nwexam.com
#1 Networking Certification Guide

FORTINET FCSS_SOC_AN-7.4 STUDY GUIDE PDF

Fortinet Security Operations Analyst Certification Questions & Answers

Details of the Exam-Syllabus-Questions

FCSS_SOC_AN-7.4

Fortinet Certified Solution Specialist - Security Operations

32 Questions Exam – Duration of 65 minutes

Table of Contents:

Get an Overview of the FCSS_SOC_AN-7.4 Certification:

Who should take the **FCSS_SOC_AN-7.4 exam**? This is the first question that comes to a candidate's mind when preparing for the Security Operations Analyst certification. The FCSS_SOC_AN-7.4 certification is suitable for candidates who are keen to earn knowledge on the Security Operations and grab their Fortinet Certified Solution Specialist - Security Operations. When it is about starting the preparation, most candidates get confused regarding the study materials and study approach. But FCSS_SOC_AN-7.4 study guide PDF is here to solve the problem. FCSS_SOC_AN-7.4 PDF combines some effective sample questions and offers valuable tips to pass the exam with ease.

Why Should You Earn the Fortinet FCSS_SOC_AN-7.4 Certification?

There are several reasons why one should grab the FCSS_SOC_AN-7.4 certification.

- The Security Operations Analyst certification proves to be one of the most recognized certifications.
- The certification badge proves the knowledge of the candidate regarding subject matters and makes his resume presentable to potential candidates.
- Thus earning the **Fortinet Certified Solution Specialist - Security Operations** is a powerful qualification for a prosperous career.

What Is the Fortinet FCSS_SOC_AN-7.4 Security Operations Analyst Certification Exam Structure?

Exam Name	Fortinet FCSS - Security Operations 7.4 Analyst
Exam Number	FCSS_SOC_AN-7.4 Security Operations Analyst
Exam Price	$400 USD
Duration	65 minutes
Number of Questions	32

Passing Score	Pass / Fail
Recommended Training	**Security Operations Analyst**
Exam Registration	**PEARSON VUE**
Sample Questions	**Fortinet FCSS_SOC_AN-7.4 Sample Questions**
Practice Exam	**Fortinet Certified Solution Specialist - Security Operations Practice Test**

Enhance Knowledge with FCSS_SOC_AN-7.4 Sample Questions:

Question: 1

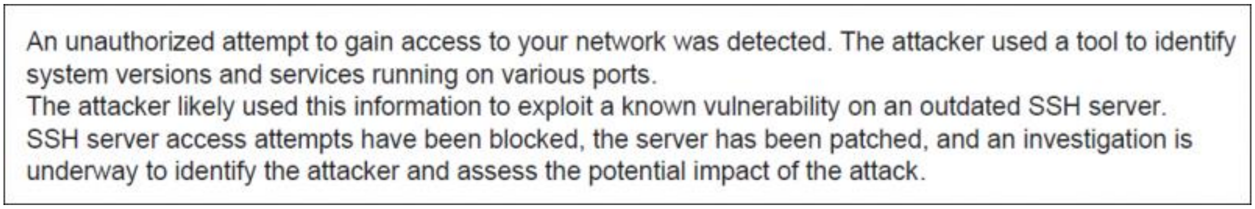
You are tasked with configuring automation to quarantine infected endpoints. Which two Fortinet SOC components can work together to fulfill this task? (Choose two.)

a) FortiAnalyzer
b) FortiClient EMS
c) FortiMail
d) FortiSandbox

Answer: a, b

Question: 2

Review the following incident report.



An unauthorized attempt to gain access to your network was detected. The attacker used a tool to identify system versions and services running on various ports.
The attacker likely used this information to exploit a known vulnerability on an outdated SSH server.
SSH server access attempts have been blocked, the server has been patched, and an investigation is underway to identify the attacker and assess the potential impact of the attack.

