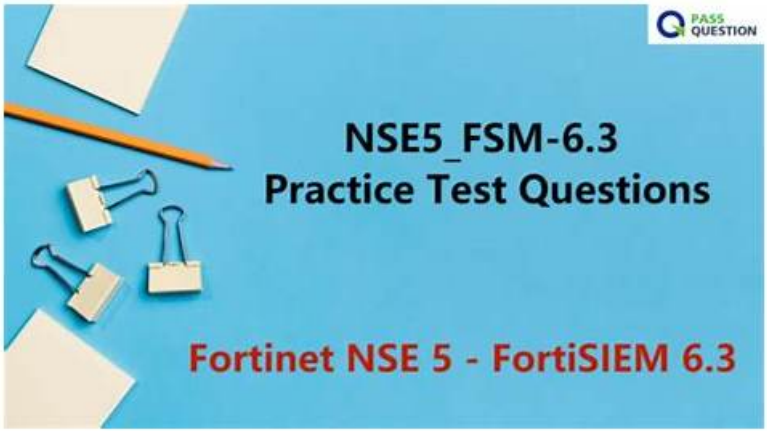
NSE5_FSM-6.3높은통과율인기시험자료 & NSE5_FSM-6.3시험대비공부자료



ExamPassdump NSE5_FSM-6.3 최신 PDF 버전 시험 문제집을 무료로 Google Drive에서 다운로드하세요: https://drive.google.com/open?id=1Lh6badmEXk3uFj_Org7q2CXGoCiLKvtL

Fortinet인증 NSE5_FSM-6.3시험취득 의향이 있는 분이 이 글을 보게 될것이라 믿고ExamPassdump에서 출시한 Fortinet인증 NSE5_FSM-6.3덤프를 강추합니다. ExamPassdump의Fortinet인증 NSE5_FSM-6.3덤프는 최강 적중율을 자랑하고 있어 시험패스율이 가장 높은 덤프자료로서 뜨거운 인기를 누리고 있습니다. IT인증시험을 패스하여 자격증을 취득하려는 분은ExamPassdump제품에 주목해주세요.

Fortinet NSE5_FSM-6.3 시험은 Fortinet FortiSIEM 6.3을 배포, 구성 및 관리하는 지식과 기술을 증명하고자 하는 IT 전문가를 대상으로한 인증 시험입니다. 이 인증 시험은 IT 산업에서 매우 존경받고 인정받는 Fortinet NSE 5 - FortiSIEM 6.3 인증 전문가가 되는 유일한 방법입니다.

>> NSE5_FSM-6.3높은 통과율 인기 시험자료 <<

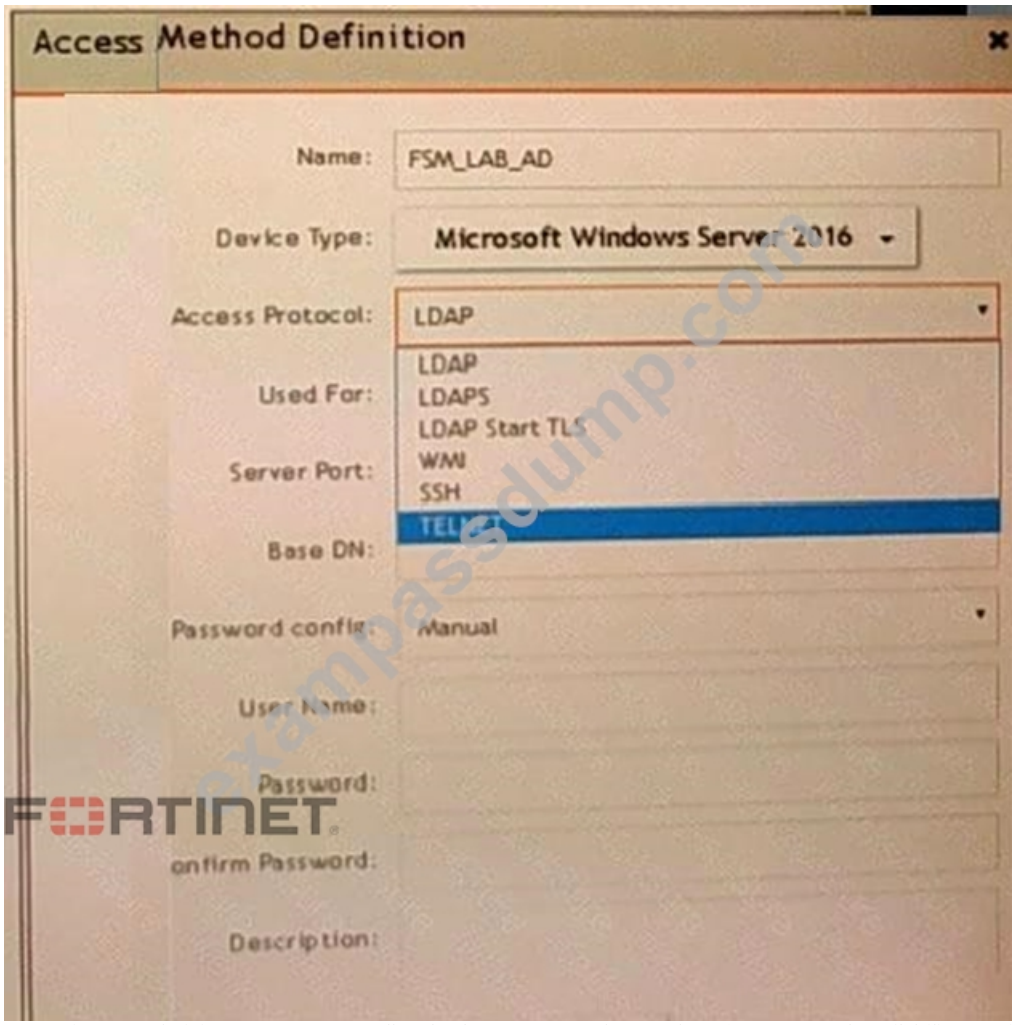
NSE5_FSM-6.3시험대비 공부자료 & NSE5_FSM-6.3 100% 시험패스 덤프자료

