

Exam Questions FCP_FCT_AD-7.2

FCP-FortiClient EMS 7.2 Administrator

https://www.2passeasy.com/dumps/FCP_FCT_AD-7.2/



NEW QUESTION 1

Which two are benefits of using multi-tenancy mode on FortiClient EMS? (Choose two.)

- A. Separate host servers manage each site.
- B. Licenses are shared among sites
- C. The fabric connector must use an IP address to connect to FortiClient EMS.
- D. It provides granular access and segmentation.

Answer: CD

Explanation:

? Understanding Multi-Tenancy Mode:

? Evaluating Benefits:

? Eliminating Incorrect Options:

References:

? FortiClient EMS multi-tenancy configuration and benefits documentation from the study guides.

NEW QUESTION 2

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?

- 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

NEW QUESTION 3

Which statement about the FortiClient enterprise management server is true?

- A. It receives the configuration information of endpoints from ForuGate.
- B. It provides centralized management of multiple endpoints running FortiClient software.
- C. It enforces compliance on the endpoints using tags
- D. It receives the CA certificate from FortiGate to validate client certificates.

Answer: C

NEW QUESTION 4

Refer to the exhibit, which shows FortiClient EMS deployment, profiles.

Deployments						+ Add	Change Priority
Name	Assigned Groups	Deployment Package	Scheduled Upgrade Time	Priority	Enabled		
Deployment-1	All Groups	First-Time-Installation		1	<input type="checkbox"/>		
Deployment-2	All Groups trainingAD.training.lab	To-Upgrade		2	<input checked="" type="checkbox"/>		

When an administrator creates a deployment profile on FortiClient EMS. which statement about the deployment profile is true?

- A. Deployment-2 will upgrade FortiClient on both the AD group and workgroup.
- B. Deployment-1 will install FortiClient on new AO group endpoints.
- C. Deployment-2 will install FortiClient on both the AD group and workgroup.
- D. Deployment-1 will upgrade FortiClient only on the workgroup.

Answer: A

Explanation:

? Deployment Profiles Analysis:

? Evaluating Deployment-2:

? Conclusion:

References:

? FortiClient EMS deployment and profile documentation from the study guides.

NEW QUESTION 5

Refer to the exhibit, which shows the output of the ZTNA traffic log on FortiGate.

```
eventtime=1633084101662546935 tz="-0700" logid="0000000013" type="traffic"
subtype="forward" level="notice" vd="root" srcip=100.64.2.253 srcport=58664 srcintf="port1"
srcintfrole="wan" dstip=100.64.1.10 dstport=9443 dstintf="root" dstintfrole="undefined"
srccountry="Reserved" dstcountry="Reserved" sessionid=5215 proto=6 action="deny" policyid=0
policytype="proxy-policy" service="tcp/9443"trandisp="noop" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0
rcvdpkt=0 appcat="unscanned" utmaction="block" countztna=1 msg="Denied: failed to match a proxy-policy"
utmref=65462-14
```

What can you conclude from the log message?

- A. The remote user connection does not match the local-in policy.
- B. The remote user connection does not match the ZTNA rule configuration.
- C. The remote user connection does not match the ZTNA server configuration.
- D. The remote user connection does not match the ZTNA firewall policy.

Answer: B

Explanation:

? Observation of ZTNA Traffic Log:

? Evaluating Log Message:

? Conclusion:

References:

? ZTNA traffic log analysis and configuration documentation from the study guides.

NEW QUESTION 6

What does FortiClient do as a fabric agent? (Choose two.)

- A. Provides IOC verdicts
- B. Creates dynamic policies
- C. Provides application inventory
- D. Automates Responses

