NSE5_EDR-5.0$^{Q\&As}$

Fortinet NSE 5 - FortiEDR 5.0

Pass Fortinet NSE5_EDR-5.0 Exam with 100% Guarantee

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

QUESTION 1

Which two types of traffic are allowed while the device is in isolation mode? (Choose two.)

A. Outgoing SSH connections

B. HTTP sessions

C. ICMP sessions D. Incoming RDP connections

Correct Answer: CD

QUESTION 2

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

A. FortiNAC

B. FortiGate

C. FortiSiem

D. FortiSandbox

Correct Answer: AB

QUESTION 3

When installing a FortiEDR collector, why is a `Registration Password\\' for collectors needed?

A. To restrict installation and uninstallation of collectors

B. To verify Fortinet support request

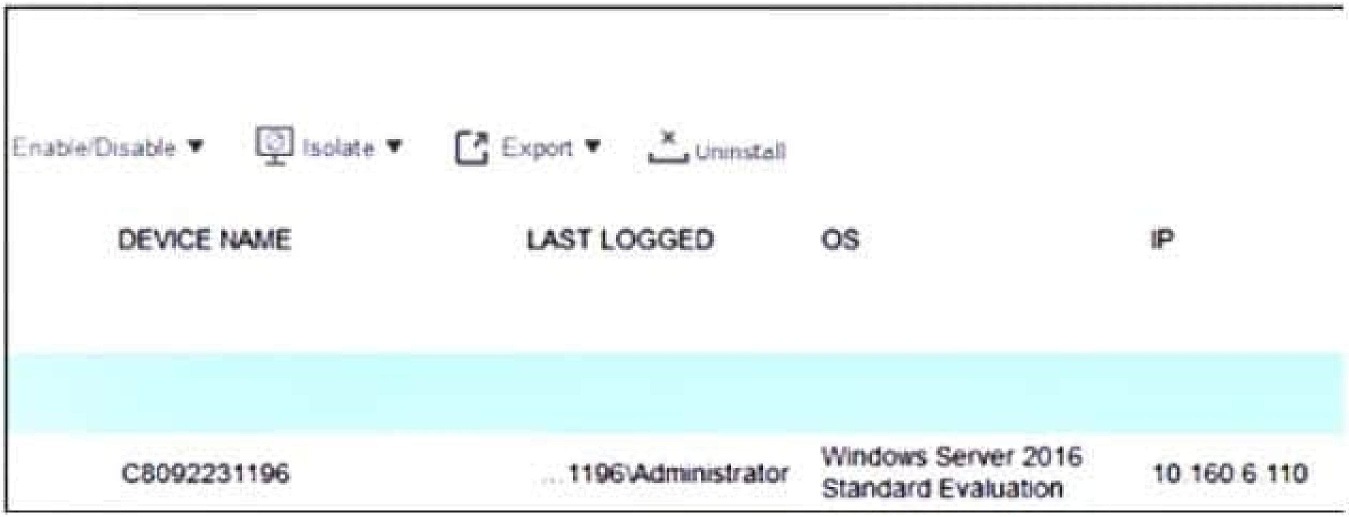
C. To restrict access to the management console

