

Fortinet

Exam Questions FCP_FMG_AD-7.4

FCP - FortiManager 7.4 Administrator



NEW QUESTION 1

Push updates are failing on a FortiGate device that is located behind a NAT device. Which two settings should the administrator check? (Choose two.)

- A. That the override server IP address is set on FortiManager and the NAT device
- B. That the external IP address on the NAT device is set to DHCP and configured with the virtual IP
- C. That the NAT device IP address and correct ports are configured on FortiManager
- D. That the virtual IP address and correct ports are set on the NAT device

Answer: AD

Explanation:

When push updates are failing on a FortiGate device behind a NAT device, the administrator should check:

- ? A. That the override server IP address is set on FortiManager and the NAT device.
 - ? D. That the virtual IP address and correct ports are set on the NAT device. Options B and C are incorrect because:
 - ? B suggests setting the external IP on the NAT device to DHCP, which is not relevant to solving the push update issue.
 - ? C implies configuring NAT device IP and ports on FortiManager, which is less likely needed compared to configuring the correct VIP and ports.
- FortiManager References:
- ? Refer to FortiManager 7.4 Administrator Guide: Device Management and NAT Configuration.

NEW QUESTION 2

Which two statements about Security Fabric integration with FortiManager are true? (Choose two.)

- A. The Fabric View module enables you to generate the Security Fabric ratings for Security Fabric devices.
- B. The Security Fabric settings are part of the device-level settings.
- C. The Fabric View module enables you to view the Security Fabric ratings for Security Fabric devices.
- D. The Security Fabric license, group name, and password are required for the FortiManager Security Fabric integration.

Answer: AC

Explanation:

Two statements about Security Fabric integration with FortiManager that are true are:

- ? A. The Fabric View module enables you to generate the Security Fabric ratings for Security Fabric devices.
 - ? C. The Fabric View module enables you to view the Security Fabric ratings for Security Fabric devices.
- Options B and D are incorrect because:
- ? B is misleading as the Security Fabric settings are generally configured and managed separately from other device-level settings.
 - ? D is incorrect as there is no specific requirement for a Security Fabric license, group name, and password solely for FortiManager integration.
- FortiManager References:
- ? Refer to FortiManager 7.4 Security Fabric Integration Guide: Managing Security Fabric and Generating Security Fabric Ratings.

NEW QUESTION 3

An administrator configures a new OSPF area on FortiManager and has not yet pushed the changes to the managed FortiGate device. In which database will the configuration be saved?

- A. Device-level database
- B. ADOM-level database
- C. Configuration-level database
- D. Revision history database

Answer: A

Explanation:

When an administrator configures a new OSPF area on FortiManager but has not yet pushed the changes to the managed FortiGate device, the configuration is saved in the Device-level database.

Explanation of Options:

- ? A. Device-level database:
- ? B. ADOM-level database:
- ? C. Configuration-level database:
- ? D. Revision history database:

NEW QUESTION 4

Which two items does an FGFM keepalive message include? (Choose two.)

- A. FortiGate IPS version
- B. FortiGate license information
- C. FortiGate configuration checksum
- D. FortiGate uptime

Answer: CD

Explanation:

The FortiGate-FortiManager (FGFM) protocol is used for communication between a FortiGate device and FortiManager. The keepalive messages are essential for maintaining communication and monitoring the health of the FortiGate devices connected to FortiManager. These messages provide important status information about the device. Here are the items included in an FGFM keepalive message:

- ? A. FortiGate IPS version
- ? B. FortiGate license information
- ? C. FortiGate configuration checksum
- ? D. FortiGate uptime

NEW QUESTION 5

An administrator is in the process of copying a system template profile between ADOMs by running the following command: `execute fmprofile import-profile ADOM2 3547 /tmp/myfile` Where does this command import the system template profile from?

- A. FortiManager file system
- B. ADOM2 object database
- C. ADOM2 device database
- D. Source ADOM policy database

Answer: A

Explanation:

The command `execute fmprofile import-profile ADOM2 3547 /tmp/myfile` is used to import a system template profile from the FortiManager file system. The path `/tmp/myfile` indicates a location in the FortiManager's local file system, from which the profile will be imported into the specified ADOM.