Answer: CD

NEW QUESTION 7

Exhibit.

```

1:40:39 PM      Information      Vulnerability      id=96521 msg="A vulnerability scan result has been logged" status=N/A vulncat="Operating
1:40:39 PM      Information      Vulnerability      id=96520 msg="The vulnerability scan status has changed" status="scanning finished" vulnc
1:41:38 PM      Information      ESNAC      id=96958 user=Admin msg="User social media information" social_srvc=os social_user=Admin
2:12:22 PM      Information      Config      id=96882 msg="Policy 'Default' was received and applied"
2:13:27 PM      Information      ESNAC      id=96958 user=Admin msg="User social media information" social_srvc=os social_user=Admin
2:14:32 PM      Information      ESNAC      id=96959 emshostname=WIN-EHVKB8EA3S71 msg="Endpoint has AV whitelist engine version 6.00134 and si
2:14:54 PM      Information      Config      id=96882 msg="Policy 'Default' was received and applied"
2:16:01 PM      Information      ESNAC      id=96958 user=Admin msg="User social media information" social_srvc=os social_user=Admin
2:20:19 PM      Information      Config      id=96883 msg="Compliance rules 'default' were received and applied"
2:20:23 PM      Debug      ESNAC      PIPEMSG_CMD_ESNAC_STATUS_RELOAD_CONFIG
2:20:23 PM      Debug      ESNAC      cb828898d1ae56916f84cc7909a1eb1a
2:20:23 PM      Debug      ESNAC      Before Reload Config
2:20:23 PM      Debug      ESNAC      ReloadConfig
2:20:23 PM      Debug      Scheduler      stop_task() called
2:20:23 PM      Debug      Scheduler      GUI change event
2:20:23 PM      Debug      Scheduler      stop_task() called
2:20:23 PM      Information      Config      id=96882 msg="Policy 'Fortinet-Training' was received and applied"
2:20:23 PM      Debug      Config      'scan on registration' is disabled - delete 'on registration' vulnerability scan.
2:20:23 PM      Debug      Config      ImportConfig: tag <\forticlient_configuration\antiexploit\exclusion_applications> value is empty.

```

Based on the FortiClient logs shown in the exhibit, which endpoint profile policy is currently applied to the FortiClient endpoint from the EMS server?

- A. Fortinet-Training
- B. Default configuration policy c
- C. Compliance rules default
- D. Default

Answer: A

Explanation:

? Observation of Logs:

? Evaluating Policies:

? Conclusion:

References:

? FortiClient EMS policy configuration and log analysis documentation from the study guides.

NEW QUESTION 8

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

Answer: C

Explanation:

? Understanding Compliance Rules:

? Enforcing Compliance:

? Conclusion:

References:

? Compliance and enforcement documentation from FortiGate and FortiClient EMS study guides.

NEW QUESTION 9

Which security fabric component sends a notification to quarantine an endpoint after IOC detection in the automation process?

- A. FortiAnalyzer
- B. FortiClient
- C. FortiClient EMS
- D. Forti Gate

Answer: D

NEW QUESTION 10


Refer to the exhibits.


Security Fabric Settings


FortiGate Telemetry


Security Fabric role **Serve as Fabric Root** Join Existing Fabric


Fabric name

Topology  FGVM010000052731 (Fabric Root)

Allow other FortiGates to join ☒ 

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

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 

IP/Domain Name

Serial Number

Admin User

Password

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.

Answer: A

Explanation:

Based on the FortiGate Security Fabric settings shown in the exhibits, to successfully quarantine an endpoint when it is detected as a compromised host (IOC), the following step is required:

? Enable Remote HTTPS Access to EMS:This setting allows FortiGate to communicate securely with FortiClient EMS over HTTPS. Remote HTTPS access is essential for the quarantine functionality to operate correctly, enabling the EMS server to receive and act upon the quarantine commands from FortiGate.

Therefore, the administrator must enable remote HTTPS access to EMS to allow the quarantine process to function properly.

References

- ? FortiGate Infrastructure 7.2 Study Guide, Security Fabric and Integration with EMS Sections
- ? Fortinet Documentation on Enabling Remote HTTPS Access to FortiClient EMS

NEW QUESTION 10

Refer to the exhibits.

Log - Provisioning

Log - Provisioning

Endpoint Policy

Endpoint Policy Name

Training

Endpoint Groups

trainingAD training lab

Edit

Users

Optional

Profile

Training

Profile (Off-Fabric)

Default

On-Fabric Detection Rules

On-Fabric

Comments

Optional

Enable the Policy

☒

Endpoint Policy

Endpoint Policy Name

Sales

Endpoint Groups

All Groups

trainingAD training lab

Edit

Users

trainingAD training labstudent

Profile

Training

Profile (Off-Fabric)

Default

On-Fabric Detection Rules

On-Fabric

Comments

Optional

Enable the Policy

☒

Log - Provisioning

Log - Provisioning

Endpoint Policies

Name	Assigned Groups	Profile	Policy Components	Endpoint Count	Priority	Enabled
Training	trainingAD training lab	PROFILE Training OFF-FABRIC Default	ON-FABRIC On-Fabric	1	1	<input checked="" type="checkbox"/>
Sales	All Groups trainingAD training lab	PROFILE Training OFF-FABRIC Default	ON-FABRIC On-Fabric	1	2	<input checked="" type="checkbox"/>
Default		PROFILE Training OFF-FABRIC Default	ON-FABRIC On-Fabric	0	3	<input type="checkbox"/>

Which shows the configuration of endpoint policies.

