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:
? Bsuggests setting the external IP on the NAT device to DHCP, which is not relevant to solving the push update issue.
? Cimplies 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:
? Bis misleading as the Security Fabric settings are generally configured and managed separately from other device-level settings.
? Dis 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 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?

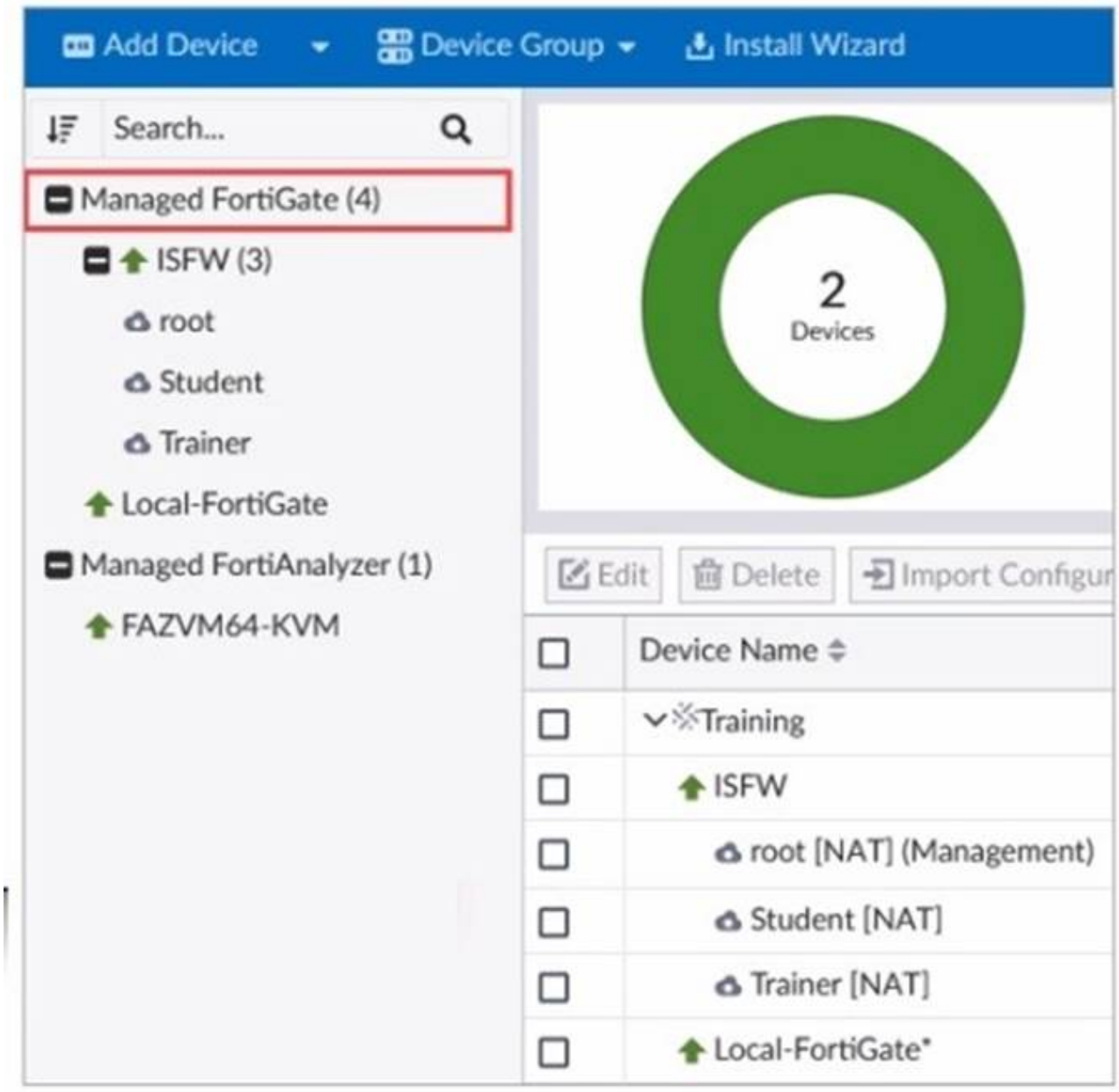
A. FortiManager file system
B. ADOM2 object database
C. ADOM2 device database
D. Source ADOM policy database

