NSE5_FCT-7.0 Q&As

Fortinet NSE 5 - FortiClient EMS 7.0

Pass Fortinet NSE5_FCT-7.0 Exam with 100% Guarantee

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

https://www.leads4pass.com/nse5_fct-7-0.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 component or device shares ZTNA tag information through Security Fabric integration?

A. FortiGate

B. FortiGate Access Proxy

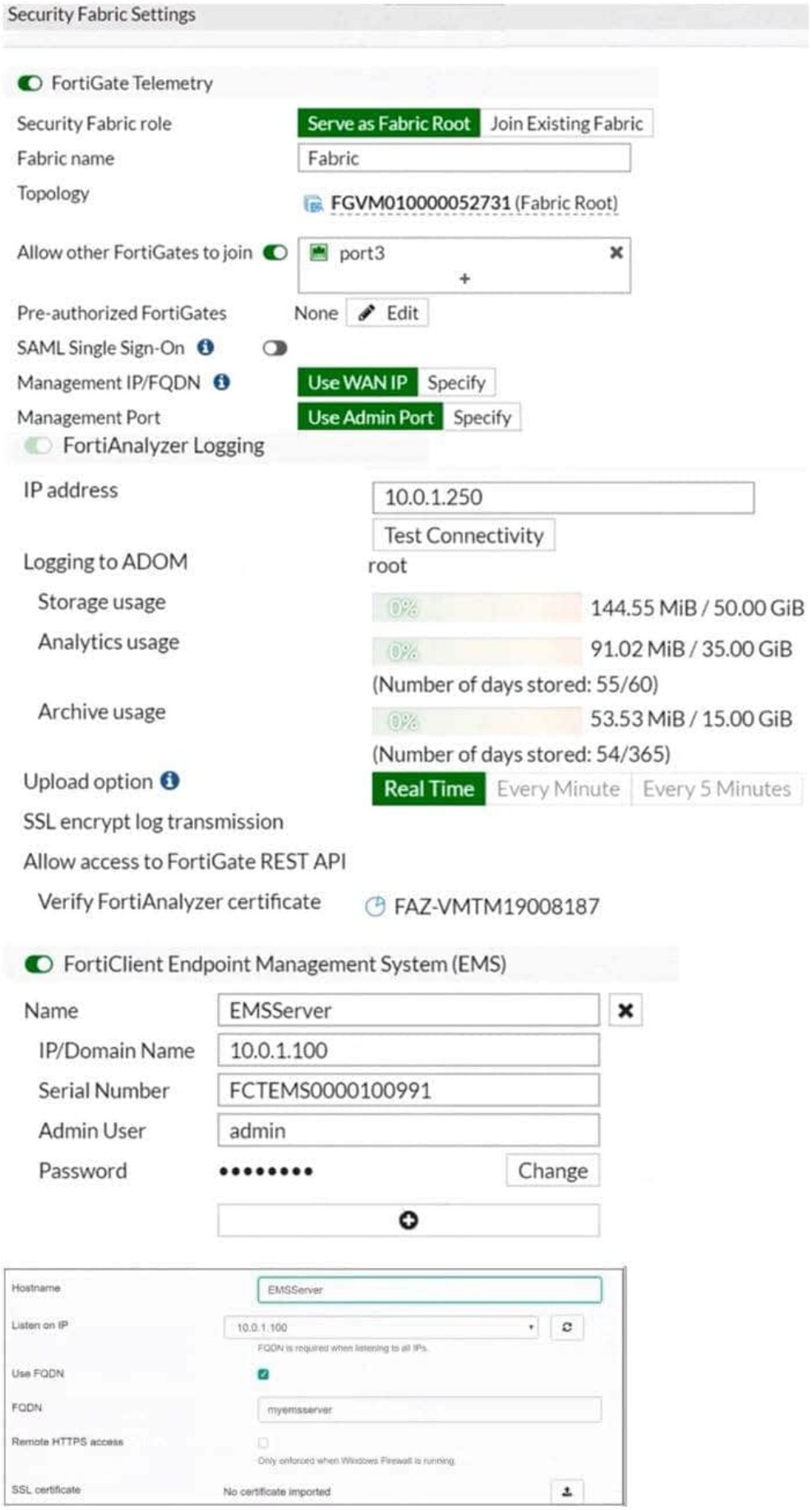
C. FortiClient

D. FortiClient EMS

Correct Answer: D

QUESTION 2

Refer to the exhibits.


Security Fabric Settings
FortiGate Telemetry
Security Fabric role
Serve as Fabric Root
Join Existing Fabric
Fabric name
Fabric
Topology
FGVM010000052731 (Fabric Root)
Allow other FortiGates to join
port3
Pre-authorized FortiGates
None
Edit
SAML Single Sign-On
Management IP/FQDN
Use WAN IP
Specify
Management Port
Use Admin Port
Specify
FortiAnalyzer Logging
IP address
10.0.1.250
Test Connectivity
Logging to ADOM
root
Storage usage
0%
144.55 MiB / 50.00 GiB
Analytics usage
0%
91.02 MiB / 35.00 GiB
(Number of days stored: 55/60)
Archive usage
0%
53.53 MiB / 15.00 GiB
(Number of days stored: 54/365)
Upload option
Real Time
Every Minute
Every 5 Minutes
SSL encrypt log transmission
Allow access to FortiGate REST API
Verify FortiAnalyzer certificate
FAZ-VMTM19008187
FortiClient Endpoint Management System (EMS)
Name
EMSServer
IP/Domain Name
10.0.1.100
Serial Number
FCTEMS0000100991
Admin User
admin
Password
Change

Hostname
EMSServer
Listen on IP
10.0.1.100
FQDN is required when listening to all IPs.
Use FQDN
FQDN
myemsserver
Remote HTTPS access
Only enforced when Windows Firewall is running.
SSL certificate
No certificate imported

Based on the FortiGate Security Fabric settings shown in the exhibits, what must an administrator do on the EMS server to successfully quarantine an endpoint. when it is detected as a compromised host (IoC)?

