

NSE5_EDR-5.0^{Q&As}

Fortinet NSE 5 - FortiEDR 5.0

Pass Fortinet NSE5_EDR-5.0 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/nse5_edr-5-0.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



QUESTION 1

Which three steps does FortiXDR perform to find and prevent cyberattacks? (Choose three.)

- A. Extended analysis
- B. Extended detection
- C. Extended discovery
- D. Extended investigation
- E. Extended response

Correct Answer: BDE

QUESTION 2

Refer to the exhibit.

EVENT EXCEPTIONS

Exceptions for event **44875**

Exception 1 +

Created from Raw Item **641717447** of event **44857**
 Last updated at 10-Dec-2021, 22:52 By FortinetCloudServices

Collector groups

All groups

Destinations

All destinations

Users

All users

Triggered Rules:

▸ File Encryptor ⓘ

.....

FortinetCloudServices at 10-Dec-2021, 22:52:59
 The file Update.exe is classified as Good. On the device "C8092231196"

Remote Exception

◆ All the Raw Data items are covered
Save Changes
Cancel

Based on the event exception shown in the exhibit which two statements about the exception are true? (Choose two)

- A. A partial exception is applied to this event
- B. FCS playbooks is enabled by Fortinet support
- C. The exception is applied only on device C8092231196
- D. The system owner can modify the trigger rules parameters

Correct Answer: AC

QUESTION 3

Refer to the exhibit.

TestApplication.exe.exe (3 events) Malicious 15-Feb-2022, 13:31:39

5894314 R2D2-kvm63 TestApplication.exe.exe Malicious 8.8.8.8 15-Feb-2022, 13:31:39 15-Feb-2022, 13:31:39

Property	Value
Logged-in User:	R2D2-KVM63\fortinet
Process owner:	R2D2-KVM63\fortinet
Certificate:	Unsigned
Process path:	C:\Users\fortinet\Desktop\

CLASSIFICATION DETAILS

Malicious Fortinet

Threat name: Unknown
Threat family: Unknown
Threat type: Unknown

History

Malicious, by Fortinet, on 15-Feb-2022, 13:31:41

Triggered Rules

- Exfiltration Prevention
 - Invalid Checksum - Connection Attempt from Application wi...
 - Malicious File Detected
 - Suspicious Packer - Activity by an Application packed by a S...
 - Writeable Code - Identified an Executable with Writable Code

TestApplication.exe.exe (3 events) Malicious

5894314 R2D2-kvm63 TestApplication.exe.exe Malicious

Property	Value
Logged-in User:	R2D2-KVM63\fortinet
Process owner:	R2D2-KVM63\fortinet
Certificate:	Unsigned
Process path:	C:\Users\fortinet\Desktop\

15-Feb-2022, 13:31:39

8.8.8.8 15-Feb-2022, 13:31:39 15-Feb-2022, 13:31:39

CLASSIFICATION DETAILS

Malicious Fortinet

Threat name: Unknown
Threat family: Unknown
Threat type: Unknown

History

Malicious, by Fortinet, on 15-Feb-2022, 13:31:41

Triggered Rules

- Exfiltration Prevention
 - Invalid Checksum - Connection Attempt from Application wi...
 - Malicious File Detected
 - Suspicious Packer - Activity by an Application packed by a S...
 - Writeable Code - Identified an Executable with Writable Code

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

- A. The NGAV policy has blocked TestApplication.exe
- B. TestApplication.exe is sophisticated malware
- C. The user was able to launch TestApplication.exe
- D. FCS classified the event as malicious

Correct Answer: BC

QUESTION 4

Refer to the exhibits.

Enable/Disable ▾ Isolate ▾ Export ▾ Uninstall

DEVICE NAME	LAST LOGGED	OS	IP
C8092231196	... 1196\Administrator	Windows Server 2016 Standard Evaluation	10.160.6.110

Search Collectors or Gro ▾ Q

MAC ADDRESS	VERSION	STATE	LAST SEEN
00-50-56-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
```

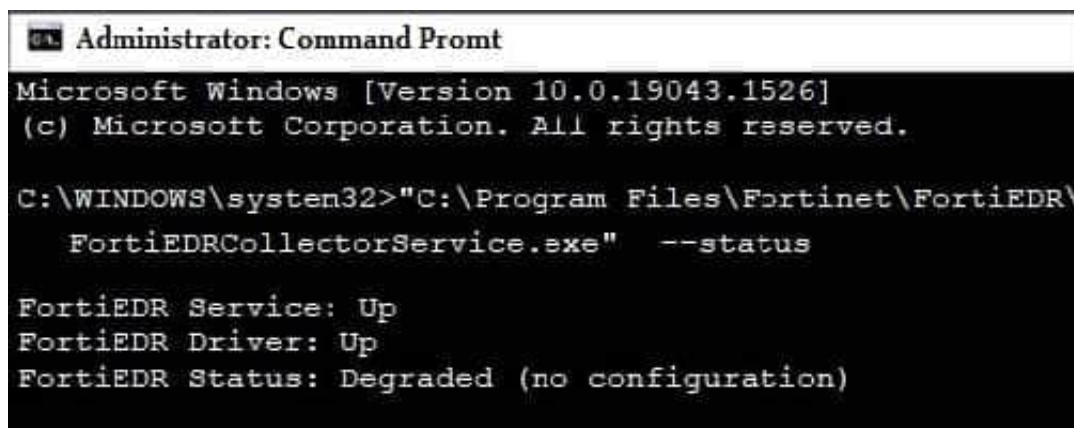
The exhibits show the collector state and active connections. The collector is unable to connect to aggregator IP address 10.160.6.100 using default port. Based on the netstat command output what must you do to resolve the connectivity issue?

- 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

Correct Answer: B

QUESTION 5

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

Correct Answer: BC

[Latest NSE5_EDR-5.0 Dumps](#)

[NSE5_EDR-5.0 Practice Test](#)

[NSE5_EDR-5.0 Braindumps](#)