

NSE5_FSM-6.3 Dumps

Fortinet NSE 5 - FortiSIEM 6.3

https://www.certleader.com/NSE5_FSM-6.3-dumps.html



NEW QUESTION 1

Refer to the exhibit.

Display Fields

Saved Displays...Clear All

Attributes	Order	Display As	Row	Move		
Event Receive Time	▼		+	-	↑	↓
Reporting IP	▼		+	-	↑	↓
Event Type	▼		+	-	↑	↓
Raw Event Log	▼		+	-	↑	↓
COUNT (Matched Events)	▼		+	-	↑	↓

Apply & RunApplyCancel

A FortiSIEM administrator wants to group some attributes for a report, but is not able to do so successfully. As shown in the exhibit, why are some of the fields highlighted in red?

- A. Unique attributes cannot be grouped.
- B. The Event Receive Time attribute is not available for logs.
- C. The attribute COUNT(Matched events) is an invalid expression.
- D. No RAW Event Log attribute is available for devices.

Answer: A

Explanation:

The red highlighting in the exhibit indicates attributes that cannot be grouped together due to their unique nature. These unique attributes include Event Receive Time, Reporting IP, Event Type, Raw Event Log, and COUNT(Matched Events).

Attribute Characteristics:

- Event Receive Time is unique for each event.
- Reporting IP and Event Type can vary greatly, making grouping them impractical in this context.
- Raw Event Log represents the unprocessed log data, which is also unique.
- COUNT(Matched Events) is a calculated field, not suitable for grouping.

References: FortiSIEM 6.3 User Guide, Reporting section, explains the constraints on grouping attributes in reports.

NEW QUESTION 2

Which FortiSIEM components are capable of performing device discovery?

- A. FortiSIEM Windows agent
- B. Worker
- C. FortiSIEM Linux agent
- D. Collector

Answer: D

Explanation:

Explanation

Device Discovery in FortiSIEM: Device discovery is the process by which FortiSIEM identifies and adds devices to its management scope.

Role of Collectors: Collectors are responsible for gathering data from network devices, including discovering new devices in the network.

- Functionality: Collectors use protocols such as SNMP, WMI, and others to discover devices and gather their details.

Capability: While agents (Windows and Linux) primarily gather data from their host systems, the collectors actively discover devices across the network.

References: FortiSIEM 6.3 User Guide, Device Discovery section, which details the role of collectors in discovering network devices.

NEW QUESTION 3

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 only traffic and IIS logs.
- B. WMI method will collect only DNS logs.
- C. WMI method will collect only DHCP logs.

D. WMI method will collect security, application, and system events logs.

Answer: D

Explanation:

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.

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

NEW QUESTION 4

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

Answer: B

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 5

Refer to the exhibit.

Which section contains the sortings that determine how many incidents are created?

- A. Actions
- B. Group By
- C. Aggregate
- D. Filters

Answer: B

Explanation:

Incident Creation in FortiSIEM: Incidents in FortiSIEM are created based on specific patterns and conditions defined within the system.

Group By Function: The "Group By" section in the "Edit SubPattern" window specifies how the data should be grouped for analysis and incident creation.

Impact of Grouping: The way data is grouped affects the number of incidents generated.

Each unique combination of the grouped attributes results in a separate incident.

Exhibit Analysis: In the provided exhibit, the "Group By" section lists "Reporting Device," "Reporting IP," and "User." This means incidents will be created for each unique combination of these attributes. References: FortiSIEM 6.3 User Guide, Rule and Pattern Creation section, which details how grouping impacts incident generation.

NEW QUESTION 6

Refer to the exhibit.

The screenshot shows the 'Access Method Definition' configuration window in FortiSIEM. The 'Name' field is 'FSM_LAB_AD'. The 'Device Type' is 'Microsoft Windows Server 2016'. The 'Access Protocol' is 'LDAP'. The 'Used For' list is expanded, showing 'LDAP', 'LDAPS', 'LDAP Start TLS', 'WMI', 'SSH', and 'TELNET'. 'TELNET' is selected. The 'Server Port' field is empty. The 'Base DN' field is empty. The 'Password config' is 'Manual'. The 'User Name', 'Password', and 'Confirm Password' fields are empty. The 'Description' field is empty.

A FortiSIEM administrator wants to collect both SIEM event logs and performance and availability metrics (PAM) events from a Microsoft Windows server. Which protocol should the administrator select in the Access Protocol drop-down list so that FortiSIEM will collect both SIEM and PAM events?

- A. TELNET
- B. WMI
- C. LDAPS
- D. LDAP start TLS

Answer: B

Explanation:

Collecting SIEM and PAM Events: To collect both SIEM event logs and Performance and Availability Monitoring (PAM) events from a Microsoft Windows server, a suitable protocol must be selected.

WMI Protocol: Windows Management Instrumentation (WMI) is the appropriate protocol for this task.

SIEM Event Logs: WMI can collect security, application, and system logs from Windows devices.

PAM Events: WMI can also gather performance metrics, such as CPU usage, memory utilization, and disk activity.

Comprehensive Data Collection: Using WMI ensures that both types of data are collected efficiently from the Windows server.

References: FortiSIEM 6.3 User Guide, Data Collection Methods section, which details the use of WMI for collecting various types of logs and performance metrics.

NEW QUESTION 7

Which three ports can be used to send Syslogs to FortiSIEM? (Choose three.)

Options:

- A. UDP9999
- B. UDP 162
- C. TCP 514
- D. UDP 514
- E. TCP 1470

Answer: CDE

Explanation:

Syslog Ports: Syslog messages can be sent over different ports using TCP or UDP protocols. Common Ports for Syslog:

UDP 514: This is the default port for sending syslog messages over UDP.

TCP 514: This is the default port for sending syslog messages over TCP, providing a more reliable transmission.

TCP 1470: This port is often used for secure or alternative syslog transmission.

Usage in FortiSIEM: FortiSIEM can be configured to receive syslog messages on these ports to ensure the logs are collected from various network devices.

References: FortiSIEM 6.3 User Guide, Syslog Integration section, which details the supported ports for syslog transmission.

NEW QUESTION 8

If an incident's status is Cleared, what does this mean?

- A. Two hours have passed since the incident occurred and the incident has not reoccurred.
- B. A clear condition set on a rule was satisfied.
- C. A security rule issue has been resolved.
- D. The incident was cleared by an operator.

Answer: B

Explanation:

Incident Status in FortiSIEM: The status of an incident indicates its current state and helps administrators track and manage incidents effectively.

Cleared Status: When an incident's status is 'Cleared,' it means that a specific condition set to clear the incident has been satisfied.

Clear Condition: This is typically a predefined condition that indicates the issue causing the incident has been resolved or no longer exists.

Automatic vs. Manual Clearance: While some incidents may be cleared automatically based on clear conditions, others might be manually cleared by an operator.

References: FortiSIEM 6.3 User Guide, Incident Management section, detailing the various incident statuses and the conditions that lead to an incident being marked as 'Cleared.'

NEW QUESTION 9

Consider the storage of anomaly baseline date that is calculated for different parameters.

Which database is used for storing this data?

- A. Event DB
- B. Profile DB
- C. SVN DB
- D. CMDB

Answer: B

Explanation:

Anomaly Baseline Data: Anomaly baseline data refers to the statistical profiles and baselines calculated for various parameters to detect deviations indicative of potential security incidents.

Profile DB: The Profile DB is specifically designed to store such baseline data in FortiSIEM.

Purpose: It maintains statistical profiles for different monitored parameters to facilitate anomaly detection.

Usage: This data is used by FortiSIEM to compare real-time metrics against the established baselines to identify anomalies.

References: FortiSIEM 6.3 User Guide, Database Architecture section, which describes the different databases used in FortiSIEM and their purposes, including the Profile DB for storing anomaly baseline data.

NEW QUESTION 10

In the advanced analytical rules engine in FortiSIEM, multiple subpatterns can be referenced using which three operation?(Choose three.)

- A. ELSE
- B. NOT
- C. FOLLOWED_BY
- D. OR
- E. AND

Answer: CDE

Explanation:

Advanced Analytical Rules Engine: FortiSIEM's rules engine allows for complex event correlation using multiple subpatterns.

Operations for Referencing Subpatterns:

FOLLOWED_BY: This operation is used to indicate that one event follows another within a specified time window.

OR: This logical operation allows for the inclusion of multiple subpatterns, where the rule triggers if any of the subpatterns match.

AND: This logical operation requires all referenced subpatterns to match for the rule to trigger.

Usage: These operations allow for detailed and precise event correlation, helping to detect complex patterns and incidents.

References: FortiSIEM 6.3 User Guide, Advanced Analytics Rules Engine section, which explains the use of different operations to reference subpatterns in rules.

NEW QUESTION 10

A FortiSIEM administrator wants to restrict a network administrator to running searches for only firewall devices. Under role management, which option does the FortiSIEM administrator need to configure to achieve this scenario?

