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.geekcert.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 statement about FortiClient enterprise management server is true?

A. It provides centralized management of FortiGate devices.

B. lt provides centralized management of multiple endpoints running FortiClient software.

C. It provides centralized management of FortiClient Android endpoints only.

D. It provides centralized management of Chromebooks running real-time protection

Correct Answer: B

QUESTION 2

What is the function of the quick scan option on FortiClient?

A. It scans programs and drivers that are currently running, for threats.

B. It allows users to select a specific file folder on their local hard disk drive (HDD), to scan for threats.

C. It performs a full system scan including all files, executable files, DLLs, and drivers for threats.

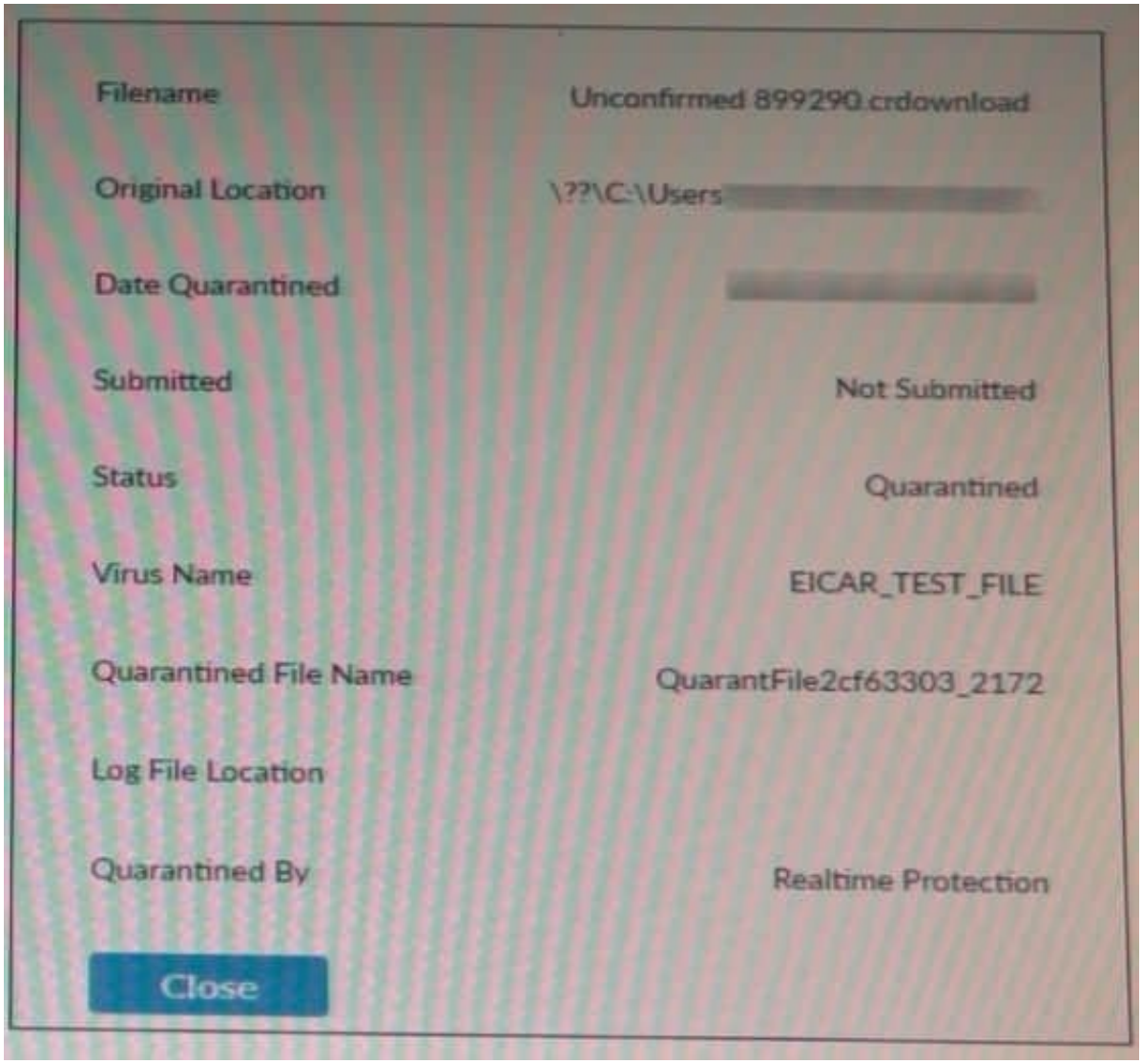
D. It scans executable files, DLLs, and drivers that are currently running, for threats.

