FORTINET NSE7_SOC_AR-7.6

Fortinet Security Operations Architect Certification Questions & Answers

Exam Summary – Syllabus – Questions

NSE7_SOC_AR-7.6

Fortinet Certified Solution Specialist - Security Operations

35-40 Questions Exam – Duration of 75 minutes

Table of Contents:

Know Your NSE7_SOC_AR-7.6 Certification Well:

The NSE7_SOC_AR-7.6 is best suitable for candidates who want to gain knowledge in the Fortinet [examcategory]. Before you start your NSE7_SOC_AR-7.6 preparation you may struggle to get all the crucial Security Operations Architect materials like NSE7_SOC_AR-7.6 syllabus, sample questions, study guide.

But don't worry the NSE7_SOC_AR-7.6 PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the NSE7_SOC_AR-7.6 syllabus?
- How many questions are there in the NSE7_SOC_AR-7.6 exam?
- Which Practice test would help me to pass the NSE7_SOC_AR-7.6 exam at the first attempt?

Passing the NSE7_SOC_AR-7.6 exam makes you Fortinet Certified Solution Specialist - Security Operations. Having the Security Operations Architect certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

Fortinet NSE7_SOC_AR-7.6 Security Operations Architect Certification Details:

Exam Name	Fortinet NSE 7 - Security Operations 7.6 Architect
Exam Code	NSE7_SOC_AR-7.6
Exam Price	$200 USD
Duration	75 minutes
Number of Questions	35-40
Passing Score	Pass / Fail
Recommended Training	**Security Operations Architect**
Exam Registration	**PEARSON VUE**
Sample Questions	**Fortinet NSE7_SOC_AR-7.6 Sample Questions**

Practice Exam	**Fortinet Certified Solution Specialist - Security Operations Practice Test**

NSE7_SOC_AR-7.6 Syllabus:

Section	Objectives
SOC Concepts and Frameworks	- Analyze security incidents and identify adversary behaviors - Explain Fortinet SOC enterprise architecture - Identify attack vectors
Detection Capabilities	- Configure FortiSIEM incident rules - Build queries to search event logs on FortiSIEM - Analyze FortiSIEM incidents
SOAR Incident Handling and Threat Hunting	- Analyze threat hunting processes and data - Manage FortiSOAR incidents - Create queues and shifts for workload management - Use war rooms for incident handling
SOAR Playbook Development	- Configure FortiSOAR playbooks - Configure FortiSOAR connectors - Manipulate data using Jinja filters - Debug and troubleshoot FortiSOAR playbooks

Fortinet NSE7_SOC_AR-7.6 Sample Questions:

Question: 1

You want to configure a playbook step that meets the following requirements:

1. If the domain field contains corp-mail.example.com, it follows path A.
2. If the domain field contains malicious-badsite.net, it follows path B.
3. Otherwise, it follows a default path C.

Which type of playbook step allows you to implement this branching logic?

a) Manual Input
b) Loop
c) Decision
d) Connector

Answer: c

Question: 2

Which three functions are supported by data ingestion wizard in FortiSOAR? (Choose three.)

a) Define a trigger to ingest data
b) Customize mapping of fields between the source system and FortiSOAR
c) Create separate data ingestion settings for each connector configuration
d) Choose between sequential, bulk, or parallel ingestion modes
e) Schedule data ingestion

Answer: b, c, e

Question: 3

During threat hunting, an analyst filters logs by malicious IP and retrieves endpoint data from FortiClient EMS via API. Which FortiSOAR feature is used?

a) Connector Action Execution
b) Playbook Debugger
c) Report Designer
d) Incident Cloning

Answer: a

Question: 4

Which component controls how FortiSIEM distributes data collection load across multiple nodes?

a) Collector Group Assignment
b) Supervisor Scheduler
c) CMDB Indexing
d) Notification Policy