Which two MITRE ATT&CK tactics are captured in this report? (Choose two.)

a) Defense Evasion
b) Priviledge Escalation
c) Reconnaissance
d) Execution

Answer: c, d

Question: 3

Which National Institute of Standards and Technology (NIST) incident handling phase involves removing malware and persistence mechanisms from a compromised host?

a) Eradication
b) Recovery
c) Containment
d) Analysis

Answer: a

Question: 4

You are managing 10 FortiAnalyzer devices in a FortiAnalyzer Fabric. In this scenario, what is a benefit of configuring a Fabric group?

a) You can apply separate data storage policies per group.
b) You can aggregate and compress logging data for the devices in the group.
c) You can filter log search results based on the group.
d) You can configure separate logging rates per group.

Answer: c

Question: 5

Which two assets are available with the outbreak alert licensed feature on FortiAnalyzer? (Choose two.)

a) Custom event handlers from FortiGuard
b) Outbreak-specific custom playbooks
c) Custom connectors from FortiGuard
d) Custom outbreak reports

Answer: a, d

Question: 6

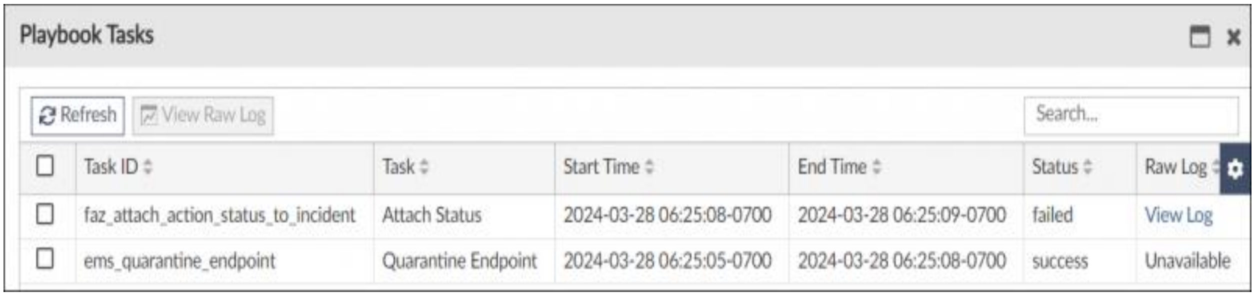
Which trigger type requires manual input to run a playbook?

a) INCIDENT_TRIGGER
b) ON_DEMAND
c) EVENT_TRIGGER
d) ON_SCHEDULE

Answer: b

Question: 7

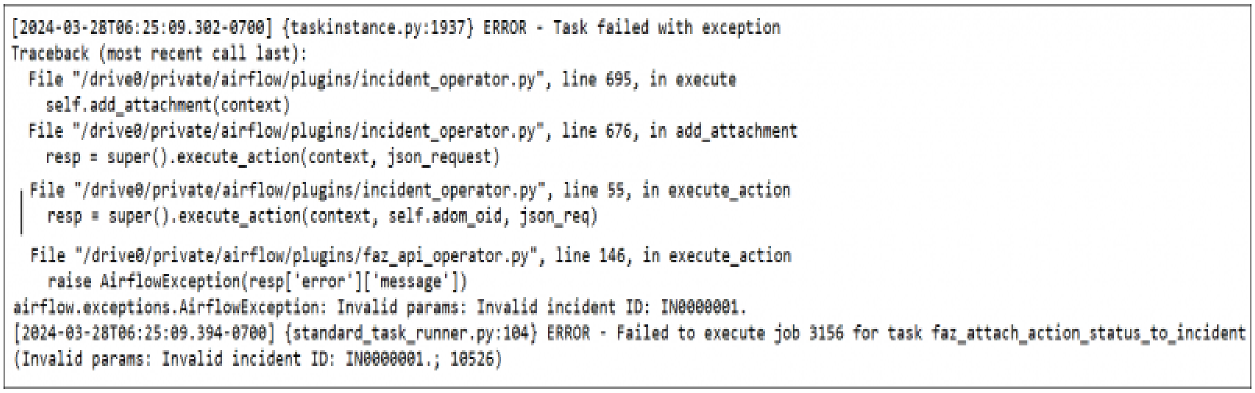
Refer to the exhibits.



