# 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.passapply.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**

An administrator finds that a newly installed collector does not display on the INVENTORY tab in the central manager.

What two troubleshooting steps must the administrator perform? (Choose two.)

A. Export the collector logs from the central manager.

B. Verify the central manager has connectivity to FCS.

C. Verify TCP ports 8081 and 555 are open.

D. Check if the FortiEDR services are running on the collector device.

Correct Answer: CD

**QUESTION 2**

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
Logged-in User:
Process owner:
Certificate:
Process path:
R2D2-KVM63\fortinet
R2D2-KVM63\fortinet
Unsigned
C:\Users\fortinet\Desktc
CLASSIFICATION DETAILS
Malicious
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
Logged-in User:
Process owner:
Certificate:
Process path:
R2D2-KVM63\fortinet
R2D2-KVM63\fortinet
Unsigned
C:\Users\fortinet\Desktc


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
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 3**

Which two criteria are requirements of integrating FortiEDR into the Fortinet Security Fabric? (Choose two.)

A. Core with Core only functionality

B. A Forensics add-on license

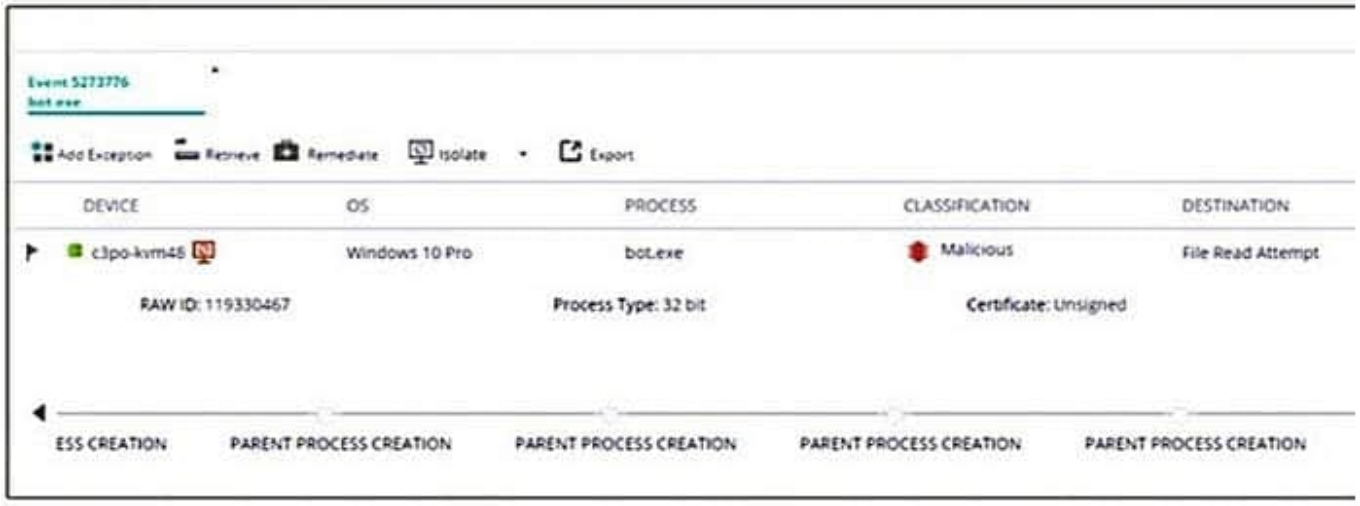
C. Central Manager connected to FCS

D. A valid API user with access to connectors

Correct Answer: CD

**QUESTION 4**

Exhibit.





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 m the stacks view

C. The device has been isolated

D. The exfiltration prevention policy has blocked this event

Correct Answer: BC

**QUESTION 5**

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

Correct Answer: A

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf