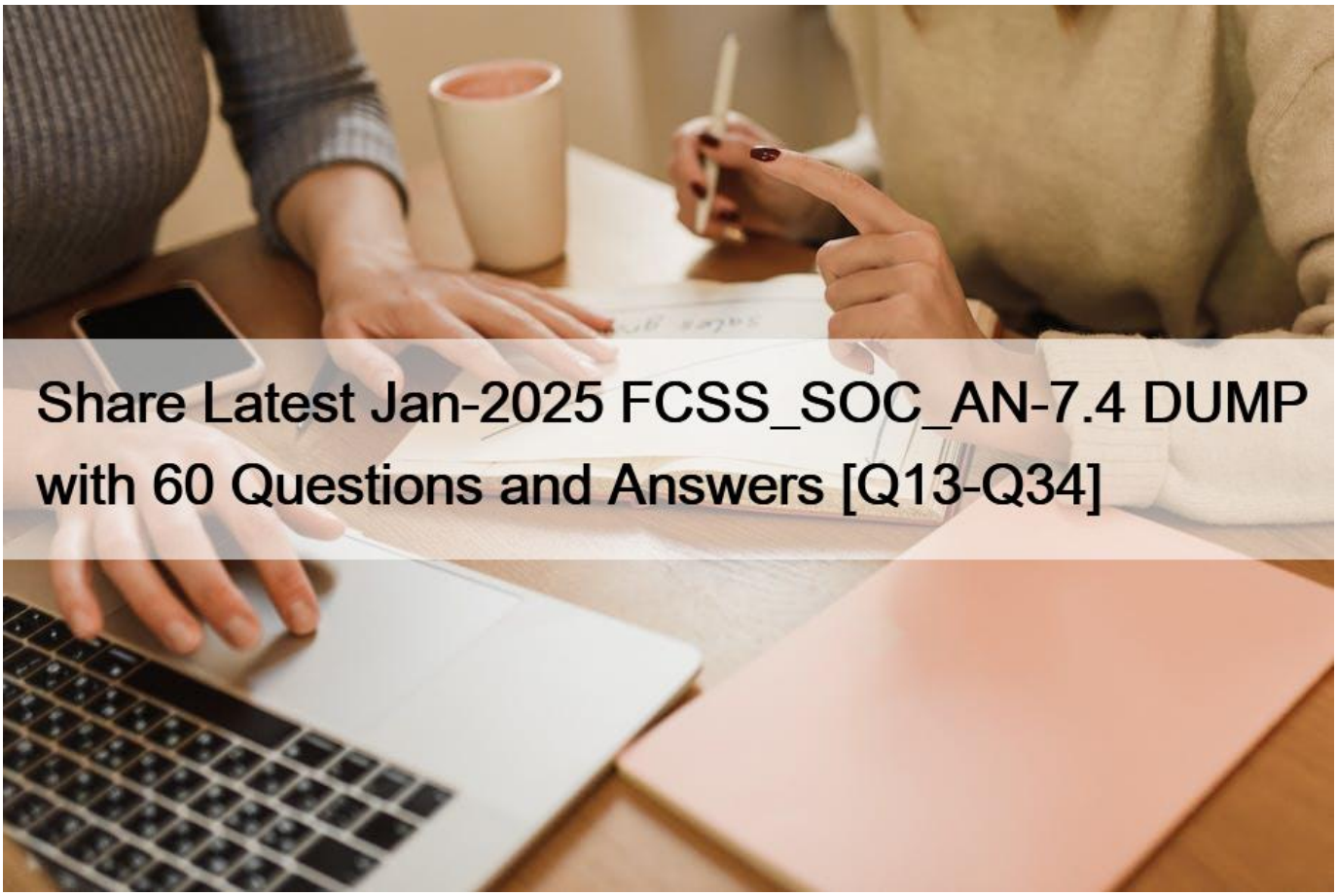
Share Latest Jan-2025 FCSS_SOC_AN-7.4 DUMP with 60 Questions and Answers [Q13-Q34



Share Latest Jan-2025 FCSS_SOC_AN-7.4 DUMP with 60 Questions and Answers
PDF Dumps 2025 Exam Questions with Practice Test

