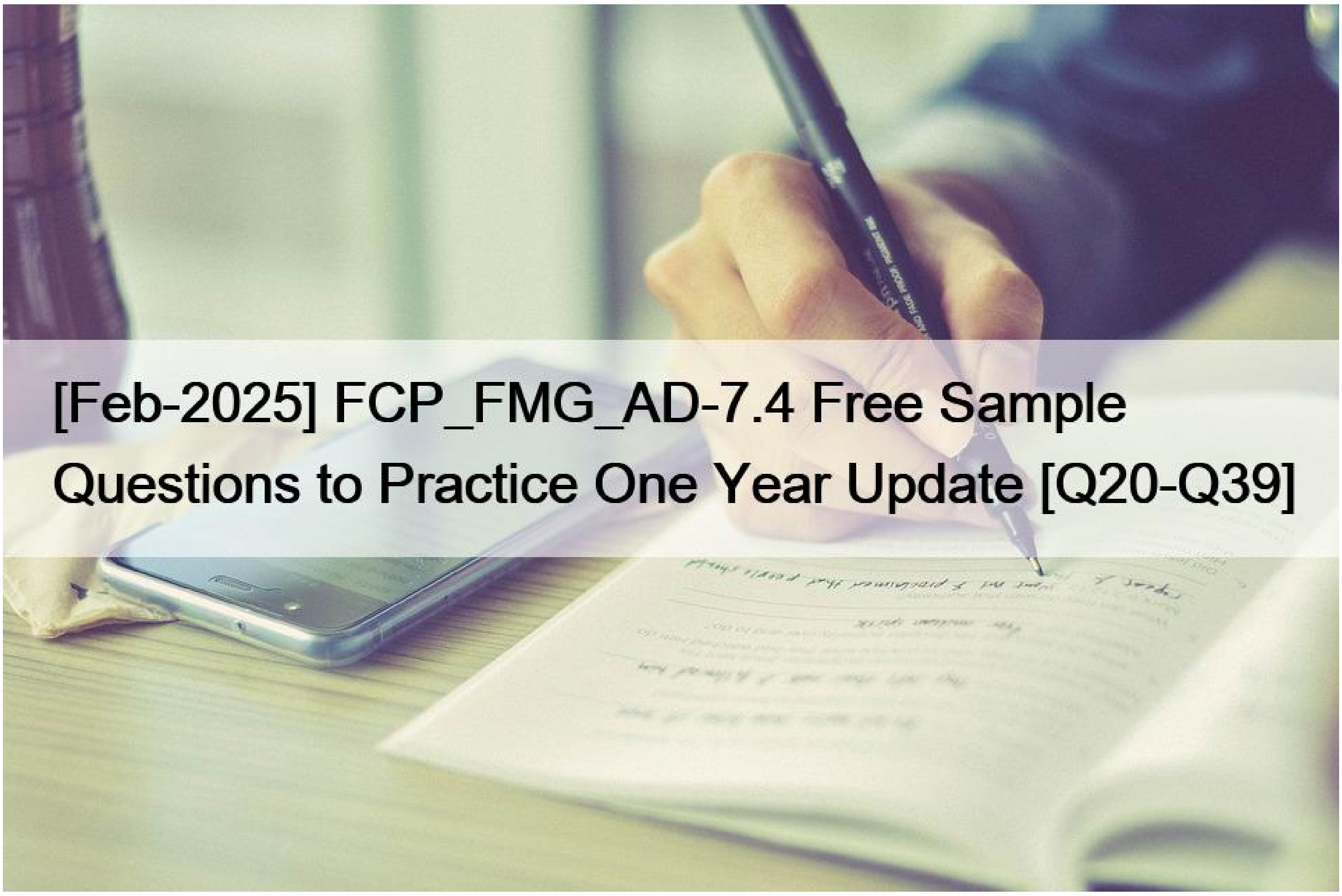
[Feb-2025 FCP_FMG_AD-7.4 Free Sample Questions to Practice One Year Update [Q20-Q39



[Feb-2025] FCP_FMG_AD-7.4 Free Sample Questions to Practice One Year Update
Download FCP_FMG_AD-7.4 exam with Fortinet FCP_FMG_AD-7.4 Real Exam Questions

NEW QUESTION 20

Push updates are failing on a FortiGate device that is located behind a NAT device.

