

Fortinet

Exam Questions NSE5_EDR-5.0

Fortinet NSE 5 - FortiEDR 5.0



NEW QUESTION 1
Refer to the exhibits.

The top screenshot shows a table of collector states. The collector with ID C8092231196 is in a 'Disconnected' state. The bottom screenshot shows the output of the 'netstat -an' command, listing active connections. A connection to 10.160.6.100:8080 is shown in a 'SYN_SENT' state.

DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
C8092231196	1196\Administrator	Windows Server 2016 Standard Evaluation	10.160.6.110	00-5D-56-A1-32-81.00...	4.1.0.361	Disconnected	Today

```

Administrator: Command Prompt
C:\Users\Administrator>netstat -an

Active Connections

Proto Local Address           Foreign Address         State
TCP   0.0.0.0:135              0.0.0.0:0               LISTENING
TCP   0.0.0.0:445              0.0.0.0:0               LISTENING
TCP   0.0.0.0:5985             0.0.0.0:0               LISTENING
TCP   0.0.0.0:49692            0.0.0.0:0               LISTENING
TCP   10.160.6.110:139         0.0.0.0:0               LISTENING
TCP   10.160.6.110:50853       10.160.6.100:8080       SYN_SENT
TCP   172.16.9.19:139         0.0.0.0:0               LISTENING
TCP   172.16.9.19:49687       52.177.165.30:443       ESTABLISHED
  
```

The exhibits show the collector state and active connections. The collector is unable to connect to aggregator IP address 10.160.6.100 using default port. Based on the netstat command output what must you do to resolve the connectivity issue?

- A. Reinstall collector agent and use port 443
- B. Reinstall collector agent and use port 8081
- C. Reinstall collector agent and use port 555
- D. Reinstall collector agent and use port 6514

Answer: B

NEW QUESTION 2
Exhibit.

The screenshot shows a forensic data view with a table of events. The event is a 'File Read Attempt' on a device with ID C8092231196. The process is 'ConnectivityTestApp.exe' and the destination is '13-Feb-2022, 23:26:30'. The event is classified as 'Malicious' and the certificate is 'Unsigned'.

DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN
C8092231196	Windows Server 2016	ConnectivityTestApp.exe	Malicious	File Read Attempt	13-Feb-2022, 23:26:30	14-Feb-2022, 00:17:30

Based on the forensics data shown in the exhibit which two statements are true? (Choose two.)

- A. The device cannot be remediated
- B. The event was blocked because the certificate is unsigned
- C. Device C8092231196 has been isolated
- D. The execution prevention policy has blocked this event.

Answer: BC

NEW QUESTION 3
What is the purpose of the Threat Hunting feature?

- A. Delete any file from any collector in the organization
- B. Find and delete all instances of a known malicious file or hash in the organization
- C. Identify all instances of a known malicious file or hash and notify affected users
- D. Execute playbooks to isolate affected collectors in the organization

