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:

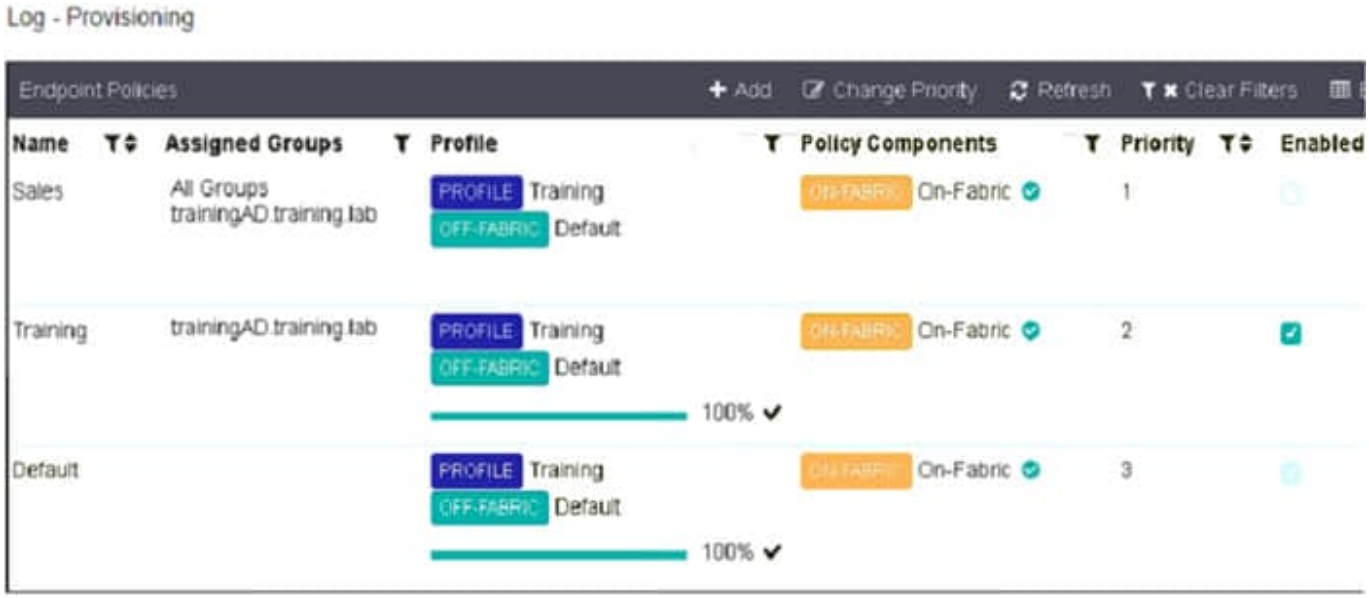
https://www.pass4itsure.com/nse5_fct-7-0.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

QUESTION 1

Refer to the exhibit.



Which shows multiple endpoint policies on FortiClient EMS.

Which policy is applied to the endpoint in the AD group trainingAD?