Which two settings should the administrator check? (Choose two.)
* That the virtual IP address and correct ports are set on the NAT device
* That the override server IP address is set on FortiManager and the NAT device
* That the external IP address on the NAT device is set to DHCP and configured with the virtual IP
* That the NAT device IP address and correct ports are configured on FortiManager
FMG should contact NAT ip address and NAT device should have VIP correctly configured.

NEW QUESTION 21

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?
* Device-level database
* ADOM-level database
* Configuration-level database
* Revision history database
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 theDevice-level database.

Explanation of Options:

* A. Device-level database:

* This istrue. When changes are made to a device&#8217;s configuration on FortiManager, they are saved in theDevice-level database. This database stores the configuration for individual managed devices. The configuration changes remain here until they are pushed to the actual FortiGate device.

* B. ADOM-level database:

* This isfalse. The ADOM-level database holds configurations related to the entire ADOM (Administrative Domain), such as global settings that apply to all devices within the ADOM, rather than configurations specific to individual devices.

* C. Configuration-level database:

* This isfalse. The term &#8220;Configuration-level database&#8221; is not typically used in FortiManager terminology. Changes are stored in the device-level database and are applied when pushed to the FortiGate.

* D. Revision history database:

* This isfalse. The revision history database keeps track of previous versions of configurations after they have been pushed to the FortiGate device. It does not store unsaved or pending configurations that have not yet been applied to the device.

NEW QUESTION 22

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.)
* FortiManager will temporarily change the status of the referenced firewall policy to disabled.
* FortiManager will disable the status of the address object until the changes are installed.
* FortiManager will not allow the administrator to delete a referenced address object until they lock the ADOM.
* FortiManager will replace the deleted address object with the none address object in the referenced firewall policy.
When operating in workspace mode on FortiManager 7.4, the administrator must understand how object references and deletions work:

* Option C- &#8220;FortiManager will not allow the administrator to delete a referenced address object until they lock the ADOM&#8221;: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.

* FortiManager Reference: &#8220;In workspace mode, changes to objects or policies require the ADOM to be locked. If an object is referenced, you must lock the ADOM before deleting or modifying the object.&#8221; (FortiManager 7.4 Administration Guide,

Section on Workspace Mode and ADOM Management)

* Option D- &#8220;FortiManager will replace the deleted address object with the none address object in the referenced firewall policy&#8221;: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 &#8216;none&#8217; 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.

* FortiManager Reference: &#8220;When a referenced object is deleted, FortiManager will replace it with a &#8216;none&#8217; object in the policy. This behavior is to ensure the integrity and continuity of the policy configurations.&#8221; (FortiManager 7.4 Administration Guide, Object Management and Policy Handling in Workspace Mode)

NEW QUESTION 23

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

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

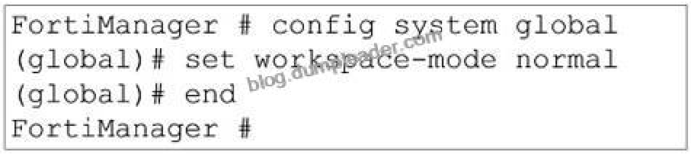
* Option D: It allows FortiManager to determine the connection status of managed devicesis incorrect because Service Access does not directly manage or check connectivity status of devices; it is used for FortiGuard service requests.

