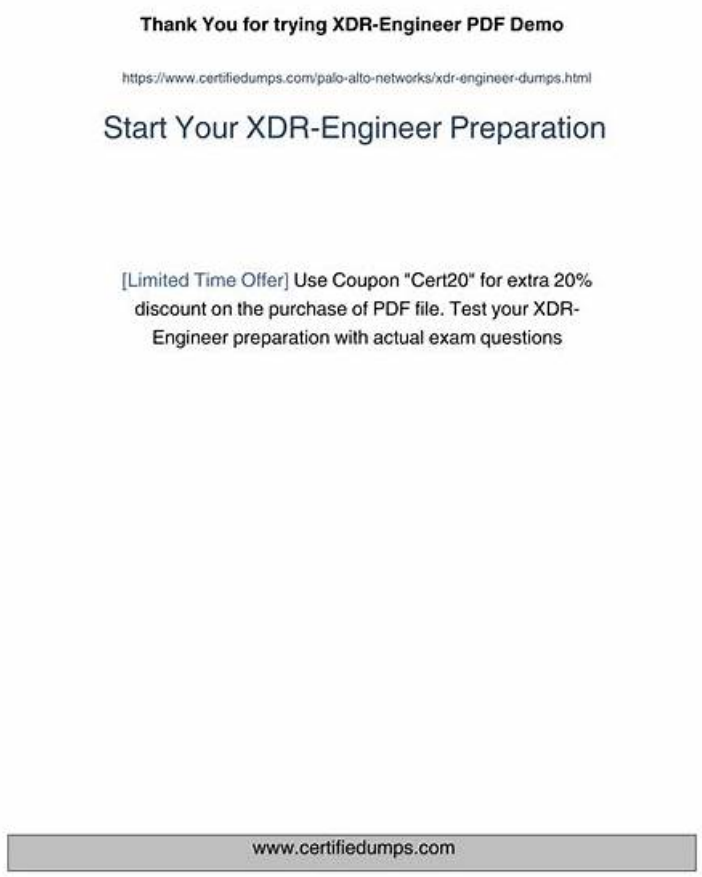
# Study Anywhere With PassReview Portable XDR-Engineer PDF Questions Format




P.S. Free & New XDR-Engineer dumps are available on Google Drive shared by PassReview: https://drive.google.com/open?id=1L-EGSU0gpoTDoqopfu4SHU2jROLK35l-

Palo Alto Networks XDR-Engineer exam questions are the best because these are so realistic! It feels just like taking a real Palo Alto Networks XDR-Engineer exam, but without the stress! Our Palo Alto Networks XDR-Engineer Practice Test software is the answer if you want to score higher on your real Palo Alto Networks XDR-Engineer certification exam and achieve your academic goals.

We've always put quality of our XDR-Engineer guide dumps on top priority. Each XDR-Engineer learning engine will go through strict inspection from many aspects such as the operation, compatibility test and so on. The quality inspection process is completely strict. The most professional experts of our company will check the XDR-Engineer study quiz and deal with the wrong parts. That is why we can survive in the market now. Our company is dedicated to carrying out the best quality XDR-Engineer study prep for you.

**>> XDR-Engineer Reliable Exam Voucher <<**

## XDR-Engineer Valid Test Guide, Valid XDR-Engineer Study Materials

To give you an idea about the top features of PassReview Palo Alto Networks XDR Engineer (XDR-Engineer) exam questions, a free demo of PassReview Palo Alto Networks XDR Engineer (XDR-Engineer) exam dumps is being offered free of cost. Just

download PassReview Palo Alto Networks XDR Engineer (XDR-Engineer) exam questions demo and checks out the top features of PassReview Palo Alto Networks XDR Engineer (XDR-Engineer) exam dumps. If you feel that PassReview Palo Alto Networks XDR-Engineer exam questions work for you then buy the full and final PassReview Palo Alto Networks XDR Engineer (XDR-Engineer) exam dumps at an affordable price and start Palo Alto Networks XDR Engineer (XDR-Engineer) exam preparation.

## Palo Alto Networks XDR Engineer Sample Questions (Q19-Q24):

**NEW QUESTION # 19**
Which step is required to configure a proxy for an XDR Collector?

- A. Connect the XDR Collector to the Pathfinder
- B. Restart the XDR Collector after configuring the proxy settings
- C. Edit the YAML configuration file with the new proxy information
- D. Configure the proxy settings on the Cortex XDR tenant

**Answer: C**

Explanation:
TheXDR Collectorin Cortex XDR is a lightweight tool for collecting logs and events from servers and endpoints. When a proxy is required for the XDR Collector to communicate with the Cortex XDR cloud, the proxy settings must be configured in the collector's configuration file. Specifically, theYAML configuration file(e.g., config.yaml) must be edited to include the proxy details, such as the proxy server's address, port, and authentication credentials (if required).
* Correct Answer Analysis (A):To configure a proxy for the XDR Collector, the engineer mustedit the YAML configuration filewith the new proxy information. This involves adding or updating the proxy settings in the file, which the collector uses to route its traffic through the specified proxy server.
* Why not the other options?
* B. Restart the XDR Collector after configuring the proxy settings: While restarting the collector may be necessary to apply changes, it is not the primary step required to configure the proxy. The YAML file must be edited first.
* C. Connect the XDR Collector to the Pathfinder: The Pathfinder is a Cortex XDR feature for discovering endpoints, not for configuring proxy settings for the XDR Collector.
* D. Configure the proxy settings on the Cortex XDR tenant: Proxy settings for the XDR Collector are configured locally on the collector, not in the Cortex XDR tenant's web interface.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains XDR Collector configuration: "To configure a proxy for the XDR Collector, edit the YAML configuration file to include the proxy server details, such as address and port" (paraphrased from the XDR Collector Configuration section). TheEDU-260: Cortex XDR Prevention and Deploymentcourse covers XDR Collector setup, stating that"proxy settings are configured by editing the collector's YAML file" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "data ingestion and integration" as a key exam topic, encompassing XDR Collector configuration.
References:
Palo Alto Networks Cortex XDR Documentation Portal:https://docs-cortex.paloaltonetworks.com/ EDU-260: Cortex XDR Prevention and Deployment Course Objectives Palo Alto Networks Certified XDR Engineer Datasheet:https://www.paloaltonetworks.com/services/education/certification#xdr-engineer

**NEW QUESTION # 20**
Some company employees are able to print documents when working from home, but not on network- attached printers, while others are able to print only to file. What can be inferred about the affected users' inability to print?

- A. They may be attached to the default extensions policy and profile
- B. They may be on different device extensions profiles set to block different print jobs
- C. They may have a host firewall profile set to block activity to all network-attached printers
- D. They may have different disk encryption profiles that are not allowing print jobs on encrypted files

**Answer: C**

Explanation:
In Cortex XDR, printing issues can be influenced by agent configurations, particularly those related to network access or device control. The scenario describes two groups of employees: one group can print when working from home but not on network-attached printers, and another can only print to file (e.g., PDF or XPS). This suggests a restriction on network printing, likely due to

a security policy enforced by the Cortex XDR agent.
* Correct Answer Analysis (B):They may have a host firewall profile set to block activity to all network-attached printersis the most likely inference. Cortex XDR'shost firewallfeature allows administrators to define rules that control network traffic, including blocking outbound connections to network-attached printers (e.g., by blocking protocols like IPP or LPD on specific ports). Employees working from home (on external networks) may be subject to a firewall profile that blocks network printing to prevent data leakage, while local printing (e.g., to USB printers) or printing to file is allowed. The group that can only print to file likely has stricter rules that block all physical printing, allowing only virtual print-to-file operations.
* Why not the other options?
* A. They may be attached to the default extensions policy and profile: The default extensions policy typically does not include specific restrictions on printing, focusing instead on general agent behavior (e.g., device control or exploit protection). Printing issues are more likely tied to firewall or device control profiles.
* C. They may have different disk encryption profiles that are not allowing print jobs on encrypted files: Cortex XDR does not manage disk encryption profiles, and disk encryption (e.
g., BitLocker) does not typically block printing based on file encryption status. This is not a relevant cause.
* D. They may be on different device extensions profiles set to block different print jobs:
While device control profiles can block USB printers, they do not typically control network printing or distinguish between print-to-file and physical printing. Network printing restrictions are more likely enforced by host firewall rules.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains host firewall capabilities: "Host firewall profiles can block outbound traffic to network-attached printers, restricting printing for remote employees to prevent unauthorized data transfers" (paraphrased from the Host-Based Firewall section). TheEDU-260: Cortex XDR Prevention and Deploymentcourse covers firewall configurations, stating that "firewall rules can block network printing while allowing local or virtual printing, often causing printing issues for remote users" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes
"Cortex XDR agent configuration" as a key exam topic, encompassing host firewall settings.
References:
Palo Alto Networks Cortex XDR Documentation Portal:https://docs-cortex.paloaltonetworks.com/ EDU-260: Cortex XDR Prevention and Deployment Course Objectives Palo Alto Networks Certified XDR Engineer
Datasheet:https://www.paloaltonetworks.com/services/education
/certification#xdr-engineer

**NEW QUESTION # 21**
Which XQL query can be saved as a behavioral indicator of compromise (BIOC) rule, then converted to a custom prevention rule?