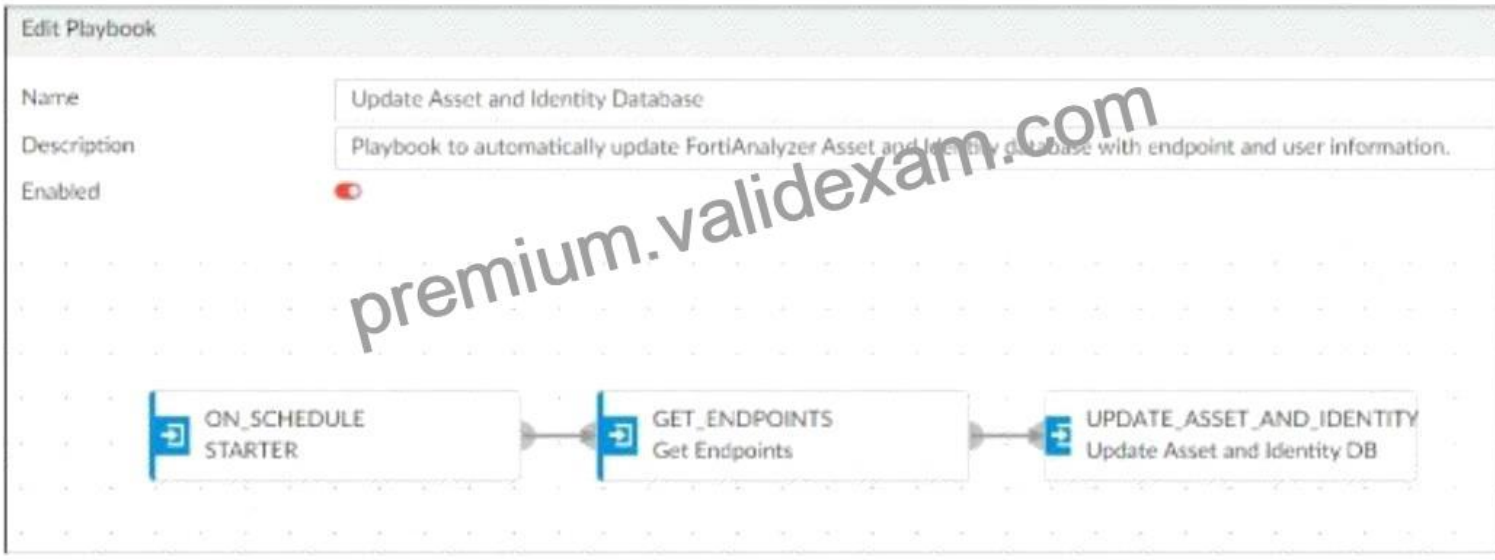
Fortinet FCSS_SOC_AN-7.4 Exam Syllabus Topics:

TopicDetailsTopic 1- SOC operation: This section of the exam measures the skills of SOC professionals and covers the day-to-day activities within a Security Operations Center. It focuses on configuring and managing event handlers, a key skill for processing and responding to security alerts. Candidates are expected to demonstrate proficiency in analyzing and managing events and incidents, as well as analyzing threat-hunting information feeds.Topic 2- SOC automation: This section of the exam measures the skills of target professionals in the implementation of automated processes within a SOC. It emphasizes configuring playbook triggers and tasks, which are crucial for streamlining incident response. Candidates should be able to configure and manage connectors, facilitating integration between different security tools and systems.Topic 3- SOC concepts and adversary behavior: This section of the exam measures the skills of Security Operations Analysts and covers fundamental concepts of Security Operations Centers and adversary behavior. It focuses on analyzing security incidents and identifying adversary behaviors. Candidates are expected to demonstrate proficiency in mapping adversary behaviors to MITRE ATT&CK tactics and techniques, which aid in understanding and categorizing cyber threats.Topic 4- Architecture and detection capabilities: This section of the exam measures the skills of SOC analysts in the designing and managing of FortiAnalyzer deployments. It emphasizes configuring and managing collectors and analyzers, which are essential for

gathering and processing security data.

NEW QUESTION 13

Refer to the exhibit.



Which two options describe how the Update Asset and Identity Database playbook is configured? (Choose two.)
* The playbook is using a local connector.
* The playbook is using a FortiMail connector.
* The playbook is using an on-demand trigger.
* The playbook is using a FortiClient EMS connector.
* Understanding the Playbook Configuration:

* The playbook named “Update Asset and Identity Database” is designed to update the FortiAnalyzer Asset and Identity database with endpoint and user information.

* The exhibit shows the playbook with three main components: ON_SCHEDULE STARTER, GET_ENDPOINTS, and UPDATE_ASSET_AND_IDENTITY.

* Analyzing the Components:

* ON_SCHEDULE STARTER:This component indicates that the playbook is triggered on a schedule, not on-demand.

* GET_ENDPOINTS:This action retrieves information about endpoints, suggesting it interacts with an endpoint management system.

* UPDATE_ASSET_AND_IDENTITY:This action updates the FortiAnalyzer Asset and Identity database with the retrieved information.

* Evaluating the Options:

* Option A:The actions shown in the playbook are standard local actions that can be executed by the FortiAnalyzer, indicating the use of a local connector.

* Option B:There is no indication that the playbook uses a FortiMail connector, as the tasks involve endpoint and identity management, not email.

* Option C:The playbook is using an “ON_SCHEDULE” trigger, which contradicts the description of an on-demand trigger.

* Option D:The action “GET_ENDPOINTS” suggests integration with an endpoint management system, likely FortiClient EMS, which manages endpoints and retrieves information from them.

* Conclusion:

* The playbook is configured to use a local connector for its actions.

* It interacts with FortiClient EMS to get endpoint information and update the FortiAnalyzer Asset and Identity database.

References:

* Fortinet Documentation on Playbook Actions and Connectors.

* FortiAnalyzer and FortiClient EMS Integration Guides.

NEW QUESTION 14

Which three end user logs does FortiAnalyzer use to identify possible IOC compromised hosts? (Choose three.)
* Email filter logs
* DNS filter logs
* Application filter logs
* IPS logs
* Web filter logs
* Overview of Indicators of Compromise (IoCs): Indicators of Compromise (IoCs) are pieces of evidence that suggest a system may have been compromised. These can include unusual network traffic patterns, the presence of known malicious files, or other suspicious activities.

* FortiAnalyzer’s Role: FortiAnalyzer aggregates logs from various Fortinet devices to provide comprehensive visibility and analysis of network events. It uses these logs to identify potential IoCs and compromised hosts.

* Relevant Log Types:

* DNS Filter Logs:

* DNS requests are a common vector for malware communication. Analyzing DNS filter logs helps in identifying suspicious domain queries, which can indicate malware attempting to communicate with command and control (C2) servers.

NEW QUESTION 15

What should be prioritized when analyzing threat hunting information feeds?

(Choose Two)
* Accuracy of the information
* Frequency of advertisement insertion
* Relevance to current security landscape
* Entertainment value of the content

NEW QUESTION 16

Which MITRE ATT&CK technique category involves collecting information about the environment and systems?
* Credential Access
* Discovery
* Lateral Movement
* Exfiltration

NEW QUESTION 17

Which connector on FortiAnalyzer is responsible for looking up indicators to get threat intelligence?
* The FortiGuard connector
* The FortiOS connector
* The FortiClient EMS connector
* The local connector

NEW QUESTION 18

In the context of SOC automation, how does effective management of connectors influence incident management?
* It decreases the effectiveness of communication channels
* It simplifies the process of handling incidents by automating data exchanges
* It increases the need for paper-based reporting
* It reduces the importance of cybersecurity training

NEW QUESTION 19

What is the primary purpose of using collectors in a FortiAnalyzer deployment?
* To store backup configurations
* To aggregate and analyze log data
* To enhance the graphical user interface
* To manage network bandwidth usage

NEW QUESTION 20

Which two statements about the FortiAnalyzer Fabric topology are true? (Choose two.)
* Downstream collectors can forward logs to Fabric members.
* Logging devices must be registered to the supervisor.
* The supervisor uses an API to store logs, incidents, and events locally.
* Fabric members must be in analyzer mode.
* Understanding FortiAnalyzer Fabric Topology:

* The FortiAnalyzer Fabric topology is designed to centralize logging and analysis across multiple devices in a network.

* It involves a hierarchy where the supervisor node manages and coordinates with other Fabric members.

* Analyzing the Options:

* Option A:Downstream collectors forwarding logs to Fabric members is not a typical configuration. Instead, logs are usually centralized to the supervisor.

* Option B:For effective management and log centralization, logging devices must be registered to the supervisor. This ensures proper log collection and coordination.

* Option C:The supervisor does not primarily use an API to store logs, incidents, and events locally. Logs are stored directly in the FortiAnalyzer database.

* Option D:For the Fabric topology to function correctly, all Fabric members need to be in analyzer mode. This mode allows them to collect, analyze, and forward logs appropriately within the topology.

