Fortinet

Exam Questions FCP_FMG_AD-7.4

FCP - FortiManager 7.4 Administrator

NEW QUESTION 1
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. Thekeepalive messagesare 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

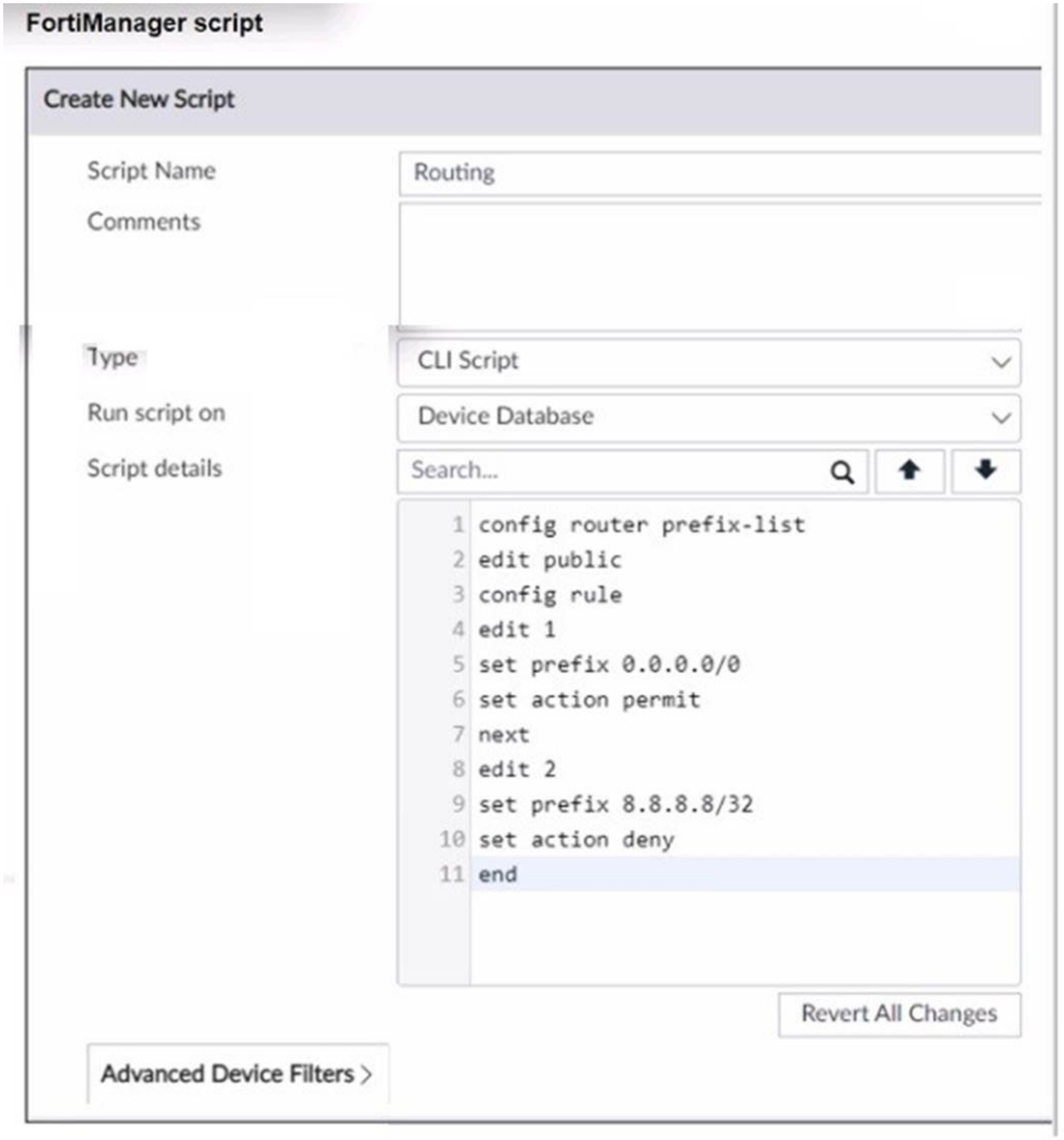
NEW QUESTION 2
An administrator has enabled Service Access on FortiManager. What is the purpose of Service Access on the FortiManager interface?

