NSE5_FCT-6.2 Q&As

Fortinet NSE 5 - FortiClient EMS 6.2

Pass Fortinet NSE5_FCT-6.2 Exam with 100% Guarantee

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

https://www.pass2lead.com/nse5_fct-6-2.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 deploys a FortiClient installation through the Microsoft AD group policy After installation is

complete all the custom configuration is missing.

What could have caused this problem?

A. The FortiClient exe file is included in the distribution package

B. The FortiClient MST file is missing from the distribution package

C. FortiClient does not have permission to access the distribution package.

D. The FortiClient package is not assigned to the group

Correct Answer: D

QUESTION 2

An administrator installs FortiClient EMS in the enterprise. Which component is responsible for enforcing endpoint protection in managed mode?

A. FortiClient

B. FortiClient vulnerability scan

C. FortiClient EMS

D. FortiClient EMS database

Correct Answer: A

QUESTION 3

Refer to the exhibit.

Based on the CLI output from FortiGate. which statement is true?

A. FortiGate is configured to pull user groups from FortiClient EMS

B. FortiGate is configured with local user group

C. FortiGate is configured to pull user groups from FortiAuthenticator

D. FortiGate is configured to pull user groups from AD Server.

Correct Answer: A

QUESTION 4

What action does FortiClient anti-exploit detection take when it detects exploits?

A. Terminates the compromised application process

B. Patches the compromised application process

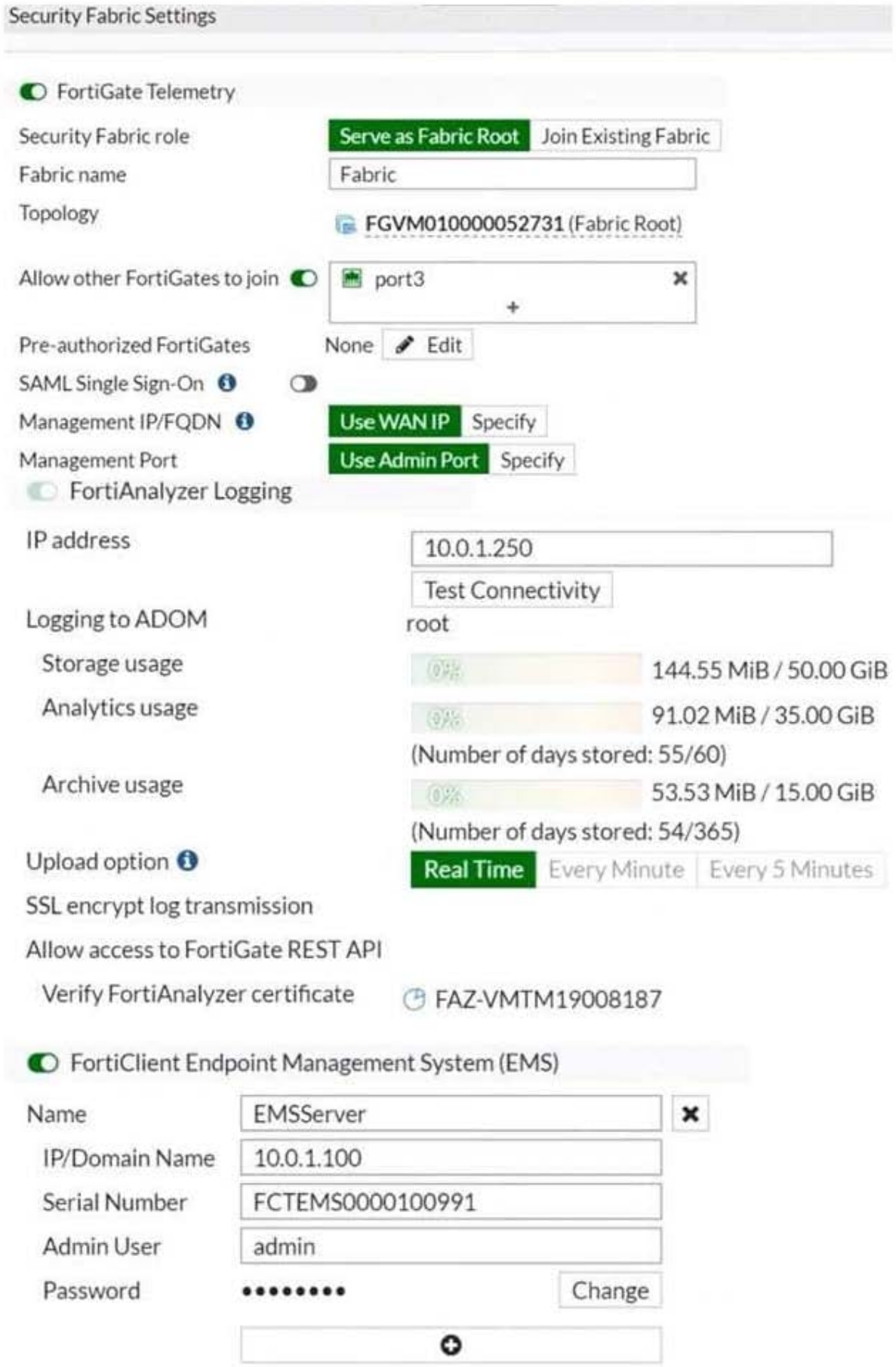
C. Blocks memory allocation to the compromised application process

D. Deletes the compromised application process

Correct Answer: A

QUESTION 5

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
144.55 MiB / 50.00 GiB
Analytics usage
91.02 MiB / 35.00 GiB
(Number of days stored: 55/60)
Archive usage
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

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