NSE5_FSM-5.2^Q&As

Fortinet NSE 5 - FortiSIEM 5.2

Pass Fortinet NSE5_FSM-5.2 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

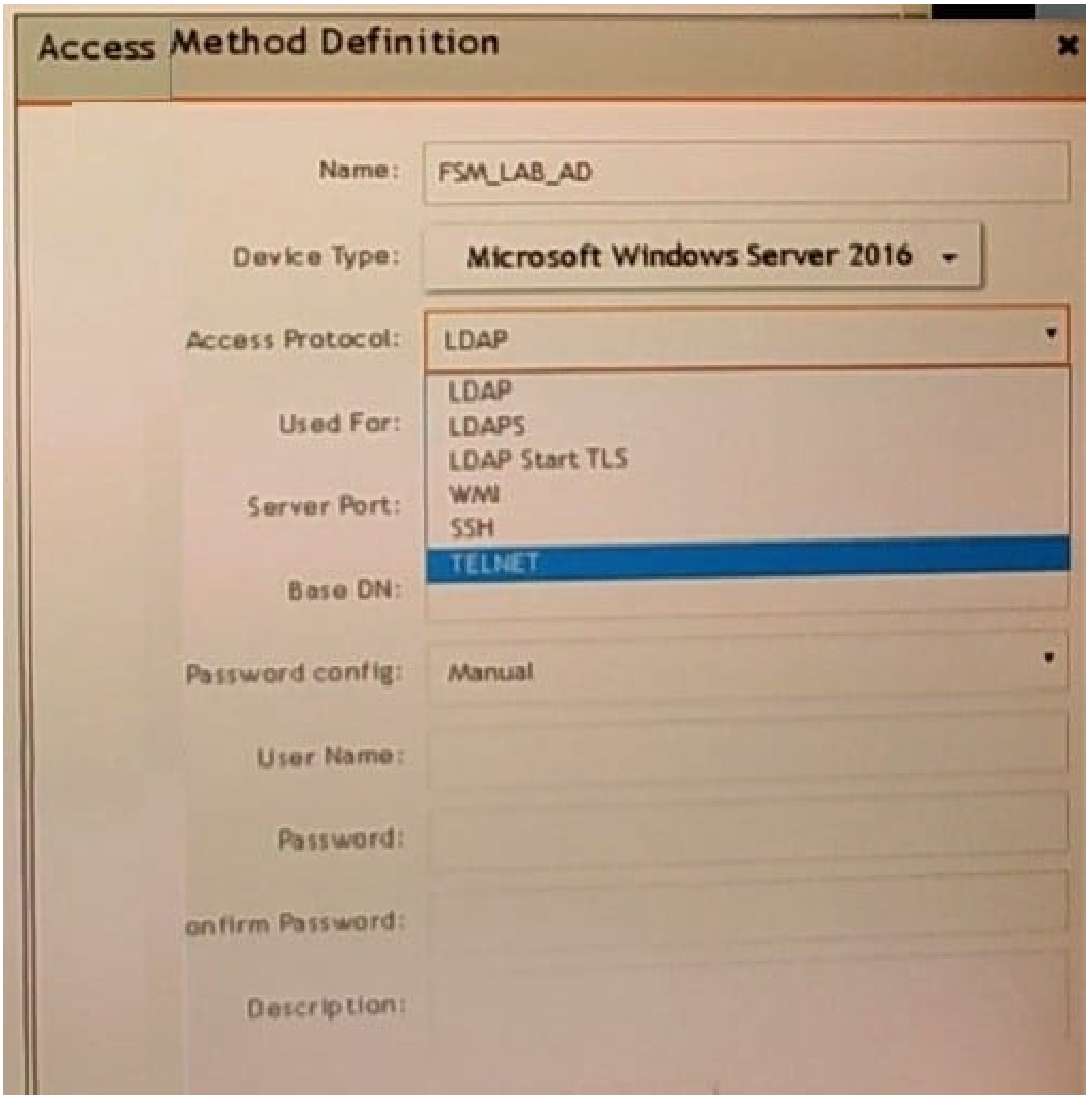
https://www.pass4itsure.com/nse5_fsm-5-2.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

QUESTION 1

Refer to the exhibit.



