Fortinet

FCP_FCT_AD-7.4 Exam

Fortinet NSE 6 - FortiClient EMS 7.4 Administrator

Questions & Answers
Demo

Version: 5.0

Question: 1

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

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:

Deployment-1 has the "First-Time-Installation" package and is assigned to "All Groups" with a priority of 1 but is not enabled.

Deployment-2 has the "To-Upgrade" package, is assigned to both "All Groups" and "trainingAD.training.lab," with a priority of 2 and is enabled.

Evaluating Deployment-2:

Deployment-2 will upgrade FortiClient on both "All Groups" and "trainingAD.training.lab" since it is enabled and assigned to these groups. This includes both AD (Active Directory) groups and workgroups.

Conclusion:

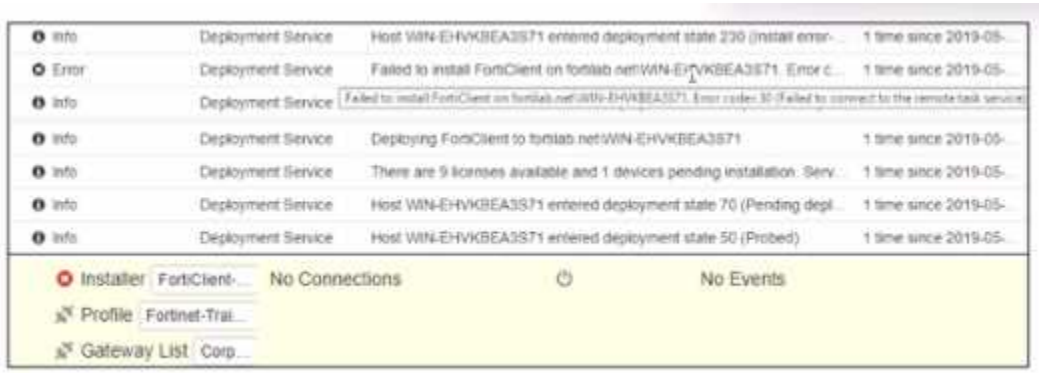
Since Deployment-2 is set to upgrade FortiClient on all the assigned groups and workgroups, the correct answer is A.

Reference:

FortiClient EMS deployment and profile documentation from the study guides.

Question: 2

Exhibit.



Based on the logs shown in the exhibit, why did FortiClient EMS tail to install FortiClient on the endpoint?

A. The FortiClient antivirus service is not running.

B. The Windows installer service is not running.

C. The remote registry service is not running.

D. The task scheduler service is not running.

Answer: D

Explanation:

https://community.fortinet.com/t5/FortiClient/Technical-Note-FortiClient-fails-to-install-from-FortiClient-EMS/ta-p/193680

The deployment service error message may be caused by any of the following. Try eliminating them all, one at a time.

1. Wrong username or password in the EMS profile

2. Endpoint is unreachable over the network

3. Task Scheduler service is not running

4. Remote Registry service is not running

5. Windows firewall is blocking connection

Question: 3

Which two statements are true about ZTNA? {Choose two.)

A. ZTNA manages access for remote users only.

B. ZTNA provides role-based access.

C. ZTNA provides a security posture check.

D. ZTNA manages access through the client only.

Answer: B, C

Explanation:

ZTNA (Zero Trust Network Access) is a security architecture that is designed to provide secure access to network resources for users, devices, and applications. It is based on the principle of "never trust, always verify," which means that all access to network resources is subject to strict verification and authentication.

Two functions of ZTNA are:

ZTNA provides a security posture check: ZTNA checks the security posture of devices and users that are attempting to access network resources. This can include checks on the device's software and hardware configurations, security settings, and the presence of malware.

ZTNA provides role-based access: ZTNA controls access to network resources based on the role of the user or device. Users and devices are granted access to only those resources that are necessary for their role, and all other access is denied. This helps to prevent unauthorized access and minimize the risk of data breaches.

Question: 4

When site categories are disabled in FortiClient web filter, which feature can be used to protect the endpoint from malicious web access?

A. Real-time protection list

B. Block malicious websites on antivirus

C. FortiSandbox URL list

D. Web exclusion list

Answer: D

Explanation:

Web Filter Functionality:

When site categories are disabled in the FortiClient web filter, the endpoint still requires protection from malicious web access.

Alternative Protection Features:

The web exclusion list can be used to manage and block specific URLs that are known to be malicious, providing a way to control and secure web access even without site categories being enabled.