Correct Answer: D

Quick Scan scans only executable files, DLLs, and drivers that are currently running for threats.

QUESTION 3

Refer to the exhibit.



Based on the FortiClient log details shown in the exhibit, which two statements are true? (Choose two.)

A. The file status is Quarantined

B. The filename is sent to ForuSandbox for further inspection.

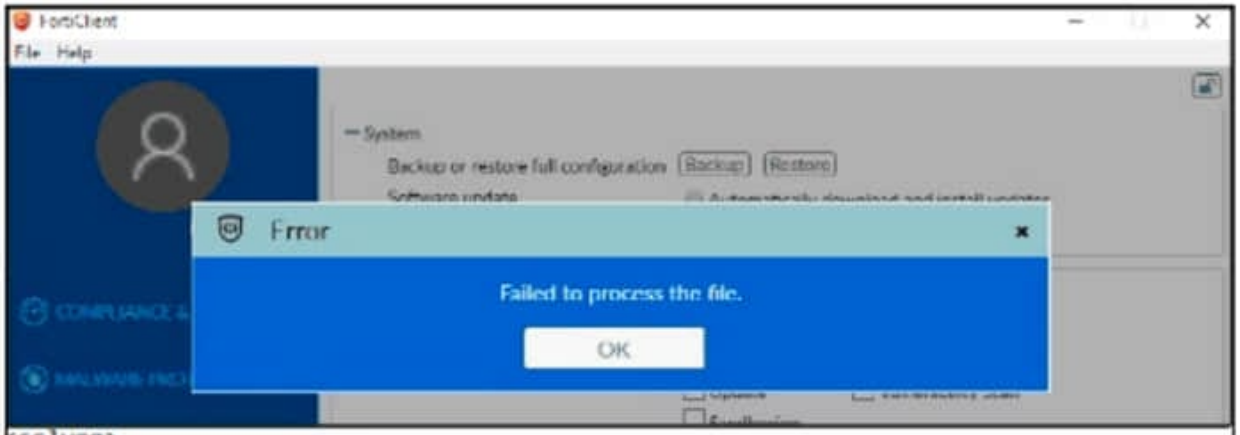
C. The file location IS \??\D:\Users\.

D. The filename is Unconfirmed 899290 .crdownload.

Correct Answer: AD

QUESTION 4

Refer to the exhibit.




```
<sslvpn>
    <options>
        <enabled>1</enabled>
        <prefer_sslvpn_dns>1</prefer_sslvpn_dns>
        <dnscache_service_control>0</dnscache_service_control>
        <use_legacy_ssl_adapter>0</use_legacy_ssl_adapter>
        <preferred_dtls_tunnel>0</preferred_dtls_tunnel>
        <no_dhcp_server_route>0</no_dhcp_server_route>
        <no_dns_registration>0</no_dns_registration>
        <disallow_invalid_server_certificate>0</disallow_invalid_server_certificate>
    </options>
    <connections>
        <connection>
            <name>Student-SSLVPN</name>
            <description>SSL VPN to Fortigate</description>
            <server>10.0.0.254:10443</server>
            <username />
            <single_user_mode>0</single_user_mode>
            <ui>
                <show_remember_password>0</show_remember_password>
            </ui>
            <password />
            <prompt_username>1</prompt_username>
            <on_connect>
                <script>
                    <os>windows</os>
                    <script>
                        <![CDATA[]]>
                    </script>
                </script>
            </on_connect>
            <on_disconnect>
                <script>
                    <os>windows</os>
                    <script>
                        <![CDATA[]]>
                    </script>
                </script>
            </on_disconnect>
        </connections>
</sslvpn>
<ipsecvpn>
```

An administrator has restored the modified XML configuration file to FortiClient and sees the error shown in the exhibit.