FortiManager References:

* Refer to the &#8220;FortiManager Administration Guide,&#8221; particularly the sections on &#8220;Service Access Settings&#8221; and &#8220;FortiGuard Services.&#8221;

NEW QUESTION 24

Refer to the exhibit. Given the configuration shown in the exhibit, what are two results from this configuration? (Choose two.)



```
FortiManager # config system global
(global)# set workspace-mode normal
(global)# end
FortiManager #
```

* Unlocking an ADOM will submit configuration changes automatically to the approval administrator.
* Ungraceful closed sessions will keep the ADOM in a locked state until the administrator session times out.
* Unlocking an ADOM will install configuration changes automatically on managed devices.
* The same administrator can lock more than one ADOM at the same time.

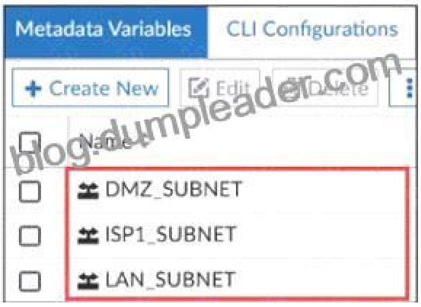
NEW QUESTION 25

Which two items does an FGFM keepalive message include? (Choose two.)
* FortiGate IPS version
* FortiGate license information
* FortiGate configuration checksum
* FortiGate uptime
Keepalive messages, including the configuration checksums, are sent from FortiGate at configured intervals.

The messages also show the intrusion prevention system (IPS) version of the FortiGate device

NEW QUESTION 26

Exhibit.



□ DMZ_SUBNET
□ ISP1_SUBNET
□ LAN_SUBNET

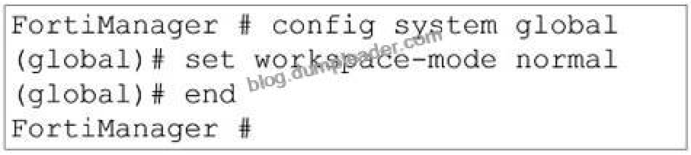
What is true about the objects highlighted in the image?
* They can be set to optional or required.
* They are available across all ADOMs by default.
* They can be used as variables in scripts.
* They cannot be created in the global database ADOM.

NEW QUESTION 27

Push updates are failing on a FortiGate device thatis located behind a NAT device. Which two settings should the administrator check? (Choose two.)
* That the override server IP address is set on FortiManager and the NAT device
* That the external IP address on the NAT device is set to DHCP and configured with the virtual IP
* That the NAT device IP address and correct ports are configured on FortiManager
* That the virtual IP address and correct ports are set on the NAT device

NEW QUESTION 28

Refer to the exhibit. Given the configuration shown in the exhibit, what are two results from this configuration? (Choose two.)



```
FortiManager # config system global
(global)# set workspace-mode normal
(global)# end
FortiManager #
```

* You can validate administrator login attempts through external servers.
* The same administrator can lock more than one ADOM at the same time.
* Two or more administrators can make configuration changes at the same time, in the same ADOM.
* Concurrent read-write access to an ADOM is disabled.

NEW QUESTION 29

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.)
* FortiManager will temporarily change the status of the referenced firewall policy to disabled.
* FortiManager will disable the status of the address object until the changes are installed.
* FortiManager will not allow the administrator to delete a referenced address object until theylockthe ADOM.
* FortiManager will replace the deleted address object with the none address object in the referenced firewall policy.

NEW QUESTION 30

What will be the result of reverting to a previous revision version in the revision history?
* It win install configuration changes to managed device automatically.
* It will tag the device settings status as Auto-Update.
* It will modify the device-level database.
* It will generate a new version ID and remove all other revision history versions.
* 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 &#8220;Auto-Update&#8221; 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 &#8220;Revision Management&#8221; section in the FortiManager Administration Guide, which provides an overview of how revisions are managed and utilized for restoring configurations.

NEW QUESTION 31

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.)

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

NEW QUESTION 32

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?

- FortiManager file system
- ADOM2 object database
- ADOM2 device database
- Source ADOM policy database

The commandexecute fmprofile import-profile ADOM2 3547 /tmp/myfileis used to import a system template profile from the FortiManager file system. The path/tmp/myfileindicates a location in the FortiManager&#8217;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 Dsuggest importing from different databases, which is not accurate since the command explicitly refers to the file system location.

