

Exam Questions FCP_FMG_AD-7.4

FCP - FortiManager 7.4 Administrator

https://www.2passeasy.com/dumps/FCP_FMG_AD-7.4/



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

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

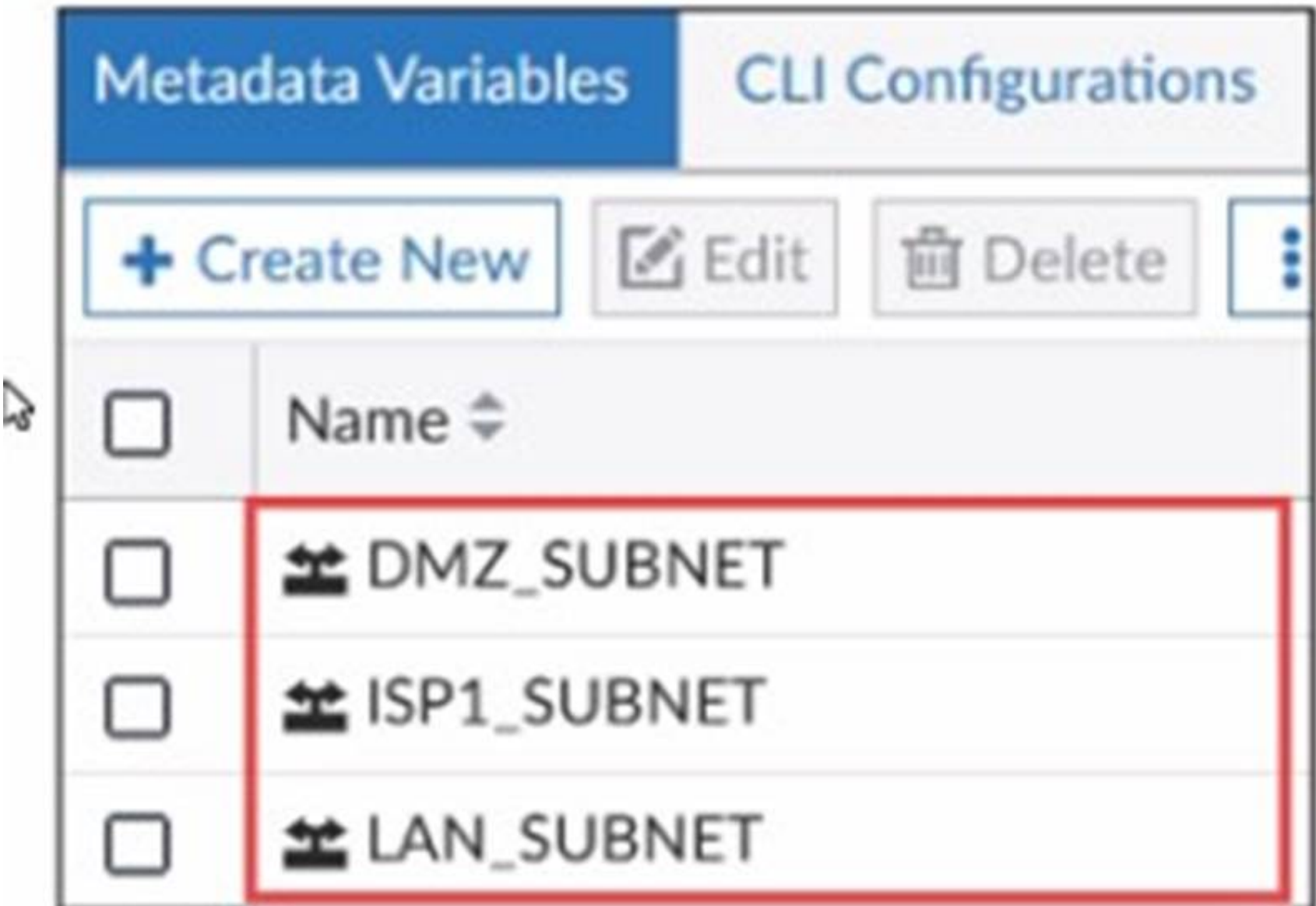
Answer: A

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 3

Exhibit.