D. To verify new group assignment

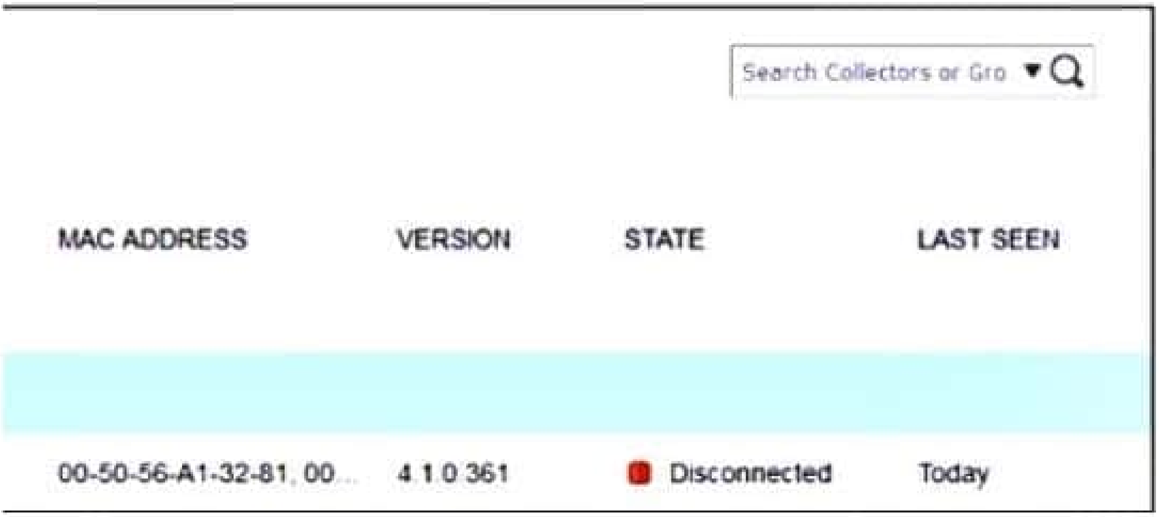
Correct Answer: A

QUESTION 4

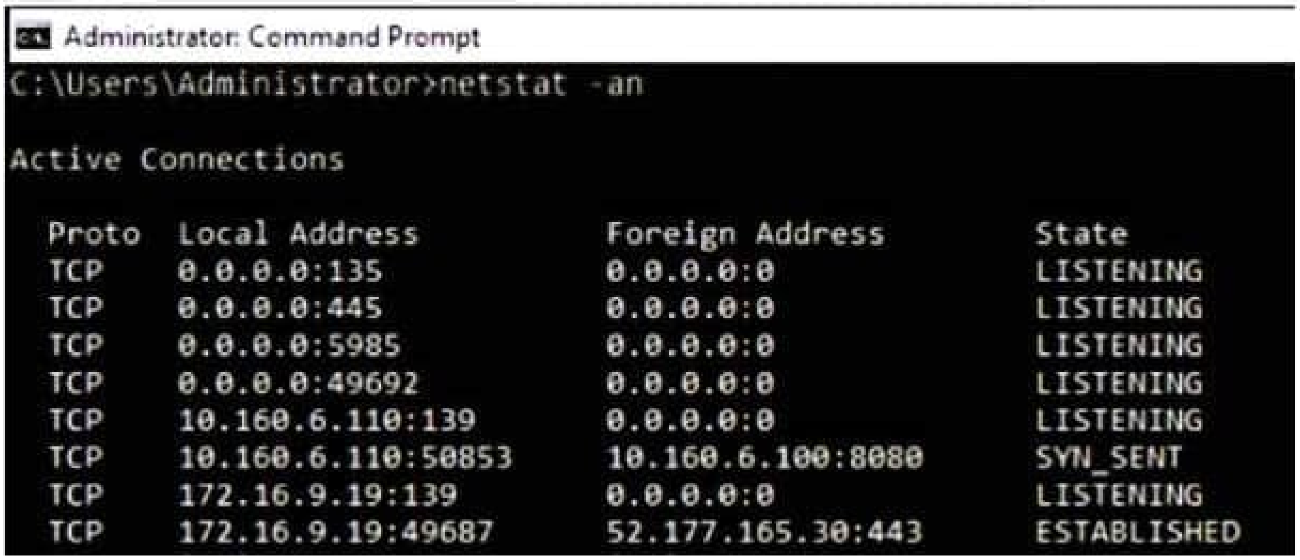
Refer to the exhibits.