Answer: A

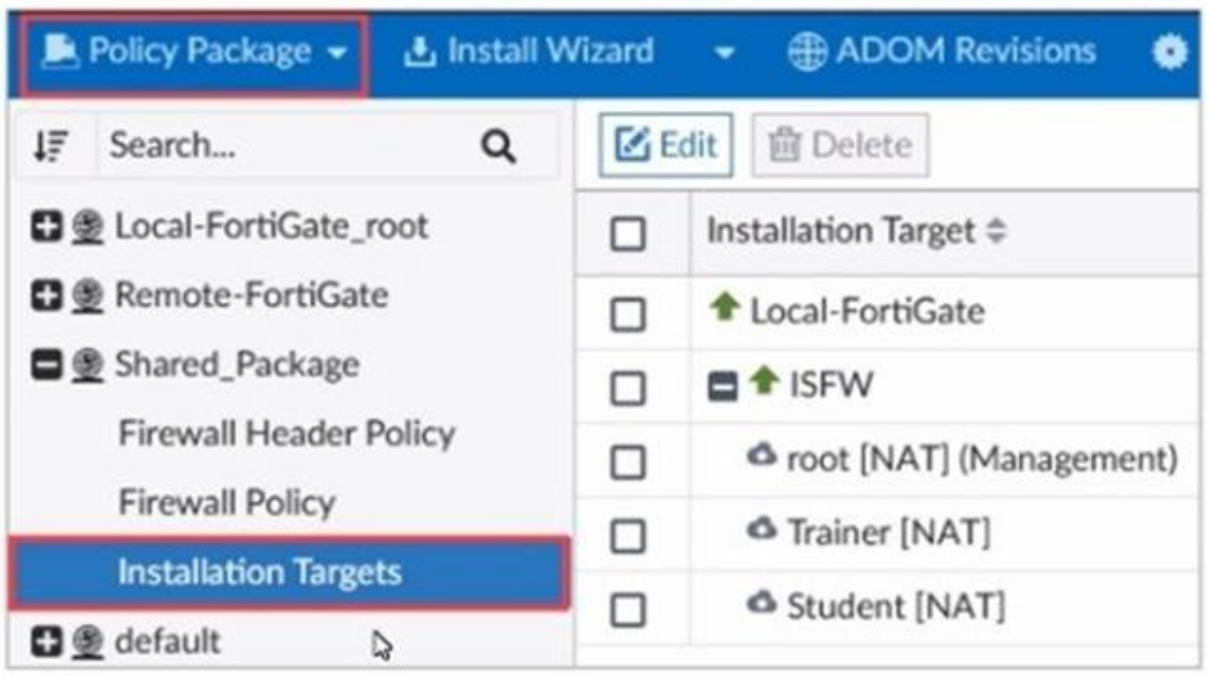
Explanation:
The commandexecute fmprofile import-profile ADOM2 3547 /tmp/myfileis used to import a system template profile from the FortiManager file system. The path/tmp/myfileindicates a location in the FortiManager's local file system, from which the profile will be imported into the specified ADOM.
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 4
Refer to the exhibit.