What is true about the objects highlighted in the image?

- A. They can be set to optional or required.
- B. They are available across all ADOMs by default.
- C. They can be used as variables in scripts.
- D. They cannot be created in the global database ADOM.

Answer: C

Explanation:

The objects highlighted in the image (DMZ_SUBNET, ISP1_SUBNET, LAN_SUBNET) are metadata variables.

? C. They can be used as variables in scripts.

Options A, B, and D are incorrect because:

? A suggests optional or required settings, which do not apply to metadata variables.

? B implies they are available across all ADOMs by default, which is not always the case.

? D states they cannot be created in the global database ADOM, but metadata variables are typically managed within ADOMs and can be utilized globally based on specific configurations.

FortiManager References:

? Refer to FortiManager 7.4 Administrator Guide: Using Metadata Variables and Script Management.

NEW QUESTION 4

In the event that one of the secondary FortiManager devices fails, which action must be performed to return the FortiManager HA manual mode to a working state?

- A. The FortiManager HA state transition is transparent to administrators and does not require any reconfiguration.
- B. Reboot the failed device to remove its IP from the primary device.
- C. Manually promote one of the working secondary devices to the primary role, and reboot the old primary device to remove the peer IP of the failed device.
- D. Reconfigure the primary device to remove the peer IP of the failed device.

Answer: C

Explanation:

When a secondary FortiManager device fails in HA manual mode, an administrator must manually promote one of the working secondary devices to the primary role and reboot the old primary device to remove the peer IP of the failed device. This ensures the HA configuration is updated correctly, and the network remains resilient.

Options A, B, and D are incorrect because:

? A suggests the transition is transparent, which is true only in automatic mode, not in manual mode.

? B and D imply simpler steps that do not fully address the HA reconfiguration process in manual mode.

FortiManager References:

? Refer to FortiManager 7.4 High Availability (HA) Configuration Guide: Manual Mode Configuration and Failover Procedures.

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

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    FGVM010000077646 -    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 7

Which configuration setting for FortiGate is part of an ADOM-level database on FortiManager?

- A. NSX-T Service Template
- B. Routing
- C. SNMP
- D. Security profiles

Answer: B

Explanation:

? Option B: Routing is the correct answer. The ADOM-level database in FortiManager stores configuration settings such as routing, firewall policies, and objects that are shared across multiple devices in the ADOM.

Explanation of Incorrect Options:

? Option A: NSX-T Service Template is incorrect as it is not a FortiGate-specific setting managed at the ADOM level.

? Option C: SNMP is incorrect because SNMP settings are typically managed on a per-device basis.

? Option D: Security profiles is incorrect because security profiles are generally device-level configurations, not ADOM-level.

FortiManager References:

? Refer to "FortiManager Administration Guide" for further details on ADOM-level and device-level configurations.

NEW QUESTION 8

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 9

Refer to the exhibit.

FortiManager managed devices

Search...

Managed FortiGate (3)

- ISFW
- Local-FortiGate
- Remote-FortiGate

Managed FortiAnalyzer (1)

- FAZVM64-KVM

Connectivity

Connection Up 3

Device Config Sta...

Auto-Updated 2

Modified 1

3 Devices

3 Devices and VDOMs

Edit Delete Import Configuration Install Table View More

Install Wizard Quick Install (Device DB) Re-install Policy

Device Name	Config Status	IP Address	Policy Package Status	Platform
Remote-FortiGate	Modified (recent)	10.200.3.1	Remote-FortiGate	FortiGate-V
ISFW	Auto-update	10.200.1.1	Never Installed	FortiGate-V
Local-FortiGate*	Auto-update	10.200.1.1	Local-FortiGate_root	FortiGate-V

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 API method is used to create objects or overwrite existing ones?