A. The Sales policy

B. The Training policy

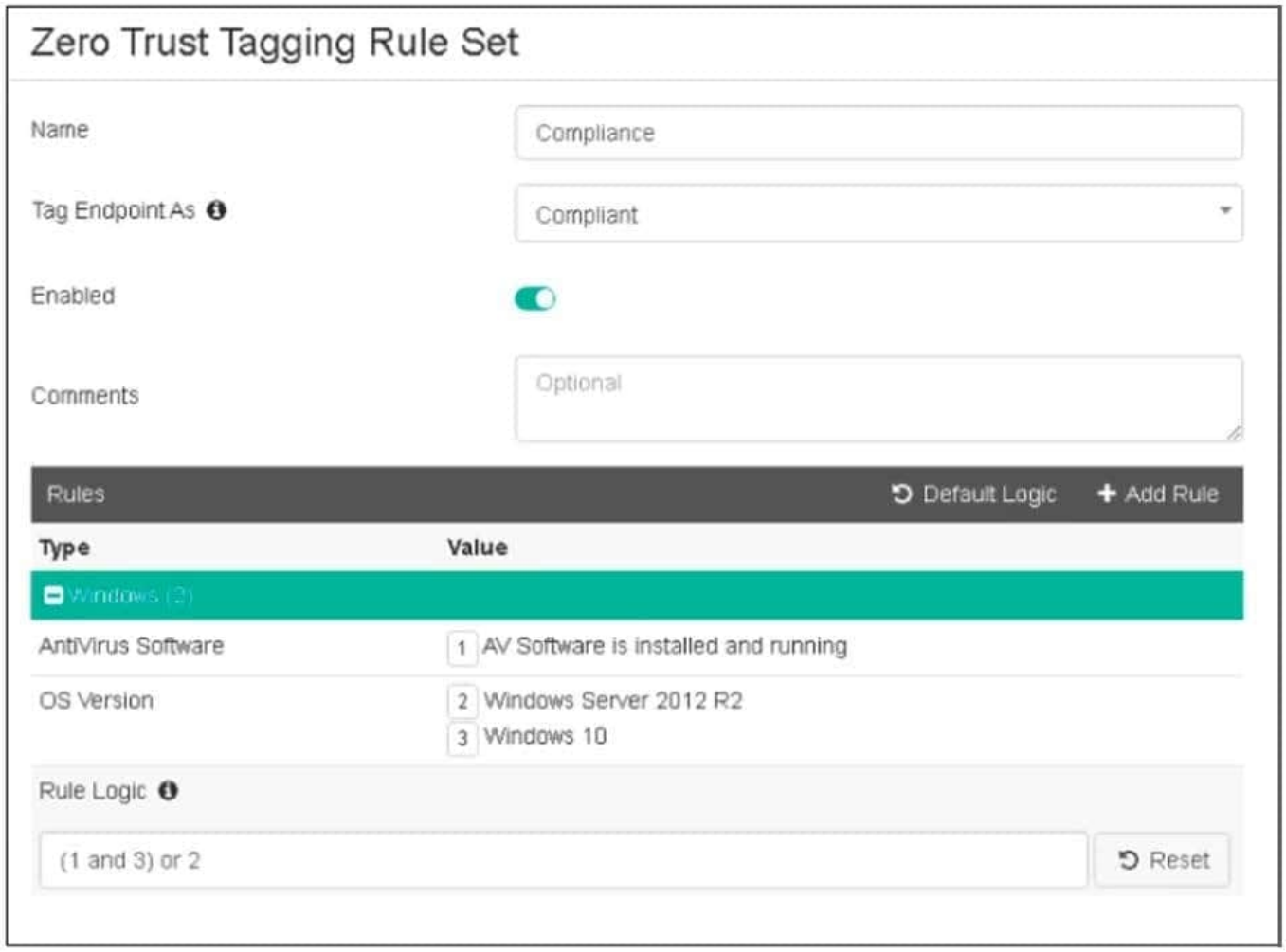
C. Both the Sales and Training policies because their priority is higher than the Default policy

D. The Default policy because it has the highest priority

Correct Answer: B

QUESTION 2

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



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

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

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

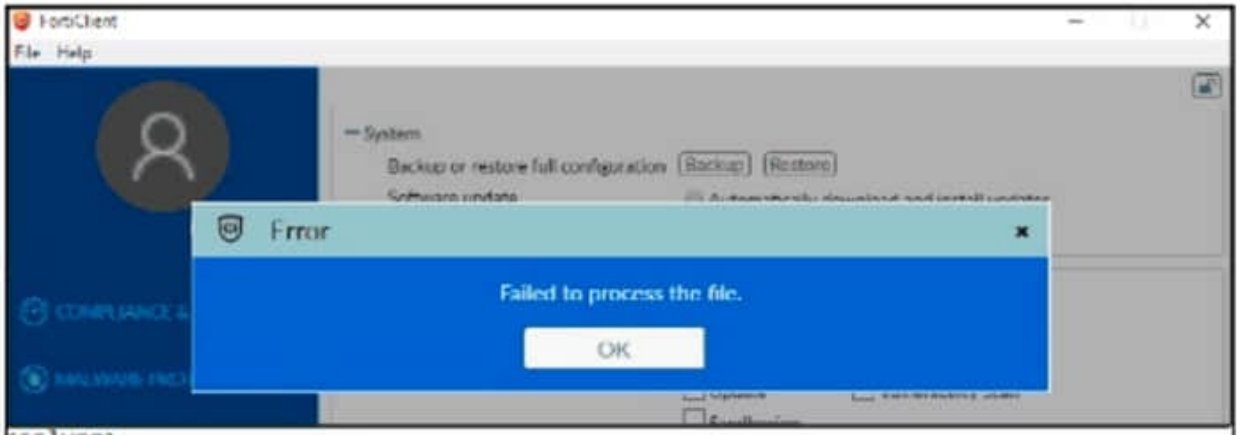
C. The endpoint must satisfy that antivirus is installed and running and Windows 10 is running.