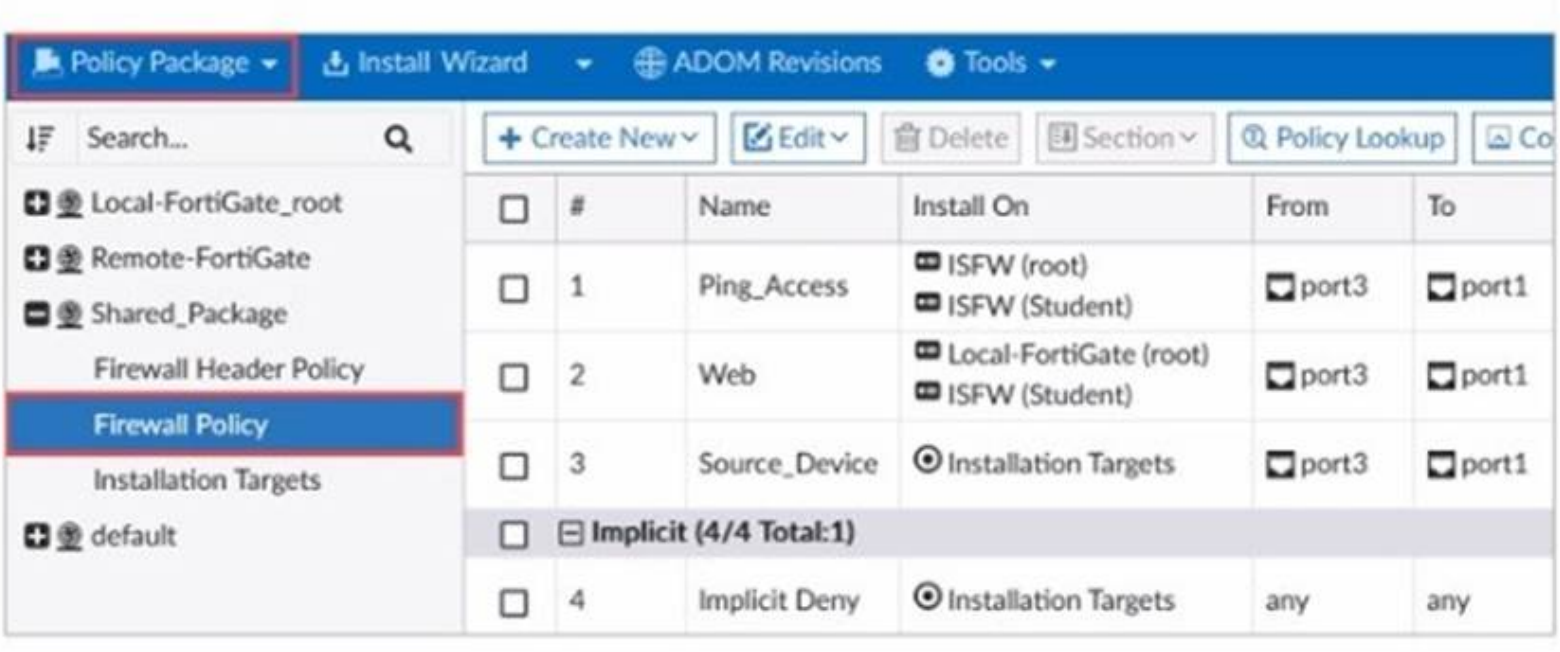
Managed FortiGate devices



FortiManager policy package



FortiManager policy package



Given the configuration shown in the exhibit, which two conclusions can you draw from the installation targets in the Install On column? (Choose two.)

A. Policy seq.S will be installed on all managed devices and VDOMs that are listed under Installation Targets
B. Policy seq.# 3 will be skipped because no installation targets are specified.
C. Policy seq.# 2 will not be installed on the Local-FortiGate root VDOM because there is no root VDOM in the Installation Target
D. Policy seq.# 1 will be installed on the ISFW device root[NAT] and Student[NAT] VDOMs only.

Answer: AD

Explanation:
? Option A: Policy seq.S will be installed on all managed devices and VDOMs that are listed under Installation Targets.This is correct. The "Install On" column indicates that the policy is targeted for installation on all listed managed devices and VDOMs under Installation Targets.
? Option D: Policy seq.# 1 will be installed on the ISFW device root[NAT] and Student[NAT] VDOMs only.This is correct. Policy sequence #1 specifies that it will be installed only on the ISFW device and the VDOMs 'root[NAT]' and 'Student[NAT]' as indicated by the "Install On" column.
Explanation of Incorrect Options:
? Option B: Policy seq.# 3 will be skipped because no installation targets are specifiedis incorrect because it is clearly listed under "Installation Targets," which means it will be installed according to the specified configuration.
? Option C: Policy seq.# 2 will not be installed on the Local-FortiGate root VDOM because there is no root VDOM in the Installation Targetis incorrect as the exhibit does not show any specific exclusion for seq.# 2 on the Local-FortiGate root VDOM.
FortiManager References:
? Refer to the FortiManager Administration Guide sections on "Policy Packages" and "Policy Installation Targets" for more details.

NEW QUESTION 5
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 6
What must you consider before deciding to use FortiManager to manage a FortiAnalyzer device?

A. Confirm that FortiManager has enough storage capacity for the expected logs.
B. Ensure that FortiAnalyzer features are installed in advance.
C. Check whether FortiManager is part of a high availability (HA) cluster.
D. Determine whether the VDOMs of the same FortiGate will be assigned to different ADOMs.

Answer: B

Explanation:
When deciding to use FortiManager to manage a FortiAnalyzer device, you must ensure certain conditions are met so that the integration works seamlessly. One key aspect to consider is whether the necessary FortiAnalyzer features are enabled on FortiManager.
Explanation of Options:
? A. Confirm that FortiManager has enough storage capacity for the expected logs.
? B. Ensure that FortiAnalyzer features are installed in advance.
? C. Check whether FortiManager is part of a high availability (HA) cluster.
? D. Determine whether the VDOMs of the same FortiGate will be assigned to different ADOMs.

NEW QUESTION 7
Which configuration setting for FortiGate is part o an ADOM-level database on FortiManager?

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

Answer: B

Explanation:
? Option B: Routingis 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 Templateis incorrect as it is not a FortiGate-specific setting managed at the ADOM level.
? Option C: SNMPis incorrect because SNMP settings are typically managed on a per-device basis.
? Option D: Security profilesis 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
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 ADOMis 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 assignmentis 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
Refer to the exhibit.

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

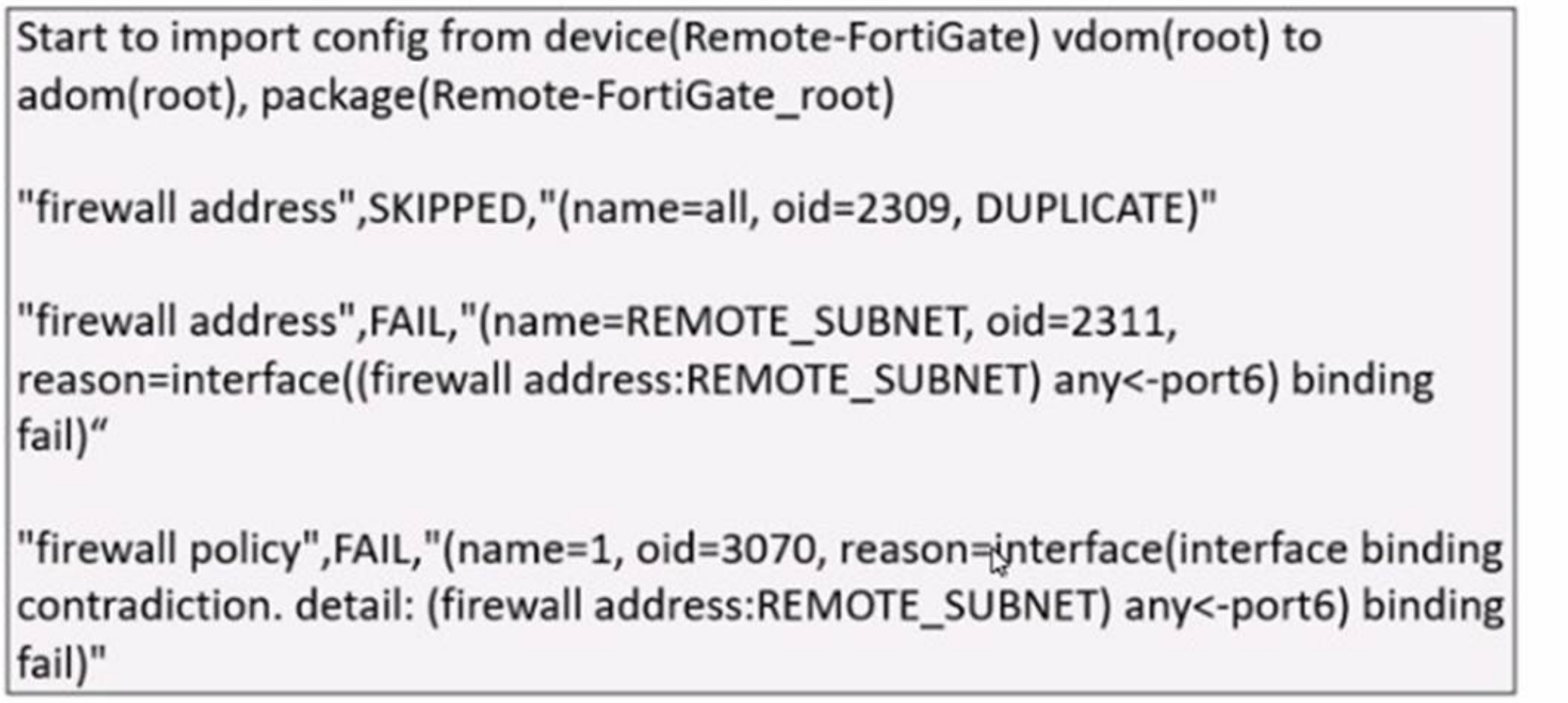
A. It installs provisioning template changes on the FortiGate device.
B. It provides the option to preview only the policy package changes before installing them.
C. It installs all the changes in the device database first and the administrator must reinstall the changes on the FortiGate device.
D. It 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 deviceis 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 deviceis 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
Refer to the exhibit which shows the Download Import Report.