FortiManager References:

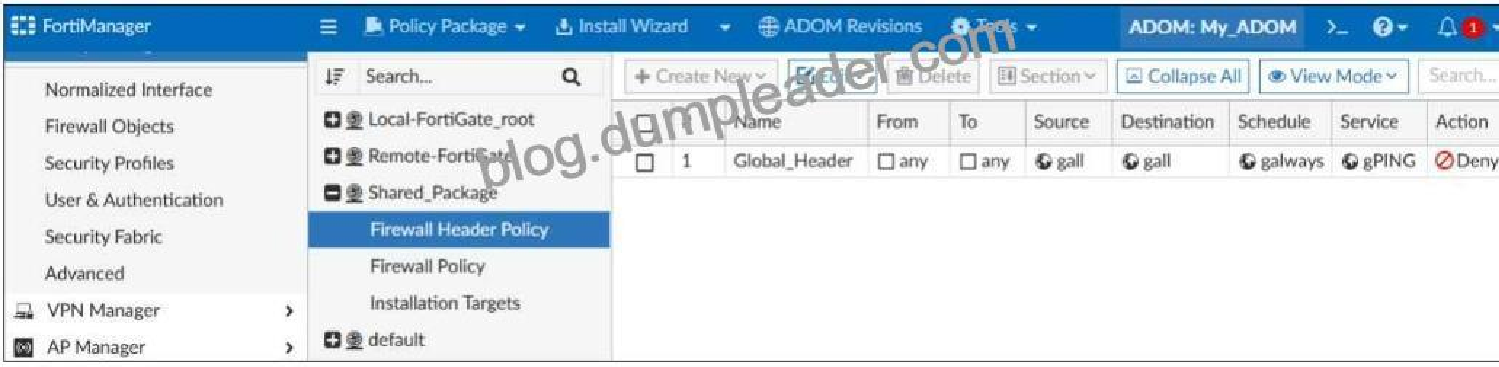
* Refer to FortiManager 7.4 CLI Reference Guide: Commands for Profile Management.

NEW QUESTION 33

Refer to the exhibit. A service provider administrator has assigned a global policy package to a managed customer ADOM named My_ADOM, which has four policy packages. The customer administrator has access only to My_ADOM.

How can the customer or service provider administrators remove the global header policy from the policy package named Shared_Package?

FortiManager policy package

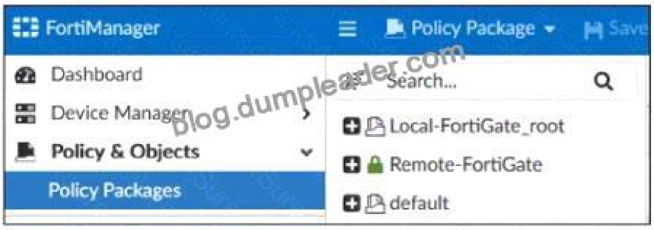


□		Name	From	To	Source	Destination	Schedule	Service	Action
□	1	Global_Header	□ any	□ any	gall	gall	galways	gPING	Deny

* The service provider administrator can unassign the global policy from My_ADOM.
* The customer administrator can unassign the global policy from My_ADOM.
* The customer administrator can unassign the policy by locking My_ADOM.
* The service provider administrator can unassign the policy from the global ADOM.

NEW QUESTION 34

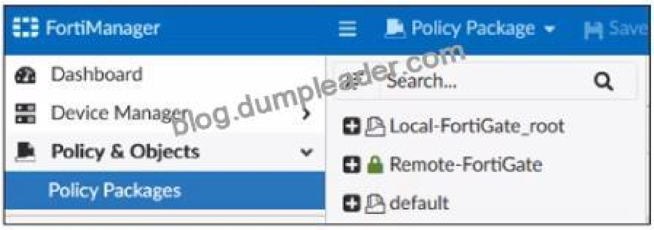
Exhibit.



