



Fortinet

Exam Questions NSE5_EDR-5.0

Fortinet NSE 5 - FortiEDR 5.0

NEW QUESTION 1
Refer to the exhibits.

Search Collectors or Go <input type="text"/>							
Enable/Disable	Isolate	Export	Uninstall				
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
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 3
Refer to the exhibit.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19043.1526]
(c) Microsoft Corporation. All rights reserved.

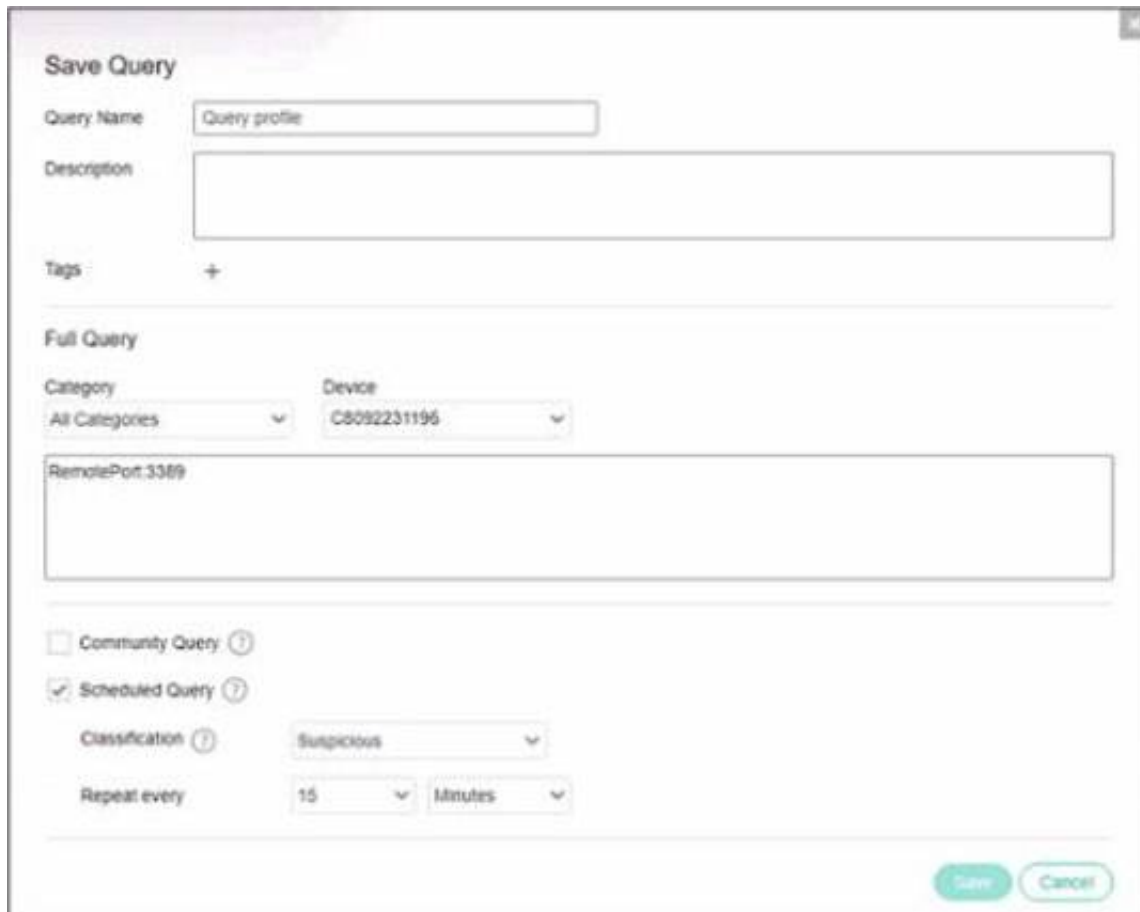
C:\WINDOWS\system32>"C:\Program Files\Fortinet\FortiEDR\FortiEDRCollectorService.exe" --status
FortiEDR Service: Up
FortiEDR Driver: Up
FortiEDR Status: Degraded (no configuration)
```

Based on the FortiEDR status output shown in the exhibit, which two statements about the FortiEDR collector are true? (Choose two.)

- A. The collector device has windows firewall enabled
- B. The collector has been installed with an incorrect port number
- C. The collector has been installed with an incorrect registration password
- D. The collector device cannot reach the central manager

Answer: BD

NEW QUESTION 4
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 5

Which FortiEDR component is required to find malicious files on the entire network of an organization?

- A. FortiEDR Aggregator
- B. FortiEDR Central Manager
- C. FortiEDR Threat Hunting Repository
- D. FortiEDR Core

Answer: A

NEW QUESTION 6

Exhibit.



DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN
c:\p0-kom45	Windows 10 Pro	dot.exe	Malicious	File Read Attempt	01-Jan-2022, 04:33:09	04-Jan-2022, 13:16:16
RAW ID: 119330467		Process Type: 32 bit	Certificate: Unsigned	Process Path: C:\Users\fortinet\Desktop\dot.exe	Count: 135	

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

- A. An exception has been created for this event
- B. The forensics data is displayed in the stacks view
- C. The device has been isolated