Playbook Tasks

Refresh | View Raw Log | Search...

☐	Task ID	Task	Start Time	End Time	Status	Raw Log
☐	faz_attach_action_status_to_incident	Attach Status	2024-03-28 06:25:08-0700	2024-03-28 06:25:09-0700	failed	View Log
☐	ems_quarantine_endpoint	Quarantine Endpoint	2024-03-28 06:25:05-0700	2024-03-28 06:25:08-0700	success	Unavailable



```
[2024-03-28T06:25:09.302-0700] {taskinstance.py:1937} ERROR - Task failed with exception
Traceback (most recent call last):
  File "/drive0/private/airflow/plugins/incident_operator.py", line 695, in execute
    self.add_attachment(context)
  File "/drive0/private/airflow/plugins/incident_operator.py", line 676, in add_attachment
    resp = super().execute_action(context, json_request)
  File "/drive0/private/airflow/plugins/incident_operator.py", line 55, in execute_action
    resp = super().execute_action(context, self.adom_oid, json_req)
  File "/drive0/private/airflow/plugins/faz_api_operator.py", line 146, in execute_action
    raise AirflowException(resp['error']['message'])
airflow.exceptions.AirflowException: Invalid params: Invalid incident ID: IN0000001.
[2024-03-28T06:25:09.394-0700] {standard_task_runner.py:104} ERROR - Failed to execute job 3156 for task faz_attach_action_status_to_incident
(Invalid params: Invalid incident ID: IN0000001.; 10526)
```

The Quarantine Endpoint by EMS playbook execution failed. What can you conclude from reviewing the playbook tasks and raw logs?

a) The local connector is incorrectly configured, which is causing JSON API errors.
b) The endpoint is quarantined, but the action status is not attached to the incident.
c) The admin user does not have the necessary rights to update incidents.
d) The playbook executed in an ADOM where the incident does not exist.

Answer: b

Question: 8

You are not able to view any incidents or events on FortiAnalyzer. What is the cause of this issue?

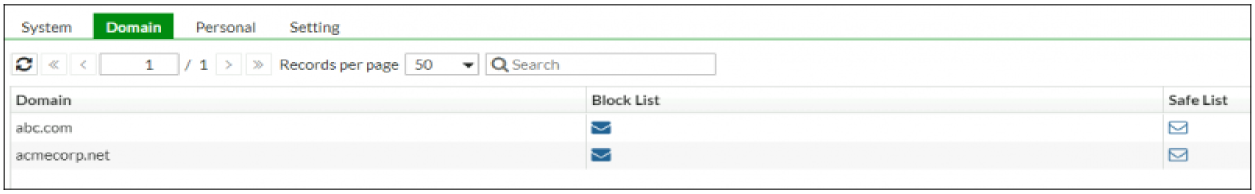
a) There are no open security incidents and events.
b) FortiAnalyzer must be in a Fabric ADOM.
c) FortiAnalyzer is operating as a Fabric supervisor.
d) FortiAnalyzer is operating in collector mode.

Answer: d

Question: 9

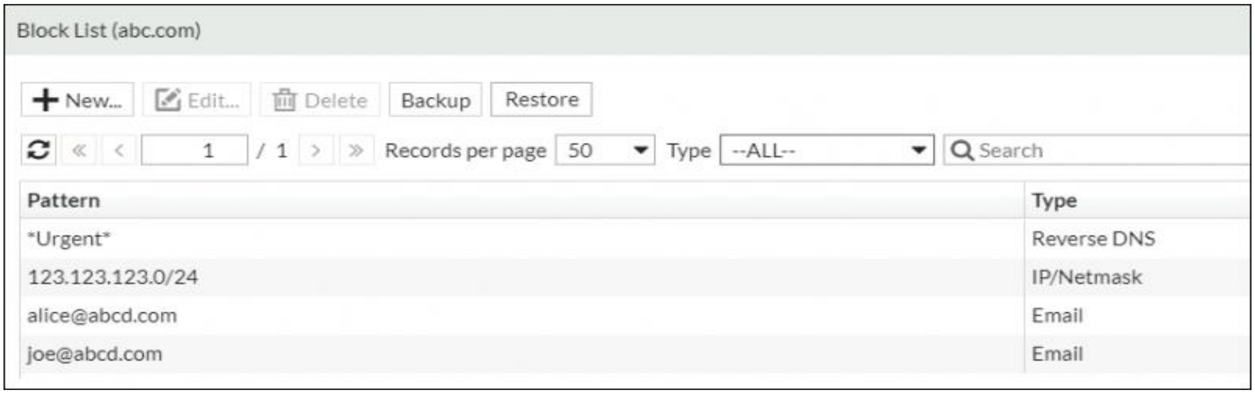
Refer to the exhibits.