Given the configuration shown in the exhibit, which two statements are true? (Choose two.)
* An administrator can also lock the Local-FortiGate_root policy package.
* FortiManager is in workflow mode.
* The FortiManager ADOM is locked by the administrator.
* The FortiManager ADOM workspace mode is set to Normal

NEW QUESTION 35

Exhibit.



Given the configuration shown in the exhibit, which two statements are true? (Choose two.)
* An administrator can also lock the Local-FortiGate_root policy package.
* FortiManager is in workflow mode.
* The FortiManager ADOM is locked by the administrator.
* The FortiManager ADOM workspace mode is set to Normal
The provided screenshot from FortiManager shows several key elements that help answer the question:

* Thepadlock iconnext to the &#8220;Remote-FortiGate&#8221; policy package indicates that this policy package is locked, which means it is currently being edited or has been checked out by an administrator. This is typical behavior when the ADOM (Administrative Domain) workspace is inuse, and a session is active where an administrator is working on a policy package.

* Theabsence of a lock iconnext to &#8220;Local-FortiGate_root&#8221; and &#8220;default&#8221; indicates that these policy packages are not locked and are available for editing.

* Statement B(FortiManager is in workflow mode): This istrue. The fact that one of the policy packages is locked suggests that FortiManager is operating inADOM workflow modeor at least in a state where it enforces locking for editing, typically seen in Normal ADOM modes. Inworkflow mode, an administrator needs to lock a workspace before making changes.

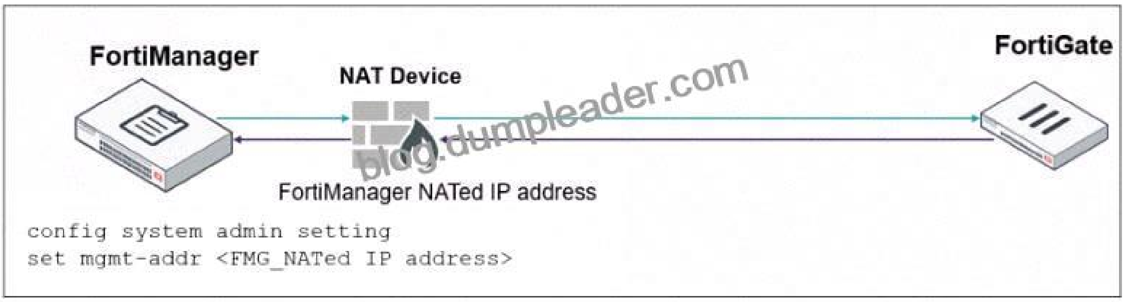
* Statement C(The FortiManager ADOM is locked by the administrator): This istrue. The presence of the padlock on &#8220;Remote-FortiGate&#8221; signifies that the ADOM, or more specifically, this policy package within the ADOM, has been locked by the administrator.

* Statement A(An administrator can also lock the Local-FortiGate_root policy package): This isnot necessarily true. The administrator can lock the &#8220;Local-FortiGate_root&#8221; policy package, but as shown in the exhibit, it iscurrently not locked, so this option is not a certainty in this state.

* Statement D(The FortiManager ADOM workspace mode is set to Normal): This istrue, but not the best option compared to B and C, as it can be inferred that the mode is set to Normal due to the locking behavior, but the more direct information is about the ADOM being locked by an administrator.