- A. dataset = xdr_data
  | filter event_type = ENUM.DEVICE and action_process_image_name = "**"
  and action_process_image_command_line = "-e cmd*"
  and action_process_image_command_line != "*cmd.exe -a /c*"
- B. dataset = xdr_data
  | filter event_type = ENUM.PROCESS and event_type = ENUM.DEVICE and
  action_process_image_name = "**"
  and action_process_image_command_line = "-e cmd*"
  and action_process_image_command_line != "*cmd.exe -a /c*"
- C. dataset = xdr_data
  | filter event_type = FILE and (event_sub_type = FILE_CREATE_NEW or event_sub_type = FILE_WRITE or event_sub_type = FILE_REMOVE or event_sub_type = FILE_RENAME) and agent_hostname = "hostname"
  | filter lowercase(action_file_path) in ("/etc/*", "/usr/local/share/*", "/usr/share/*") and action_file_extension in ("conf", "txt")
  | fields action_file_name, action_file_path, action_file_type, agent_ip_addresses, agent_hostname, action_file_path
- D. dataset = xdr_data
  | filter event_type = ENUM.PROCESS and action_process_image_name = "**" and action_process_image_command_line = "-e cmd*" and action_process_image_command_line != "*cmd.exe -a /c*"

**Answer: D**

Explanation:
In Cortex XDR, aBehavioral Indicator of Compromise (BIOC)rule defines a specific pattern of endpoint behavior (e.g., process execution, file operations, or network activity) that can trigger an alert. BIOCs are often created usingXQL (XDR Query Language)queries, which are then saved as BIOC rules to monitor for the specified behavior. To convert a BIOC into acustom prevention rule, the BIOC must be associated with a Restriction profile, which allows the defined behavior to be blocked rather than just detected. For a query to be suitable as a BIOC and convertible to a prevention rule, it must meet the following criteria:
* It must monitor a behavior that Cortex XDR can detect on an endpoint, such as process execution, file operations, or device