- D. The exfiltration prevention policy has blocked this event

Answer: CD

NEW QUESTION 7

Refer to the exhibits.

APPLICATIONS				
All ▼ 🏠 Mark As ▼ 🗑️ Delete ↻ Modify Action 🔍 Advanced Filter 📄 Export ▼				
<input type="checkbox"/>	APPLICATION		VENDOR	REPUTATION VULNERABILITY
<input checked="" type="checkbox"/>	FileZilla	Signed	Tim Kosse	Unknown Unknown
<input type="checkbox"/>	3.50.0			Unknown Unknown
<input checked="" type="checkbox"/>	FileZilla	Signed	FileZilla Project	Unknown Unknown
<input type="checkbox"/>	COLLECTOR GROUP NAME			DEVICE NAME
<input checked="" type="checkbox"/>	High Security Collector Group (1/1)			
<input checked="" type="checkbox"/>	DBA (1/1)			
				<input type="checkbox"/> C8092231196
<input checked="" type="checkbox"/>	Default Collector Group (0/0)			

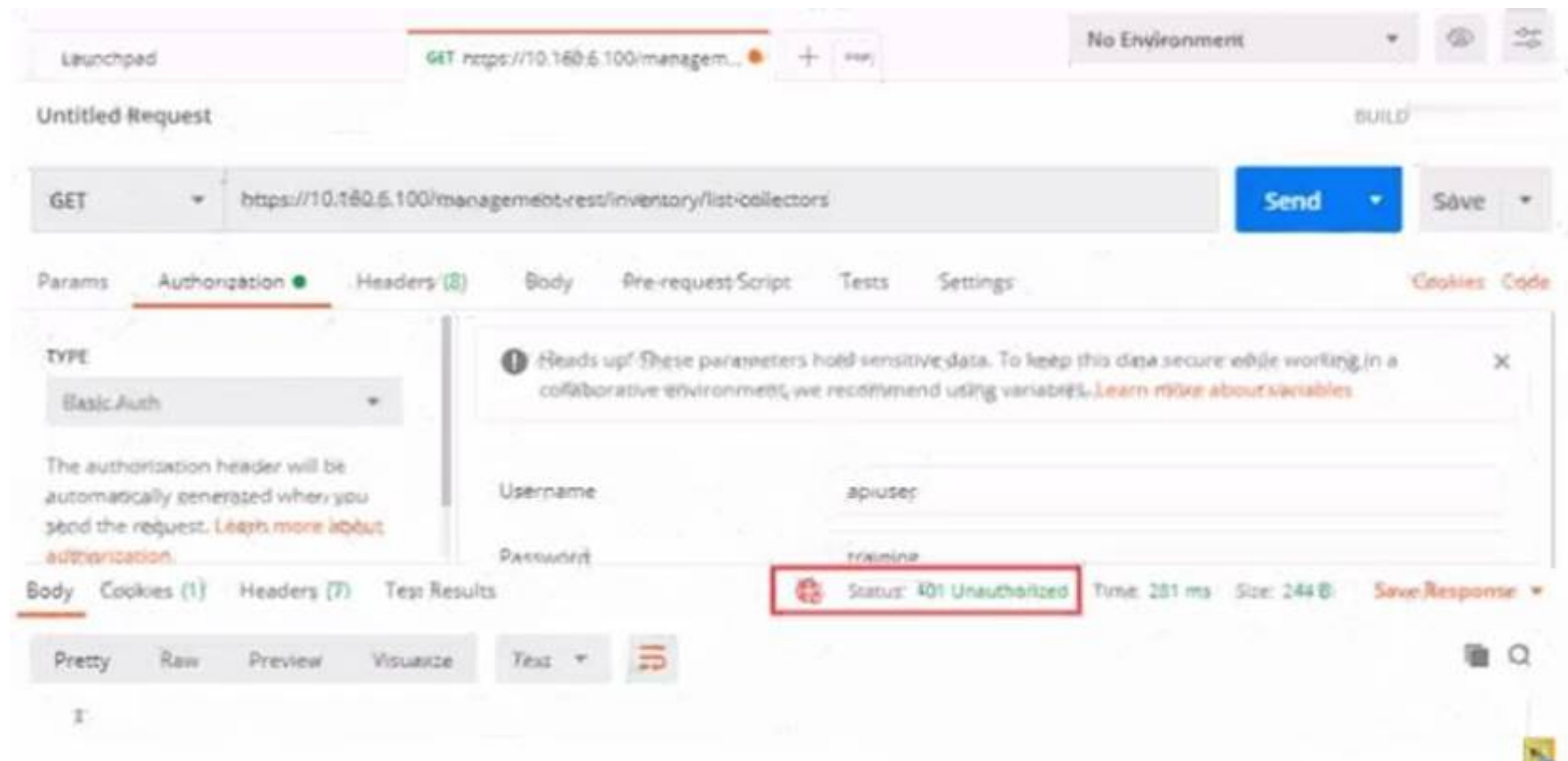
APPLICATION DETAILS			
FileZilla			
Policies			
Policy	Action		
Default Communication Control ...	FORTINET	Allow	According to policy
Servers Policy	FORTINET	Deny	According to policy
Finance Policy		Deny	Manually
Simulation Communication Control Policy		Allow	According to policy
Isolation Policy	FORTINET	Deny	According to policy
ASSIGNED COLLECTOR GROUPS			
Finance Policy			
Unassign Group			

The exhibits show application policy logs and application details Collector C8092231196 is a member of the Finance group
What must an administrator do to block the FileZilia application?

- A. Deny application in Finance policy
- B. Assign Finance policy to DBA group
- C. Assign Finance policy to Default Collector Group
- D. Assign Simulation Communication Control Policy to DBA group

Answer: D

NEW QUESTION 8
Refer to the exhibit.



Based on the postman output shown in the exhibit why is the user getting an unauthorized error?

- A. The user has been assigned Admin and Rest API roles
- B. FortiEDR requires a password reset the first time a user logs in
- C. Postman cannot reach the central manager