Options B, C, and D are incorrect because:

? B, C, and D suggest importing from different databases, which is not accurate since the command explicitly refers to the file system location.

FortiManager References:

? Refer to FortiManager 7.4 CLI Reference Guide: Commands for Profile Management.

NEW QUESTION 6

Refer to the exhibit.

FortiManager script

Create New Script

Script Name

Routing

Comments

Type

CLI Script

Run script on

Device Database

Script details

Search...

1 config router prefix-list

2 edit public

3 config rule

4 edit 1

5 set prefix 0.0.0.0/0

6 set action permit

7 next

8 edit 2

9 set prefix 8.8.8.8/32

10 set action deny

11 end

Advanced Device Filters >

Revert All Changes

Which two results occur if the script is run using the Device Database option? (Choose two.)

- A. You must install these changes on a managed device using the Install Wizard.
- B. The successful execution of a script on the Device Database creates a new revision history.
- C. The script history shows successful installation of the script on the remote FortiGate device.
- D. The device Config Status is tagged as Modified.

Answer: AD

Explanation:

If the script is run using the "Device Database" option on FortiManager, the following occurs:
? A.You must install these changes on a managed device using the Install Wizard.
? D.The device Config Status is tagged as Modified. Options B and C are incorrect because:
? Bsuggests a new revision history is created, but this only happens when changes are actually installed on the managed device.
? Cimplies the script is directly executed on the FortiGate, which is not the case when using the Device Database option.
FortiManager References:
? Refer to FortiManager 7.4 Administrator Guide: Scripting and Configuration Management.

NEW QUESTION 7

Exhibit.

```
FortiManager # diagnose dvm device list
--- There are currently 1 devices/vdoms managed ---
--- There are currently 1 devices/vdoms count for license ---

TYPE              OID    SN              HA    IP              NAME              ADOM    IPS              FIRMWARE
fmgfaz-managed    325    FGV010000077646 -    10.0.1.200    ISFW              ADOM2    6.00741 (regular)  7.0 MR4 (2463)
|- STATUS: dev-db: modified; conf: in sync; cond: pending; dm: retrieved; conn: up
|- vdom:[3]root flags:1 adom:ADOM2 pkg: [imported]ISFW
```

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

- A. The latest revision history for the managed FortiGate does not match the device-level database.
- B. Configuration changes have been installed on FortiGate, which means the FortiGate configuration has been changed.
- C. Configuration changes directly made on FortiGate have been automatically updated to the device-level database.
- D. The latest revision history for the managed FortiGate does match the FortiGate running configuration.

Answer: AB

Explanation:

The output indicates that:

? The device's status is shown as "dev-db: modified" and "conf: in sync," which means that there is a difference between the device-level database on FortiManager and the actual running configuration of the managed FortiGate. Therefore, the latest revision history for the managed FortiGate does not match the device-level database, which confirms statement A as true.

? "dm: retrieved" status indicates that configuration changes have been installed on the FortiGate, confirming statement B as true. It also means that the configuration has been modified, and those changes have been pulled from the FortiGate to the FortiManager.

Statements C and D are incorrect because:

? C is incorrect as it implies an automatic update, whereas "dev-db: modified" indicates changes have been made on the FortiGate device that are not yet reflected in the FortiManager's database.

? D is incorrect because "dev-db: modified" shows that the device-level database and running configuration are not in sync.

FortiManager References:

? Refer to the FortiManager 7.4 Administrator Guide: Device Manager > Device Status to understand the "dev-db" and "conf" status meanings.

NEW QUESTION 8

An administrator created a new global policy package that includes header and footer policies and then assigned it to an ADOM. What are two outcomes of this action? (Choose two.)

- A. To assign another global policy package later to the same ADO
- B. you must unassign this policy first.
- C. After you assign the global policy package to an ADO
- D. the impacted policy packages become hidden in that ADOM.
- E. You can edit or delete all the global objects in the global ADOM.
- F. You must manually move the header and footer policies after the policy assignment.