- A. Set
- B. Add
- C. Exec
- D. Update

Answer: A

Explanation:

In the context of the FortiManager JSON API, the set method is used to create new objects or overwrite existing ones. The API allows administrators to manage FortiManager and its associated devices by automating tasks like configuration changes, policy updates, and object creation.

Explanation of Options:

- ? A. Set:
- ? B. Add:
- ? C. Exec:
- ? D. Update:

NEW QUESTION 10

Which output is displayed right after moving the ISFW device from one ADOM to another?

A)

```
FortiManager # diagnose dvm device list ISFW
--- There are currently 4 devices/vdoms managed ---
--- There are currently 4 devices/vdoms count for license ---

TYPE          OID    SN              HA      IP          NAME      ADOM      IPS          FIRMWARE
fmgfaz-managed 325    FGVM010000077646 -      10.0.1.200  ISFW      ADOM74    6.00741 (regular) 7.0 MR4 (2463)
|- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; conn: up
|- vdom: [3]root flags:0 adom:ADOM74 pkg:[unknown]ISFW
```

B)

```
FortiManager # diagnose dvm device list ISFW
--- There are currently 4 devices/vdoms managed ---
--- There are currently 4 devices/vdoms count for license ---

TYPE          OID    SN              HA      IP          NAME          ADOM      IPS          FIRMWARE
fmgfaz-managed 325    FGVM010000077646 -      10.0.1.200    ISFW          ADOM74      6.00741 (regular) 7.0 MR4 (2463)
|- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: autoupdated; conn: up
|- vdom:[3]root flags:1 adom:ADOM74 pkg:[out-of-sync]ISFW
```

C)

```
FortiManager # FortiManager # diagnose dvm device list ISFW
--- There are currently 4 devices/vdoms managed ---
--- There are currently 4 devices/vdoms count for license ---

TYPE          OID    SN              HA      IP          NAME          ADOM      IPS          FIRMWARE
fmgfaz-managed 325    FGVM010000077646 -      10.0.1.200    ISFW          ADOM74      6.00741 (regular) 7.0 MR4 (2463)
|- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: installed; conn: up
|- vdom:[3]root flags:0 adom:ADOM74 pkg:[never-installed]
```

