Free Questions for NSE5_FCT-7.0 by actualtestdumps

Shared by Robinson on 27-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

A- Proxy scan

B- Full scan

C- Custom scan

D- Flow scan

E- Quick scan

Answer:

B, C, E

Question 2

Question Type: MultipleChoice

An administrator installs FortiClient on Windows Server.

What is the default behavior of real-time protection control?

Options:

A- Real-time protection must update AV signature database

B- Real-time protection sends malicious files to FortiSandbox when the file is not detected locally

C- Real-time protection is disabled

D- Real-time protection must update the signature database from FortiSandbox

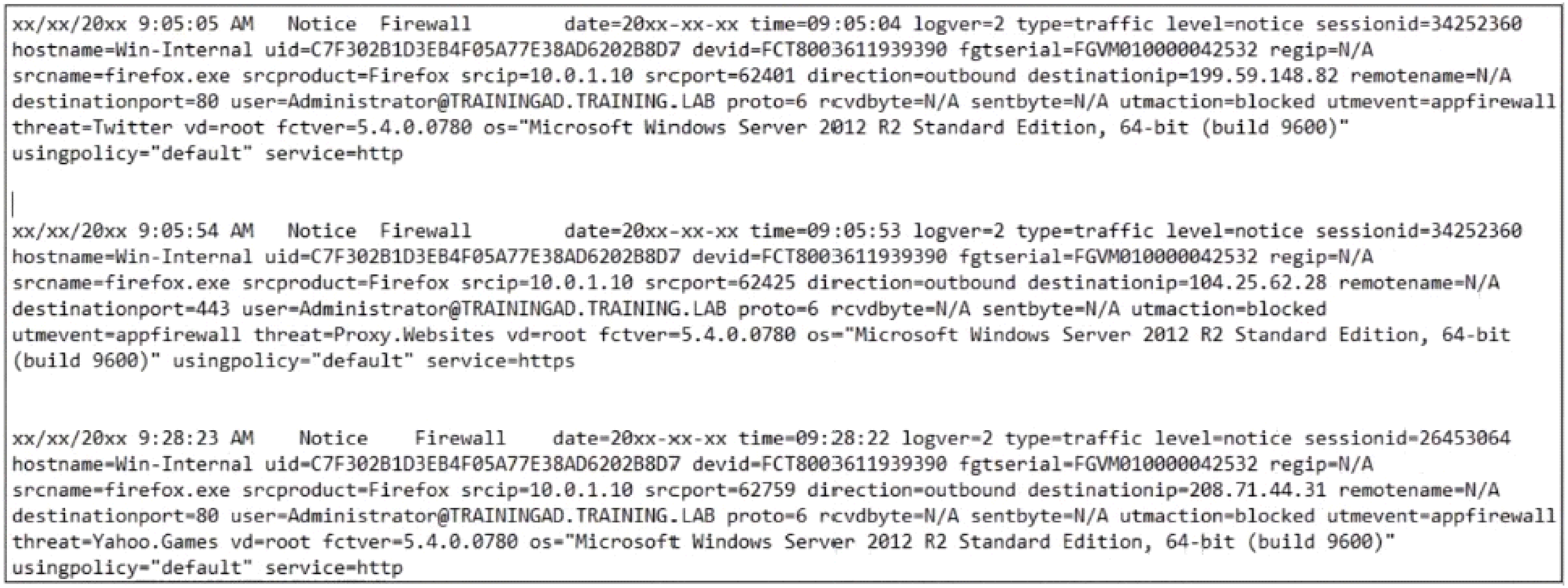
Answer:

C

Question 3

Question Type: **MultipleChoice**

Refer to the exhibit.



```
xx/xx/20xx 9:05:05 AM   Notice  Firewall        date=20xx-xx-xx time=09:05:04 logver=2 type=traffic level=notice sessionid=34252360
hostname=Win-Internal uid=C7F302B1D3EB4F05A77E38AD6202B8D7 devid=FCT8003611939390 fgtserial=FGVM010000042532 regip=N/A
srcname=firefox.exe srcproduct=Firefox srcip=10.0.1.10 srcport=62401 direction=outbound destinationip=199.59.148.82 remotename=N/A
destinationport=80 user=Administrator@TRAININGAD.TRAINING.LAB proto=6 rcvdbyte=N/A sentbyte=N/A utmaction=blocked utmevent=appfirewall
threat=Twitter vd=root fctver=5.4.0.0780 os="Microsoft Windows Server 2012 R2 Standard Edition, 64-bit (build 9600)"
usingpolicy="default" service=http

|
xx/xx/20xx 9:05:54 AM   Notice  Firewall        date=20xx-xx-xx time=09:05:53 logver=2 type=traffic level=notice sessionid=34252360
hostname=Win-Internal uid=C7F302B1D3EB4F05A77E38AD6202B8D7 devid=FCT8003611939390 fgtserial=FGVM010000042532 regip=N/A
srcname=firefox.exe srcproduct=Firefox srcip=10.0.1.10 srcport=62425 direction=outbound destinationip=104.25.62.28 remotename=N/A
destinationport=443 user=Administrator@TRAININGAD.TRAINING.LAB proto=6 rcvdbyte=N/A sentbyte=N/A utmaction=blocked
utmevent=appfirewall threat=Proxy.Websites vd=root fctver=5.4.0.0780 os="Microsoft Windows Server 2012 R2 Standard Edition, 64-bit
(build 9600)" usingpolicy="default" service=https


xx/xx/20xx 9:28:23 AM    Notice    Firewall    date=20xx-xx-xx time=09:28:22 logver=2 type=traffic level=notice sessionid=26453064
hostname=Win-Internal uid=C7F302B1D3EB4F05A77E38AD6202B8D7 devid=FCT8003611939390 fgtserial=FGVM010000042532 regip=N/A
srcname=firefox.exe srcproduct=Firefox srcip=10.0.1.10 srcport=62759 direction=outbound destinationip=208.71.44.31 remotename=N/A
destinationport=80 user=Administrator@TRAININGAD.TRAINING.LAB proto=6 rcvdbyte=N/A sentbyte=N/A utmaction=blocked utmevent=appfirewall
threat=Yahoo.Games vd=root fctver=5.4.0.0780 os="Microsoft Windows Server 2012 R2 Standard Edition, 64-bit (build 9600)"
usingpolicy="default" service=http
```

Based on the FortiClient logs shown in the exhibit which application is blocked by the application firewall?

Options:

A- Twitter

B- Facebook

C- Internet Explorer

D- Firefox

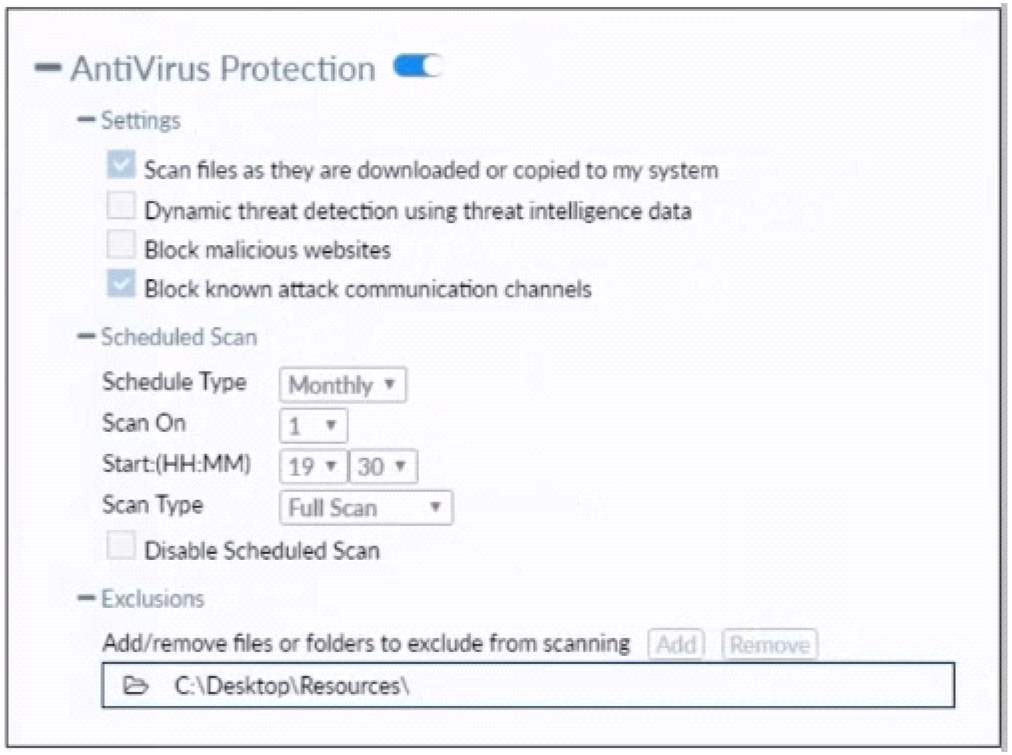
Answer:

D

Question 4

Question Type: MultipleChoice

Refer to the exhibit.



AntiVirus Protection

Settings

☑ Scan files as they are downloaded or copied to my system

□ Dynamic threat detection using threat intelligence data

□ Block malicious websites

☑ Block known attack communication channels

Scheduled Scan

Schedule Type	Monthly ▾
Scan On	1 ▾
Start:(HH:MM)	19 ▾ 30 ▾
Scan Type	Full Scan ▾

□ Disable Scheduled Scan

Exclusions

Add/remove files or folders to exclude from scanning

C:\Desktop\Resources\

Based on the settings shown in the exhibit which statement about FortiClient behavior is true?

Options:

A- FortiClient quarantines infected files and reviews later, after scanning them.

B- FortiClient blocks and deletes infected files after scanning them.

C- FortiClient scans infected files when the user copies files to the Resources folder

D- FortiClient copies infected files to the Resources folder without scanning them.

Answer:

A

Question 5

Question Type: **MultipleChoice**

Which statement about FortiClient enterprise management server is true?

Options:

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

Answer:

B

Question 6

Question Type: MultipleChoice

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

Options:

A- The administrator must use default endpoint profile

B- The administrator must not select the vulnerability scan feature in the deployment package.

C- The administrator must select the vulnerability scan feature in the deployment package, but disable the feature on the endpoint profile