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



MAC ADDRESS	VERSION	STATE	LAST SEEN
00-50-56-A1-32-81, 00...	4.1.0.361	● Disconnected	Today



```
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

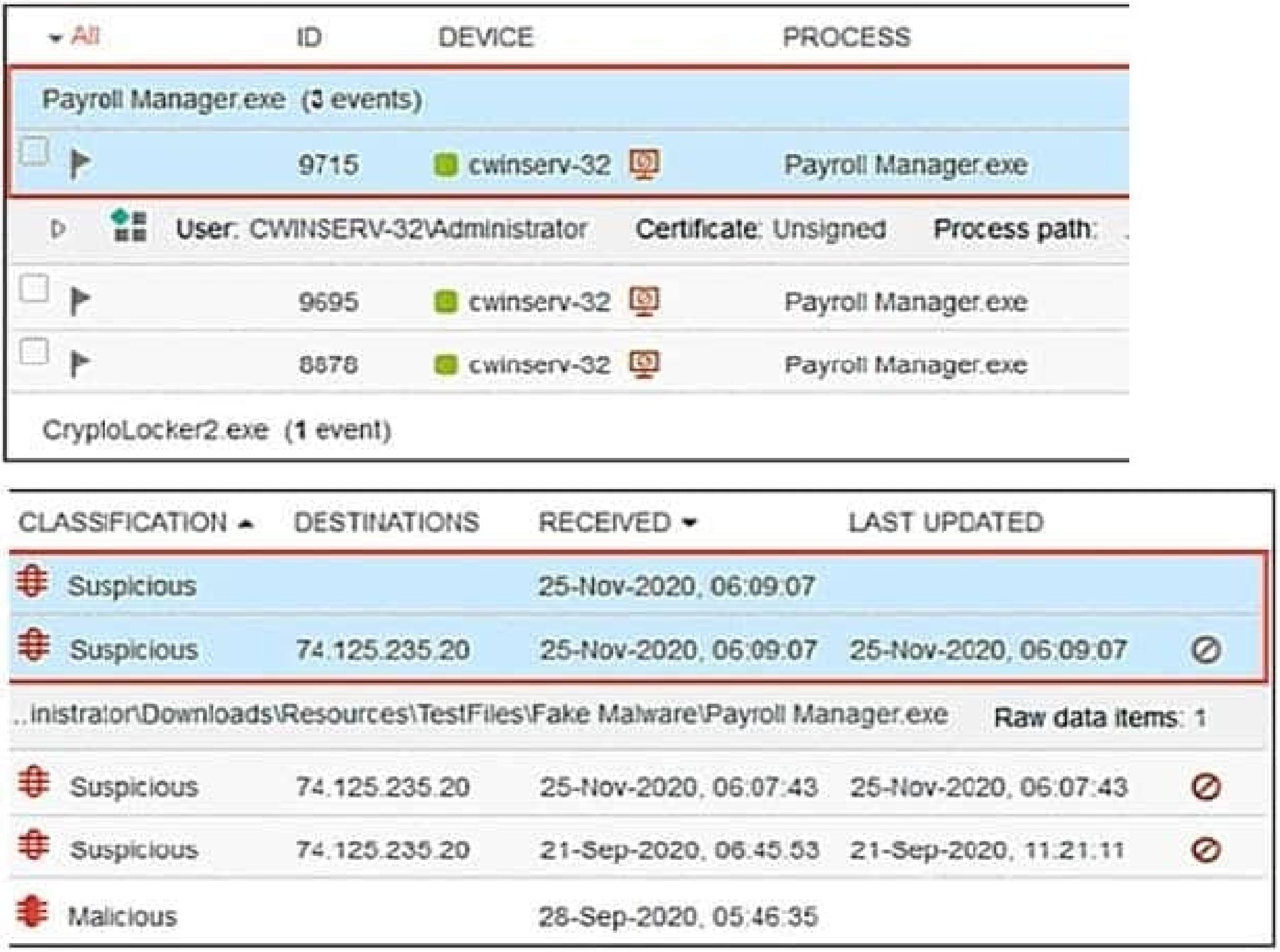
D. Reinstall collector agent and use port 6514

Correct Answer: B

QUESTION 5

Refer to the exhibit.

The exhibit shows an event viewer.



▾ All	ID	DEVICE	PROCESS
Payroll Manager.exe (3 events)			
□ ⚑	9715	🟩 cwinserv-32	Payroll Manager.exe
▷ User: CWINSERV-32\Administrator		Certificate: Unsigned	Process path:
□ ⚑	9695	🟩 cwinserv-32	Payroll Manager.exe
□ ⚑	8878	🟩 cwinserv-32	Payroll Manager.exe
CryploLocker2.exe (1 event)			

CLASSIFICATION ▴	DESTINATIONS	RECEIVED ▾	LAST UPDATED	
Suspicious		25-Nov-2020, 06:09:07		
Suspicious	74.125.235.20	25-Nov-2020, 06:09:07	25-Nov-2020, 06:09:07	⊘
..inistrator\Downloads\Resources\TestFiles\Fake Malware\Payroll Manager.exe			Raw data items: 1	
Suspicious	74.125.235.20	25-Nov-2020, 06:07:43	25-Nov-2020, 06:07:43	⊘
Suspicious	74.125.235.20	21-Sep-2020, 06:45:53	21-Sep-2020, 11:21:11	⊘
Malicious		28-Sep-2020, 05:46:35		

What is true about the Payroll Manager.exe event?

A. An event has not been handled by a console admin

B. An event has been deleted

C. A rule assigned action is set to block but the policy is in simulation mode

D. An event has been handled by the communication control policy

Correct Answer: C