- A. CMDB Report Conditions
- B. Data Conditions
- C. UI Access

Answer: B

NEW QUESTION 14

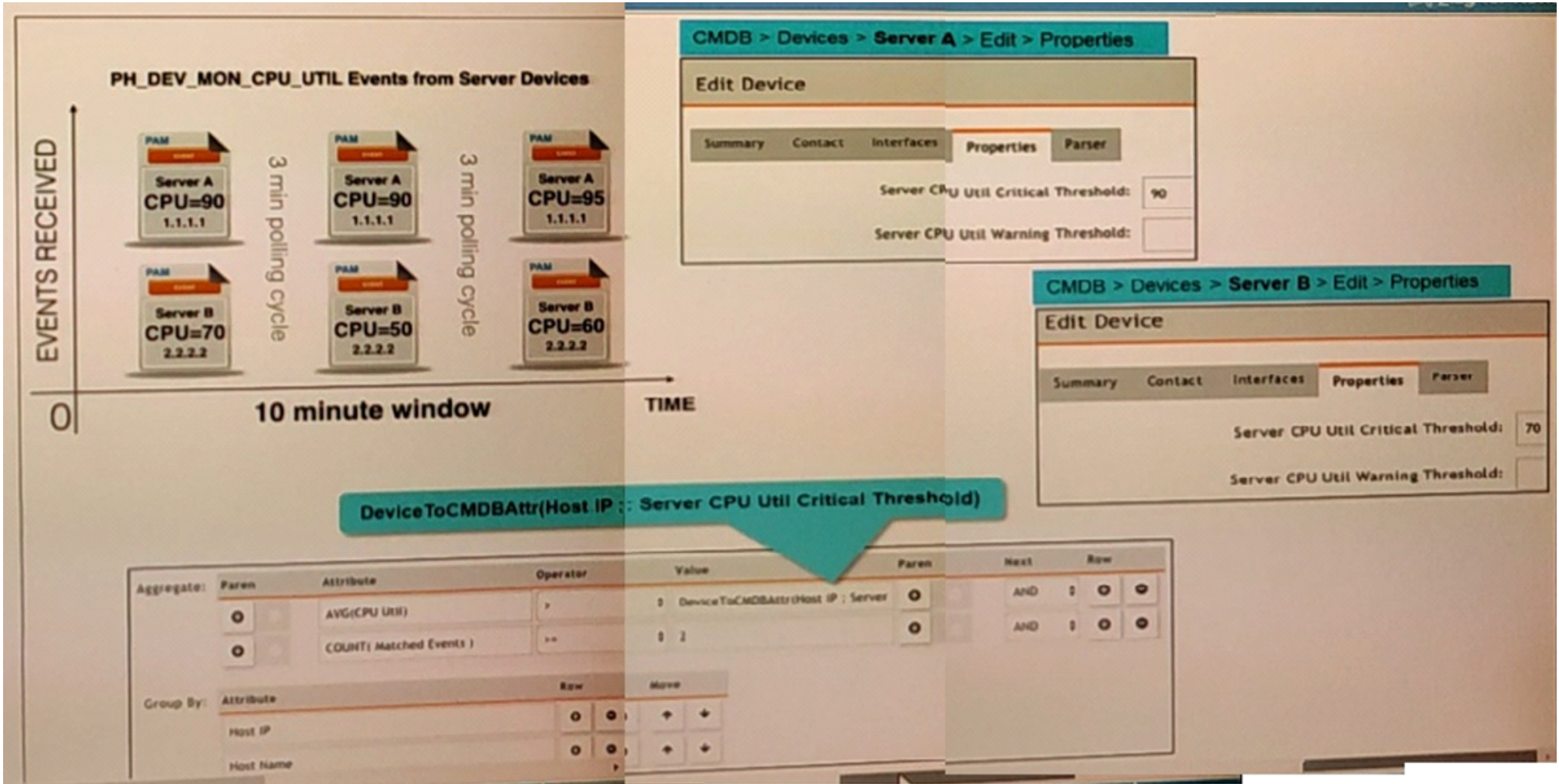
Which protocol is almost always required for the FortiSIEM GUI discovery process?

- A. SNMP
- B. WMI
- C. Syslog
- D. Telnet

Answer: A

NEW QUESTION 16

Refer to the exhibit.



Three events are collected over a 10-minute time period from two servers Server A and Server B. Based on the settings being used for the rule subpattern, how many incidents will the servers generate?

- A. Server A will not generate any incidents and Server B will not generate any incidents
- B. Server A will generate one incident and Server B will generate one incident
- C. Server A will generate one incident and Server B will not generate any incidents
- D. Server B will generate one incident and Server A will not generate any incidents

