Free Questions for FCP_FCT_AD-7.2 by braindumpscollection

Shared by Mcknight on 03-06-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibit, which shows the Zero Trust Tagging Rule Set configuration.

Zero Trust Tagging Rule Set

Name: Compliance

Tag Endpoint As: Compliant

Enabled

Comments: Optional

Rules — Default Logic — + Add Rule

Type	Value
Windows (2)	
AntiVirus Software	1 AV Software is installed and running
OS Version	2 Windows Server 2012 R2 3 Windows 10

Rule Logic

(1 and 3) or 2 — Reset

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

Options:

A- The endpoint must satisfy that only Windows 10 is running.

B- The endpoint must satisfy that only AV software is installed and running.

C- The endpoint must satisfy that antivirus is installed and running and Windows 10 is running.

D- The endpoint must satisfy that only Windows Server 2012 R2 is running.

Answer:

C, D

Explanation:

Based on the Zero Trust Tagging Rule Set configuration shown in the exhibit:

The rule set includes two conditions:

AV Software is installed and running

OS Version is Windows Server 2012 R2 or Windows 10

The Rule Logic is specified as '(1 and 3) or 2,' meaning:

The endpoint must have antivirus software installed and running and must be running Windows 10.

Alternatively, the endpoint must be running Windows Server 2012 R2.

Therefore, the endpoint must satisfy either:

Antivirus is installed and running and Windows 10 is running.

Windows Server 2012 R2 is running.

Reference

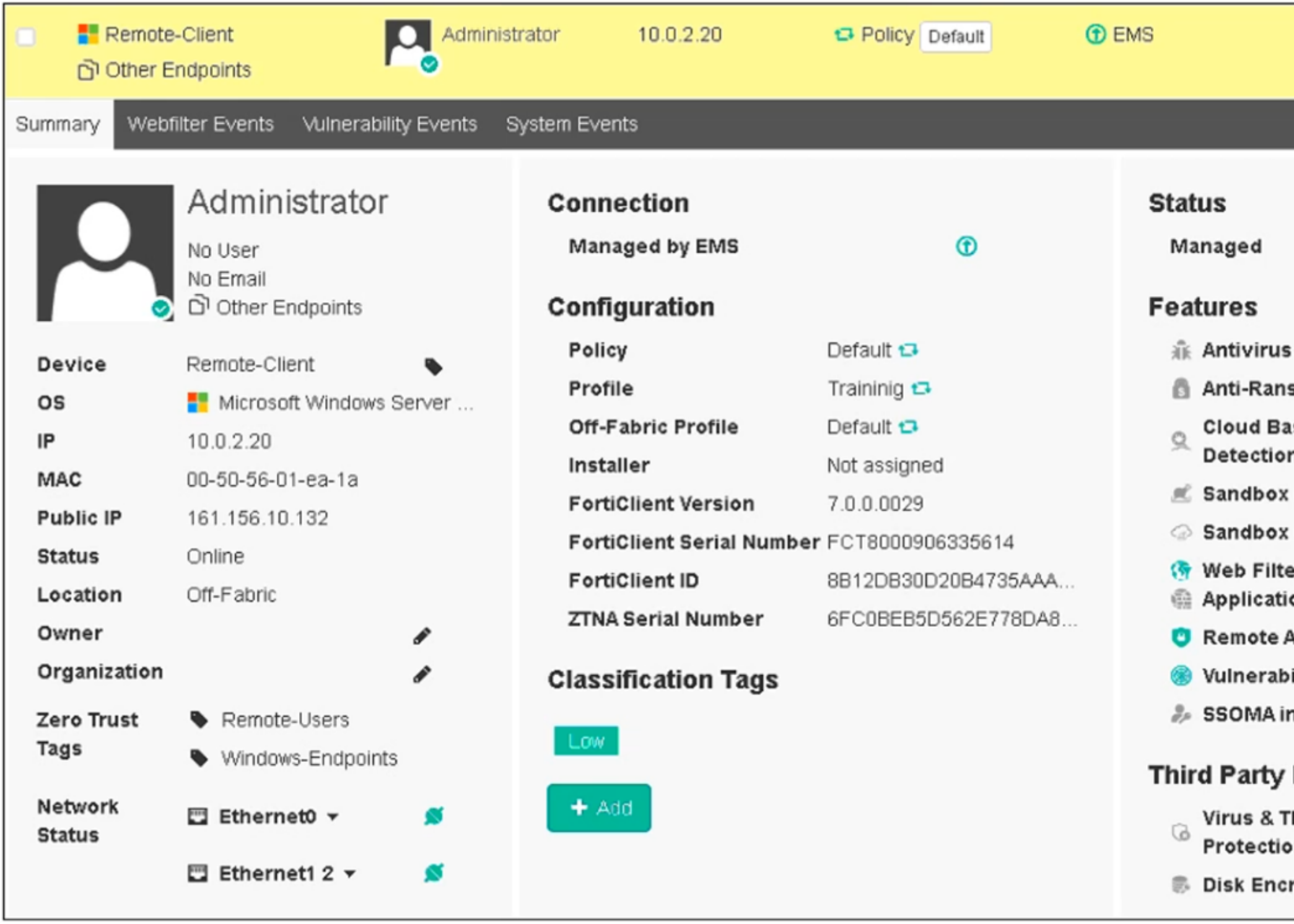
FortiClient EMS 7.2 Study Guide, Zero Trust Tagging Rule Set Configuration Section

