

Pass Guaranteed 2026 Valid Fortinet FCSS_ADA_AR-6.7: New FCSS—Advanced Analytics 6.7 Architect Study Plan



P.S. Free & New FCSS_ADA_AR-6.7 dumps are available on Google Drive shared by ExamCost: https://drive.google.com/open?id=1sYR36vzys29dzwbAn5aE-zngCAR_5M16

There have many shortcomings of the traditional learning methods. If you choose our FCSS_ADA_AR-6.7 test training, the intelligent system will automatically monitor your study all the time. Once you study our FCSS_ADA_AR-6.7 certification materials, the system begins to record your exercises. Also, we have invited for many volunteers to try our study materials. The results show our products are suitable for them. In addition, the system of our FCSS_ADA_AR-6.7 test training is powerful. You will never come across system crashes. The system we design has strong compatibility. High speed running completely has no problem at all.

Fortinet FCSS_ADA_AR-6.7 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none">Multi-Tenancy SOC Solution for MSSP: This section of the exam measures the skills of MSSP Architects and SOC Engineers in designing and deploying multi-tenant Security Operations Center (SOC) environments using FortiSIEM. It covers defining collectors and agents, deploying FortiSIEM in hybrid setups, managing resource allocation, and installingmanaging Windows and Linux agents for scalable event monitoring in multi-tenant architectures.
Topic 2	<ul style="list-style-type: none">Conditions and Remediation: This section measures the skills of Incident Responders and SOAR Specialists in remediating security incidents. It includes configuring manual and automated remediation workflows, integrating FortiSOAR with FortiSIEM for streamlined incident resolution, and deploying scripts to address threats while maintaining compliance
Topic 3	<ul style="list-style-type: none">FortiSIEM Rules and Analytics: This section evaluates the expertise of Security Analysts and Automation Engineers in configuring FortiSIEM rules and analytics. It includes constructing security rules based on event patterns, leveraging MITRE ATT&CK® frameworks, and configuring advanced nested queries and lookup tables for complex threat detection and correlation.

Topic 4	<ul style="list-style-type: none"> FortiSIEM Baseline and UEBA: This section tests the knowledge of Compliance Officers and Threat Analysts in implementing baseline profiles and User and Entity Behavior Analytics (UEBA). It covers creating baseline reports, configuring UEBA agents, and analyzing log-based behavioral patterns to detect anomalies and insider threats.
---------	--

>> New FCSS_ADA_AR-6.7 Study Plan <<

100% Pass Quiz Fortinet - FCSS_ADA_AR-6.7 - Accurate New FCSS—Advanced Analytics 6.7 Architect Study Plan

As one of the most professional dealer of FCSS_ADA_AR-6.7 practice questions, we have connection with all academic institutions in this line with proficient researchers of the knowledge related with the FCSS_ADA_AR-6.7 exam materials to meet your tastes and needs, please feel free to choose. And we have three versions of FCSS_ADA_AR-6.7 training guide: the PDF, Software and APP online for you. You can choose the one which you like best.

Fortinet FCSS—Advanced Analytics 6.7 Architect Sample Questions (Q24-Q29):

NEW QUESTION # 24

Refer to the exhibit.

PROCESS	UPTIME
phParser	DOWN
phAgentManager	DOWN
phCheckpoint	DOWN
phDiscover	DOWN
phEventPackager	DOWN
phPerfMonitor	DOWN
phEventForwarder	DOWN
phMonitor	13:04
phMonitorAgent	DOWN
Rsyslogd	DOWN

An administrator deploys a new collector for the first time, and notices that all the processes except the phMonitor are down. How can the administrator bring the processes up?

- A. The collector was not deployed properly and must be redeployed.
- B. The administrator needs to run the command `phtools --start` all on the collector.
- C. Rebooting the collector will bring up the processes.
- D. The processes will come up after the collector is registered to the supervisor.

Answer: D

NEW QUESTION # 25

Refer to the exhibit.

<div> <div> <div>1</div> <div>1</div> <div>0</div> <div>0</div> <div>0</div> </div> <div> <div>Routers</div> <div>Firewalls</div> <div>Windows</div> <div>Unix</div> <div>ESX</div> <div>AWS</div> <div>Azure</div> </div> </div>									
<div> <div>CMDB > Devices</div> <div> <div>New</div> <div>Edit</div> <div>Delete</div> <div>Discovered by All</div> <div>Q</div> </div> <div> <div>Actions</div> <div></div> <div></div> <div></div> <div></div> </div> </div>									
Name	IP	Device Type	Status	Discovered	Method	Agent Policy	Agent Status	Monitor Status	Event Status
FortiBANK_DC	10.10.2.63	Windows Server	Pending	Oct 28, 2021, 3:02:21 PM	WMI, PING			Normal	
FortiBank_Collector	10.10.2.64	Generic Unix	Pending	Oct 28, 2021, 5:48:32 PM	LOG				Normal

Why is the windows device still in the CMDB, even though the administrator uninstalled the windows agent?