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

Correct Answer: CD

QUESTION 3

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

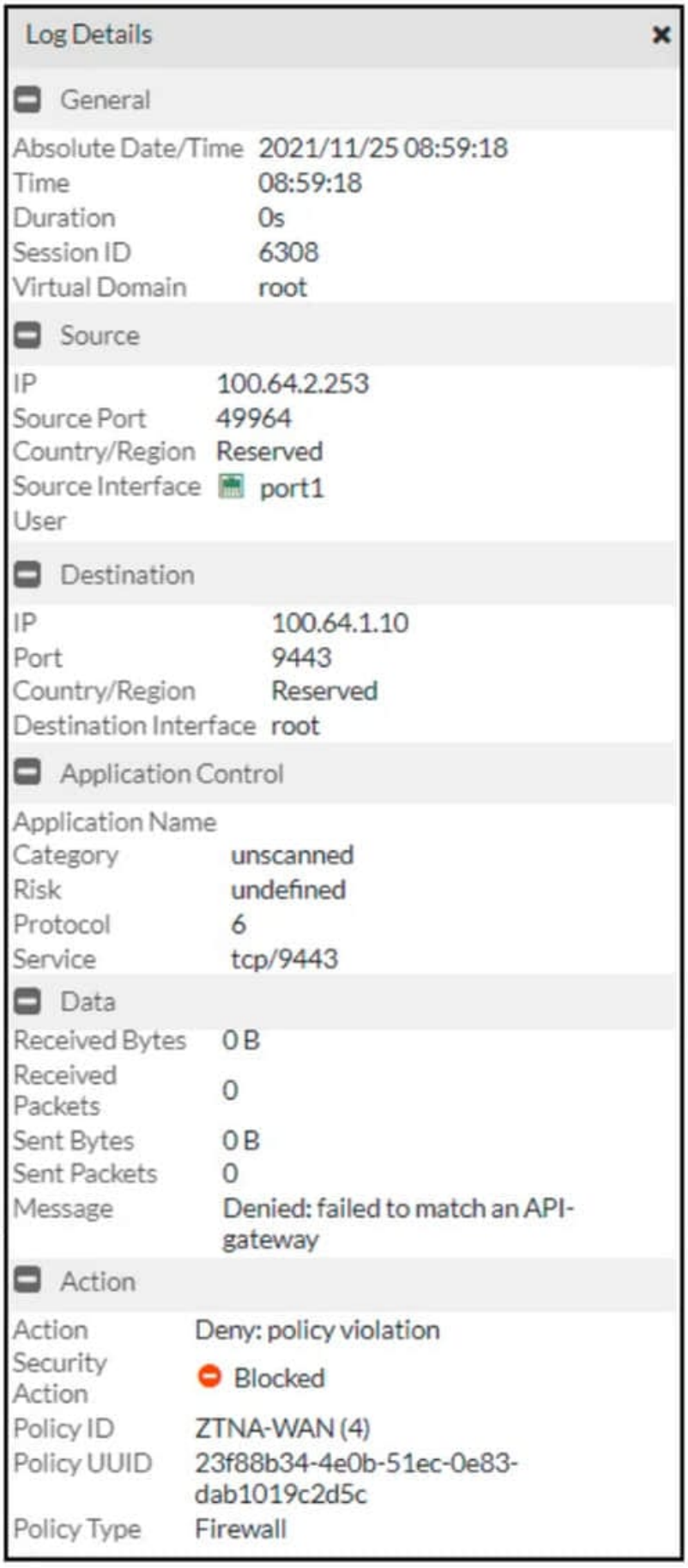
C. The administrator must change the file size

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

Correct Answer: A

QUESTION 4

Refer to the exhibit.


Log Details

General

Absolute Date/Time	2021/11/25 08:59:18
Time	08:59:18
Duration	0s
Session ID	6308
Virtual Domain	root

Source

IP	100.64.2.253
Source Port	49964
Country/Region	Reserved
Source Interface	port1
User	

Destination

IP	100.64.1.10
Port	9443
Country/Region	Reserved
Destination Interface	root

Application Control

Application Name	
Category	unscanned
Risk	undefined
Protocol	6
Service	tcp/9443

Data

Received Bytes	0 B
Received Packets	0
Sent Bytes	0 B
Sent Packets	0
Message	Denied: failed to match an API-gateway

Action

Action	Deny: policy violation
Security Action	Blocked
Policy ID	ZTNA-WAN (4)
Policy UUID	23f88b34-4e0b-51ec-0e83-dab1019c2d5c
Policy Type	Firewall

Which shows the output of the ZTNA traffic log on FortiGate. What can you conclude from the log message?

A. The remote user connection does not match the explicit proxy policy.

B. The remote user connection does not match the ZTNA server configuration.

C. The remote user connection does not match the ZTNA rule configuration.

D. The remote user connection does not match the ZTNA firewall policy

Correct Answer: B

API gateway cannot be matched or real servers cannot be reached

QUESTION 5

A FortiClient EMS administrator has enabled the compliance rule for the sales department. Which Fortinet device will enforce compliance with dynamic access control?