* Conclusion:

* The correct statements regarding the FortiAnalyzer Fabric topology are that logging devices must be registered to the supervisor and that Fabric members must be in analyzer mode.

References:

* Fortinet Documentation on FortiAnalyzer Fabric Topology.

* Best Practices for Configuring FortiAnalyzer in a Fabric Environment.

NEW QUESTION 21

Which of the following should be a priority when monitoring SOC playbooks?
* Watching for unusual increases in playbook file sizes
* Checking for the timely execution of tasks
* Ensuring that playbooks are printed and distributed
* Monitoring the personal emails of SOC analysts

NEW QUESTION 22

What is the primary function of event handlers in a SOC operation?
* To provide technical support to end-users
* To automate responses to detected events
* To monitor the health of IT equipment
* To generate financial reports

NEW QUESTION 23

When configuring a FortiAnalyzer to act as a collector device, which two steps must you perform?(Choose two.)
* Configure log forwarding to a FortiAnalyzer in analyzer mode.
* Configure Fabric authorization on the connecting interface.
* Configure the data policy to focus on archiving.

* Enable log compression.

NEW QUESTION 24

During a security incident analysis, if an adversary’s behavior is identified as ‘Credential Dumping’, it maps to which MITRE ATT&CK technique?
* T1003
* T1059
* T1566
* T1110

NEW QUESTION 25

What should be monitored in playbooks to ensure they are functioning as intended?
* The number of coffee breaks taken by SOC staff
* The frequency of playbook activation
* The physical health of SOC analysts
* The execution paths and outcomes of the playbooks

NEW QUESTION 26

Configuring playbook triggers correctly is crucial for which aspect of SOC automation?
* Ensuring that all security incidents receive a human response
* Automating responses to detected incidents based on predefined conditions
* Making sure that SOC analysts are kept busy
* Increasing the manual tasks in the SOC

NEW QUESTION 27

Your company is doing a security audit To pass the audit, you must take an inventory of all software and applications running on all Windows devices Which FortiAnalyzer connector must you use?
* FortiClient EMS
* ServiceNow
* FortiCASB
* Local Host
* Requirement Analysis:

* The objective is to inventory all software and applications running on all Windows devices within the organization.

* This inventory must be comprehensive and accurate to pass the security audit.

* Key Components:

* FortiClient EMS (Endpoint Management Server):

* FortiClient EMS provides centralized management of endpoint security, including software and application inventory on Windows devices.

* It allows administrators to monitor, manage, and report on all endpoints protected by FortiClient.

* Connector Options:

* FortiClient EMS:

* Best suited for managing and reporting on endpoint software and applications.

* Provides detailed inventory reports for all managed endpoints.

* Selected as it directly addresses the requirement of taking inventory of software and applications on Windows devices.

* ServiceNow:

* Primarily a service management platform.

* While it can be used for asset management, it is not specifically tailored for endpoint software inventory.

* Not selected as it does not provide direct endpoint inventory management.

* FortiCASB:

* Focuses on cloud access security and monitoring SaaS applications.

* Not applicable for managing or inventorying endpoint software.

* Not selected as it is not related to endpoint software inventory.

* Local Host:

* Refers to handling events and logs within FortiAnalyzer itself.

* Not specific enough for detailed endpoint software inventory.

* Not selected as it does not provide the required endpoint inventory capabilities.

* Implementation Steps:

* Step 1: Ensure all Windows devices are managed by FortiClient and connected to FortiClient EMS.

* Step 2: Use FortiClient EMS to collect and report on the software and applications installed on these devices.

* Step 3: Generate inventory reports from FortiClient EMS to meet the audit requirements.

References:

* Fortinet Documentation on FortiClient EMS FortiClient EMS Administration Guide By using the FortiClient EMS connector, you can effectively inventory all software and applications on Windows devices, ensuring compliance with the security audit requirements.