Answer: AC

Explanation:

? Option A: To assign another global policy package later to the same ADOM, you must unassign this policy first. This is correct. FortiManager does not allow multiple global policy packages to be assigned to a single ADOM simultaneously. If you want to assign a different global policy package, the existing one must be unassigned first.

? Option C: You can edit or delete all the global objects in the global ADOM. This is correct. Once a global policy package is assigned, you have the flexibility to edit or delete global objects in the global ADOM, affecting all ADOMs to which this package is assigned.

Explanation of Incorrect Options:

? Option B: After you assign the global policy package to an ADOM, the impacted policy packages become hidden in that ADOM is incorrect because the policy packages do not become hidden; they are modified according to the global policies.

? Option D: You must manually move the header and footer policies after the policy assignment is incorrect because header and footer policies are automatically applied when assigned.

FortiManager References:

? See the "Global Policy and ADOM Management" section in the FortiManager Administration Guide.

NEW QUESTION 9

Which statement about the policy lock feature on FortiManager is true?

- A. Policy locking is available in workspace normal mode.
- B. Locking a policy takes precedence over a locked ADOM.
- C. When a policy is locked, the ADOM that contains it is also locked.
- D. Administrators in the approval group can work concurrently on a locked policy.

Answer: A

Explanation:

The statement that is true about the policy lock feature on FortiManager is:

? A. Policy locking is available in workspace normal mode.

In FortiManager, when working in "workspace-mode normal," policies can be locked by administrators to prevent other administrators from editing them simultaneously. This ensures that only one administrator makes changes at any given time, reducing conflicts or mistakes due to concurrent modifications.

Statements B, C, and D are incorrect because:

? B is incorrect since locking a policy does not override a locked ADOM. The ADOM lock takes precedence.

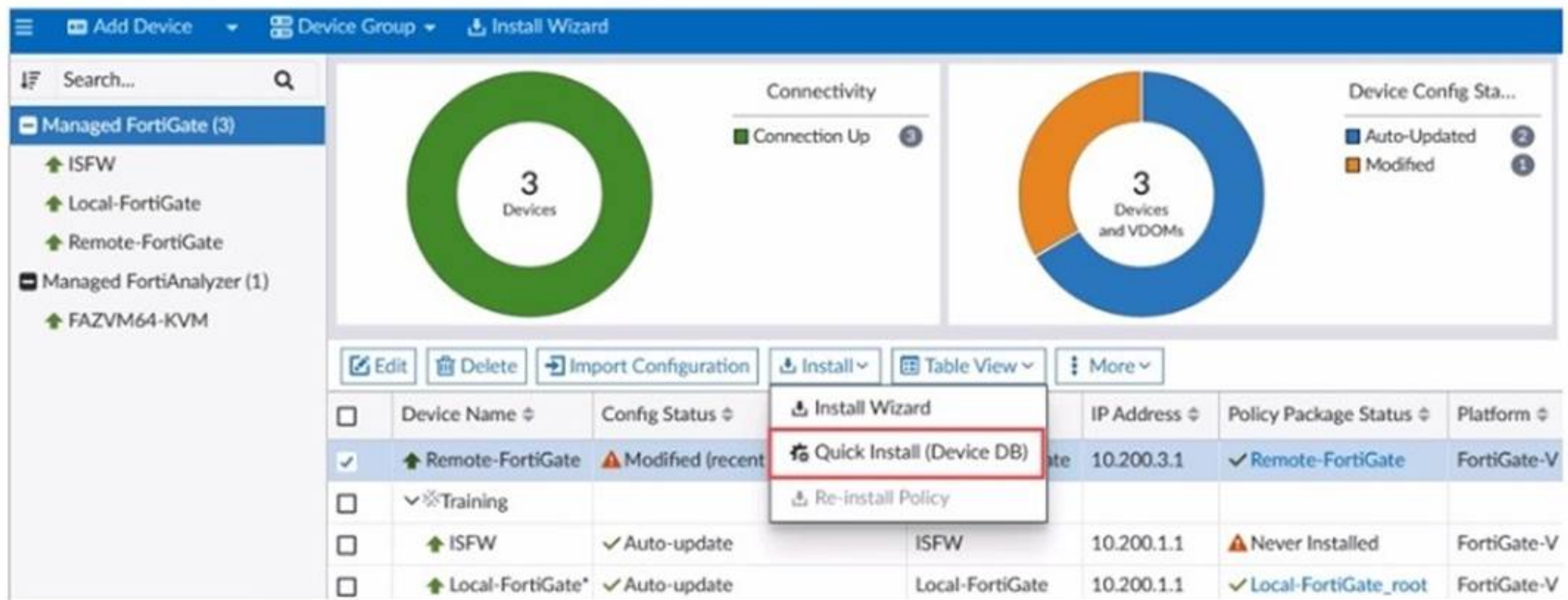
? C is incorrect because when a policy is locked, it does not necessarily mean the ADOM is locked.