- A. The device was not installed properly
- B. The device has performance jobs assigned
- C. The device must be deleted manually from the CMDB
- **D. The device must be deleted from backend of FortiSIEM**

Answer: D

NEW QUESTION # 26

What will be the correct data type for inner query?

Outer Query			Inner Query	
Query Condition Attribute	Query Condition Value Type	Validation	SubQuery Result Display Column Attribute	SubQuery Result Display Column Value Type
Source IP	IP	✓	Source IP	IP
Source IP	IP	✗	Application Protocol	STRING
Source IP	IP	✓	Reporting IP	IP

Attribute value type does not match the required type: ?

- A. INT32
- B. INT16
- C. STRING
- **D. IP**

Answer: D

NEW QUESTION # 27

What happens to UEBA events when a user is off-net?

- A. The agent will upload the events to the Worker if it cannot upload them to a FortiSIEM collector
- **B. The agent will cache events locally if it cannot upload them to a FortiSIEM collector**
- C. The agent will drop the events if it cannot upload them to a FortiSIEM collector
- D. The agent will upload the events the events to the Supervisor if it cannot upload them to a FortiSIEM collector

Answer: B

Explanation:

When a User and Entity Behavior Analytics (UEBA) agent is off-net, meaning it is disconnected from the network and cannot reach the FortiSIEM collector, it temporarily stores (caches) events locally until it can re-establish a connection.

This caching mechanism prevents data loss by ensuring events are retained even when the agent is offline.

Once the connection to the FortiSIEM collector is restored, the agent uploads the cached events.

This ensures continuity in user behavior monitoring, even when users are disconnected.

NEW QUESTION # 28

Refer to the exhibit.

Hour Of Day	Host IP	Host Name	Min CPU Util	AVG CPU Util	Max CPU Util	Std Dev CPU Util	numPoints
9	1.1.1.1	ServerA	33.50	33.50	33.50	0	1
10	1.1.1.1	ServerA	37.06	37.06	37.06	0	1
11	1.1.1.1	ServerA	40.12	40.12	40.12	0	1
12	1.1.1.1	ServerA	45.96	45.96	45.96	0	1

Hour Of Day	Host IP	Host Name	Min CPU Util	AVG CPU Util	Max CPU Util	Std Dev CPU Util	numPoints
9	1.1.1.1	ServerA	32.31	32.31	32.31	0	1

The profile database contains CPU utilization values from day one. At midnight on the second day, the CPU utilization values from the daily database will be merged with the profile database.

In the profile database, in the Hour of Day column where 9 is the value, what will be the updated minimum, maximum, and average CPU utilization values?

- A. Min CPU Util=32.31, Max CPU Util=33.50 and AVG CPU Util=32.67
- B. Min CPU Util=32.31, Max CPU Util=33.50 and AVG CPU Util 33.50
- C. Min CPU Util=32.31, Max CPU Util=32.31 and AVG CPU Util=32.31
- D. Min CPU Util=33.50, Max CPU Util=33.50 and AVG CPU Util=33.50

Answer: A

Explanation:

At midnight, the daily database values merge into the profile database. The new values for Hour 9 are calculated as follows:

*Minimum CPU Utilization: The new minimum is the lower of the existing (32.31) and new (33.50) values → 32.31

*Maximum CPU Utilization: The new maximum is the higher of the existing (32.31) and new (33.50) values → 33.50

*Average CPU Utilization:

*The previous average was 32.31 (from one point).

*The new value from the daily database is 33.50 (one additional point).

*The new average is calculated as:

$$\frac{(32.31 \times 1) + (33.50 \times 1)}{1 + 1} = \frac{32.31 + 33.50}{2} = 32.67$$

Thus, after merging, the updated profile database values for Hour 9 are:

*Min CPU Util = 32.31

*Max CPU Util = 33.50

*Avg CPU Util = 32.67

NEW QUESTION # 29

.....

ExamCost field is leaping up day by day and more people are pursuing it as a career than ever. Due to these reasons, candidates find it difficult to land their dream job and often face difficulty in finding the right career opportunities. But to overcome this issue, the FCSS_ADA_AR-6.7 Exam is introduced by Fortinet that provides candidates with a sustainable platform to examine their true capabilities and surf through their desired opportunities.

Latest FCSS_ADA_AR-6.7 Study Notes: https://www.examcost.com/FCSS_ADA_AR-6.7-practice-exam.html

- BTW, DOWNLOAD part of ExamCost FCSS_ADA_AR-6.7 dumps from Cloud Storage: https://drive.google.com/open?id=1sYR36vzys29dzwBAn5aE-zngCAR_5M16

BTW, DOWNLOAD part of ExamCost FCSS_ADA_AR-6.7 dumps from Cloud Storage: https://drive.google.com/open?id=1sYR36vzys29dzwBAn5aE-zngCAR_5M16