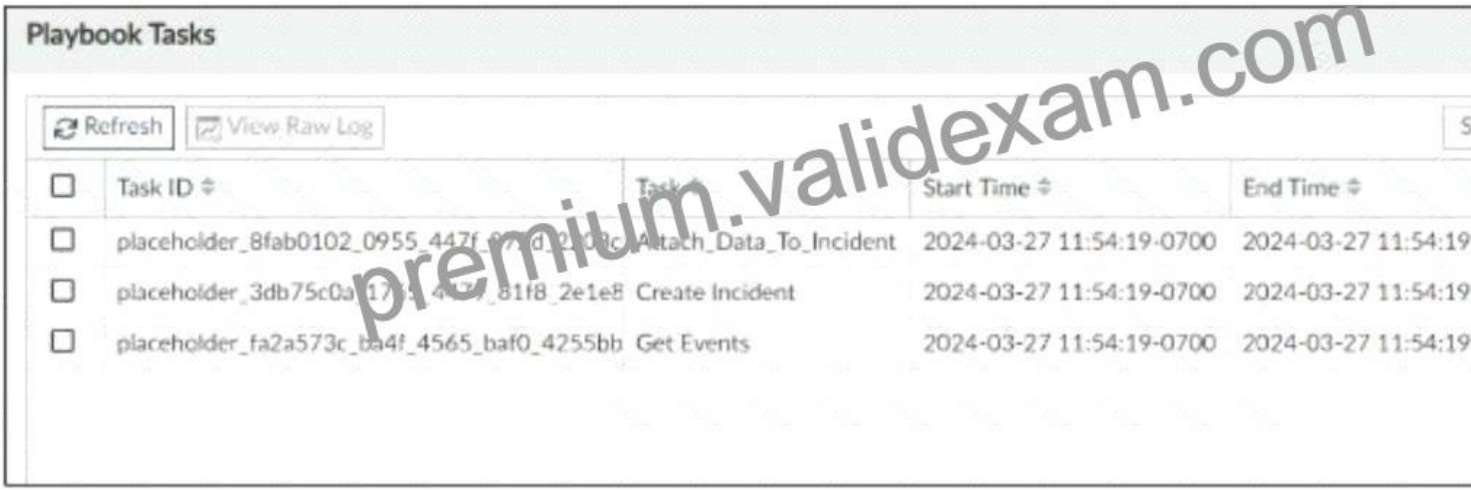
NEW QUESTION 28

Refer to the exhibits.

Playbook

Job ID	Playbook	Trigger	Start Time	End Time	Status
2024-03-27 11:54:16.858411-07	Malicious File Detect	event[20240327100(	2024-03-27 11:54:17-0700	2024-03-27 11:54:20-0700	failed

Playbook Tasks

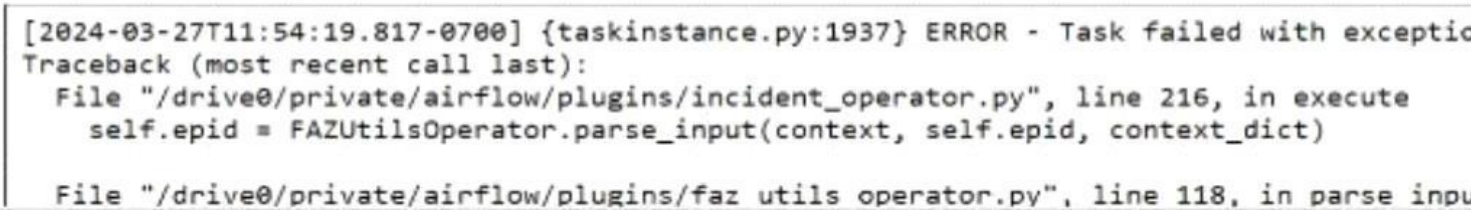


Playbook Tasks

Refresh | View Raw Log

Task ID	Task	Start Time	End Time
placeholder_8fab0102_0955_447f_	Attach_Data_To_Incident	2024-03-27 11:54:19-0700	2024-03-27 11:54:19
placeholder_3db75c0a_	Create Incident	2024-03-27 11:54:19-0700	2024-03-27 11:54:19
placeholder_fa2a573c_ba4f_4565_baf0_4255bb	Get Events	2024-03-27 11:54:19-0700	2024-03-27 11:54:19

Raw Logs



```
[2024-03-27T11:54:19.817-0700] {taskinstance.py:1937} ERROR - Task failed with exceptio
Traceback (most recent call last):
  File "/drive0/private/airflow/plugins/incident_operator.py", line 216, in execute
    self.epid = FAZUtilsOperator.parse_input(context, self.epid, context_dict)

  File "/drive0/private/airflow/plugins/faz utils operator.py", line 118, in parse inpu
```

The Malicious File Detect playbook is configured to create an incident when an event handler generates a malicious file detection event.