Domain List:



Domain	Block List	Safe List
abc.com	✉	✉
acmecorp.net	✉	✉

Domain abc.com:



Pattern	Type
Urgent	Reverse DNS
123.123.123.0/24	IP/Netmask
alice@abcd.com	Email
joe@abcd.com	Email

Which connector and action on FortiAnalyzer can you use to add the entries show in the exhibits?

a) The FortiClient EMS connector and the quarantine action
b) The FortiMail connector and the add send to blocklist action
c) The Local connector and the update asset and identity action
d) The FortiMail connector and the get sender reputation action

Answer: b

Question: 10

Which connector on FortiAnalyzer is responsible for looking up indicators to get threat intelligence?

a) The local connector
b) The FortiClient EMS connector
c) The FortiOS connector
d) The FortiGuard connector

Answer: d

What Study Guide Works Best in Acing the Fortinet FCSS_SOC_AN-7.4 Security Operations Analyst Certification?

The FCSS_SOC_AN-7.4 study guide is a combination of some proven study tips and the combination of all valuable study materials like sample questions, syllabus and practice tests in one place.

Explore the Syllabus Topics and Learn from the Core:

If you are determined to earn success in the Security Operations Analyst exam, getting in full touch of the **syllabus** is mandatory. During preparation, you might not like all syllabus sections or topics, but try to get at least the fundamental knowledge from the sections you don’t like. The more you possess knowledge on all syllabus sections, the more is the chance to attempt maximum number of questions during the actual exam.

Make Your Schedule:

Studying and completing the syllabus becomes easier, if you work on the syllabus topics after making a schedule. Your syllabus must mention what areas you want to cover and within what time. Once you make a schedule and follow it regularly, syllabus completion becomes easier and preparation becomes smoother.

Get Expert Advice from the Training:

Do not forget to join the Fortinet FCSS_SOC_AN-7.4 training if it is providing any. Training enhances the practical knowledge of a candidate, which helps them to work well in the practical field during projects.

Get Access to the PDF Sample Questions:

If your study material is in a **PDF format** or the materials are mobile-friendly, what could be better than that? Get access to the free sample questions and keep enhancing your knowledge beyond the syllabus.

Avoid Dumps and Utilize the Fortinet FCSS_SOC_AN-7.4 Practice Test:

Why should you rely on practice tests? The reason is simple: you must get familiar with the exam pattern before reaching the exam hall. An aspirant aware of the exam structure and time management during the exam preparation can perform well in the actual exam and attempt the maximum number of questions during the exam.

Many aspirants prefer to read from dumps, but they miss out on the self assessment method. Therefore, FCSS_SOC_AN-7.4 practice tests always stand out to be the better choice than dumps PDF.

Avail the Proven FCSS_SOC_AN-7.4 Practice Test for Success!!!

Do you want to pass the FCSS_SOC_AN-7.4 exam on your first attempt? Stop worrying; we, NWExam.com are here to provide you the best experience during your Fortinet FCSS - Security Operations 7.4 Analyst preparation. Try out our free mock tests to get a glimpse of our quality study materials, and build your confidence with the premium **FCSS_SOC_AN-7.4 practice tests**. Our expert-designed questions help you to improve performance and pass the exam on your first attempt.