Answer: A

NEW QUESTION 18

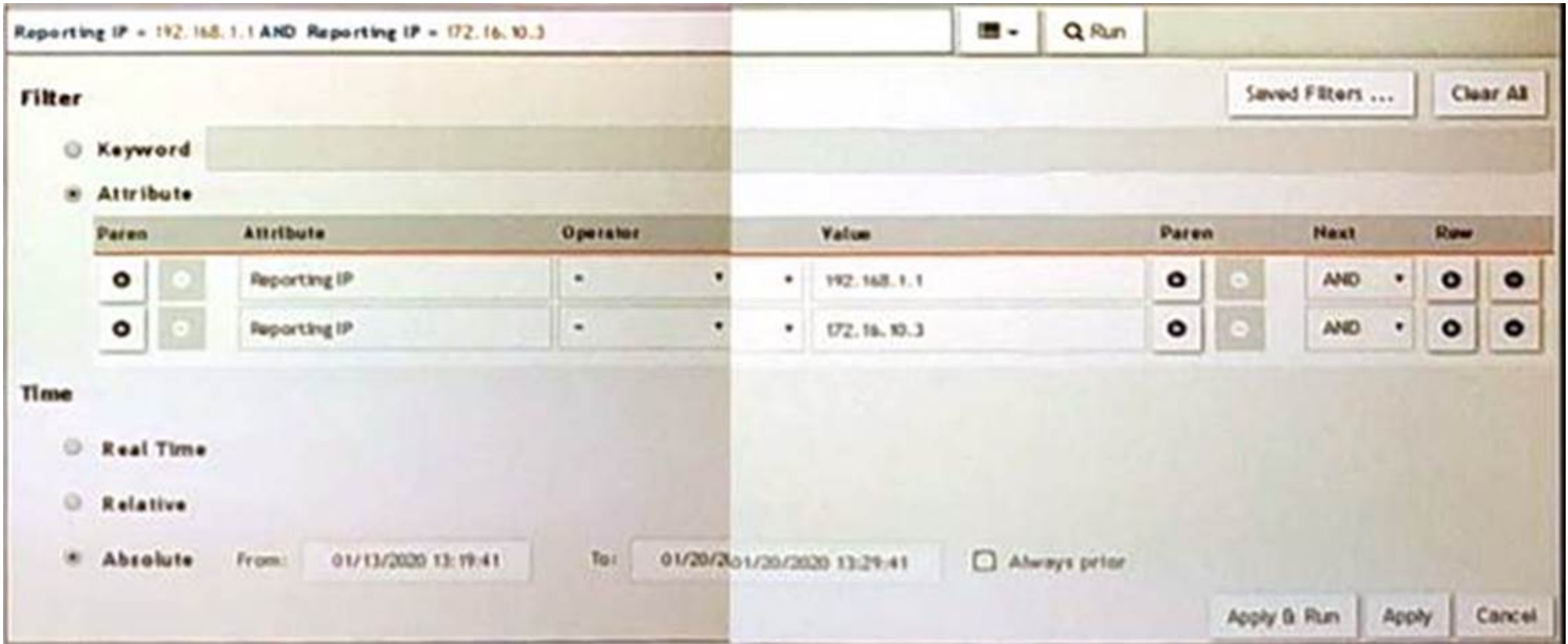
What is the best discovery scan option for a network environment where ping is disabled on all network devices?

- A. Smart scan
- B. Range scan
- C. CMDB scan
- D. L2 scan

Answer: A

NEW QUESTION 22

Refer to the exhibit.



The FortiSIEM administrator is examining events for two devices to investigate an issue. However, the administrator is not getting any results from their search. Based on the selected filters shown in the exhibit, why is the search returning no results?

- A. Parenthesis are missing

- B. The wrong boolean operator is selected in the Next column
- C. The wrong option is selected in the Operator column
- D. An invalid IP subnet is typed in the Value column

Answer: B

NEW QUESTION 27

If an incident's status is Cleared, what does this mean?

- A. Two hours have passed since the incident occurred and the incident has not reoccurred.
- B. A clear condition set on a rule was satisfied.
- C. A security rule issue has been resolved.
- D. The incident was cleared by an operator.

Answer: B

NEW QUESTION 31

What are the minimum memory requirements for the FortiSIEM supervisor virtual appliance, when the proprietary flat file database is used?

- A. 16GB RAM
- B. 32GB RAM
- C. 64GB RAM
- D. 24GB RAM

Answer: D

NEW QUESTION 33

A FortiSIEM supervisor at headquarters is struggling to keep up with an increase of EPS (Events Per Second) being reported across the enterprise. What components should an administrator consider deploying to assist the supervisor with processing data?

- A. Supervisor
- B. Worker
- C. Collector
- D. Agent

Answer: B

NEW QUESTION 34

Which item is required to register a FortiSIEM appliance license?

- A. Static storage
- B. Static MAC address
- C. Static IP address
- D. Static Hardware ID

Answer: D

NEW QUESTION 37

Device discovery information is stored in which database?

- A. CMDB
- B. Profile DB
- C. Event DB
- D. SVN DB

Answer: A

NEW QUESTION 40

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your NSE5_FSM-6.3 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE5_FSM-6.3-dumps.html