Why did the Malicious File Detect playbook execution fail?
* The Create Incident task was expecting a name or number as input, but received an incorrect data format
* The Get Events task did not retrieve any event data.
* The Attach_Data_To_lncident incident task wasexpecting an integer, but received an incorrect data format.
* The Attach Data To Incident task failed, which stopped the playbook execution.
* Understanding the Playbook Configuration:

* The “Malicious File Detect” playbook is designed to create an incident when a malicious file detection event is triggered.

* The playbook includes tasks such asAttach_Data_To_Incident,Create Incident, andGet Events.

* Analyzing the Playbook Execution:

* The exhibit shows that theCreate Incidenttask has failed, and theAttach_Data_To_Incidenttask has also failed.

* TheGet Eventstask succeeded, indicating that it was able to retrieve event data.

* Reviewing Raw Logs:

* The raw logs indicate an error related to parsing input in theincident_operator.pyfile.

* The error traceback suggests that the task was expecting a specific input format (likely a name or number) but received an incorrect data format.

* Identifying the Source of the Failure:

* TheCreate Incidenttask failure is the root cause since it did not proceed correctly due to incorrect input format.

* TheAttach_Data_To_Incidenttask subsequently failed because it depends on the successful creation of an incident.

* Conclusion:

* The primary reason for the playbook execution failure is that theCreate Incidenttask received an incorrect data format, which was not a name or number as expected.

References:

* Fortinet Documentation on Playbook and Task Configuration.

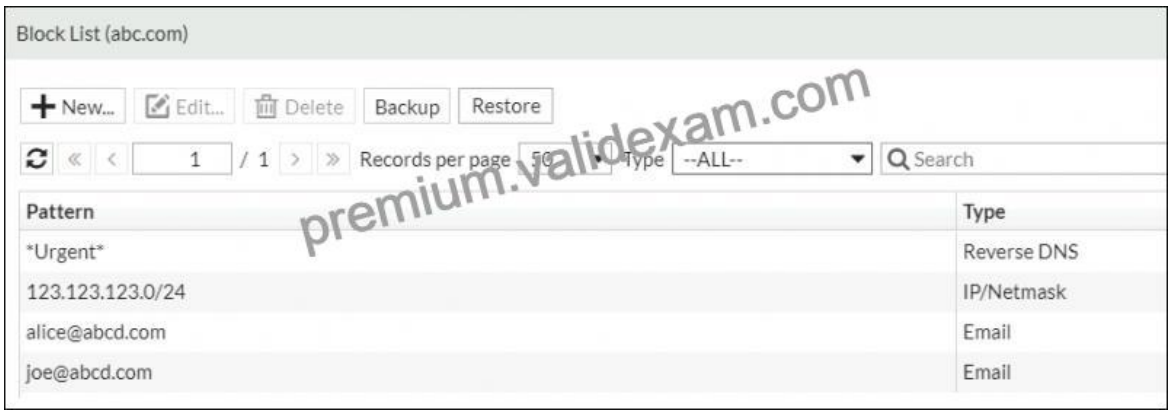
* Error handling and debugging practices in playbook execution.

NEW QUESTION 29

Refer to the exhibits.

Domain List:

Domain abc.com:

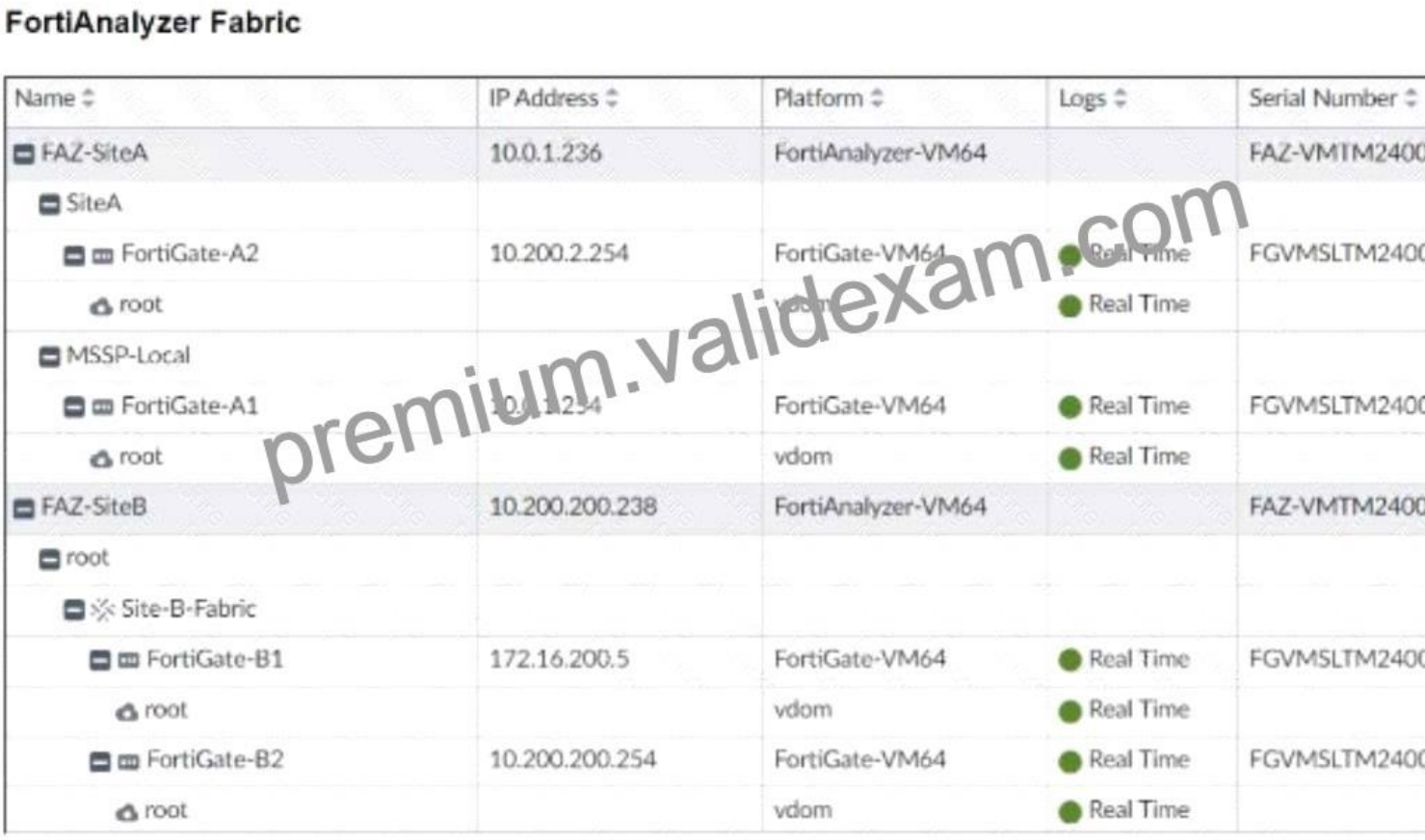


Which connector and action on FortiAnalyzer can you use to add the entries show in the exhibits?

* The FortiClient EMS connector and the quarantine action
* The FortiMail connector and the add send to blocklist action
* The Local connector and the update asset and identity action
* The FortiMail connector and the get sender reputation action

NEW QUESTION 30

Refer to the exhibit.



Assume that all devices in the FortiAnalyzer Fabric are shown in the image.

Which two statements about the FortiAnalyzer Fabric deployment are true? (Choose two.)
* FortiGate-B1 and FortiGate-B2 are in a Security Fabric.
* There is no collector in the topology.
* All FortiGate devices are directly registered to the supervisor.
* FAZ-SiteA has two ADOMs enabled.
* Understanding the FortiAnalyzer Fabric:

* The FortiAnalyzer Fabric provides centralized log collection, analysis, and reporting for connected FortiGate devices.

* Devices in a FortiAnalyzer Fabric can be organized into different Administrative Domains (ADOMs) to separate logs and management.

* Analyzing the Exhibit:

* FAZ-SiteAandFAZ-SiteBare FortiAnalyzer devices in the fabric.

* FortiGate-B1andFortiGate-B2are shown under theSite-B-Fabric, indicating they are part of the same Security Fabric.

* FAZ-SiteAhas multiple entries under it:SiteAandMSSP-Local, suggesting multiple ADOMs are enabled.

* Evaluating the Options:

* Option A:FortiGate-B1 and FortiGate-B2 are underSite-B-Fabric, indicating they are indeed part of the same Security Fabric.

* Option B:The presence of FAZ-SiteA and FAZ-SiteB as FortiAnalyzers does not preclude the existence of collectors. However, there is no explicit mention of a separate collector role in the exhibit.

* Option C:Not all FortiGate devices are directly registered to the supervisor. The exhibit shows hierarchical organization under different sites and ADOMs.

* Option D:The multiple entries underFAZ-SiteA(SiteA and MSSP-Local) indicate that FAZ-SiteA has two ADOMs enabled.

* Conclusion:

* FortiGate-B1 and FortiGate-B2 are in a Security Fabric.

* FAZ-SiteA has two ADOMs enabled.

References:

* Fortinet Documentation on FortiAnalyzer Fabric Topology and ADOM Configuration.

* Best Practices for Security Fabric Deployment with FortiAnalyzer.

NEW QUESTION 31

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

What is the cause of this issue?
* FortiAnalyzer is operating in collector mode.
* FortiAnalyzer is operating as a Fabric supervisor.
* FortiAnalyzer must be in a Fabric ADOM.
* There are no open security incidents and events.

NEW QUESTION 32

Which two assets are available with the outbreak alert licensed feature on FortiAnalyzer?

(Choose two.)
* Custom event handlers from FortiGuard
* Outbreak-specific custom playbooks
* Custom connectors from FortiGuard
* Custom outbreak reports

NEW QUESTION 33

Refer to the Exhibit:

An analyst wants to create an incident and generate a report whenever FortiAnalyzer generates a malicious attachment event based on FortiSandbox analysis. The endpoint hosts are protected by FortiClient EMS integrated with FortiSandbox. All devices are logging to FortiAnalyzer.

Which connector must the analyst use in this playbook?
* FortiSandbox connector
* FortiClient EMS connector
* FortiMail connector
* Local connector
* Understanding the Requirements:

* The objective is to create an incident and generate a report based on malicious attachment events detected by FortiAnalyzer from FortiSandbox analysis.

* The endpoint hosts are protected by FortiClient EMS, which is integrated with FortiSandbox. All logs are sent to FortiAnalyzer.

* Key Components:

* FortiAnalyzer: Centralized logging and analysis for Fortinet devices.

* FortiSandbox: Advanced threat protection system that analyzes suspicious files and URLs.

* FortiClient EMS: Endpoint management system that integrates with FortiSandbox for endpoint protection.

* Playbook Analysis:

* The playbook in the exhibit consists of three main actions:GET_EVENTS,RUN_REPORT, andCREATE_INCIDENT.

* EVENT_TRIGGER: Starts the playbook when an event occurs.

* GET_EVENTS: Fetches relevant events.

* RUN_REPORT: Generates a report based on the events.

* CREATE_INCIDENT: Creates an incident in the incident management system.

* Selecting the Correct Connector:

* The correct connector should allow fetching events related to malicious attachments analyzed by FortiSandbox and facilitate integration with FortiAnalyzer.

* Connector Options:

* FortiSandbox Connector:

* Directly integrates with FortiSandbox to fetch analysis results and events related to malicious attachments.

* Best suited for getting detailed sandbox analysis results.

* Selected as it is directly related to the requirement of handling FortiSandbox analysis events.

* FortiClient EMS Connector:

* Used for managing endpoint security and integrating with endpoint logs.

* Not directly related to fetching sandbox analysis events.

* Not selected as it is not directly related to the sandbox analysis events.

* FortiMail Connector:

* Used for email security and handling email-related logs and events.

* Not applicable for sandbox analysis events.

* Not selected as it does not relate to the sandbox analysis.

* Local Connector:

* Handles local events within FortiAnalyzer itself.

* Might not be specific enough for fetching detailed sandbox analysis results.

* Not selected as it may not provide the required integration with FortiSandbox.

* Implementation Steps:

* Step 1: Ensure FortiSandbox is configured to send analysis results to FortiAnalyzer.

* Step 2: Use the FortiSandbox connector in the playbook to fetch events related to malicious attachments.

* Step 3: Configure theGET_EVENTSaction to use the FortiSandbox connector.

* Step 4: Set up theRUN_REPORTandCREATE_INCIDENTactions based on the fetched events.

References:

* Fortinet Documentation on FortiSandbox Integration FortiSandbox Integration Guide

* Fortinet Documentation on FortiAnalyzer Event Handling FortiAnalyzer Administration Guide By using the FortiSandbox connector, the analyst can ensure that the playbook accurately fetches events based on FortiSandbox analysis and generates the required incident and report.

NEW QUESTION 34

How does identifying adversary behavior benefit SOC operations in terms of incident response?
* By allowing for a quicker isolation of affected systems
* By increasing the time it takes to respond to incidents
* By reducing the importance of endpoint security
* By providing data for marketing strategies