



# FORTINET FCSS\_SOC\_AN-7.4

---

**Fortinet Security Operations Analyst Certification Questions & Answers**

---

**Exam Summary – Syllabus – Questions**

**FCSS\_SOC\_AN-7.4**

**[Fortinet Certified Solution Specialist - Security Operations](#)**

**32 Questions Exam – Pass / Fail Cut Score – Duration of 65 minutes**

## Table of Contents:

|   |   |
|---|---|
| Know Your FCSS_SOC_AN-7.4 Certification Well:.....                                      | 2 |
| Fortinet FCSS_SOC_AN-7.4 Security Operations Analyst<br>Certification Details: .....    | 2 |
| FCSS_SOC_AN-7.4 Syllabus: .....   | 3 |
| Fortinet FCSS_SOC_AN-7.4 Sample Questions:.....   | 3 |
| Study Guide to Crack Fortinet Security Operations Analyst<br>FCSS_SOC_AN-7.4 Exam:..... | 7 |

## Know Your FCSS\_SOC\_AN-7.4 Certification Well:

The FCSS\_SOC\_AN-7.4 is best suitable for candidates who want to gain knowledge in the Fortinet Security Operations. Before you start your FCSS\_SOC\_AN-7.4 preparation you may struggle to get all the crucial Security Operations Analyst materials like FCSS\_SOC\_AN-7.4 syllabus, sample questions, study guide.

But don't worry the FCSS\_SOC\_AN-7.4 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 FCSS\_SOC\_AN-7.4 syllabus?
- How many questions are there in the FCSS\_SOC\_AN-7.4 exam?
- Which Practice test would help me to pass the FCSS\_SOC\_AN-7.4 exam at the first attempt?

Passing the FCSS\_SOC\_AN-7.4 exam makes you Fortinet Certified Solution Specialist - Security Operations. Having the Security Operations Analyst 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 FCSS\_SOC\_AN-7.4 Security Operations Analyst Certification Details:

|                             |   |
|-----------------------------|---|
| <b>Exam Name</b>            | Fortinet FCSS - Security Operations 7.4 Analyst           |
| <b>Exam Code</b>            | FCSS_SOC_AN-7.4   |
| <b>Exam Price</b>           | \$400 USD   |
| <b>Duration</b>             | 65 minutes  |
| <b>Number of Questions</b>  | 32  |
| <b>Passing Score</b>        | Pass / Fail   |
| <b>Recommended Training</b> | <a href="#">Security Operations Analyst</a>               |
| <b>Exam Registration</b>    | <a href="#">PEARSON VUE</a>                               |
| <b>Sample Questions</b>     | <a href="#">Fortinet FCSS SOC AN-7.4 Sample Questions</a> |

|                      |   |
|----------------------|---|
| <b>Practice Exam</b> | <b>Fortinet Certified Solution Specialist - Security Operations Practice Test</b> |
|----------------------|---|

## FCSS\_SOC\_AN-7.4 Syllabus:

| Section                                 | Objectives  |
|---|---|
| SOC concepts and adversary behavior     | <ul style="list-style-type: none"> <li>- Analyze security incidents and identify adversary behaviors</li> <li>- Map adversary behaviors to MITRE ATT&amp;CK tactics and techniques</li> <li>- Identify components of the Fortinet SOC solution</li> </ul> |
| Architecture and detection capabilities | <ul style="list-style-type: none"> <li>- Configure and manage collectors and analyzers</li> <li>- Design stable and efficient FortiAnalyzer deployments</li> <li>- Design, configure, and manage FortiAnalyzer Fabric deployments</li> </ul>              |
| SOC operation                           | <ul style="list-style-type: none"> <li>- Configure and manage event handlers</li> <li>- Analyze and manage events and incidents</li> <li>- Analyze threat hunting information feeds</li> <li>- Manage outbreak alert handlers and reports</li> </ul>      |
| SOC automation                          | <ul style="list-style-type: none"> <li>- Configure playbook triggers and tasks</li> <li>- Configure and manage connectors</li> <li>- Manage playbook templates</li> <li>- Monitor playbooks</li> </ul>  |

## Fortinet 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**

Refer to the exhibits.

| <input type="checkbox"/> | Job ID                 | Playbook                   | Trigger     | Start Time               | End Time                 | Status   | Details |
|--------------------------|------------------------|----------------------------|-------------|--------------------------|--------------------------|--|---------|
| <input type="checkbox"/> | 2024-03-28 06:25:00-07 | Quarantine Endpoint by EMS | user(admin) | 2024-03-28 06:25:04-0700 | 2024-03-28 06:25:08-0700 | failed(Scheduled:0/Running:0/Success:1/Failed:1) |         |

**Playbook Tasks** ☰ ✕

Search...