ExamPassdump는 여러분이Fortinet 인증NSE5_FSM-6.3인증시험 패스와 추후사업에 모두 도움이 되겠습니다. ExamPassdump제품을 선택함으로 여러분은 시간도 절약하고 돈도 절약하는 일석이조의 득을 얻을수 있습니다. 또한 구매후 일년무료 업데이트 버전을 받을수 있는 기회를 얻을수 있습니다. Fortinet 인증NSE5_FSM-6.3 인증시험패스는 아주 어렵습니다. 자기에 맞는 현명한 학습자료 선택은 성공의 지름길을 내딛는 첫발입니다. 퍼펙트한 자료만이 시험에서 성공할수 있습니다. ExamPassdump시험문제와 답이야 말로 퍼펙트한 자료이죠. ExamPassdump Fortinet 인증NSE5_FSM-6.3인증시험자료는 100% 패스보장을 드립니다.

Fortinet NSE5_FSM-6.3 인증 시험은 Fortinet FortisieM 기술에 대한 전문 지식을 보여 주려는 IT 전문가에게 귀중한 인증입니다. IT 전문가가 실제 환경에서 Fortinet Fortisiem 솔루션을 설계, 배포, 구성 및 관리하는 능력을 테스트하는 고급 수준의 시험입니다. 이 시험을 통과함으로써 IT 전문가는 업계에서 인정을 받고 네트워크 및 보안 관리 분야에서 경력을 발전시킬 수 있습니다.

최신 NSE 5 Network Security Analyst NSE5_FSM-6.3 무료샘플문제 (Q48-Q53):

질문 # 48
Refer to the exhibit.



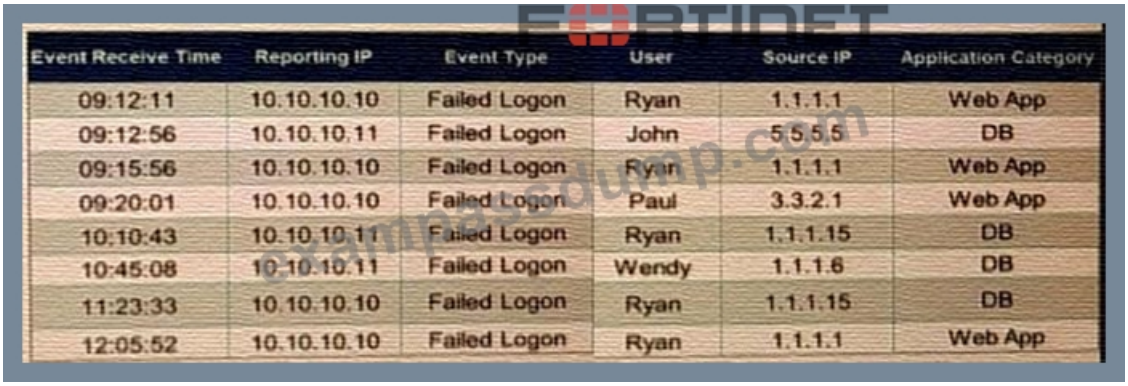
A FortiSIEM administrator wants to collect both SIEM event logs and performance and availability metrics (PAM) events from a Microsoft Windows server Which protocol should the administrator select in the Access Protocol drop-down list so that FortiSIEM will collect both SIEM and PAM events?

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

정답：B

설명：
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.

질문 # 49
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. Unique attribute cannot be grouped.
- B. Seven results will be displayed.
- C. There results will be displayed.
- D. Five results will be displayed.

정답： B

설명:
Grouping Events: Grouping events by specific attributes allows for the aggregation of similar events.
Grouping Criteria: For this question, events are grouped by "Reporting IP," "Event Type," and "User." Unique Combinations Analysis:
* 10.10.10.10, Failed Logon, Ryan, 1.1.1.1, Web App
* 10.10.10.11, Failed Logon, John, 5.5.5.5, DB
* 10.10.10.10, Failed Logon, Ryan, 1.1.1.1, Web App(duplicate, counted as one unique result)
* 10.10.10.10, Failed Logon, Paul, 3.3.2.1, Web App
* 10.10.10.11, Failed Logon, Ryan, 1.1.1.15, DB
* 10.10.10.11, Failed Logon, Wendy, 1.1.1.6, DB
* 10.10.10.10, Failed Logon, Ryan, 1.1.1.15, DB
Result Calculation: There are seven unique combinations based on the specified grouping attributes.
References: FortiSIEM 6.3 User Guide, Event Management and Reporting sections, explaining how events are grouped and reported based on selected attributes.

질문 # 50
To determine SNMP discovery issues, which is the best command from the backend?

- A. snmptest
- B. snmpwalk
- C. phSNMPTest

정답： B

질문 # 51
Consider the storage of anomaly baseline date that is calculated for different parameters. Which database is used for storing this data?

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

정답： D

설명:
* 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.
* Reference: 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.

질문 # 52
Where must you configure rule notifications and automated remediation on FortiSIEM?

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

정답：C

질문 # 53
.....