A. The administrator must enable remote HTTPS access to EMS.

B. The administrator must enable FQDN on EMS.

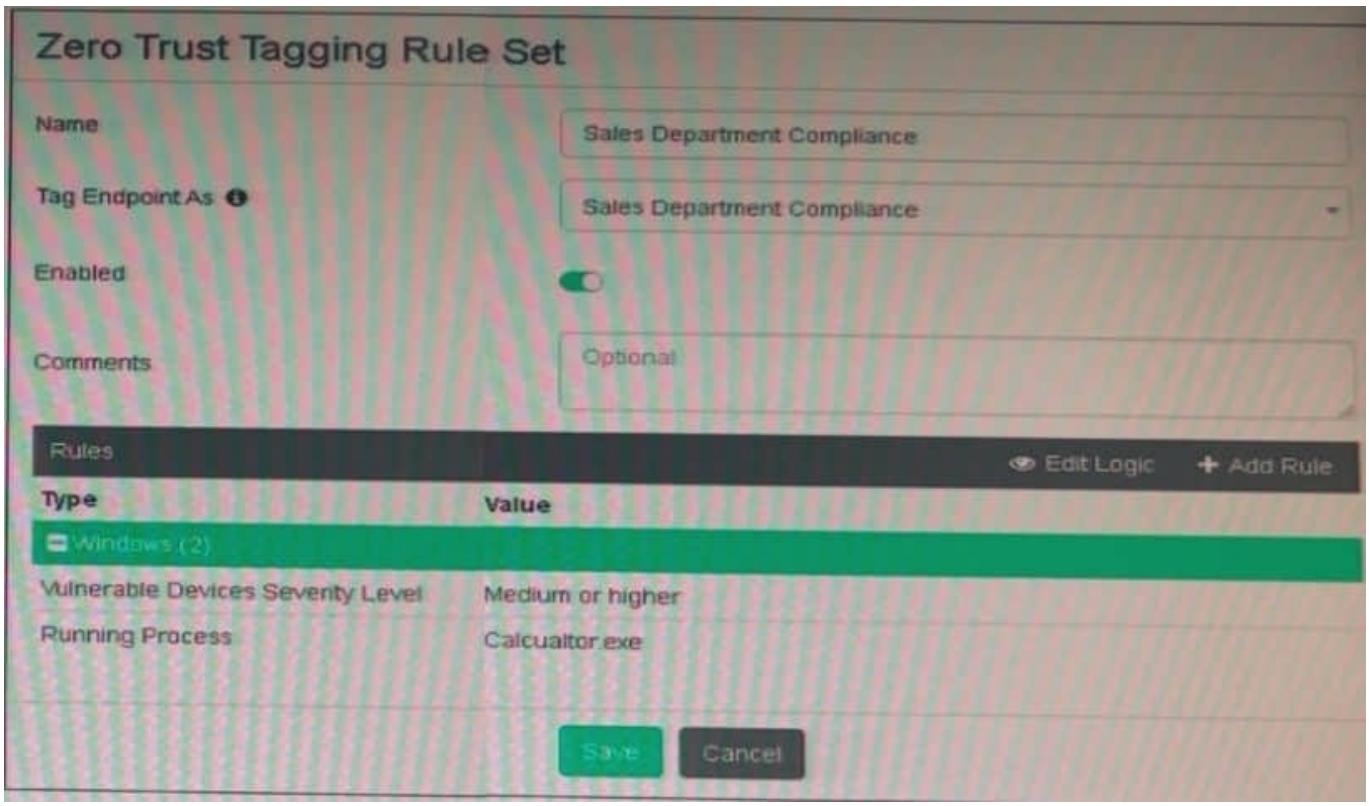
C. The administrator must authorize FortiGate on FortiAnalyzer.

D. The administrator must enable SSH access to EMS.

Correct Answer: A

QUESTION 3

Refer to the exhibit.



Based on the settings shown in the exhibit, which two actions must the administrator take to make the endpoint compliant? (Choose two.)

A. Enable the webfilter profile

B. Integrate FortiSandbox for infected file analysis

C. Patch applications that have vulnerability rated as high or above

D. Run Calculator application on the endpoint

Correct Answer: CD

QUESTION 4

An administrator wants to simplify remote access without asking users to provide user credentials. Which access control method provides this solution"?

A. SSL VPN

B. ZTNA full mode

C. L2TP

D. ZTNA IP/MAC filtering mode

Correct Answer: B

QUESTION 5

Which two statements are true about the ZTNA rule? (Choose two.)

A. It enforces access control

B. It redirects the client request to the access proxy

C. It defines the access proxy

D. It applies security profiles to protect traffic

Correct Answer: AD

"A ZTNA rule is a proxy policy used to enforce access control. ZTNA tags or tag groups can be defined to enforce zero trust role based access. Security profiles can be configured to protect this traffic."

"ZTNA rules help control access by defining users and ZTNA tags to perform user authentication and security posture checks. And just like firewall policies, you can control the source and destination addresses, and apply appropriate security

profiles to scan the traffic."

https://docs.fortinet.com/document/fortigate/7.0.0/ztna-deployment/899992/configuring-ztna-rules-to-control-access