Fortinet Documentation on Configuring Zero Trust Tagging Rules and Logic

Question 2

Question Type: MultipleChoice

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


Remote-Client
Other Endpoints
Administrator
10.0.2.20
Policy
Default
EMS
Summary
Webfilter Events
Vulnerability Events
System Events
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
Anti-Rans
Cloud Ba
Detectior
Sandbox
Sandbox
Web Filte
Applicatic
Remote A
Vulnerabi
SSOMA in
Third Party
Virus & T
Protectio
Disk Encr

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

Options:

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.

Answer:

B, D

Explanation:

Based on the Remote-Client status shown in the exhibit:

Endpoint Policy: The 'Policy' field shows 'Default,' indicating that the endpoint has been assigned the Default endpoint policy.

Connection Status: The 'Location' field shows 'Off-Fabric,' meaning that the endpoint is currently off the corporate network (off-net).

Therefore, the two conclusions that can be made are:

The endpoint has been assigned the Default endpoint policy.

The endpoint is currently off-net.

Reference

FortiClient EMS 7.2 Study Guide, Endpoint Summary Information Section

Fortinet Documentation on Endpoint Policies and Status Indicators

Question 3

Question Type: **MultipleChoice**

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

Options:

A- FortiClient

B- FortiGate

C- FortiGate Access Proxy

D- FortiClient EMS

Answer:

A

Explanation:

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

Question 4

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

Explanation:

FortiClient offers several types of antivirus scans to ensure comprehensive protection:

Full scan: Scans the entire system for malware, including all files and directories.

Custom scan: Allows the user to specify particular files, directories, or drives to be scanned.

Quick scan: Scans the most commonly infected areas of the system, providing a faster scanning option.

These three types of scans provide flexibility and thoroughness in detecting and managing malware threats.

Reference

FortiClient EMS 7.2 Study Guide, Antivirus Scanning Options Section

Question 5

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

Explanation:

When FortiClient is installed on a Windows Server, the default behavior for real-time protection control is:

Real-time protection is disabled: By default, FortiClient does not enable real-time protection on server installations to avoid potential performance impacts and because servers typically have different security requirements compared to client endpoints.

Thus, real-time protection is disabled by default on Windows Server installations.

Reference

FortiClient EMS 7.2 Study Guide, Real-time Protection Section

Fortinet Documentation on FortiClient Default Settings for Server Installations

Question 6

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:

A

Explanation:

Based on the FortiClient logs shown in the exhibit:

The first log entry shows the application 'firefox.exe' trying to access a destination IP, with the threat identified as 'Twitter.'

The action taken by the application firewall is 'blocked' with the event type 'appfirewall.'

This indicates that the application firewall has blocked access to Twitter.

Reference

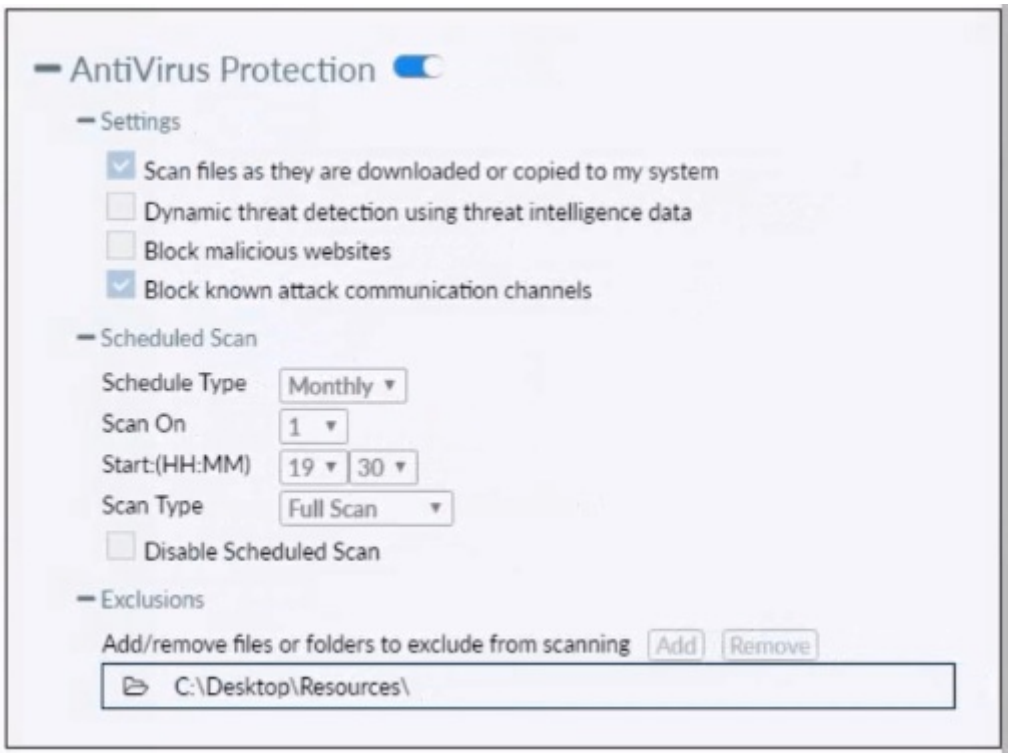
FortiClient EMS 7.2 Study Guide, Application Firewall Logs Section