? D is incorrect because administrators in the approval group cannot work concurrently on a locked policy; the policy lock prevents concurrent modifications.
 FortiManager References:
 ? Refer to FortiManager 7.4 Administrator Guide: Policy and Objects > Policy Locking to understand how the policy lock feature functions in different workspace modes.

NEW QUESTION 10

Refer to the exhibit.

FortiManager managed devices



You are using the Quick Install option to install configuration changes on the managed FortiGate.
 Which two statements correctly describe the result? (Choose two.)

- A. It installs provisioning template changes on the FortiGate device.
- B. It provides the option to preview only the policy package changes before installing them.
- C. It installs all the changes in the device database first and the administrator must reinstall the changes on the FortiGate device.
- D. It installs device-level changes on the FortiGate device without launching the Install Wizard

Answer: BD

Explanation:

? Option B: It provides the option to preview only the policy package changes before installing them. This is correct. The Quick Install option in FortiManager provides a preview of policy changes before they are applied, allowing administrators to review and confirm the changes.

? Option D: It installs device-level changes on the FortiGate device without launching the Install Wizard. This is correct. Quick Install allows for the immediate installation of device-level changes, such as interface or routing configurations, directly onto the FortiGate without going through the full Install Wizard.

Explanation of Incorrect Options:

? Option A: It installs provisioning template changes on the FortiGate device is incorrect because Quick Install does not specifically deal with provisioning templates.

? Option C: It installs all the changes in the device database first and the administrator must reinstall the changes on the FortiGate device is incorrect because Quick Install directly applies changes to the FortiGate device, not requiring a separate reinstall step.

FortiManager References:

? Refer to "FortiManager Administration Guide" for details on "Quick Install" functionality under "Device Management."

NEW QUESTION 10

Which statement about the upgrade of ADOMs on FortiManager is true?

- A. To ensure database consistency, you must upgrade an ADOM before you upgrade the devices in it.
- B. Upgrading the FortiManager version upgrades all existing ADOMs automatically.
- C. You cannot import policies from a device until its FortiOS version matches the ADOM version.
- D. ADOMs using global objects can be upgraded before or after upgrading the global database ADOM.

Answer: A

Explanation:

? Option A: To ensure database consistency, you must upgrade an ADOM before you upgrade the devices in it. This is the correct answer. When upgrading ADOMs on FortiManager, the ADOM must be upgraded first to match the FortiOS version of the devices it manages. This is necessary to ensure compatibility and consistency between the ADOM's database schema and the FortiGate's configuration.

Explanation of Incorrect Options:

? Option B: Upgrading the FortiManager version upgrades all existing ADOMs automatically is incorrect because the ADOMs must be upgraded manually or individually after upgrading the FortiManager.

? Option C: You cannot import policies from a device until its FortiOS version matches the ADOM version is incorrect because while version matching is important, it is not strictly necessary for policy import.

? Option D: ADOMs using global objects can be upgraded before or after upgrading the global database ADOM is incorrect as the order of upgrade matters to maintain compatibility.