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-FortiGateis 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 FortiGateis 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 FortiManageris 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 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, thesetmethod is used tocreate new objects oroverwrite 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 12
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 displayedimmediately after movingthe ISFW device from one ADOM to another isOption 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 13
Exhibit.

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

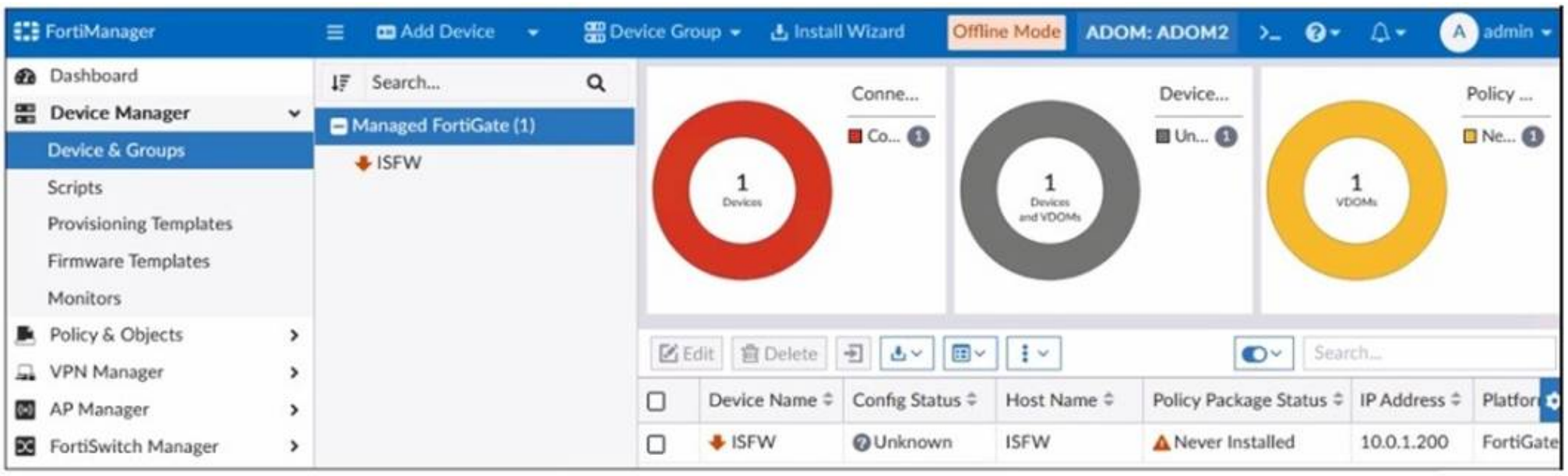
Given the configuration shown in the exhibit, what are two results from this configuration?
{Choose two.)

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

Answer: BD

Explanation:
The configuration shown in the exhibit sets theworkspace-mode to normal. The workspace mode in FortiManager defines how configuration changes and administrative tasks are handled, specifically regarding locking and collaboration in ADOMs (Administrative Domains).
Understanding the workspace modes:
? Normal Mode:In this mode, only one administrator at a time can lock and edit an ADOM. The changes made by one administrator must be completed and saved before another administrator can make changes. It prevents concurrent read-write access within the same ADOM.
? Workflow Mode:This mode allows multiple administrators to work on different tasks within the same ADOM, but changes still need to be approved before being committed.
Explanation of Options:
? A. You can validate administrator login attempts through external servers.
? B. The same administrator can lock more than one ADOM at the same time.
? C. Two or more administrators can make configuration changes at the same time, in the same ADOM.
? D. Concurrent read-write access to an ADOM is disabled.

NEW QUESTION 15
Refer to the exhibit.



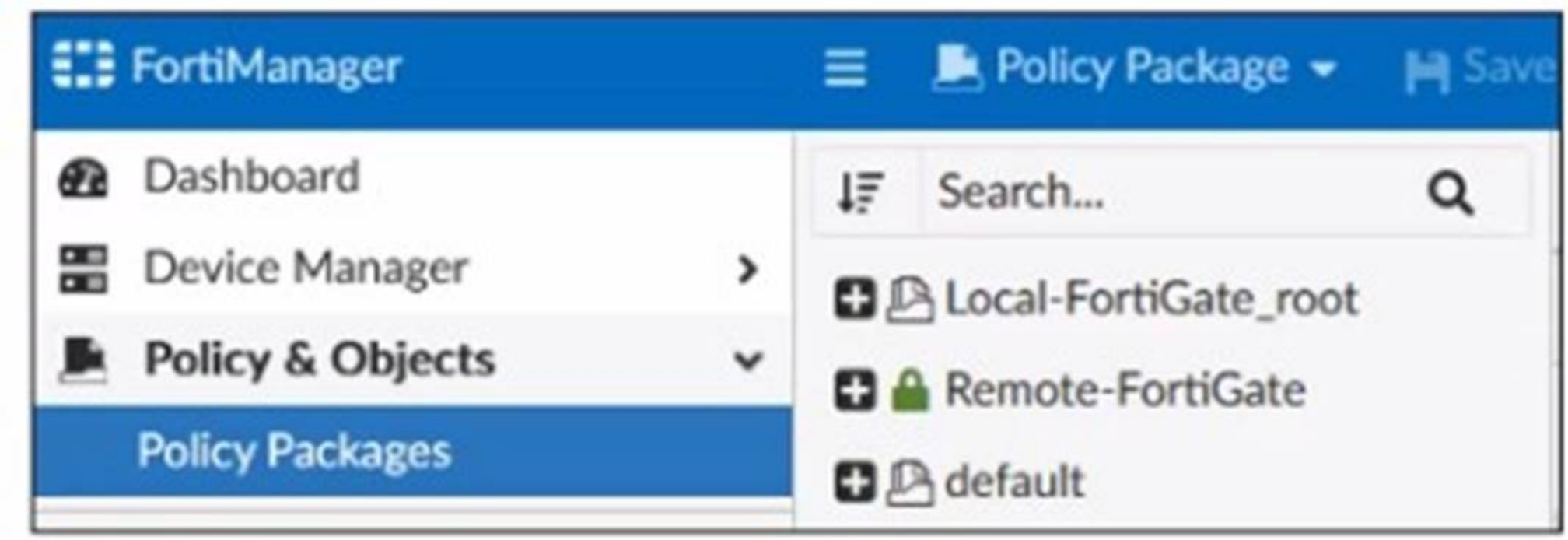
A junior administrator is troubleshooting a FortiManager connectivity issue that is occurring with a managed FortiGate device.
Given the FortiManager device manager settings shown in the exhibit, what can you conclude from this scenario?

A. The administrator must refresh the device to restore connectivity.
B. FortiManager lost internet connectivity, therefore, the device appears to be down.
C. The administrator can reclaim the FortiGate to FortiManager protocol (FGFM) tunnel to get the device online.
D. The administrator recently restored a FortiManager configuration file.

Answer: C

Explanation:
? Option C: The administrator can reclaim the FortiGate to FortiManager protocol (FGFM) tunnel to get the device online.This is the correct answer. The exhibit shows a device in "Unknown" status, which indicates that the FortiManager cannot currently communicate with the device. Reclaiming the FGFM tunnel will help to restore connectivity by re-establishing the management tunnel between the FortiManager and the FortiGate.
Explanation of Incorrect Options:
? Option A: The administrator must refresh the device to restore connectivityis incorrect because refreshing the device is unlikely to solve the connection issue when the status is "Unknown."
? Option B: FortiManager lost internet connectivity, therefore, the device appears to be downis incorrect because FortiManager does not require internet connectivity to manage a FortiGate; it needs a direct connection to the device.
? Option D: The administrator recently restored a FortiManager configuration fileis incorrect because the exhibit does not indicate a recent restoration of configuration.
FortiManager References:
? Refer to "FortiManager Administration Guide" and the section on "Device Management and Connectivity" for more information about reclaiming FGFM tunnels.

NEW QUESTION 16
Exhibit.



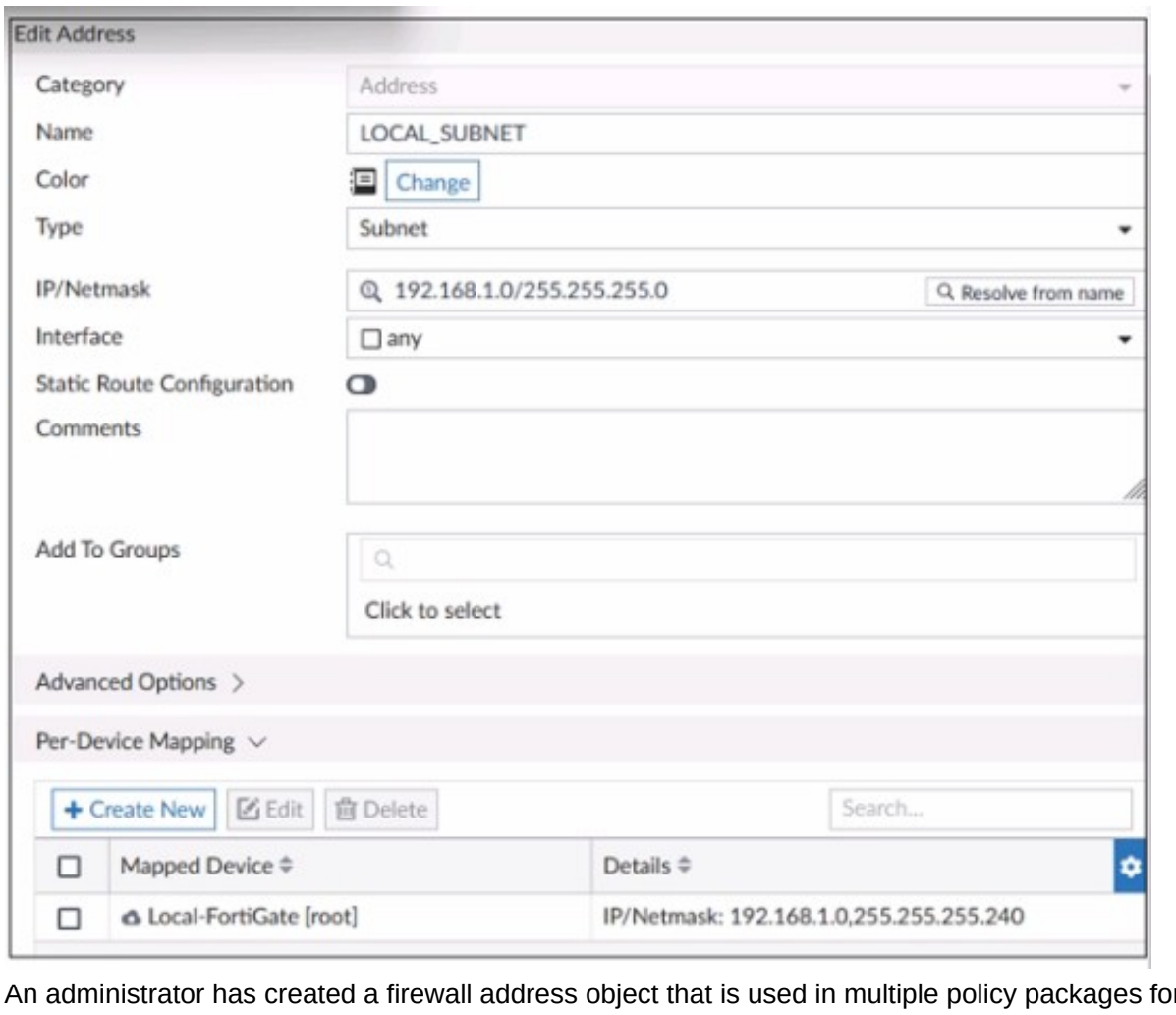
Given the configuration shown in the exhibit, which two statements are true? (Choose two.)

A. An administrator can also lock the Local-FortiGate_root policy package.
B. FortiManager is in workflow mode.
C. The FortiManager ADOM is locked by the administrator.
D. The FortiManager ADOM workspace mode is set to Normal

Answer: BC

Explanation:
The provided screenshot from FortiManager shows several key elements that help answer the question:
? Thepadlock iconnext to the "Remote-FortiGate" policy package indicates that this
policy package islocked, 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 "Local-FortiGate_root" and "default" 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 "Remote-FortiGate" 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 isnotnecessarily true. The administrator can lock the "Local- FortiGate_root" 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 20
Refer to the exhibit.



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 mappingdefined 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: 192.168.1.0/24is 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 objectLOCAL_SUBNEThas a default IP/netmask of192.168.1.0/24. 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 23
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 27
.....

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