- D. API access is disabled on the central manager

Answer: A

NEW QUESTION 9

A company requires a global communication policy for a FortiEDR multi-tenant environment. How can the administrator achieve this?

- A. An administrator creates a new communication control policy and shares it with other organizations
- B. A local administrator creates new a communication control policy and shares it with other organizations
- C. A local administrator creates a new communication control policy and assigns it globally to all organizations
- D. An administrator creates a new communication control policy for each organization

Answer: C

NEW QUESTION 10

What is true about classifications assigned by Fortinet Cloud Sentinel (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 10

FortiXDR relies on which feature as part of its automated extended response?

- A. Playbooks
- B. Security Policies
- C. Forensic
- D. Communication Control

Answer: B

NEW QUESTION 13

Which connectors can you use for the FortiEDR automated incident response? (Choose two.)

- A. FortiNAC
- B. FortiGate
- C. FortiSiem
- D. FortiSandbox

Answer: BC

NEW QUESTION 17

Which scripting language is supported by the FortiEDR action managed?

- A. TCL

- B. Python
- C. Perl
- D. Bash

Answer: A

NEW QUESTION 22

Which two statements about the FortiEDR solution are true? (Choose two.)

- A. It provides pre-infection and post-infection protection
- B. It is Windows OS only
- C. It provides central management
- D. It provides pant-to-point protection

Answer: AD

NEW QUESTION 25

How does FortiEDR implement post-infection protection?

- A. By preventing data exfiltration or encryption even after a breach occurs
- B. By using methods used by traditional EDR
- C. By insurance against ransomware
- D. By real-time filtering to prevent malware from executing

Answer: D

NEW QUESTION 28

.....

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](#)