FortiManager References:

? Refer to "FortiManager Upgrade Guide" for detailed procedures on upgrading ADOMs and devices.

NEW QUESTION 12

Refer to the exhibit which shows the Download Import Report.

```
Start to import config from device(Remote-FortiGate) vdom(root) to
adom(root), package(Remote-FortiGate_root)

"firewall address",SKIPPED,"(name=all, oid=2309, DUPLICATE)"

"firewall address",FAIL,"(name=REMOTE_SUBNET, oid=2311,
reason=interface((firewall address:REMOTE_SUBNET) any<-port6) binding
fail)"

"firewall policy",FAIL,"(name=1, oid=3070, reason=interface(interface binding
contradiction. detail: (firewall address:REMOTE_SUBNET) any<-port6) binding
fail)"
```

Why is FortiManager failing to import firewall policy ID 1?

- A. Policy ID 1 is configured from the interface any to port6. FortiManager rejects the request to import this policy because the any interface does not exist on FortiManager
- B. Policy ID 1 for this managed FortiGate already exists on FortiManager in the policy package named Remote-FortlGate.
- C. Policy ID 1 has an address object that already exists in the ADOM database with any as the interface association, and conflicts with the address object interface association locally on FortiGate.
- D. Policy ID 1 does not have the ADOM Interface mapping configured on FortiManager.

Answer: A

Explanation:

? Option A: Policy ID 1 is configured from the interface any to port6. FortiManager rejects the request to import this policy because the any interface does not exist on FortiManager. This is the correct answer. FortiManager fails to import firewall policy ID 1 because it cannot map the "any" interface to a valid interface in its ADOM database. The error indicates that there is a binding failure due to an interface mismatch.

Explanation of Incorrect Options:

? Option B: Policy ID 1 for this managed FortiGate already exists on FortiManager in the policy package named Remote-FortiGate is incorrect because the error is related to interface mapping, not a duplicate policy ID.

? Option C: Policy ID 1 has an address object that already exists in the ADOM database with any as the interface association and conflicts with the address object interface association locally on FortiGate is incorrect because the error specifies an interface issue, not an address object conflict.

? Option D: Policy ID 1 does not have the ADOM Interface mapping configured on FortiManager is incorrect because the error directly mentions a binding failure due to the "any" interface.

FortiManager References:

? For more information, refer to the "Device Manager" section and "Configuration Import and Mapping" in the FortiManager Administration Guide.

NEW QUESTION 14

An administrator has assigned a global policy package to custom ADOM1. Then the administrator creates a new policy package. Fortinet. in the custom ADOM1. What happens to the Fortinet policy package when it is created?

- A. You must assign the global policy package from the global ADOM.
- B. The global policy package is automatically assigned.
- C. You must reapply the global policy package to ADOM1.
- D. You can select the option to assign the global policies.

Answer: B

Explanation:

When a new policy package is created in a custom ADOM that already has a global policy package assigned, the global policy package is automatically assigned to the

new policy package. This behavior ensures consistent policy enforcement across different ADOMs.

Options A, C, and D are incorrect because:

? A and C incorrectly suggest that manual reassignment or reapplication is needed.

? D implies optional assignment, whereas it is automatically done.

FortiManager References:

? Refer to FortiManager 7.4 Administrator Guide: Working with Global and Custom ADOM Policy Packages

NEW QUESTION 17

An administrator wants to create a policy on an ADOM that is in backup mode and install it on a FortiGate device in the same ADOM. How can the administrator perform this task?

- A. The administrator must use the Policy & Objects section to create a policy first.
- B. The administrator must use a FortiManager script.

- C. The administrator must disable the FortiManager offline mode first.
D. The administrator must change the ADOM mode to Advanced to bring the FortiManager online.

Answer: B

Explanation:

To create and install a policy on a FortiGate device in an ADOM (Administrative Domain) that is in backup mode, the administrator must use a FortiManager script. This is because backup mode restricts direct configuration changes, and scripts can be used to push specific configuration changes without altering the ADOM mode.

Options A, C, and D are incorrect because:

? A requires the ADOM to be in normal or advanced mode to create policies directly in the Policy & Objects section.