D- The administrator must click the hide icon on the vulnerability scan tab

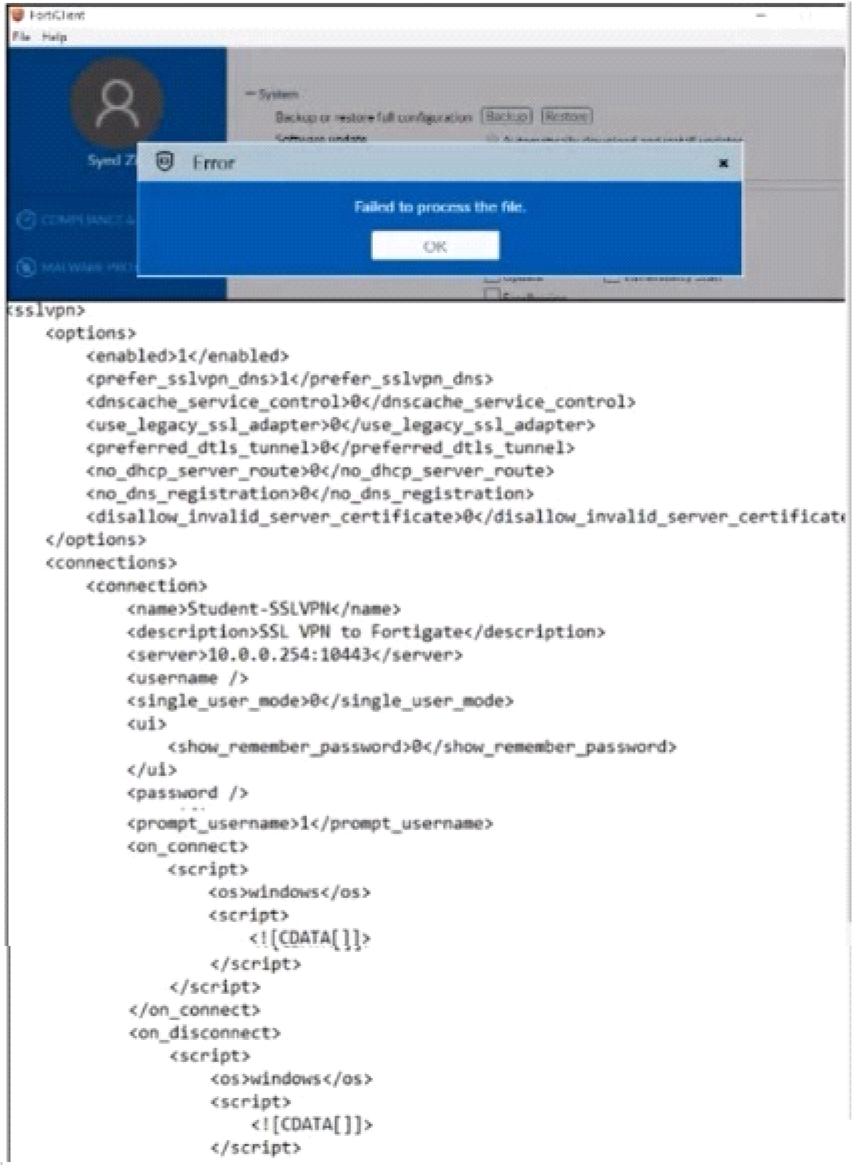
Answer:

C

Question 7

Question Type: **MultipleChoice**

Refer to the exhibit.



Failed to process the file.

```
<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>
```

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?

Options:

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.

Answer:

A

Question 8

Question Type: **MultipleChoice**

Which two VPN types can a FortiClient endpoint user inmate from the Windows command prompt? (Choose two)

Options:

A- L2TP

B- PPTP

C- IPSec

D- SSL VPN

Answer:

C, D

Question 9

Question Type: **MultipleChoice**

In a FortiSandbox integration, what does the remediation option do?

Options:

A- Wait for FortiSandbox results before allowing files

B- Exclude specified files

C- Alert and notify only

D- Deny access to a file when it sees no results

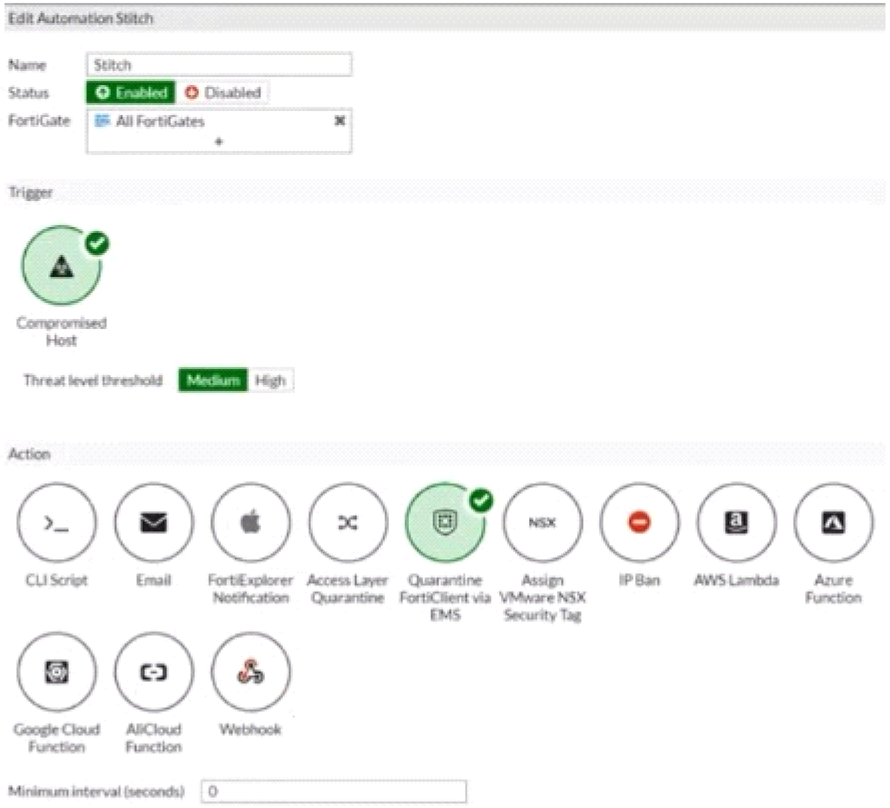
Answer:

A

Question 10

Question Type: **MultipleChoice**

Refer to the exhibit.


Edit Automation Stitch

Name: Stitch

Status: [✓ Enabled] Disabled

FortiGate: All FortiGates

Trigger

[✓ Compromised Host]

Threat level threshold: [✓ Medium] High

Action

Minimum interval (seconds): 0

Based on the Security Fabric automation settings, what action will be taken on compromised endpoints?

Options:

A- Endpoints will be quarantined through EMS

B- Endpoints will be banned on FortiGate

C- An email notification will be sent for compromised endpoints

D- Endpoints will be quarantined through FortiSwitch

Answer:

A

Question 11

Question Type: **MultipleChoice**

Which statement about FortiClient comprehensive endpoint protection is true?

Options:

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.