events.
* The behavior must be actionable for prevention (e.g., blocking a process or file operation), typically involving events like process launches (ENUM.PROCESS) or file modifications (ENUM.FILE).
* The query should not include overly complex logic (e.g., multiple event types with conflicting conditions) that cannot be translated into a BIOC rule.
Let's analyze each query to determine which one meets these criteria:
* Option A: dataset = xdr_data | filter event_type = ENUM.DEVICE ...This query filters for event_type = ENUM.DEVICE, which relates to device-related events (e.g., USB device connections).
While device events can be monitored, the additional conditions (action_process_image_name = "**" and action_process_image_command_line) are process-related attributes, which are typically associated with ENUM.PROCESS events, not ENUM.DEVICE. This mismatch makes the query invalid for a BIOC, as it combines incompatible event types and attributes. Additionally, device events are not typically used for custom prevention rules, as prevention rules focus on blocking processes or fileoperations, not device activities.
* Option B: dataset = xdr_data | filter event_type = ENUM.PROCESS and event_type = ENUM.
DEVICE ...This query attempts to filter for events that are both ENUM.PROCESS and ENUM.
DEVICE (event_type = ENUM.PROCESS and event_type = ENUM.DEVICE), which is logically incorrect because an event cannot have two different event types simultaneously. In XQL, the event_type field must match a single type (e.g., ENUM.PROCESS or ENUM.DEVICE), and combining them with an and operator results in no matches. This makes the query invalid for creating a BIOC rule, as it will not return any results and cannot be used for detection or prevention.
* Option C: dataset = xdr_data | filter event_type = FILE ...This query monitors file-related events (event_type = FILE) with specific sub-types (FILE_CREATE_NEW, FILE_WRITE, FILE_REMOVE, FILE_RENAME) on a specific hostname, targeting file paths (/etc/*, /usr/local/share/*, /usr/share/*) and extensions (conf, txt). While this query can be saved as a BIOC to detect file operations, it is not ideal for conversion to a custom prevention rule. Cortex XDR prevention rules typically focus on blocking process executions (via Restriction profiles), not file operations. While file-based BIOCs can generate alerts, converting them to prevention rules is less common, as Cortex XDR's prevention mechanisms are primarily process-oriented (e.g., terminating a process), not file-oriented (e.g., blocking a file write). Additionally, the query includes complex logic (e.g., multiple sub-types, lowercase() function, fields clause), which may not fully translate to a prevention rule.
* Option D: dataset = xdr_data | filter event_type = ENUM.PROCESS ...This query monitors process execution events (event_type = ENUM.PROCESS) where the process image name matches a pattern (action_process_image_name = "**"), the command line includes -e cmd*, and excludes commands matching *cmd.exe -a /c*. This query is well-suited for a BIOC rule, as it defines a specific process behavior (e.g., a process executing with certain command-line arguments) that Cortex XDR can detect on an endpoint. Additionally, this type of BIOC can be converted to a custom prevention rule by associating it with aRestriction profile, which can block the process execution if the conditions are met. For example, the BIOC can be configured to detect processes with action_process_image_name =
"**" and action_process_image_command_line = "-e cmd*", and a Restriction profile can terminate such processes to prevent the behavior.
Correct Answer Analysis (D):
Option D is the correct choice because it defines a process-based behavior (ENUM.PROCESS) that can be saved as a BIOC rule to detect the specified activity (processes with certain command-line arguments). It can then be converted to a custom prevention rule by adding it to a Restriction profile, which will block the process execution when the conditions are met. The query's conditions are straightforward and compatible with Cortex XDR's BIOC and prevention framework, making it the best fit for the requirement.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains BIOC and prevention rules: "XQL queries monitoring process events (ENUM.PROCESS) can be saved as BIOC rules to detect specific behaviors, and these BIOCs can be added to a Restriction profile to create custom prevention rules that block the behavior" (paraphrased from the BIOC and Restriction Profile sections).
TheEDU-260: Cortex XDR Prevention and Deployment course covers BIOC creation, stating that "process-based XQL queries are ideal for BIOCs and can be converted to prevention rules via Restriction profiles to block executions" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "detection engineering" as a key exam topic, encompassing BIOC rule creation and conversion to prevention rules.
References:
Palo Alto Networks Cortex XDR Documentation Portal:https://docs-cortex.paloaltonetworks.com/ EDU-260: Cortex XDR Prevention and Deployment Course Objectives Palo Alto Networks Certified XDR Engineer
Datasheet:https://www.paloaltonetworks.com/services/education
/certification#xdr-engineer

**NEW QUESTION # 22**
Based on the Malware profile image below, what happens when a new custom-developed application attempts to execute on an endpoint?


- A. It will not execute
- B. It will immediately execute
- C. It will execute after one hour
- D. It will execute after the second attempt

**Answer: A**

Explanation:
Since no image was provided, I assume the Malware profile is configured with default Cortex XDR settings, which typically enforce strict malware prevention for unknown or untrusted executables. In Cortex XDR, the Malware profilewithin the security policy determines how executables are handled on endpoints. For anew custom-developed application(an unknown executable not previously analyzed or allow-listed), the default behavior is toblock executionuntil the file is analyzed byWildFire(Palo Alto Networks' cloud-based threat analysis service) or explicitly allowed via policy.
* Correct Answer Analysis (B):By default, Cortex XDR's Malware profile is configured toblock unknown executables, including new custom-developed applications, to prevent potential threats. When the application attempts ilustrator execute, the Cortex XDR agent intercepts it, sends it to WildFire for analysis (if not excluded), and blocks execution until a verdict is received. If the application is not on an allow list or excluded, itwill not executeimmediately, aligning with option B.
* Why not the other options?
* A. It will immediately execute: This would only occur if the application is on an allow list or if the Malware profile is configured to allow unknown executables, which is not typical for default settings.
* C. It will execute after one hour: There is no default setting in Cortex XDR that delays execution for one hour. Execution depends on the WildFire verdict or policy configuration, not a fixed time delay.
* D. It will execute after the second attempt: Cortex XDR does not have a mechanism that allows execution after a second attempt. Execution is either blocked or allowed based on policy and analysis results.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains Malware profile behavior: "By default, unknown executables are blocked until a WildFire verdict is received, ensuring protection against new or custom- developed applications" (paraphrased from the Malware Profile Configuration section). TheEDU-260:
Cortex XDR Prevention and Deploymentcourse covers Malware profiles, stating that "default settings block unknown executables to prevent potential threats until analyzed" (paraphrased from course materials).
ThePalo Alto Networks Certified XDR Engineer datasheetincludes "Cortex XDR agent configuration" as a key exam topic, encompassing Malware profile settings.
References:
Palo Alto Networks Cortex XDR Documentation Portal:https://docs-cortex.paloaltonetworks.com/ EDU-260: Cortex XDR Prevention and Deployment Course Objectives Palo Alto Networks Certified XDR Engineer