Based on the configuration, what will happen when someone logs in with the user account student on an endpoint in the trainingAD domain?

- A. FortiClient EMS will assign the Sales policy
- B. FortiClient EMS will assign the Training policy
- C. FortiClient EMS will assign the Default policy
- D. FortiClient EMS will assign the Training policy for on-fabric endpoints and the Sales policy for the off-fabric endpoint

Answer: B

Explanation:

Based on the configuration shown in the exhibits:

- ? There are three endpoint policies configured: Training, Sales, and Default.
- ? The "Training" policy is assigned to the "trainingAD.training.lab" group.
- ? The "Sales" policy is assigned to "All Groups" and "trainingAD.training.lab/student."
- ? The "Default" policy has no specific groups assigned.

When someone logs in with the user account "student" on an endpoint in the "trainingAD" domain:

- ? The "Training" policy is specifically assigned to the "trainingAD.training.lab" group.
- ? The "Sales" policy includes "trainingAD.training.lab/student" but not the general "trainingAD.training.lab" group.
- ? The system will prioritize the most specific match for the group.

Therefore, FortiClient EMS will assign the "Training" policy to the "student" account logging into the "trainingAD" domain as it matches the group "trainingAD.training.lab" directly. References

- ? FortiClient EMS 7.2 Study Guide, Endpoint Policy Configuration Section
- ? FortiClient EMS Documentation on Group Policy Assignment and Matching

NEW QUESTION 15

Which two VPNtypes can a FortiClientendpoint user inmate from the Windows command prompt? (Choose two)

- A. L2TP
- B. PPTP
- C. IPSec
- D. SSL VPN

Answer: CD

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.

References

- ? FortiClient EMS 7.2 Study Guide, VPN Configuration Section
- ? Fortinet Documentation on Command Line Options for FortiClient VPN

NEW QUESTION 19

Refer to the exhibit.

```
config user fsso
  edit "Server"
    set type fortiems
    set server "10.0.1.200"
    set password ENC ebT9fHIMXIBykhWCSnG;P+Tpi/EjEdQu4hAa24LiKxHolWI7JyX.
    set ssl enable
  next
end
```

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.

Answer: A

Explanation:

Based on the CLI output from FortiGate:

- ? The configuration shows the use of "type fortiems," indicating that FortiGate is set up to interact with FortiClient EMS.

- ? The "server" field points to an IP address (10.0.1.200), which is typically the address of the FortiClient EMS server.

- ? The configuration includes an SSL-enabled connection, which is a common setup for secure communication between FortiGate and FortiClient EMS.

Thus, the configuration indicates that FortiGate is set up to pull user groups from FortiClient EMS.

References

- ? FortiGate Security 7.2 Study Guide, FSSO Configuration Section
- ? Fortinet Documentation on FortiGate and FortiClient EMS Integration

NEW QUESTION 24

Refer to the exhibit.

Compliance Profile

Zero Trust Tagging Rule Set

Name

Sales Department Compliance

Tag Endpoint As

Sales Department Compliance

Enabled

Comments

Optional

Rules

Edit Logic

Add Rule

Type

Value

Windows (2)

Vulnerable Devices Severity Level

Medium or higher

Running Process

Calculator.exe

Save

Cancel

Based on the settings shown in the exhibit, which two actions must the administrator take to make the endpoint compliant? (Choose two.)

- A. Enable the web filter profile.

B. Run Calculator application on the endpoint.

C. Integrate FortiSandbox for infected file analysis

D. Patch applications that have vulnerability rated as high or above.

Answer: BD

Explanation:

- ? Observation of Compliance Profile:

? Evaluating Actions for Compliance:

? Eliminating Incorrect Options:

? Conclusion:

References:

? FortiClient EMS compliance profile configuration documentation from the study guides.

NEW QUESTION 27

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual FCP_FCT_AD-7.2 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the FCP_FCT_AD-7.2 Product From:

https://www.2passeasy.com/dumps/FCP_FCT_AD-7.2/

Money Back Guarantee

FCP_FCT_AD-7.2 Practice Exam Features:

- * FCP_FCT_AD-7.2 Questions and Answers Updated Frequently
- * FCP_FCT_AD-7.2 Practice Questions Verified by Expert Senior Certified Staff
- * FCP_FCT_AD-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * FCP_FCT_AD-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year