Conclusion:

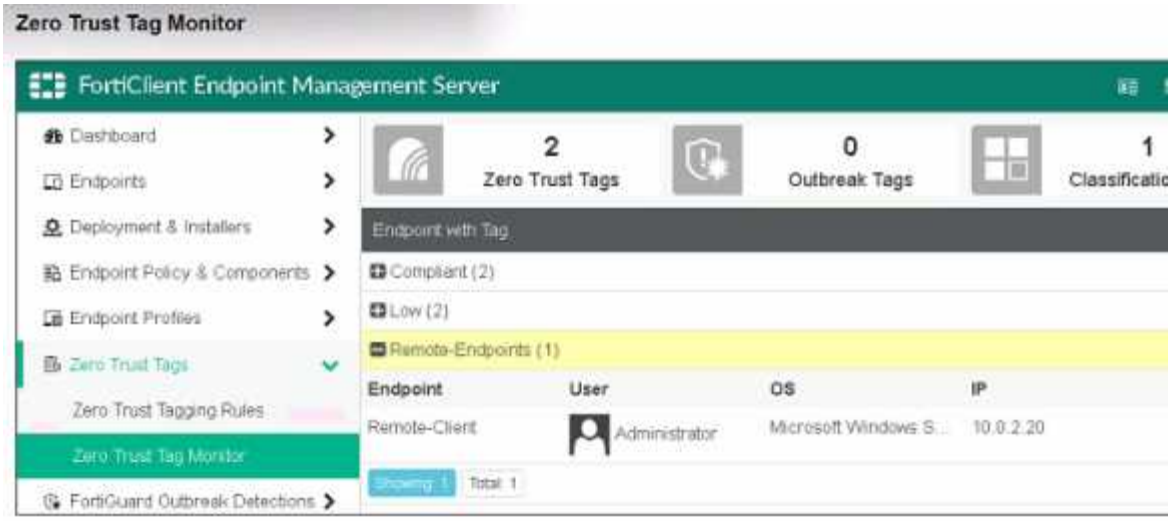
The correct feature that can be used to protect the endpoint in this scenario is the web exclusion list (D).

Reference:

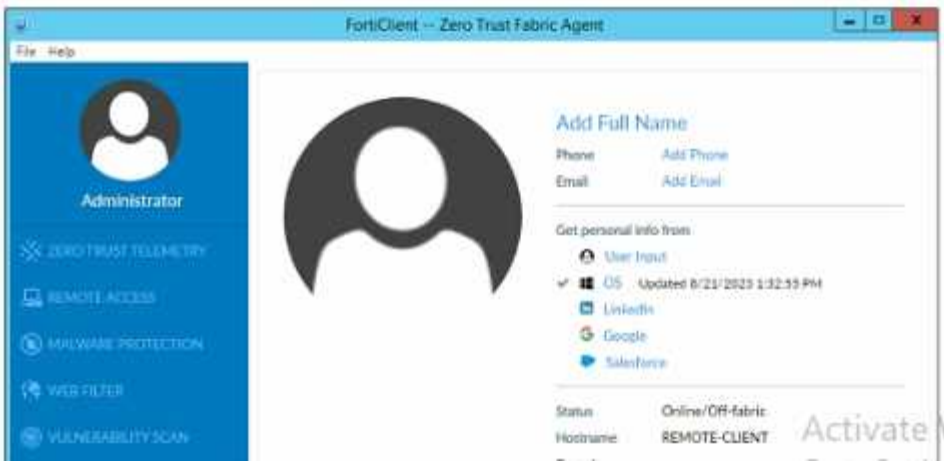
FortiClient web filter configuration and features from the study guides.

Question: 5

Exhibit.



FortiClient Status - GUI



Refer to the exhibits, which show the Zero Trust Tag Monitor and the FortiClient GUI status.

Remote-Client is tagged as Remote-User* on the FortiClient EMS Zero Trust Tag Monitor.

What must an administrator do to show the tag on the FortiClient GUI?

A. Change the FortiClient EMS shared settings to enable tag visibility.

B. Change the endpoint alerts configuration to enable tag visibility.

C. Update tagging rule logic to enable tag visibility.

D. Change the FortiClient system settings to enable lag visibility.

Answer: B

Explanation:

Observation of Exhibits:

The exhibits show the Zero Trust Tag Monitor on FortiClient EMS and the FortiClient GUI status.

Remote-Client is tagged as "Remote-Endpoints" on the FortiClient EMS Zero Trust Tag Monitor.

Enabling Tag Visibility:

To show the tag on the FortiClient GUI, the endpoint alerts configuration must be adjusted to enable tag visibility.

Verification:

The correct action is to change the endpoint alerts configuration to enable tag visibility, ensuring that the tag appears in the FortiClient GUI.

Reference:

FortiClient EMS and FortiClient configuration documentation from the study guides.