



**Vendor:** Fortinet

**Exam Code:** FCP\_FCT\_AD-7.4

**Exam Name:** Fortinet NSE 6 - FortiClient EMS 7.4  
Administrator

**Version:** DEMO

### QUESTION 1

Which two statements apply to FortiClient forensics analysis? (Choose two.)

- A. FortiClient sends an alert notification when malicious activity is triggered.
- B. The administrator must request analysis for the desired endpoint.
- C. The endpoint is quarantined until forensics is completed.
- D. Forensics analysis features must be enabled in the system settings profile.

**Answer: AD**

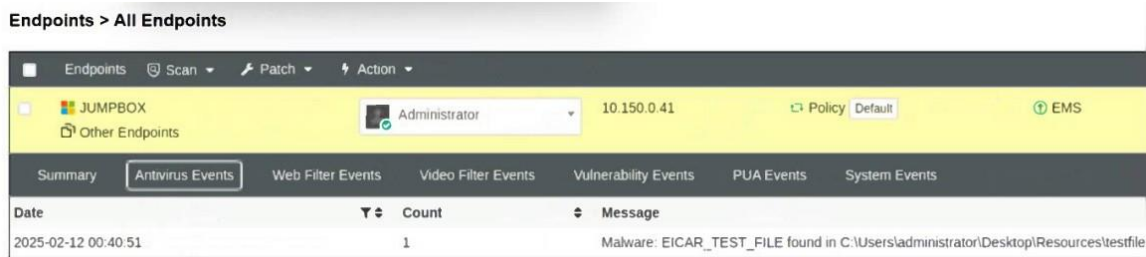
#### Explanation:

FortiClient forensics requires enabling the feature in the system settings profile. When malicious activity is detected, FortiClient generates an alert notification to inform the administrator for further analysis.

### QUESTION 2

Refer to the exhibit. You provide a webserver hosting service. An endpoint downloads a test file, `testfile.txt`, that gets blocked by FortiClient.

Which configuration can you use to make the file accessible on the endpoint?



The screenshot shows the FortiClient EMS console interface. At the top, there's a navigation bar with 'Endpoints > All Endpoints'. Below that, a header bar shows 'Endpoints', 'Scan', 'Patch', and 'Action' menus. A yellow banner displays 'JUMBOX' as the endpoint, 'Administrator' as the user, and '10.150.0.41' as the IP address. Below the banner, a tabbed interface shows 'Summary', 'Antivirus Events' (selected), 'Web Filter Events', 'Video Filter Events', 'Vulnerability Events', 'PUA Events', and 'System Events'. The 'Antivirus Events' tab displays a table with columns 'Date', 'Count', and 'Message'. One entry is visible: Date '2025-02-12 00:40:51', Count '1', and Message 'Malware: EICAR\_TEST\_FILE found in C:\Users\administrator\Desktop\Resources\testfile'.

| Date                | Count | Message                                                                             |
|---------------------|-------|-------------------------------------------------------------------------------------|
| 2025-02-12 00:40:51 | 1     | Malware: EICAR_TEST_FILE found in C:\Users\administrator\Desktop\Resources\testfile |

- A. Restore access to file directly using FortiClient.
- B. Allow the webserver URL in the exclusion list in the web filter profile.
- C. Exclude `testfile.txt` from the malware protection profile.
- D. Add the file to the allowlist in quarantine management on FortiClient EMS.

**Answer: D**

#### Explanation:

To allow a specific file that was blocked by FortiClient, the administrator can add it to the allowlist in FortiClient EMS quarantine management. This permits the endpoint to access the file without triggering malware protection.

### QUESTION 3

Which statement about deploying FortiClient EMS in an air-gapped environment is true?

- A. You can generate FortiClient installers on the FortiClient EMS instance.
- B. You can sync a license on the FortiClient EMS GUI using your FortiCloud account.
- C. You can configure FortiClient EMS to receive updates from FortiManager.
- D. You can use offline antimalware data on FortiClient EMS to operate in an air-gapped deployment.

**Answer: D**

#### Explanation:

In an air-gapped environment, FortiClient EMS cannot access the internet for updates. Using offline antimalware data allows FortiClient EMS to provide endpoint protection and operate without internet connectivity.

#### QUESTION 4

An administrator is configuring a zero trust network access (ZTNA) access proxy solution to share endpoint information with a FortiGate device.

Which two configuration actions will achieve this solution? (Choose two.)

- A. Add the FortiGate IP address to the Fabric device configurations on FortiClient EMS.
- B. Authorize FortiGate on FortiClient EMS as a Fabric connector.
- C. Use the FortiClient EMS connector on FortiGate to connect to FortiClient EMS.
- D. Apply the ZTNA license on FortiGate.

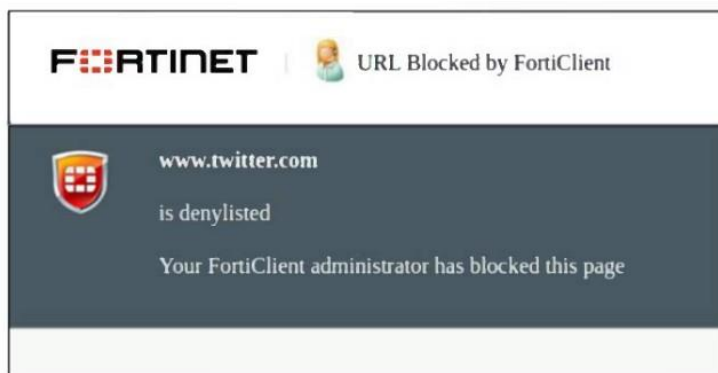
**Answer:** BC

**Explanation:**

To share endpoint information for ZTNA, the FortiGate must be authorized as a Fabric connector on FortiClient EMS, and the FortiClient EMS connector on FortiGate must be configured to establish the connection and exchange endpoint telemetry.

#### QUESTION 5

Refer to the exhibit. Why is the end user denied access to `twitter.com`?



- A. They are being blocked by the application firewall endpoint profile.
- B. They are being blocked by the exclusion list in the web filter endpoint profile.
- C. They are being blocked by FortiGuard categories in the web filter endpoint profile.
- D. They are being blocked by the deny list in the malware protection endpoint profile.

**Answer:** C

**Explanation:**

The block message indicates that the URL is denylisted by FortiClient. This occurs when FortiGuard categories in the web filter profile restrict access to specific websites, such as twitter.com, based on policy.

#### QUESTION 6

You are performing a proof-of-concept for a Fortinet Endpoint Protection solution.

Which endpoint should you install, in addition to FortiClient, as a part of a FortiEndpoint deployment?

- A. FortiPAM
- B. FortiEDR
- C. FortiNAC
- D. FortiMonitor

**Answer: B**

**Explanation:**

FortiEDR is installed alongside FortiClient in a FortiEndpoint deployment to provide advanced endpoint detection and response capabilities, complementing antivirus and security management functions.

### QUESTION 7

Refer to the exhibit. An administrator notes that no new endpoint data is populated on FortiGate.

What is the possible issue?

```
# diagnose test application fcncd 2
EMS context status:

FortiClient EMS number 1:
  name(id): ems(1) confirmed: yes
  is global: true
  interface vdom: root
  fetched-serial-number: FCTEM58824008072
  fetched-tenant-id: 00000000000000000000000000000000
  user-data:
    verified capabilities: true
    verified identity: true
    interface-selection-method: 0
    verify-peer-method: 3
    ztna-public-key:0x7f618e572e80
Websocket status: disconnected, oif: 0
```

- A. The FortiGate connector port is being blocked on FortiClient EMS server.
- B. The FortiClient EMS CA certificate is not trusted on FortiGate.
- C. FortiGate is not able to reach FortiClient EMS on telemetry port 8013.
- D. FortiGate is not able to reach the IP address or FQDN of the FortiClient EMS server.

**Answer: C**

**Explanation:**

The "Websocket status: disconnected" indicates that FortiGate cannot establish a telemetry connection with FortiClient EMS. This typically occurs if FortiGate cannot reach EMS on the required telemetry port 8013.

### QUESTION 8

Refer to the exhibit. FortiGate has lost connectivity with FortiClient EMS.

What is causing this problem?