Fortinet Documentation on Interpreting FortiClient Logs

Question 7

Question Type: MultipleChoice

Refer to the exhibit.



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

Explanation:

Action On Virus Discovery Warn the User If a Process Attempts to Access Infected Files Quarantine Infected Files. You can use FortiClient to view, restore, or delete the quarantined file, as well as view the virus name, submit the file to FortiGuard, and view logs. Deny Access to Infected Files Ignore Infected Files

Question 8

Question Type: MultipleChoice

Which statement about FortiClient enterprise management server is true?

Options:

A- It provides centralized management of FortiGate devices.

B- It 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

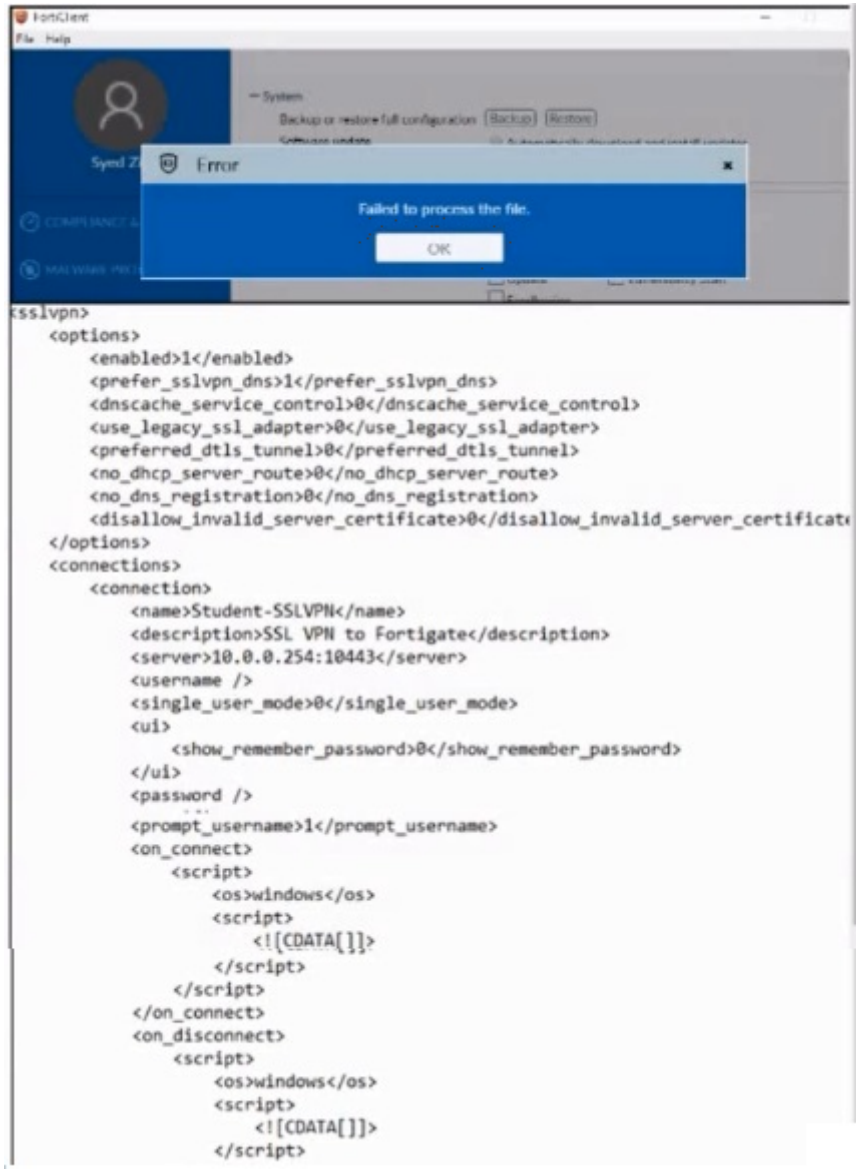
Explanation:

FortiClient EMS is designed to provide centralized management and control of multiple endpoints running FortiClient software. It serves as a central management server that allows administrators to efficiently manage and configure a large number of FortiClient installations across the network.