A. It allows administrative access to FortiManager.
B. It allows FortiManager to respond to requests for FortiGuard services from FortiGate devices.
C. It allows third-party applications to gain read/write access to FortiManager.
D. It allows FortiManager to determine the connection status of managed devices.

Answer: B

Explanation:
? Option B: It allows FortiManager to respond to requests for FortiGuard services
from FortiGate devices.This is the correct answer. When Service Access is enabled on FortiManager, it allows FortiManager to act as a local FortiGuard server for the managed FortiGate devices. This enables the FortiManager to respond to requests for FortiGuard services, such as updates for antivirus, web filtering, and other security services.
Explanation of Incorrect Options:
? Option A: It allows administrative access to FortiManageris incorrect because Service Access is specifically for FortiGuard service communication, not for administrative access.
? Option C: It allows third-party applications to gain read/write access to FortiManageris incorrect because Service Access does not provide API or third- party access capabilities.
? Option D: It allows FortiManager to determine the connection status of managed devicesis incorrect because Service Access does not directly manage or check connectivity status of devices; it is used for FortiGuard service requests.
FortiManager References:
? Refer to the "FortiManager Administration Guide," particularly the sections on "Service Access Settings" and "FortiGuard Services."

NEW QUESTION 3
Refer to the exhibit.



