NSE5_FSM-5.2$^{\text{Q\&As}}$

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.passapply.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

What protocol can be used to collect Windows event logs in an agentless method?

A. SSH

B. SNMP

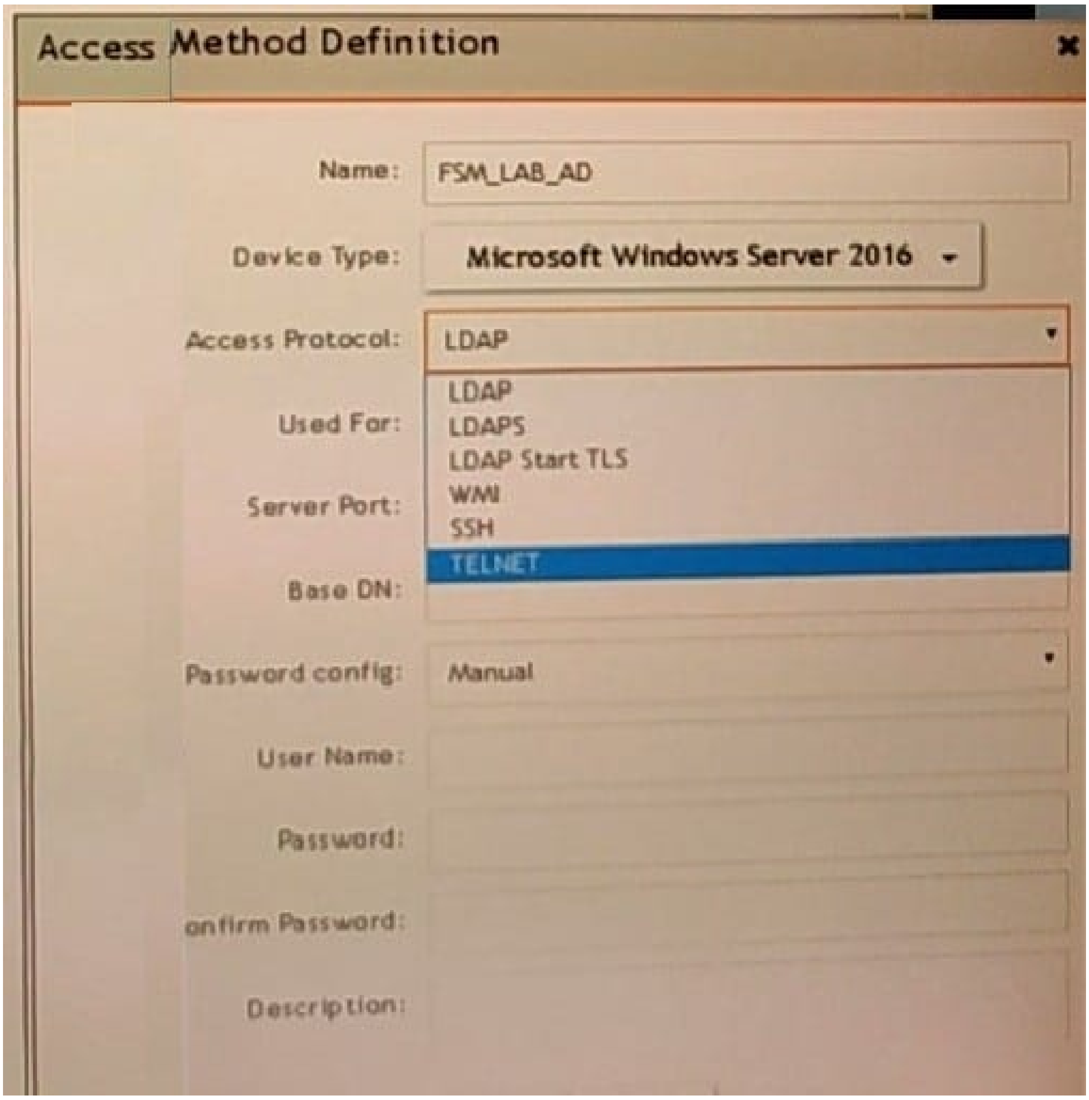
C. WMI

D. SMTP

Correct Answer: C

QUESTION 2

Refer to the exhibit.



Access Method Definition

Name: FSM_LAB_AD

Device Type: Microsoft Windows Server 2016

Access Protocol: LDAP

Used For:

Server Port:

Base DN:

Password config: Manual

User Name:

Password:

onfirm Password:

Description:

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

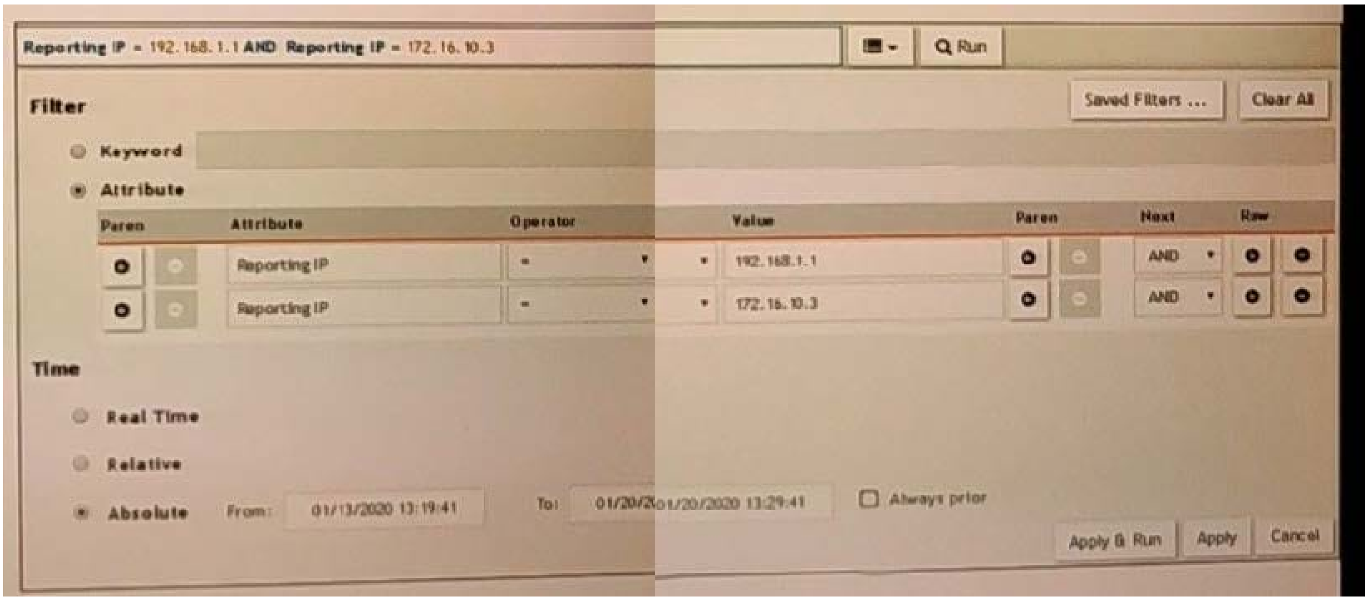
C. LDAPS

D. LDAP start TLS

Correct Answer: A

QUESTION 3

Refer to the exhibit.



Reporting IP = 192.168.1.1 AND Reporting IP = 172.16.10.3

Filter

○ Keyword

● Attribute

Paren	Attribute	Operator	Value	Paren	Next	Row
	Reporting IP	=	192.168.1.1		AND	
	Reporting IP	=	172.16.10.3		AND	

Time

○ Real Time

○ Relative

● Absolute From: 01/13/2020 13:19:41 To: 01/20/201/20/2020 13:29:41 □ Always prior

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 fillers 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

Correct Answer: D

QUESTION 4

If the reported packet loss is between 50% and 98%. which status is assigned to the device in the Availability column of summary dashboard?

A. Down status is assigned because of packet loss.

B. Up status is assigned because of received packets

C. Critical status is assigned because of reduction in number of packets received

D. Degraded status is assigned because of packet loss

Correct Answer: D

QUESTION 5

Which FortiSIEM components are capable of performing device discovery?

A. FortiSIEM Windows agent

B. Worker

C. FortiSIEM Linux agent

D. Collector

Correct Answer: D