Question 9

Question Type: MultipleChoice

Refer to the exhibit.



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

Explanation:

Based on the error message and the XML configuration file shown in the exhibit:

The error 'Failed to process the file' typically indicates an issue with the XML syntax.

Upon reviewing the XML content, it is crucial to ensure that all tags are correctly formatted, properly opened and closed, and that there are no syntax errors.

Resolving any XML syntax errors will allow FortiClient to successfully process and restore the configuration file.

Therefore, the administrator must resolve the XML syntax error to fix the issue.

Reference

FortiClient EMS 7.2 Study Guide, Configuration File Management Section

General XML Syntax Guidelines and Best Practices

Question 10

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

Explanation:

FortiClient supports initiating the following VPN types from the Windows command prompt:

IPSec VPN: FortiClient can establish IPSec VPN connections using command line instructions.

SSL VPN: FortiClient also supports initiating SSL VPN connections from the Windows command prompt.

These two VPN types can be configured and initiated using specific command line parameters provided by FortiClient.

Reference

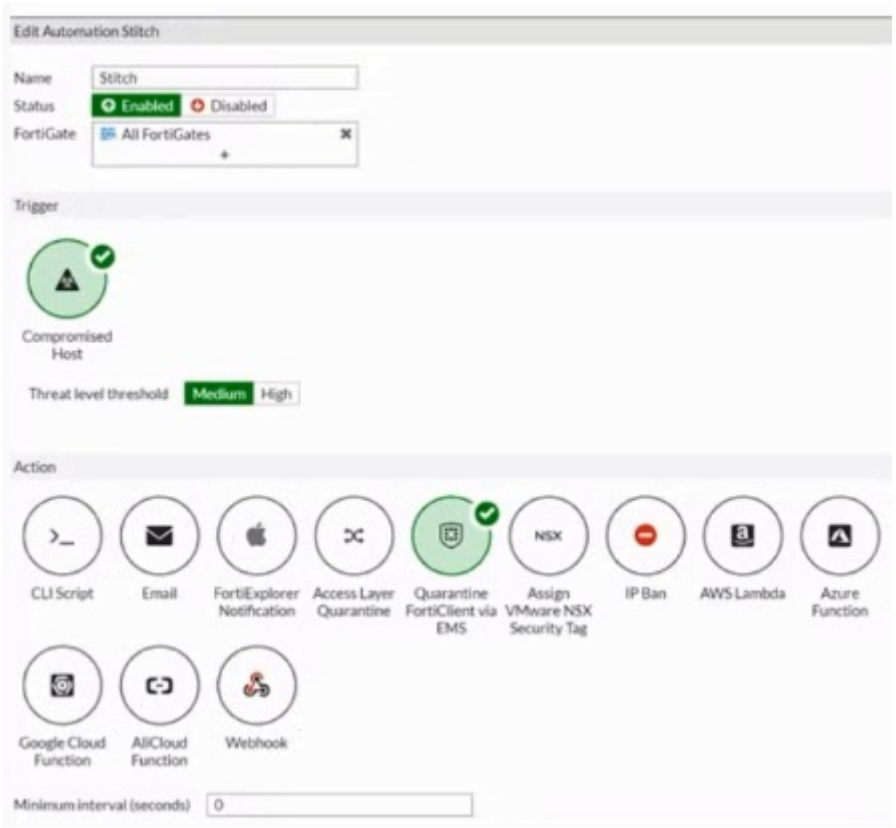
FortiClient EMS 7.2 Study Guide, VPN Configuration Section

Fortinet Documentation on Command Line Options for FortiClient VPN

Question 11

Question Type: MultipleChoice

Refer to the exhibit.



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

Explanation:

Based on the Security Fabric automation settings shown in the exhibit:

The automation stitch is configured with a trigger for a 'Compromised Host.'

The action specified for this trigger is 'Quarantine FortiClient via EMS.'

This indicates that when an endpoint is detected as compromised, FortiClient EMS will quarantine the endpoint as part of the automation process.

Therefore, the action taken on compromised endpoints will be to quarantine them through EMS.

Reference

FortiGate Security 7.2 Study Guide, Automation Stitches and Actions Section

Fortinet Documentation on Configuring Automation Stitches and Quarantine Actions