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 4

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
```

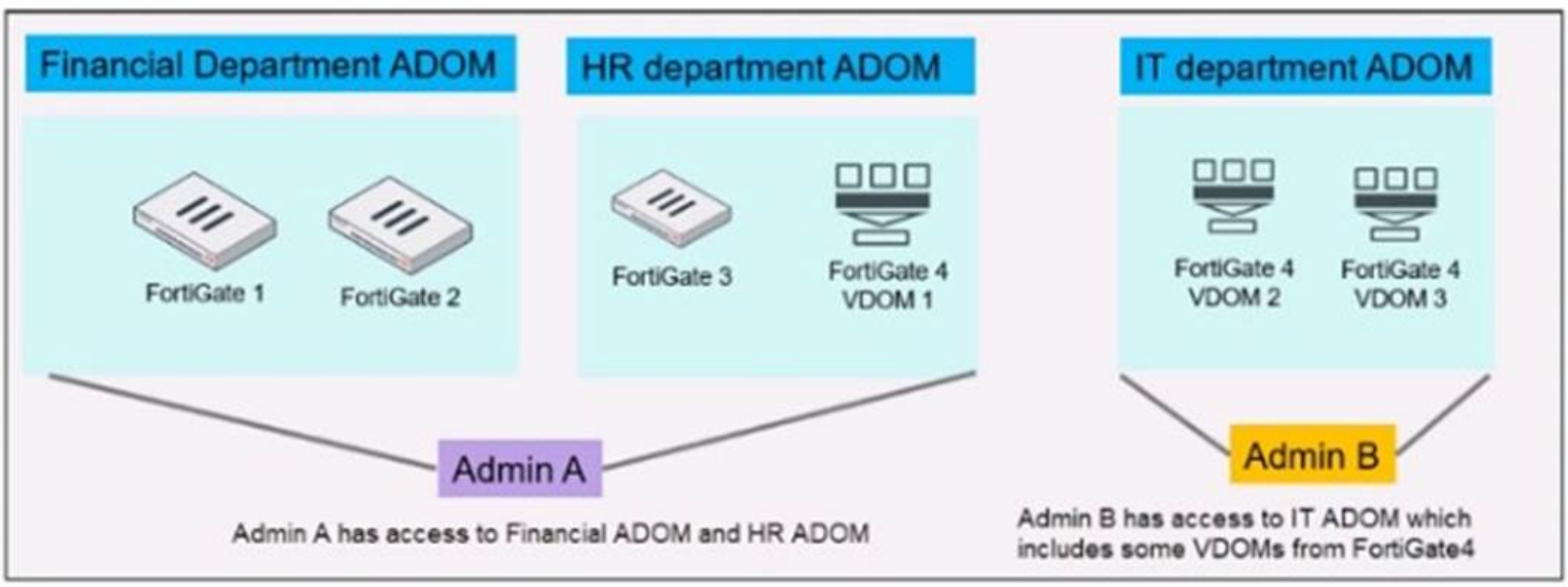
Which two statements about the output are true? (Choose two.)

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 5
Exhibit.



An administrator would like to create three ADOMs on FortiManager with different access levels based on departments. What two conclusions can you draw from the design shown in the exhibit? (Choose two.)

A. The FortiManager administrator must set the ADOM device mode to Advanced
B. Policies and objects databases can be shared between the Financial and HR ADOMs.
C. An administrator with the super user profile can access all the VDOMs.
D. The administrator must configure FortiManager in workspace normal mode.

Answer: AC

Explanation:
Based on the exhibit, the FortiManager administrator is setting up three ADOMs (Administrative Domains) that correspond to different departments (Financial, HR, and IT). Each ADOM has specificFortiGate devices or VDOMs (Virtual Domains) assigned to it, with different administrators managing the ADOMs.
Explanation of Options:
? A. The FortiManager administrator must set the ADOM device mode to Advanced.
? B. Policies and objects databases can be shared between the Financial and HR ADOMs.
? C. An administrator with the super user profile can access all the VDOMs.
? D. The administrator must configure FortiManager in workspace normal mode.
Conclusion:
? Ais correct becauseAdvanced modeis necessary for managing VDOMs within ADOMs.
? Cis correct because asuper usercan access all VDOMs and ADOMs without restrictions.

NEW QUESTION 6
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 automaticallyis 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 versionis 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 ADOMis 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 7
What is the purpose of ADOM revisions?

A. To save the current state of the whole ADOM
B. To save the current state of all policy packages and objects for an ADOM
C. To revert individual policy packages and device-level settings for a managed FortiGate
D. To save the FortiManager configuration in the System Checkpoints

Answer: B

Explanation:
? Option B: To save the current state of all policy packages and objects for an ADOMis the correct answer. ADOM (Administrative Domain) revisions in FortiManager are used to create a snapshot of the current state of all policy packages and objects associated with an ADOM. This allows administrators to save a specific configuration state and revert to it if necessary. It helps in managing changes and recovering from configuration errors or unintended changes.
? Explanation of Incorrect Options:
FortiManager References:
? Refer to the FortiManager 7.4 Administration Guide, "ADOM Management" section, which describes the purpose and usage of ADOM revisions for configuration management and restoration.

NEW QUESTION 8
What will be the result of reverting to a previous revision version in the revision history?

A. It win install configuration changes to managed device automatically.
B. It will tag the device settings status as Auto-Update.
C. It will modify the device-level database.
D. It will generate a new version ID and remove all other revision history versions.

Answer: C

Explanation:
? Option C: It will modify the device-level database.This is correct. Reverting to a previous revision version in the revision history affects the device-level database by restoring it to the state saved in the selected revision. This ensures that any changes made after the selected revision are discarded, and the device configuration is returned to the earlier state.
Explanation of Incorrect Options:
? Option A: It will install configuration changes to managed devices automaticallyis incorrect because reverting a revision does not automatically push changes to the devices; it merely reverts the configuration on the FortiManager.
? Option B: It will tag the device settings status as Auto-Updateis incorrect because "Auto-Update" is not a status related to the revision history mechanism.
? Option D: It will generate a new version ID and remove all other revision history versionsis incorrect as reverting to a previous revision does not delete all other versions; it creates a new revision point for tracking.
FortiManager References:
? Refer to the "Revision Management" section in the FortiManager Administration Guide, which provides an overview of how revisions are managed and utilized for restoring configurations.

NEW QUESTION 9
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_svrd
 1470 root      20   0    6.3m   3.5m  0.0   0.0   0:00.09 S /bin/webconsoled
 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 thetopcommand, which shows system processes, CPU usage, and memory (RAM) usage. We are specifically looking for the process responsible for downloading theweb and email filter databases from the public FortiGuard servers. This process is typically handled by thefgdlinkd process.
Key information from the output:
? Thefgdlinkdprocess is listed with aPID of 1463.
? The%MEMcolumn shows that this process is using2.9%of the available RAM.
Evaluation of Options:
? A. 2.9: This iscorrect. Thefgdlinkdprocess, which handles the web and email filter database downloads, is using2.9%of the available memory, as indicated in the%MEMcolumn.
? B. 3.1: This is incorrect. The3.1%memory usage belongs to thefwmsvrdprocess, not the fgdlinkd process.
? C. 1.5: This is incorrect. The1.5%memory usage belongs to thefclinkdprocess, not the fgdlinkd process.
? D. 4.1: This is incorrect. The4.1%memory usage belongs to thefgdsvrprocess, not the fgdlinkd process.

NEW QUESTION 10
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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