Datasheet:https://www.paloaltonetworks.com/services/education
/certification#xdr-engineer
Note on Image: Since the image was not provided, I assumed a default Malware profile configuration. If you can share the image or describe its settings (e.g., specific allow lists, exclusions, or block rules), I can refine the answer to match the exact configuration.

**NEW QUESTION # 23**
During deployment of Cortex XDR for Linux Agents, the security engineering team is asked to implement memory monitoring for agent health monitoring. Which agent service should be monitored to fulfill this request?

- A. clad
- B. pyxd
- C. dypdng
- D. pmd

**Answer: D**

Explanation:
Cortex XDR agents on Linux consist of several services that handle different aspects of agent functionality, such as event collection, policy enforcement, and health monitoring.Memory monitoringfor agent health involves tracking the memory usage of the agent's core processes to ensure they are operating within acceptable limits, which is critical for maintaining agent stability and performance. Thepmd(Process Monitoring Daemon) service is responsible for monitoring the agent's health, including memory usage, on Linux systems.
* Correct Answer Analysis (D):Thepmdservice should be monitored to fulfill the request for memory monitoring. The Process Monitoring Daemon tracks the Cortex XDR agent's resource usage, including memory consumption, and reports health metrics to the console. Monitoring this service ensures the agent remains healthy and can detect issues like memory leaks or excessive resource usage.
* Why not the other options?
* A. dypdng: This is not a valid Cortex XDR service on Linux. It appears to be a typo or a misnamed service.
* B. clad: The clad service (Cortex Linux Agent Daemon) is responsible for core agent operations, such as communication with the Cortex XDR tenant, but it is not specifically focused on memory monitoring for health purposes.
* C. pyxd: The pyxd service handles Python-based components of the agent, such asscript execution for certain detections, but it is not responsible for memory monitoring or agent health.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains Linux agent services: "The pmd (Process Monitoring Daemon) service on Linux monitors agent health, including memory usage, to ensure stable operation" (paraphrased from the Linux Agent Deployment section). TheEDU-260: Cortex XDR Prevention and Deploymentcourse covers Linux agent setup, stating that "pmd is the service to monitor for agent health, including memory usage, on Linux systems" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "planning and installation" as a key exam topic, encompassing Linux agent deployment and monitoring.
References:
Palo Alto Networks Cortex XDR Documentation Portal:https://docs-cortex.paloaltonetworks.com/ EDU-260: Cortex XDR Prevention and Deployment Course Objectives Palo Alto Networks Certified XDR Engineer
Datasheet:https://www.paloaltonetworks.com/services/education
/certification#xdr-engineer

**NEW QUESTION # 24**
.....

All smart devices are suitable to use Palo Alto Networks XDR Engineer pdf dumps of PassReview. Therefore, you can open this Palo Alto Networks XDR Engineer real dumps document and study for the Palo Alto Networks XDR-Engineer test at any time from your comfort zone. These Palo Alto Networks XDR-Engineer are updated, and PassReview regularly amends the content as per new changes in the Palo Alto Networks XDR-Engineer real certification test.

**XDR-Engineer Valid Test Guide**: https://www.passreview.com/XDR-Engineer_exam-braindumps.html

As a brand now, many companies strive to get our XDR-Engineer practice materials to help their staffs achieve more certifications for our quality and accuracy, PassReview designed Palo Alto Networks XDR Engineer exam preparation material in Palo Alto Networks XDR-Engineer PDF and practice test (online and offline), The best way for candidates to know our Palo Alto Networks XDR-Engineer training dumps is downloading our free demo, Palo Alto Networks XDR-Engineer Reliable Exam Voucher We also

welcome the suggestions from our customers, as long as our clients propose rationally.