Answer: a

Question: 5

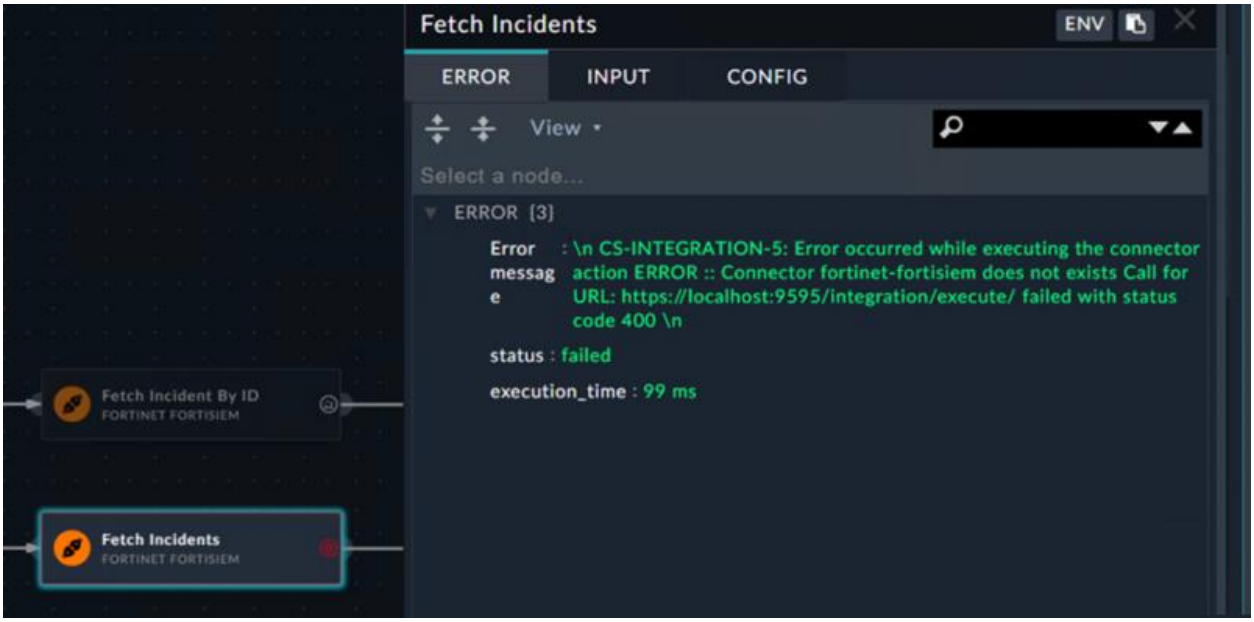
Which FortiSOAR feature enables export and import of playbooks between environments (e.g., staging → production)?

a) Playbook Package Manager
b) Connector Library
c) Automation Center
d) System Diagnostics

Answer: a

Question: 6

Refer to the exhibit.



Based on the error message, where should you begin your troubleshooting?

a) Ensure the user has the Execute permission for the Playbooks module
b) Confirm that incidents matching your search criteria exist on FortiSIEM
c) Check the FortiSIEM connector configuration
d) Install the FortiSIEM connector from the content hub

Answer: c

Question: 7

An administrator wants to detect if the CPU usage of a server exceeds 90% on average during a 10-minute window, at least twice. Which two aggregate conditions should you use together?