NEW QUESTION 36

Refer to the exhibit.



```
config system admin setting
set mgmt-addr <FMG_NATed IP address>
```

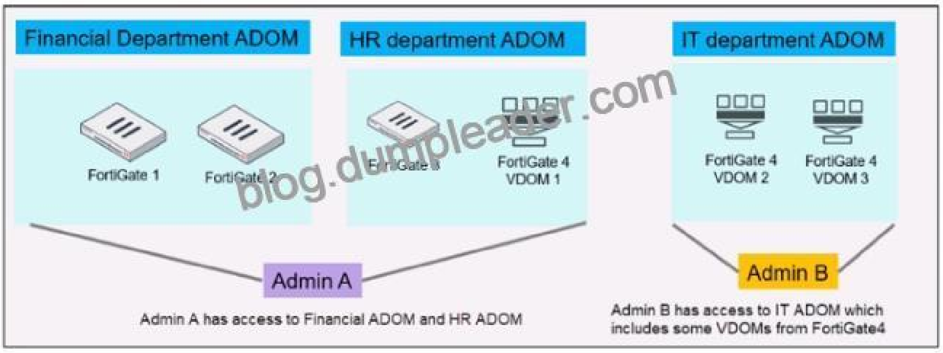
An administrator is about to add the FortiGate device to FortiManager using the discovery process.

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?
* During discovery. FortiManager uses only the FortiGate serial number to establish the connection.
* During discovery, FortiManager sets both the FortiManager NATed IP address and NAT device IP address on FortiGate.
* During discovery. FortiManager sets the NATed device IP address on FortiGate.
* During discovery, FortiManager sets the FortiManager NATed IP address on FortiGate.

NEW QUESTION 37

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

* This istrue. In FortiManager, when there areVDOMs(Virtual Domains) involved, you must set the ADOM toAdvanced modeto manage VDOMs properly. The IT department ADOM includes different VDOMs from FortiGate 4 (VDOM 2 and VDOM 3), which means the ADOM mode must be inAdvancedto support managing VDOMs separately from other ADOMs.

* B. Policies and objects databases can be shared between the Financial and HR ADOMs.

* This isfalse. By default, ADOMs are separate, and policies and objects cannot be shared between them unless they are specifically designed to do so. The exhibit shows distinct ADOMs for each department, implying no direct sharing of policies and objects between Financial and HR ADOMs.

* C. An administrator with the super user profile can access all the VDOMs.

* This istrue. A FortiManager administrator with thesuper userprofile hasfull accessto all ADOMs and VDOMs, regardless of how access is restricted for individual administrators. In this case, an admin with the super user profile could access Financial, HR, and IT ADOMs, including all the VDOMs from FortiGate 4.

* D. The administrator must configure FortiManager in workspace normal mode.

* This isfalse. There is no requirement mentioned in the exhibit or scenario that mandates using workspace normal mode. Workspace mode is more related to how configuration changes are managed (locking, editing, etc.), but it doesn&#8217;t affect the creation or access control of ADOMs.

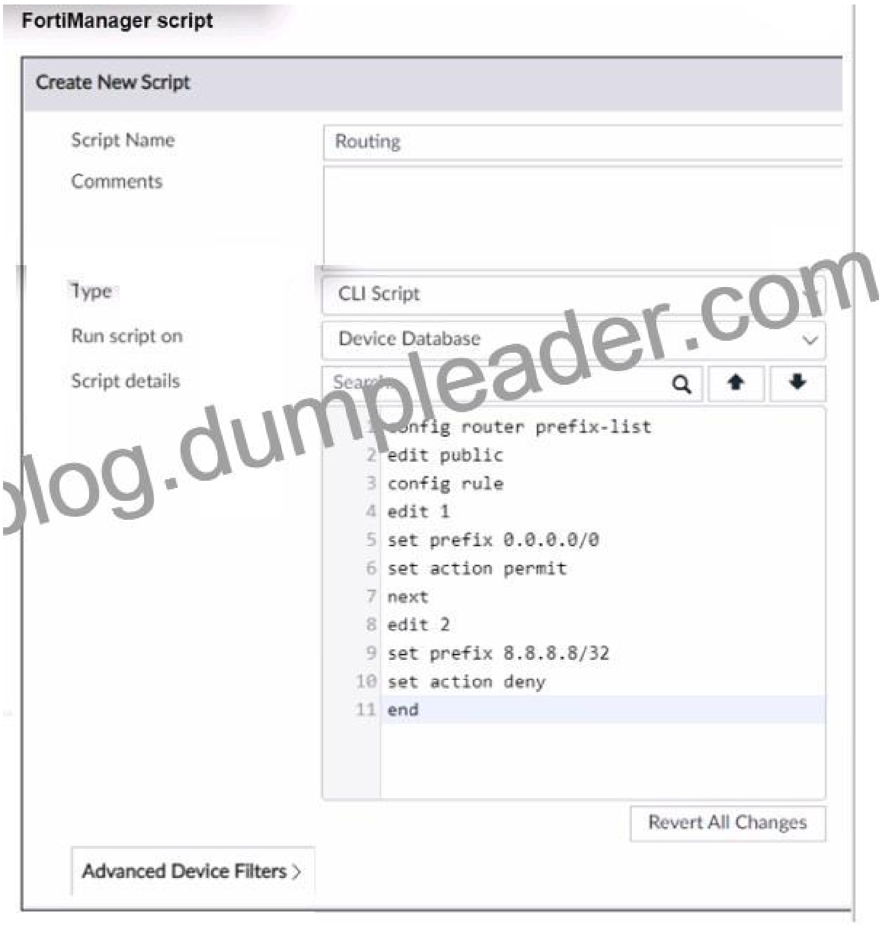
Conclusion:

* Ais correct becauseAdvanced modeis necessary for managing VDOMs within ADOMs.

* Cis correct because asuper usercan access all VDOMs and ADOMs without restrictions.

NEW QUESTION 38

Refer to the exhibit.



FortiManager script

Create New Script

Script Name: Routing

Comments:

Type: CLI Script

Run script on: Device Database

Script details:

```
config router prefix-list
edit public
config rule
edit 1
set prefix 0.0.0.0/0
set action permit
next
edit 2
set prefix 8.8.8.8/32
set action deny
end
```

Which two results occur if the script is run using the Device Database option? (Choose two.)
* You must install these changes on a managed device using the Install Wizard.
* The successful execution of a script on the Device Database creates a new revision history.
* The script history shows successful installation of the script on the remote FortiGate device.
* The device Config Status is tagged as Modified.
If the script is run using the &#8220;Device Database&#8221; option on FortiManager, the following occurs:

* A.You must install these changes on a managed device using the Install Wizard.

* Running the script on the Device Database updates only the configuration in the FortiManager&#8217;s database, not on the actual FortiGate device. To apply the changes, you need to use the Install Wizard to push these configurations to the managed device.

* D.The device Config Status is tagged as Modified.

* After running the script on the Device Database, FortiManager tags the device&#8217;s configuration status as &#8220;Modified,&#8221; indicating that there are pending changes that have not yet been installed on the device.

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 39

When an installation is performed from FortiManager, what is the recovery logic used between FortiManager and FortiGate for an FGFM tunnel?
* FortiManager will not push the CLI commands as part of the installation that will cause the tunnel to go down.
* After 15 minutes, FortiGate will unset all CLI commands that were part of the installation that caused the tunnel to go down.
* FortiManager will revert and install a previous configuration revision on the managed FortiGate.
* FortiGate will reject the CLI commands that will cause the tunnel to go down.

Fortinet FCP_FMG_AD-7.4 Exam Syllabus Topics:

TopicDetailsTopic 1- Troubleshooting: This section covers how to fmiliarize with FortiManager deployment scenarios and troubleshoot issues related to imports, installations, device-level, ADOM-level, and system-level concerns.Topic 2- Device Manager: In this domain, the focus is on how to register devices within ADOMs, implement configuration changes using scripts, and troubleshoot using the revision history.Topic 3- Advanced Configuration: This domain explains FortiManager's high availability (HA), configures FortiGuard services and works with the global database ADOM.Topic 4- Policy and Objects: This section deals with how to manage policies and objects, oversee ADOM revisions, configure workspace mode, and conduct policy imports and installations.Topic 5- Administration: This section covers how to understand FortiManager capabilities, perform initial configurations, and set up administrative domains (ADOMs).