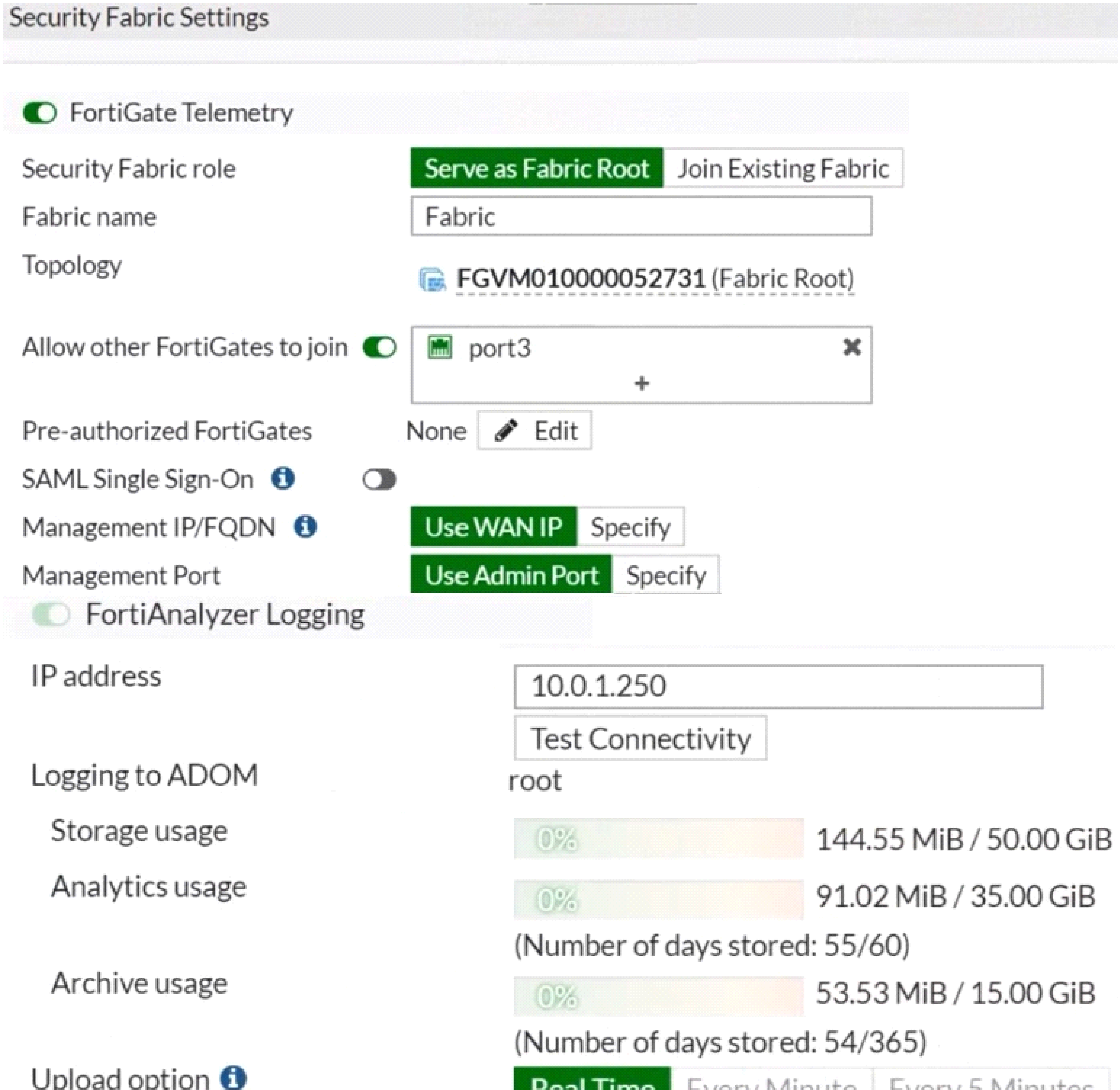
Answer:

D

Question 12

Question Type: MultipleChoice

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

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

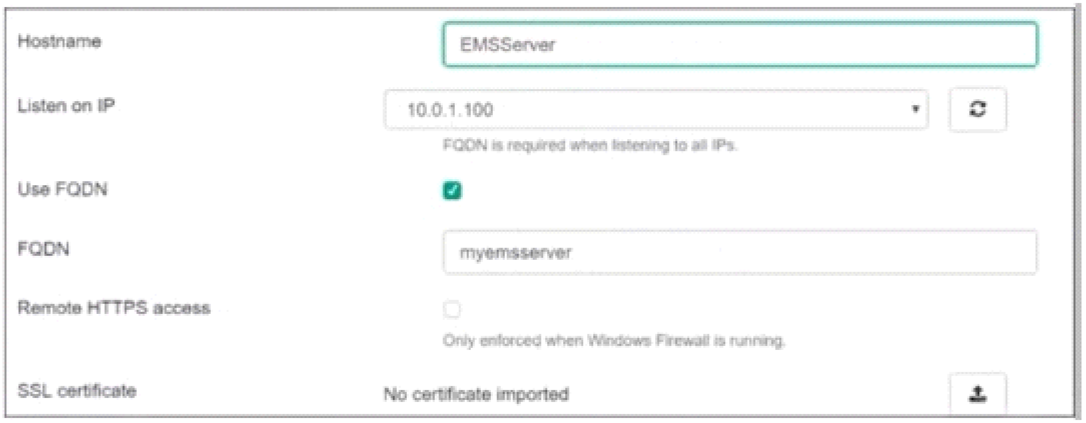
Logging to ADOM: root

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



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)?

Options:

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.

Answer:

A

20%
DISCOUNT