| <input type="checkbox"/> | Task ID                              | Task                | Start Time               | End Time                 | Status  | Raw Log                  |
|--------------------------|--------------------------------------|---------------------|--------------------------|--------------------------|---------|--------------------------|
| <input type="checkbox"/> | faz_attach_action_status_to_incident | Attach Status       | 2024-03-28 06:25:08-0700 | 2024-03-28 06:25:09-0700 | failed  | <a href="#">View Log</a> |
| <input type="checkbox"/> | 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: 3**

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: 4**

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) Privilege Escalation
- c) Reconnaissance
- d) Execution

**Answer: c, d**

**Question: 5**

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: 6**

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

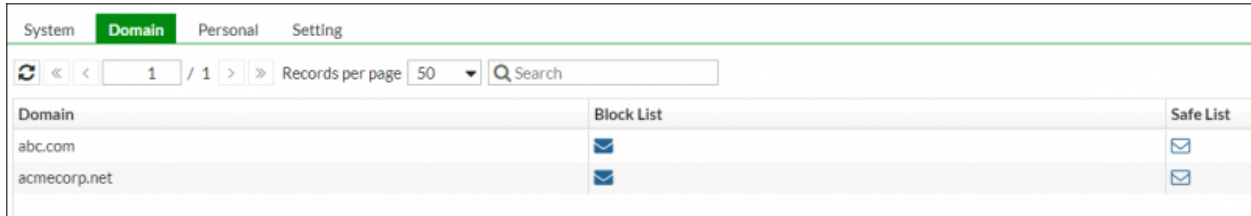
- a) The local connector
- b) The FortiClient EMS connector
- c) The FortiOS connector
- d) The FortiGuard connector





**Answer: d**

Question: 7

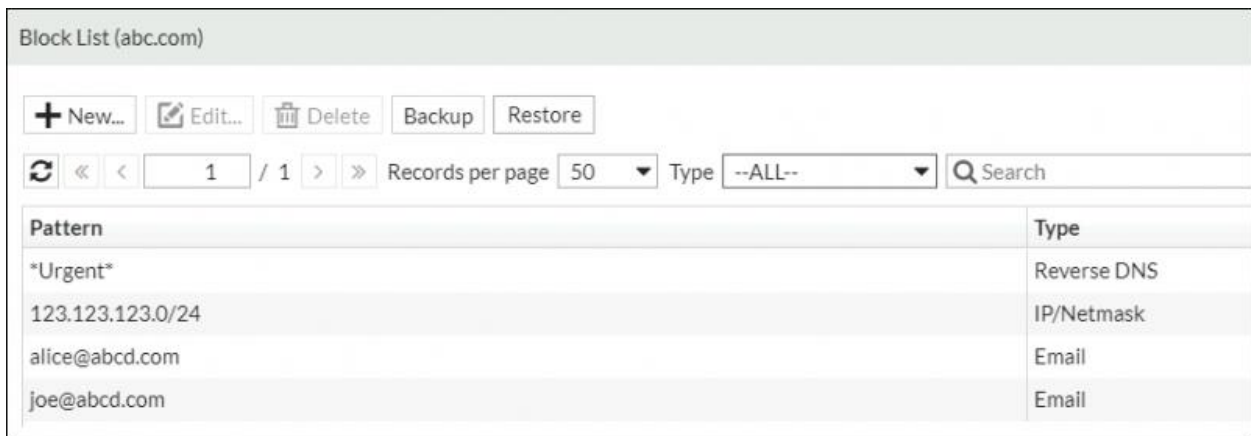
Refer to the exhibits.

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 exhibits?

- a) The FortiClient EMS connector and the quarantine action
- b) The FortiMail connector and the add send to blacklist 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: 8

You are not able to view any incidents or events on FortiAnalyzer. What is 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**

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: 10**

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**

## Study Guide to Crack Fortinet Security Operations

### Analyst FCSS\_SOC\_AN-7.4 Exam:

- Getting details of the FCSS\_SOC\_AN-7.4 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 FCSS\_SOC\_AN-7.4 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 FCSS\_SOC\_AN-7.4 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 FCSS\_SOC\_AN-7.4 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 FCSS\_SOC\_AN-7.4 practice tests is must. Continuous practice will make you an expert in all syllabus areas.

## Reliable Online Practice Test for FCSS\_SOC\_AN-7.4 Certification

Make NWExam.com your best friend during your Fortinet FCSS - Security Operations 7.4 Analyst exam preparation. We provide authentic practice tests for the FCSS\_SOC\_AN-7.4 exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual FCSS\_SOC\_AN-7.4 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 FCSS\_SOC\_AN-7.4 exam.

**Start Online practice of FCSS\_SOC\_AN-7.4 Exam by visiting URL**  
<https://www.nwexam.com/fortinet/fcss-soc-7-4-fortinet-fcss-security-operations-7-4-analyst>