? C suggests disabling offline mode, which is irrelevant to the backup mode configuration.

? D implies changing the ADOM mode, which is unnecessary if using a script to perform the task.

FortiManager References:

? Refer to FortiManager 7.4 Administrator Guide: Working with ADOMs and Using Scripts for managing policies in backup mode.

NEW QUESTION 22

Refer to the exhibit.

FortiManager CLI output

```
FortiManager # execute top
top - 13:08:23 up 1 day,  1:01,  0 users,  load average: 2.40, 3.19, 3.34

Tasks: 188 total,   2 running, 186 sleeping,   0 stopped,   0 zombie

%Cpu(s): 15.4 us,  7.7 sy,  0.0 ni, 76.9 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st

MiB Mem : 7955.5 total,  2235.6 free,  2895.6 used,  2824.1 buff/cache

MiB Swap: 2048.0 total,  2048.0 free,    0.0 used.  4011.0 avail Mem

   PID USER      PR  NI   VIRT   RES  %CPU  %MEM     TIME+ S COMMAND
 1163 root        20   0   17.6m   2.1m   7.1   0.1   0:00.05 R top
    1 root        20   0 602.2m  14.9m   0.0   0.7   0:11.67 S /bin/initXXXXXXXXXX
    2 root        20   0    0.0m   0.0m   0.0   0.0   0:00.00 S [kthreadd]
 1462 root        20   0 303.2m 248.0m   0.0   3.1   0:14.72 S fwmsvrd
 1463 root        20   0 288.2m 232.3m   0.0   2.9   0:16.47 S fgdlinkd
 1465 root        20   0 383.7m 328.0m   0.0   4.1   0:15.26 S fgdsvr
 1467 root        20   0  84.0m  23.6m   0.0   0.3   0:00.06 S /bin/fgdhttpd
 1468 root        20   0  63.9m  13.1m   0.0   0.2   0:13.00 S fgdupd
 1469 root        20   0  63.5m  12.6m   0.0   0.2   0:00.07 S fmtr_svr
 1470 root        20   0   6.3m   3.5m   0.0   0.0   0:00.09 S /bin/webconsole
 1471 root        20   0 996.4m 850.6m   0.0  10.7   0:00.01 S srchd
 1475 root        20   0 996.4m 120.6m   0.0   1.5   0:00.00 S fclinkd
```

What percent of the available RAM is being used by the process in charge of downloading the web and email filter databases from the public FortiGuard servers?

- A. 2.9
B. 3.1
C. 1.5
D. 4.1

Answer: A

Explanation:

In the exhibit, the FortiManager CLI output displays the results of the `top` command, which shows system processes, CPU usage, and memory (RAM) usage. We are specifically looking for the process responsible for downloading the web and email filter databases from the public FortiGuard servers. This process is typically handled by the `thefgdlinkd` process.

Key information from the output:

? The `thefgdlinkd` process is listed with a PID of 1463.

? The `%MEM` column shows that this process is using 2.9% of the available RAM.

Evaluation of Options:

? A. 2.9: This is incorrect. The `thefgdlinkd` process, which handles the web and email filter database downloads, is using 2.9% of the available memory, as indicated in the `%MEM` column.

? B. 3.1: This is incorrect. The 3.1% memory usage belongs to the `thefwmsvrd` process, not the `fgdlinkd` process.

? C. 1.5: This is incorrect. The 1.5% memory usage belongs to the `thefclinkd` process, not the `fgdlinkd` process.

? D. 4.1: This is incorrect. The 4.1% memory usage belongs to the `thefgdsvr` process, not the `fgdlinkd` process.

NEW QUESTION 24

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

FCP_FMG_AD-7.4 Practice Exam Features:

- * FCP_FMG_AD-7.4 Questions and Answers Updated Frequently
- * FCP_FMG_AD-7.4 Practice Questions Verified by Expert Senior Certified Staff
- * FCP_FMG_AD-7.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * FCP_FMG_AD-7.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The FCP_FMG_AD-7.4 Practice Test Here](#)