Based on the XML settings shown in the exhibit, what must the administrator do to resolve the issue with the XML configuration file?

A. The administrator must resolve the XML syntax error.

B. The administrator must use a password to decrypt the file

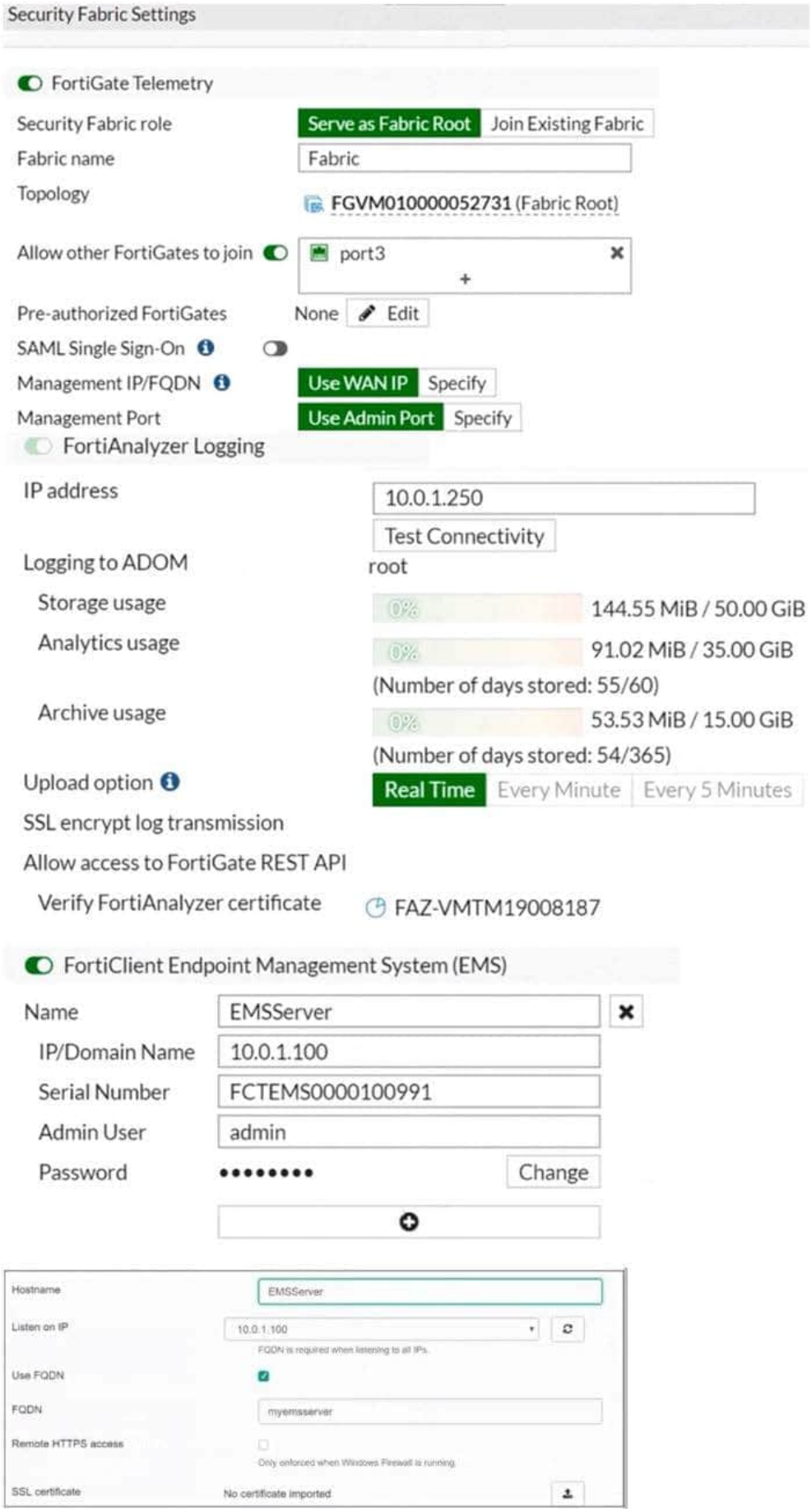
C. The administrator must change the file size

D. The administrator must save the file as FortiClient-config conf.

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
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