It's a straightforward operation, so I expected this to be more automatic, XDR-Engineer While reviewing the security logs for your server, you notice that a user on the Internet has attempted to access your internal mail server.

## Valid Palo Alto Networks - XDR-Engineer Reliable Exam Voucher

As a brand now, many companies strive to get our XDR-Engineer practice materials to help their staffs achieve more certifications for our quality and accuracy, PassReview designed Palo Alto Networks XDR Engineer exam preparation material in Palo Alto Networks XDR-Engineer PDF and practice test (online and offline).

The best way for candidates to know our Palo Alto Networks XDR-Engineer training dumps is downloading our free demo, We also welcome the suggestions from our customers, as long as our clients propose rationally.

By and large, the majority of the customers who have passed the exam after buying our XDR-Engineer : Palo Alto Networks XDR Engineer valid test questions will at the same time gain many benefits accompanied by high scores.

- Free PDF 2026 Palo Alto Networks Pass-Sure XDR-Engineer: Palo Alto Networks XDR Engineer Reliable Exam Voucher □ Easily obtain free download of [ XDR-Engineer ] by searching on ➥ www.pass4test.com □ □Latest XDR-Engineer Study Materials
- XDR-Engineer Training Materials - XDR-Engineer Exam Torrent - XDR-Engineer Study Guide □ Open 《 www.pdfvce.com 》 enter ✔ XDR-Engineer □✔□ and obtain a free download □XDR-Engineer Reliable Exam Preparation
- XDR-Engineer Reliable Exam Voucher | 100% Pass | Real Questions □ Search on □ www.torrentvce.com □ for " XDR-Engineer " to obtain exam materials for free download □XDR-Engineer Reliable Real Test
- XDR-Engineer Reliable Exam Question □ XDR-Engineer Latest Braindumps Ppt □ Valid XDR-Engineer Exam Voucher □ Download ▸ XDR-Engineer ◂ for free by simply entering ☀ www.pdfvce.com □☀□ website □Exam XDR-Engineer Tutorial
- XDR-Engineer test braindump, Palo Alto Networks XDR-Engineer test exam, XDR-Engineer real braindump □ The page for free download of ▸ XDR-Engineer ◂ on 「 www.practicevce.com 」 will open immediately □Exam XDR-Engineer Vce
- Three formats of the Palo Alto Networks XDR-Engineer Exam Dumps □ Download " XDR-Engineer " for free by simply entering ▹ www.pdfvce.com ◃ website □Latest XDR-Engineer Real Test
- XDR-Engineer Reliable Exam Voucher Fantastic Questions Pool Only at www.practicevce.com 👆 Search on ➥ www.practicevce.com □ for ⇛ XDR-Engineer ⇚ to obtain exam materials for free download □XDR-Engineer Latest Exam Fee
- XDR-Engineer Latest Exam Simulator □ Exam XDR-Engineer Vce □ XDR-Engineer Reliable Exam Question □ Simply search for ➽ XDR-Engineer □ for free download on ✔ www.pdfvce.com □✔□ □XDR-Engineer Study Guide Pdf
- XDR-Engineer Latest Braindumps Ppt □ Exam XDR-Engineer Vce ↴ XDR-Engineer Latest Exam Fee ❤ Immediately open ✔ www.prep4sures.top □✔□ and search for 【 XDR-Engineer 】 to obtain a free download □Exam XDR-Engineer Tutorial
- XDR-Engineer Reliable Exam Voucher | 100% Pass | Real Questions □ Search for （ XDR-Engineer ） on ✔ www.pdfvce.com □✔□ immediately to obtain a free download □XDR-Engineer Reliable Exam Question
- Exam XDR-Engineer Tutorial □ XDR-Engineer Study Guide Pdf □ XDR-Engineer Latest Exam Fee □ Search for ▹ XDR-Engineer ◃ and download exam materials for free through □ www.examcollectionpass.com □ □XDR-Engineer Reliable Test Test
- 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.campfirewriting.com, www.stes.tyc.edu.tw, whatoplay.com, pinoyseo.ph, www.dssmymdiv.com, 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, www.skudci.com, shortcourses.russellcollege.edu.au, Disposable vapes

BTW, DOWNLOAD part of PassReview XDR-Engineer dumps from Cloud Storage: https://drive.google.com/open?id=1L-EGSU0gpoTDoqopfu4SHU2jROLK35l-