Output of fcnacd debugs

```
# diagnose debug application fcnacd -1
# diagnose debug enable

[ec_ez_worker_base_prep_resolver:381] Outgoing interface index 0 for 1 (ems).
[ec_ez_worker_base_prep_ssl:428] verify peer method: 3, current ssl_cb: (nil), new ssl_cb: 0x55abb196ced0
[ec_ems_context_submit_work:641] Call submitted successfully.
obj-id: 0, desc: REST API to get EMS Serial Number., entry: api/v1/system/serial_number.
[_match_server_cert_key:462] verify_peer_method: 3
[_match_server_cert_key:480] EMS CN does not match verified CN!
[_match_server_cert_key:519] ret=0
[ec_ez_worker_process:400] Processing call for obj-id: 0, entry: "api/v1/system/serial_number"
[_update_obj_stats:365] Storing (0, ems, 7)
[ec_ez_worker_process:458] Call completed with failure.
obj-id: 0, desc: "REST API to get EMS Serial Number.", entry: "api/v1/system/serial_number".
error info: Error (-1@_generic_process_result_ex:148). EMS verification data has changed on host or peer. Must reverify.
[ec_ez_worker_base_prep_resolver:381] Outgoing interface index 0 for 1 (ems).
[ec_ez_worker_base_prep_ssl:428] verify peer method: 3, current ssl_cb: (nil), new ssl_cb: 0x55abb196ced0
[ec_ems_context_submit_work:641] Call submitted successfully.
obj-id: 0, desc: REST API to get EMS Serial Number., entry: api/v1/system/serial_number.
[_match_server_cert_key:462] verify_peer_method: 3
```

- A. FortiGate is not able to reach the IP address or FQDN of the FortiClient EMS server.
- B. FortiGate is not able to verify the FortiClient EMS serial number.
- C. FortiGate is not able to establish trust using the FortiClient EMS CA certificate.
- D. FortiGate is not able to reach FortiClient EMS on telemetry port 8013.

**Answer: B**

**Explanation:**

The debug output shows "EMS verification data has changed on host or peer. Must reverify," indicating that FortiGate cannot verify the FortiClient EMS serial number, causing the connectivity issue.

**QUESTION 9**

How do you remove FortiClient from a quarantine list?

- A. Disconnect the endpoint from FortiClient telemetry.
- B. Revoke the FortiClient certificate.
- C. Shut down FortiClient on the endpoint.
- D. Use FortiAnalyzer playbooks.

**Answer: D**

**Explanation:**

FortiAnalyzer playbooks can be used to manage and remove files or endpoints from the FortiClient quarantine list, automating the remediation process across multiple endpoints.

**QUESTION 10**

An administrator has configured an organization's Security Fabric with FortiGate, FortiClient EMS, and FortiAnalyzer. The organization must provide only compliant endpoints access to their private servers by running FortiClient 7.4 and antivirus with the latest updates.

Which tags must the administrator configure to achieve this outcome?

- A. Fabric tags
- B. Classification tags
- C. FortiGuard outbreak alert tags

D. Security posture tags

**Answer: D**

**Explanation:**

Security posture tags are used to enforce compliance by identifying endpoints that meet specific security requirements, such as running FortiClient with up-to-date antivirus, and allowing only compliant endpoints access to private servers.

#### QUESTION 11

A security architect has designed a high availability (HA) solution with three FortiClient EMS nodes across two datacenters connected through site-to-site IPsec VPN with 1GB of dedicated bandwidth.

How can the architect ensure a seamless failover between FortiClient EMS nodes?

- A. License each FortiClient EMS server separately.
- B. Provide layer 2 connectivity for the FortiClient EMS servers.
- C. Include a remote SQL server in the design.
- D. Provide support for active-active HA mode.

**Answer: C**

**Explanation:**

Including a remote SQL server ensures that all FortiClient EMS nodes share a common database. This allows seamless failover between nodes, maintaining consistent endpoint data and configurations across the HA deployment.

#### QUESTION 2

An administrator must perform an initial deployment of FortiClient on domain-joined endpoints.

Which method is recommended for the deployment?

- A. Send an email to all domain users including the FortiClient installer.
- B. Import domain endpoints on FortiClient EMS and deploy FortiClient installers to the endpoints.
- C. Configure domain endpoints to download installers directly from FortiClient cloud service.
- D. Use Group Policy Object (GPO) to install FortiClient on domain endpoints.

**Answer: B**

**Explanation:**

The recommended method for deploying FortiClient on domain-joined endpoints is to import the endpoints into FortiClient EMS and deploy the FortiClient installers directly from EMS. This ensures centralized management and proper policy assignment.

## Thank You for Trying Our Product

### Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



Microsoft



ORACLE



CITRIX



JUNIPER  
NETWORKS



EMC<sup>2</sup>  
where information lives

**10% Discount Coupon Code: ASTR14**