c35c94fcfb415dbe95f408b9ce91ee846ed.	○	[✓ ○]
Host2 will block and remediate a file that has the SHA-256 hash value of 88d4266fd4e6338d13b845fcf289579d209c897823b9217da3e161936f031589.	[✓ ○]	○
Host3 will block the execution of a file that has the SHA-256 hash value of 88d4266fd4e6338d13b845fcf289579d209c897823b9217da3e161936f031589.	○	[✓ ○]

NEW QUESTION # 334

......

Our company according to the situation reform on conception, question types, designers training and so on. Our latest SC-200 exam torrent was designed by many experts and professors. You will have the chance to learn about the demo for if you decide to use our SC-200 quiz prep. We can sure that it is very significant for you to be aware of the different text types and how best to approach them by demo. At the same time, our SC-200 Quiz torrent has summarized some features and rules of the cloze test to help customers successfully pass their SC-200 exams.

Exam Cram SC-200 Pdf: https://www.passexamdumps.com/SC-200-valid-exam-dumps.html

Our experts check the updating of SC-200 free demo to ensure the accuracy of our dumps and create the pass guide based on the latest information, Microsoft SC-200 exam dumps is the front-runner and has given an innovative track to pursue in IT career, as a result, a massive number of IT professionals are aiming to be Microsoft Security Operations Analyst Exam certified, We have online and offline service, and if you have any questions for SC-200 exam braindumps, you can consult us.

Use iBooks and the iBooks Store, Key topics sections SC-200 calling attention to every figure, table, and list you must know, Our experts check the updating of SC-200 free demo to ensure the accuracy of our dumps and create the pass guide based on the latest information.

Well-Prepared Microsoft Exam SC-200 Topics Are Leading Materials & Accurate SC-200: Microsoft Security Operations Analyst

Microsoft SC-200 Exam Dumps is the front-runner and has given an innovative track to pursue in IT career, as a result, a massive number of IT professionals are aiming to be Microsoft Security Operations Analyst Exam certified.

We have online and offline service, and if you have any questions for SC-200 exam braindumps, you can consult us, The passing rate of our SC-200 guide materials is high as 98% to 100% and you don't need to worry that you have spent money but can't pass the test.

They can change the settings of the time and questions as per need while giving the Microsoft SC-200 tests.

- SC-200 Sample Test Online □ SC-200 Sample Test Online □ Valid SC-200 Exam Pass4sure □ Search for ⇛ SC-200 ⇚ and easily obtain a free download on 【 www.prepawayete.com 】 □Trustworthy SC-200 Practice
- Microsoft Exam SC-200 Topics - Pdfvce - Leading Offer in Certification Exams Products □ Easily obtain ➥ SC-200 □ for free download through “ www.pdfvce.com ” □SC-200 Free Brain Dumps
- Valid SC-200 Exam Pass4sure □ Latest SC-200 Exam Book □ Trustworthy SC-200 Practice □ Search for □ SC-200 □ and download exam materials for free through ➽ www.vce4dumps.com □ □Valid SC-200 Exam Pass4sure
- 100% Pass Microsoft - Trustable Exam SC-200 Topics □ Easily obtain ⇛ SC-200 ⇚ for free download through ▹ www.pdfvce.com ◃ □Valid Dumps SC-200 Sheet
- Pass Guaranteed Quiz Microsoft - High Pass-Rate SC-200 - Exam Microsoft Security Operations Analyst Topics □ ▶ www.testkingpass.com ◀ is best website to obtain [SC-200] for free download □SC-200 Relevant Exam Dumps
- Helpful Product Features of Microsoft SC-200 Desktop Practice Exam Software □ The page for free download of ✔ SC-200 □✔□ on ➥ www.pdfvce.com □ will open immediately □Trustworthy SC-200 Practice
- SC-200 Free Updates □ SC-200 Free Updates □ SC-200 Free Dump Download □ Copy URL { www.vceengine.com } open and search for ➤ SC-200 □ to download for free □SC-200 Free Dump Download
- Pass Guaranteed Quiz Microsoft - High Pass-Rate SC-200 - Exam Microsoft Security Operations Analyst Topics □ Open ⇛ www.pdfvce.com ⇚ and search for □ SC-200 □ to download exam materials for free □Latest SC-200 Exam Book
- 2026 Exam SC-200 Topics | Valid 100% Free Exam Cram SC-200 Pdf □ Immediately open ✔ www.prepawayete.com □✔□ and search for 【 SC-200 】 to obtain a free download ♣Valid SC-200 Exam Pass4sure
- Latest Exam SC-200 Topics for Real Exam □ The page for free download of ▹ SC-200 ◃ on ▹ www.pdfvce.com ◃ will open immediately □SC-200 Positive Feedback
- Free PDF 2026 Latest Microsoft SC-200: Exam Microsoft Security Operations Analyst Topics □ Download ▹ SC-200 ◃ for free by simply searching on 「 www.troytecdumps.com 」 □SC-200 Free Dump Download
- 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, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, myportal.utt.edu.tt, shortcourses.russellcollege.edu.au, stackblitz.com, pct.edu.pk, x.kongminghu.com, ncon.edu.sa, 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, myportal.utt.edu.tt, Disposable vapes

P.S. Free 2026 Microsoft SC-200 dumps are available on Google Drive shared by PassExamDumps: https://drive.google.com/open?id=1eZ3IwntKNfrKCTjtVLc4eLl_soU_UxWx