A. FortiClient

B. FortiClient EMS

C. FortiGate

D. FortiAnalyzer

Correct Answer: C

QUESTION 6

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 7

An administrator installs FortiClient EMS in the enterprise.

Which component is responsible for enforcing protection and checking security posture?

A. FortiClient vulnerability scan

B. FortiClient EMS tags

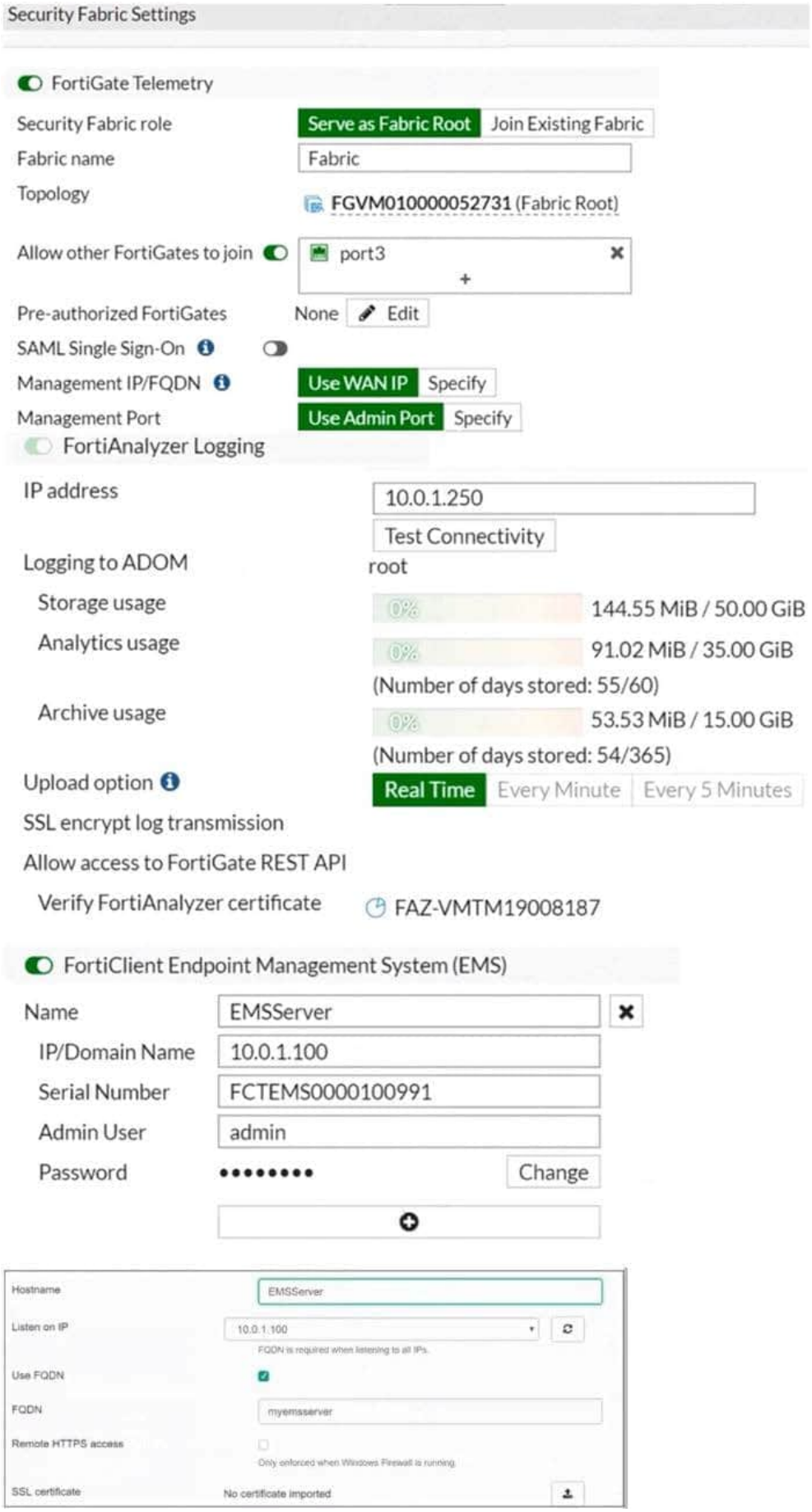
C. FortiClient EMS

D. FortiClient

Correct Answer: D

QUESTION 8

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 9

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

A. Disable select the vulnerability scan feature in the deployment package

B. Use the default endpoint profile

C. Select the vulnerability scan feature in the deployment package, but disable the feature on the endpoint profile

D. Click the hide icon on the vulnerability scan tab

Correct Answer: D

QUESTION 10

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

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

Correct Answer: C