Access Method Definition

Name: FSM_LAB_AD

Device Type: Microsoft Windows Server 2016

Access Protocol: LDAP

Password config: Manual

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 AccessProtocol drop-down list so that FortiSIEM will collect both SIEM and PAM events?

A. TELNET

B. WMI

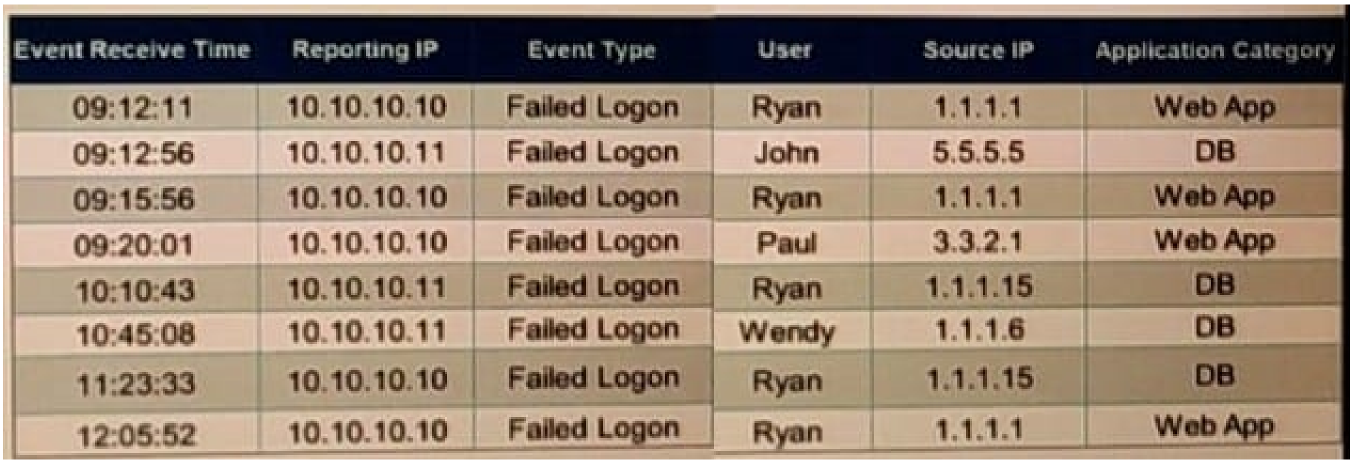
C. LDAPS

D. LDAP start TLS

Correct Answer: A

QUESTION 2

Refer to the exhibit.



Event Receive Time	Reporting IP	Event Type	User	Source IP	Application Category
09:12:11	10.10.10.10	Failed Logon	Ryan	1.1.1.1	Web App
09:12:56	10.10.10.11	Failed Logon	John	5.5.5.5	DB
09:15:56	10.10.10.10	Failed Logon	Ryan	1.1.1.1	Web App
09:20:01	10.10.10.10	Failed Logon	Paul	3.3.2.1	Web App
10:10:43	10.10.10.11	Failed Logon	Ryan	1.1.1.15	DB
10:45:08	10.10.10.11	Failed Logon	Wendy	1.1.1.6	DB
11:23:33	10.10.10.10	Failed Logon	Ryan	1.1.1.15	DB
12:05:52	10.10.10.10	Failed Logon	Ryan	1.1.1.1	Web App

If events are grouped by Reporting IP, Event Type, and user attributes in FortiSIEM, how ,many results will be displayed?

A. Seven results will be displayed.

B. There results will be displayed.

C. Unique attribute cannot be grouped.

D. Five results will be displayed.

Correct Answer: D

QUESTION 3

An administrator defines SMTP as a critical process on a Linux server. If the SMTP process is stopped, FortiSIEM would generate a critical event with which event type?

A. PH_DEV_MON_PROC_STOP

B. Postfix-Mail-Slop

C. Generic_SMTP_Process_Exit

D. PH_DEV_MON_SMTP_STOP

Correct Answer: D

QUESTION 4

What is a prerequisite for FortiSIEM Linux agent installation?

A. The web server must be installed on the Linux server being monitored

B. The auditd service must be installed on the Linux server being monitored

C. The Linux agent manager server must be installed.

D. Both the web server and the audit service must be installed on the Linux server being monitored

Correct Answer: D

QUESTION 5

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

Correct Answer: D