DUMPSARENA

Fortinet NSE 6FortiClient EMS 7.4 Administrator

Fortinet FCP_FCT_AD-7.4

Version Demo

Total Demo Questions: 2

Total Premium Questions: 23

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, FortiClient EMS deployment and configuration	3
Topic 2, Endpoint deployment and management	8
Topic 3, Endpoint security	7
Topic 4, ZTNA	3
Topic 5, Troubleshooting	2
Total	23

QUESTION NO: 1

An administrator creates a dynamic endpoint group for Windows endpoints that meet a specified condition. An endpoint is upgraded and now meets the group condition while it remains connected to EMS.

What is the expected result?

A. The endpoint remains outside the group until a user restarts FortiClient

B. The endpoint is added only after the administrator approves it manually

C. The endpoint is added only after it is reinstalled by using a new deployment package

D. EMS reevaluates the endpoint and updates dynamic group membership

ANSWER: D

Explanation:

Dynamic endpoint groups are based on endpoint information and membership is updated when EMS evaluates the endpoint against the configured conditions. After the endpoint meets the condition, EMS can place it in the dynamic group and evaluate the endpoint-policy assignment associated with that group. The administrator does not need to add the endpoint manually to a static group.

QUESTION NO: 2

A development tool stores unsigned test binaries in a dedicated local folder. FortiClient antivirus repeatedly detects files in that folder as malicious, but security policy requires real-time antivirus protection to remain enabled for all other files and locations.

What is the most appropriate FortiClient EMS configuration?

A. Add a narrowly scoped antivirus exclusion for the approved folder.

B. Disable real-time antivirus protection for the development endpoints.

C. Exclude the entire local drive from antivirus scanning.

D. Remove the endpoints from FortiClient EMS management.

ANSWER: A

Explanation:

The administrator should configure a narrowly scoped antivirus exclusion for the specific approved folder in the antivirus profile applied to the development endpoints. This preserves real-time protection for the rest of the endpoint. Disabling antivirus protection or excluding the entire drive would create unnecessarily broad exposure.