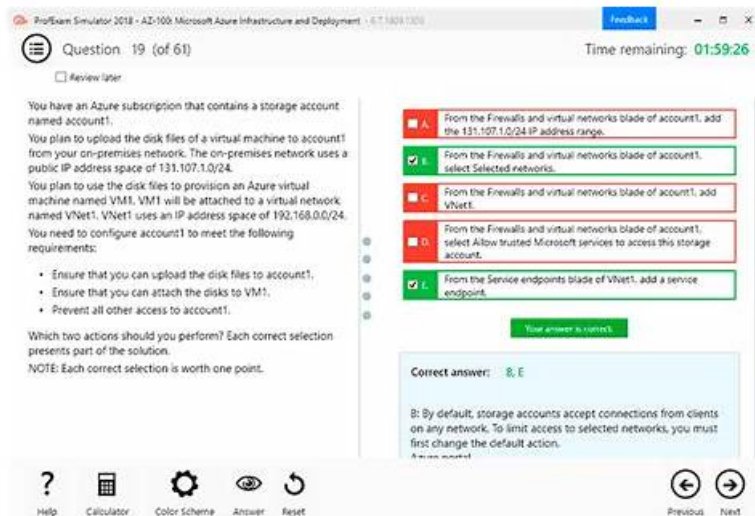


NSE5_FSM-6.3 Free Download & Certificate

NSE5_FSM-6.3 Exam



P.S. Free 2026 Fortinet NSE5_FSM-6.3 dumps are available on Google Drive shared by Prep4sures:
<https://drive.google.com/open?id=1kP-DTFh0-heuLt853EW58pPUniTct9gg>

Our Fortinet NSE5_FSM-6.3 practice exam simulator mirrors the Fortinet NSE5_FSM-6.3 exam experience, so you know what to anticipate on Fortinet NSE 5 - FortiSIEM 6.3 day. Our Fortinet NSE5_FSM-6.3 practice test software features various question styles and levels, so you can customize your Fortinet NSE5_FSM-6.3 Exam Questions preparation to meet your needs.

Fortinet NSE5_FSM-6.3 Exam is intended for security professionals who have experience with FortiSIEM 6.3 and want to validate their skills and knowledge. NSE5_FSM-6.3 exam covers a wide range of topics, including FortiSIEM architecture, deployment, configuration, and management. Candidates must have a solid understanding of network security, threat detection, and incident response to pass the exam.

>> NSE5_FSM-6.3 Free Download <<

Latest Fortinet NSE 5 - FortiSIEM 6.3 exam pdf & NSE5_FSM-6.3 exam torrent

You can free download part of Prep4sures's practice questions and answers about Fortinet Certification NSE5_FSM-6.3 Exam online. Once you decide to select Prep4sures, Prep4sures will make every effort to help you pass the exam. If you find that our exam practice questions and answers is very different from the actual exam questions and answers and can not help you pass the exam, we will immediately 100% full refund.

Fortinet NSE5_FSM-6.3 Exam is intended for security professionals who have experience in network security and Fortinet products. NSE5_FSM-6.3 exam tests the candidate's knowledge and skills in deploying and managing FortiSIEM 6.3 in complex network environments. Fortinet NSE 5 - FortiSIEM 6.3 certification is ideal for professionals who are responsible for managing large networks, analyzing security data, and responding to security incidents.

Fortinet NSE 5 - FortiSIEM 6.3 Sample Questions (Q41-Q46):

NEW QUESTION # 41

When configuring collectors located in geographically separated sites, what ports must be open on a front end firewall?

- A. HTTPS, from the collector to the supervisor and worker upload settings addresses
- B. HTTPS, from the Internet to the collector and from the collector to the FortiSIEM cluster
- C. HTTPS, from the Internet to the collector
- D. HTTPS, from the collector to the worker upload settings address only

Answer: A

Explanation:

FortiSIEM Architecture: In FortiSIEM, collectors gather data from various sources and send this data to supervisors and workers within the FortiSIEM architecture.

Communication Requirements: For collectors to effectively send data to the FortiSIEM system, specific communication channels must be open.

Port Usage: The primary port used for secure communication between the collectors and the FortiSIEM infrastructure is HTTPS (port 443).

Network Configuration: When configuring collectors in geographically separated sites, the HTTPS port must be open for the collectors to communicate with both the supervisor and the worker upload settings addresses. This ensures that the collected data can be securely transmitted to the appropriate processing and analysis components.

References: FortiSIEM 6.3 Administration Guide, Network Ports section details the necessary ports for communication within the FortiSIEM architecture.

NEW QUESTION # 42

An administrator is using SNMP and WMI credentials to discover a Windows device. How will the WMI method handle this?

- A. WMI method will collect security, application, and system events logs.
- **B. WMI method will collect only traffic and IIS logs.**
- C. WMI method will collect only DNS logs.
- D. WMI method will collect only DHCP logs.

Answer: B

Explanation:

* WMI Method: Windows Management Instrumentation (WMI) is a set of specifications from Microsoft for consolidating the management of devices and applications in a network.

* Log Collection: WMI is used to collect various types of logs from Windows devices.

Security Logs: Contains records of security-related events such as login attempts and resource access.

Application Logs: Contains logs generated by applications running on the system.

System Logs: Contains logs related to the operating system and its components.

* Comprehensive Data Collection: By using WMI, FortiSIEM can gather a wide range of event logs that are crucial for monitoring and analyzing the security and performance of Windows devices.

* Reference: FortiSIEM 6.3 User Guide, Data Collection Methods section, which details the use of WMI for collecting event logs from Windows devices.

NEW QUESTION # 43

Where must you configure rule notifications and automated remediation on FortiSIEM?

- A. Notification engine
- B. Notification policy
- **C. Response policies**
- D. Email and scripting alerts

Answer: C

NEW QUESTION # 44

If FortiSIEM supervisor is deployed with the worker using the proprietary flat file database, which action is required?

- **A. An event database must be placed on NFS**
- B. A FortiSIEM service provider license must be obtained
- C. A separate network interface must be used for the storage network
- D. Collectors must be deployed

Answer: A

What operating system is FortiSIEM based on?

- Answer: C**

• • • • •

[illegible]

What's more, part of that Prep4sures NSE5_FSM-6.3 dumps now are free: <https://drive.google.com/open?id=1kP-DTFh0-heuLt853EW58pUniTct9gg>