D)

```
FortiManager # diagnose dvm device list ISFW
--- There are currently 4 devices/vdoms managed ---
--- There are currently 4 devices/vdoms count for license ---

TYPE          OID    SN              HA      IP          NAME          ADOM      IPS          FIRMWARE
fmgfaz-managed 325    FGVM010000077646 -      10.0.1.200    ISFW          ADOM74      6.00741 (regular) 7.0 MR4 (2463)
|- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: installed; conn: up
|- vdom:[3]root flags:0 adom:ADOM74 pkg:[imported]ISFW
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

Explanation:

When a FortiGate device, like the ISFW (Internal Segmentation Firewall), is moved from one ADOM to another in FortiManager, the status of the device in the new ADOM will temporarily show some level of inconsistency or unknown state until the ADOM fully syncs and integrates the device.

In the provided options, we are analyzing the FortiManager diagnose dvm device list output for the ISFW device.

Explanation of the Outputs:

? Option A:

? Option B:

? Option C:

? Option D:

Conclusion:

The output that is displayed immediately after moving the ISFW device from one ADOM to another is Option A, where the package status is still unknown (pkg: [unknown]) because FortiManager has not yet fully synchronized the device's configuration in the new ADOM.

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 16

Refer to the exhibit.



An administrator is about to add the FortiGate device to FortiManager using the discovery process. FortiManager is operating behind a NAT device, and the administrator configured the FortiManager NATed IP address under the FortiManager system administration settings. What is the expected result?

- A. During discover
- B. FortiManager uses only the FortiGate serial number to establish the
- C. During discovery, FortiManager sets both the FortiManager NATed IP address and NAT device IP address on FortiGate.
- D. During discover
- E. FortiManager sets the NATed device IP address on FortiGate.
- F. During discovery, FortiManager sets the FortiManager NATed IP address on FortiGate.

Answer: D

Explanation:

When adding a FortiGate device to FortiManager that is operating behind a NAT device, and the FortiManager NATed IP address is configured under the system administration settings, FortiManager will set the FortiManager NATed IP address on the FortiGate device during the discovery process. This ensures that the FortiGate knows how to reach the FortiManager through the NAT device.

Options A, B, and C are incorrect because:

? A is incorrect because the discovery process also requires knowing the NATed IP to establish a connection, not just the serial number.

? B is incorrect because FortiManager does not set the NAT device's IP address on the FortiGate.

? C is incorrect because it implies that the NAT device IP is set on FortiGate, which is not the expected outcome.

FortiManager References:

? Refer to FortiManager 7.4 Administrator Guide: Device Discovery and Management with NAT.

NEW QUESTION 21

Refer to the exhibit.

Mapped Device	Details
Local-FortiGate [root]	IP/Netmask: 192.168.1.0,255.255.255.240

An administrator has created a firewall address object that is used in multiple policy packages for multiple FortiGate devices in an ADOM. After the installation operation is performed, which IP/netmask is shown on FortiManager for this firewall address object for devices without a Per-Device Mapping set?

- A. FortiManager generates an error for each FortiGate without a per-device mapping defined for that object.
- B. 192.168.1.0/24
- C. 192.168.1.0/28
- D. FortiManager replaces the address object to none.

Answer: B

Explanation:

? Option B: 192.168.1.0/24 is the correct answer. In FortiManager, when a firewall address object is defined and used across multiple policy packages without any Per-Device Mapping, the default value configured in the object definition (192.168.1.0/255.255.255.0) is applied to all devices. The exhibit shows that the address object LOCAL_SUBNET has a default IP/netmask of 192.168.1.0/24. Therefore, FortiManager will use this default value for any FortiGate device that does not have a specific Per-Device Mapping configured.

? Explanation of Incorrect Options:

FortiManager References:

? Refer to the FortiManager 7.4 Administration Guide, specifically in sections related to "Address Object Management" and "Per-Device Mapping," which detail the behavior of address objects without specific device mappings.

NEW QUESTION 26

An administrator enabled workspace mode and now wants to delete an address object that is currently referenced in a firewall policy. Which two results can the administrator expect? (Choose two.)

- A. FortiManager will temporarily change the status of the referenced firewall policy to disabled.
- B. FortiManager will disable the status of the address object until the changes are installed.
- C. FortiManager will not allow the administrator to delete a referenced address object until they lock the ADOM.
- D. FortiManager will replace the deleted address object with the none address object in the referenced firewall policy.

Answer: CD

Explanation:

When operating in workspace mode on FortiManager 7.4, the administrator must understand how object references and deletions work:

? Option C- "FortiManager will not allow the administrator to delete a referenced

address object until they lock the ADOM": In workspace mode, all changes are managed within an Administrative Domain (ADOM) scope. When an object (like an address object) is referenced in a policy, FortiManager prevents its deletion to maintain configuration integrity. The ADOM must be locked by the administrator to make changes to any referenced objects. This locking mechanism ensures that no unintended deletions or changes occur that could disrupt the policies or configuration.

? Option D- "FortiManager will replace the deleted address object with the none

address object in the referenced firewall policy": If the administrator attempts to delete an address object that is currently referenced by a firewall policy, FortiManager will replace the deleted object with the 'none' address object. This is done to maintain the policy structure and avoid policy corruption due to a missing reference. This behavior ensures that the firewall policy remains syntactically correct, even though the specific address object is no longer in use.

NEW QUESTION 27

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 `thefgdsrvr` process, not the `fgdlinkd` process.

NEW QUESTION 28

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual FCP_FMG_AD-7.4 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the FCP_FMG_AD-7.4 Product From:

https://www.2passeasy.com/dumps/FCP_FMG_AD-7.4/

Money Back Guarantee

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