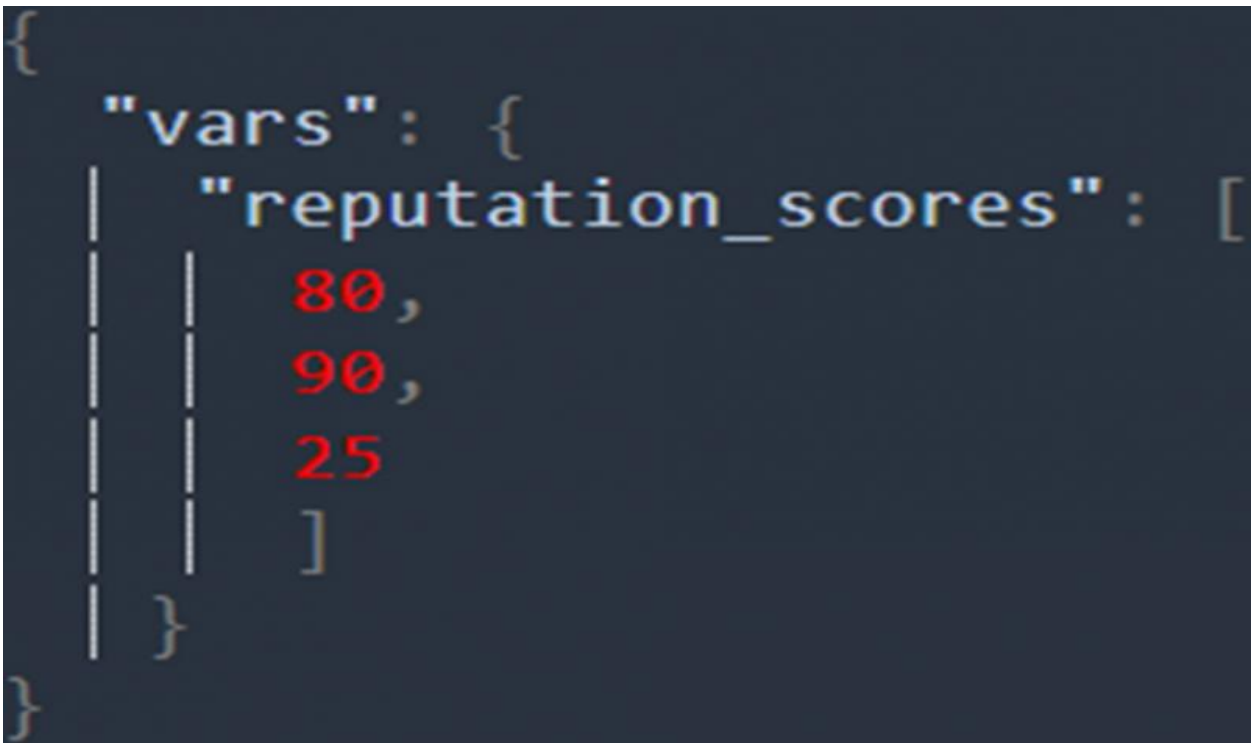
(Choose two.)

a) SUM(Matched Events)
b) COUNT(DISTINCT CPU Util)
c) AVG(CPU Util)
d) COUNT(Matched Events)

Answer: c, d

Question: 8

Refer to the exhibit.



Which Jinja expression will find the average of the three scores?

a) ((avg | vars.reputation_scores))
b) {{ (vars.reputation_scores | sum) / (vars.reputation_scores | length) }}
c) ((vars.reputation_scores.sum / length))
d) {{ sum(vars.reputation_scores) / length(vars.reputation_scores) }}

Answer: b

Question: 9

What is the minimum number of FortiSIEM VMs required to collect event logs and generate incidents from matching rules?

a) 3
b) 2
c) 4
d) 1

Answer: d

Question: 10

Which statement best describes the relationship between FortiSOAR and FortiSIEM in SOC operations?

a) FortiSOAR collects raw logs; FortiSIEM responds to incidents
b) FortiSIEM detects incidents; FortiSOAR automates response actions.
c) FortiSOAR correlates events; FortiSIEM manages queues.
d) They operate independently with no integration possible.

Answer: b

Study Guide to Crack Fortinet Security Operations Architect NSE7_SOC_AR-7.6 Exam:

- Getting details of the NSE7_SOC_AR-7.6 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the NSE7_SOC_AR-7.6 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the Fortinet provided training for NSE7_SOC_AR-7.6 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the NSE7_SOC_AR-7.6 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on NSE7_SOC_AR-7.6 practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for NSE7_SOC_AR-7.6 Certification

Make NWExam.com your best friend during your Fortinet NSE 7 - Security Operations 7.6 Architect exam preparation. We provide authentic practice tests for the NSE7_SOC_AR-7.6 exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual NSE7_SOC_AR-7.6 exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the NSE7_SOC_AR-7.6 exam.

Start Online practice of NSE7_SOC_AR-7.6 Exam by visiting URL
https://www.nwexam.com/fortinet/nse7-soc-ar-7-6-fortinet-nse-7-security-operations-7-6-architect