NSE5_FCT-7.0Q&As

Fortinet NSE 5 - FortiClient EMS 7.0

Pass Fortinet NSE5_FCT-7.0 Exam with 100% Guarantee

QUESTION 1

Which component or device shares device status information through ZTNA telemetry?

A. FortiClient

B. FortiGate

C. FortiGate Access Proxy

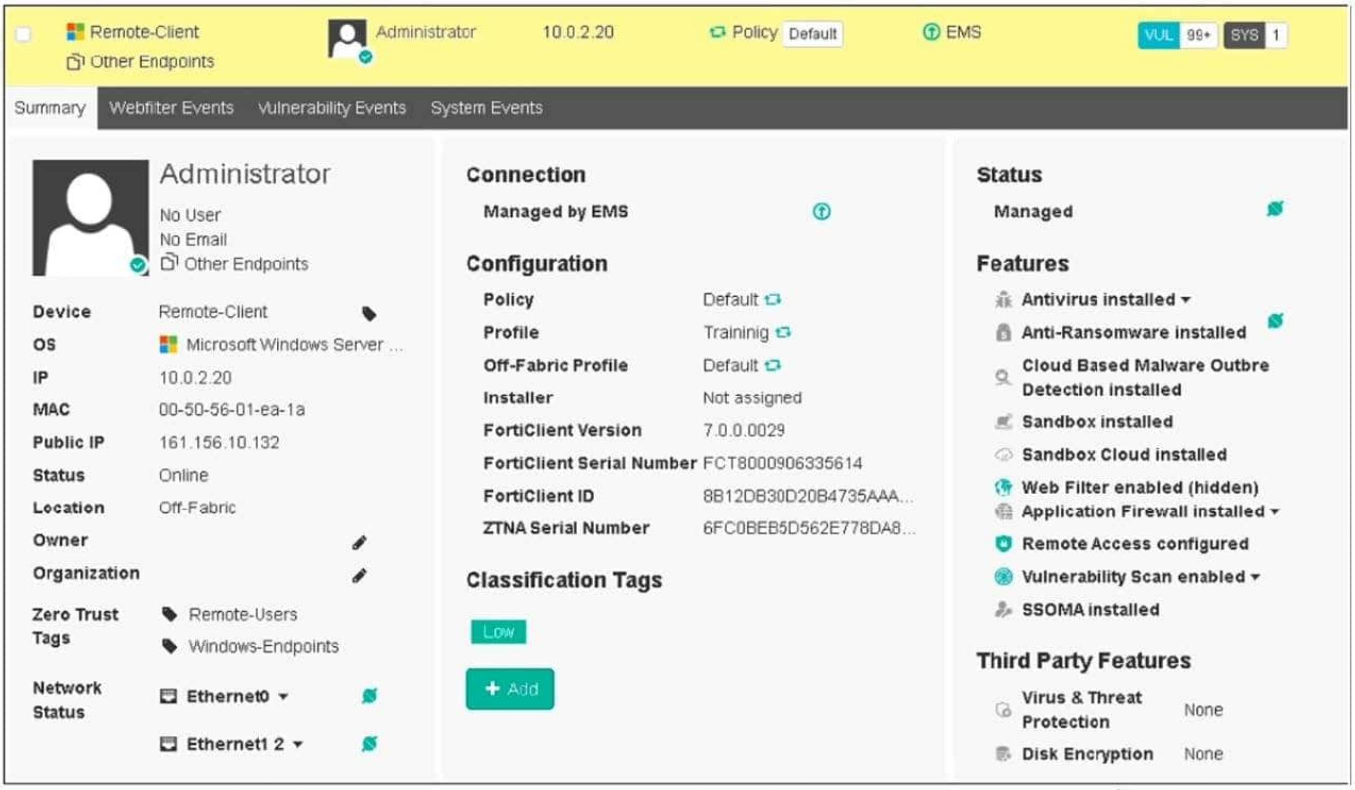
D. FortiClient EMS

Correct Answer: A

FortiClient communicates directly with FortiClient EMS to continuously share device status information through ZTNA telemetry.

QUESTION 2

Refer to the exhibit, which shows the endpoint summary information on FortiClient EMS.



Administrator

No User
No Email
Other Endpoints

Device	Remote-Client
OS	Microsoft Windows Server ...
IP	10.0.2.20
MAC	00-50-56-01-ea-1a
Public IP	161.156.10.132
Status	Online
Location	Off-Fabric
Owner	
Organization	
Zero Trust Tags	Remote-Users Windows-Endpoints
Network Status	Ethernet0 Ethernet1 2

Connection

Managed by EMS

Configuration

Policy	Default
Profile	Traininig
Off-Fabric Profile	Default
Installer	Not assigned
FortiClient Version	7.0.0.0029
FortiClient Serial Number	FCT8000906335614
FortiClient ID	8B12DB30D20B4735AAA...
ZTNA Serial Number	6FC0BEB5D562E778DA8...

Classification Tags

Low

+ Add

Status

Managed

Features

- Antivirus installed
- Anti-Ransomware installed
- Cloud Based Malware Outbre Detection installed
- Sandbox installed
- Sandbox Cloud installed
- Web Filter enabled (hidden)
- Application Firewall installed
- Remote Access configured
- Vulnerability Scan enabled
- SSOMA installed

Third Party Features

Virus & Threat Protection	None
Disk Encryption	None

What two conclusions can you make based on the Remote-Client status shown above? (Choose two.)

A. The endpoint is classified as at risk.

B. The endpoint has been assigned the Default endpoint policy.

C. The endpoint is configured to support FortiSandbox.

D. The endpoint is currently off-net.

Correct Answer: BD

QUESTION 3

An administrator is required to maintain a software vulnerability on the endpoints, without showing the feature on the FortiClient dashboard. What must the administrator do to achieve this requirement?

A. Disable select the vulnerability scan feature in the deployment package

B. Use the default endpoint profile

C. Select the vulnerability scan feature in the deployment package, but disable the feature on the endpoint profile

D. Click the hide icon on the vulnerability scan tab

Correct Answer: D

QUESTION 4

Which three types of antivirus scans are available on FortiClient? (Choose three)

A. Proxy scan

B. Full scan

C. Custom scan

D. Flow scan

E. Quick scan

Correct Answer: BCE

QUESTION 5

Which statement about FortiClient comprehensive endpoint protection is true?

A. It helps to safeguard systems from email spam

B. It helps to safeguard systems from data loss.

C. It helps to safeguard systems from DDoS.

D. It helps to safeguard systems from advanced security threats, such as malware.

Correct Answer: D

FortiClient provides comprehensive endpoint protection for your Windows- based, Mac-based, and Linuxbased desktops, laptops, file servers, and mobile devices such as iOS and Android. It helps you to safeguard your systems with advanced security technologies, all of which you can manage from a single management console.