Answer: C

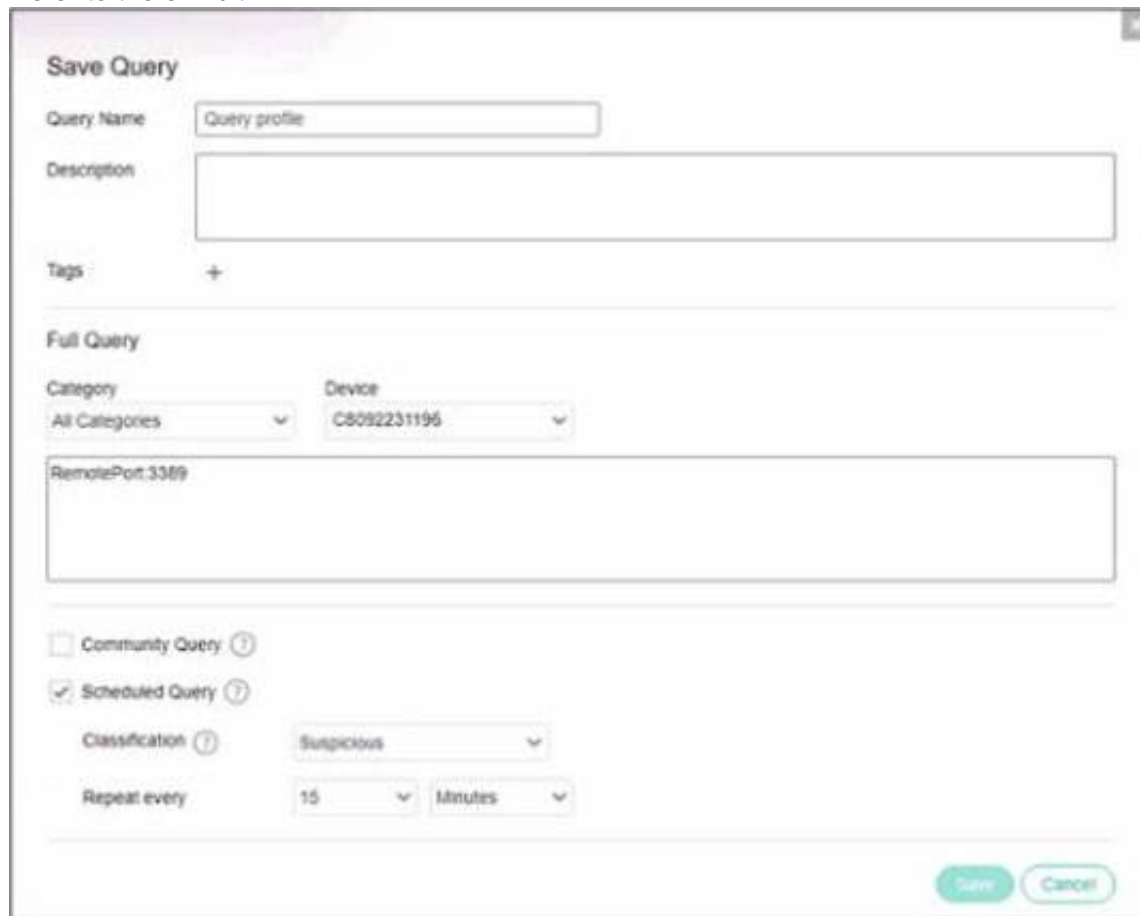
NEW QUESTION 4
An administrator needs to restrict access to the ADMINISTRATION tab in the central manager for a specific account. What role should the administrator assign to this account?

- A. Admin
- B. User
- C. Local Admin
- D. REST API

Answer: C

NEW QUESTION 5

Refer to the exhibit.



Based on the threat hunting query shown in the exhibit which of the following is true?

- A. RDP connections will be blocked and classified as suspicious
- B. A security event will be triggered when the device attempts a RDP connection
- C. This query is included in other organizations
- D. The query will only check for network category

Answer: B

NEW QUESTION 6

What is true about classifications assigned by Fortinet Cloud Sen/ice (FCS)?

- A. The core is responsible for all classifications if FCS playbooks are disabled
- B. The core only assigns a classification if FCS is not available
- C. FCS revises the classification of the core based on its database
- D. FCS is responsible for all classifications

Answer: C

NEW QUESTION 7

What is the benefit of using file hash along with the file name in a threat hunting repository search?

- A. It helps to make sure the hash is really a malware
- B. It helps to check the malware even if the malware variant uses a different file name
- C. It helps to find if some instances of the hash are actually associated with a different file
- D. It helps locate a file as threat hunting only allows hash search

Answer: C

NEW QUESTION 10

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

NSE5_EDR-5.0 Practice Exam Features:

- * NSE5_EDR-5.0 Questions and Answers Updated Frequently
- * NSE5_EDR-5.0 Practice Questions Verified by Expert Senior Certified Staff
- * NSE5_EDR-5.0 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE5_EDR-5.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE5_EDR-5.0 Practice Test Here](#)