Fortinet

Exam Questions FCP_FMG_AD-7.4

FCP - FortiManager 7.4 Administrator

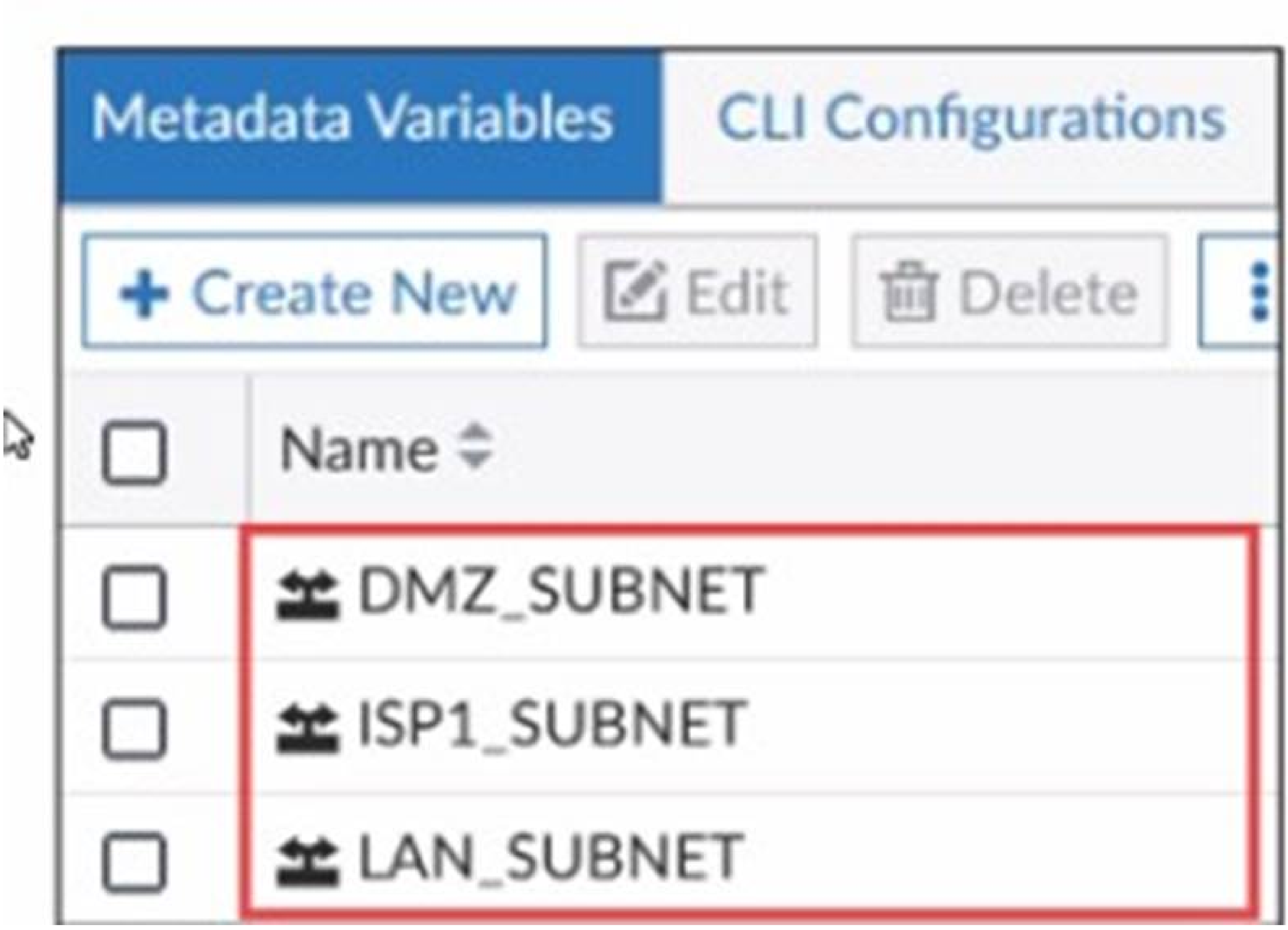
NEW QUESTION 1
An administrator configures a new OSPF area on FortiManager and has not yet pushed the changes to the managed FortiGate device. In which database will the configuration be saved?

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 2
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) aremetadata variables.
? C.They can be used as variables in scripts.
Options A, B, and D are incorrect because:
? Asuggests optional or required settings, which do not apply to metadata variables.
? Bimplies they are available across all ADOMs by default, which is not always the case.
? Dstates 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 3

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 4
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 5
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 6
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.

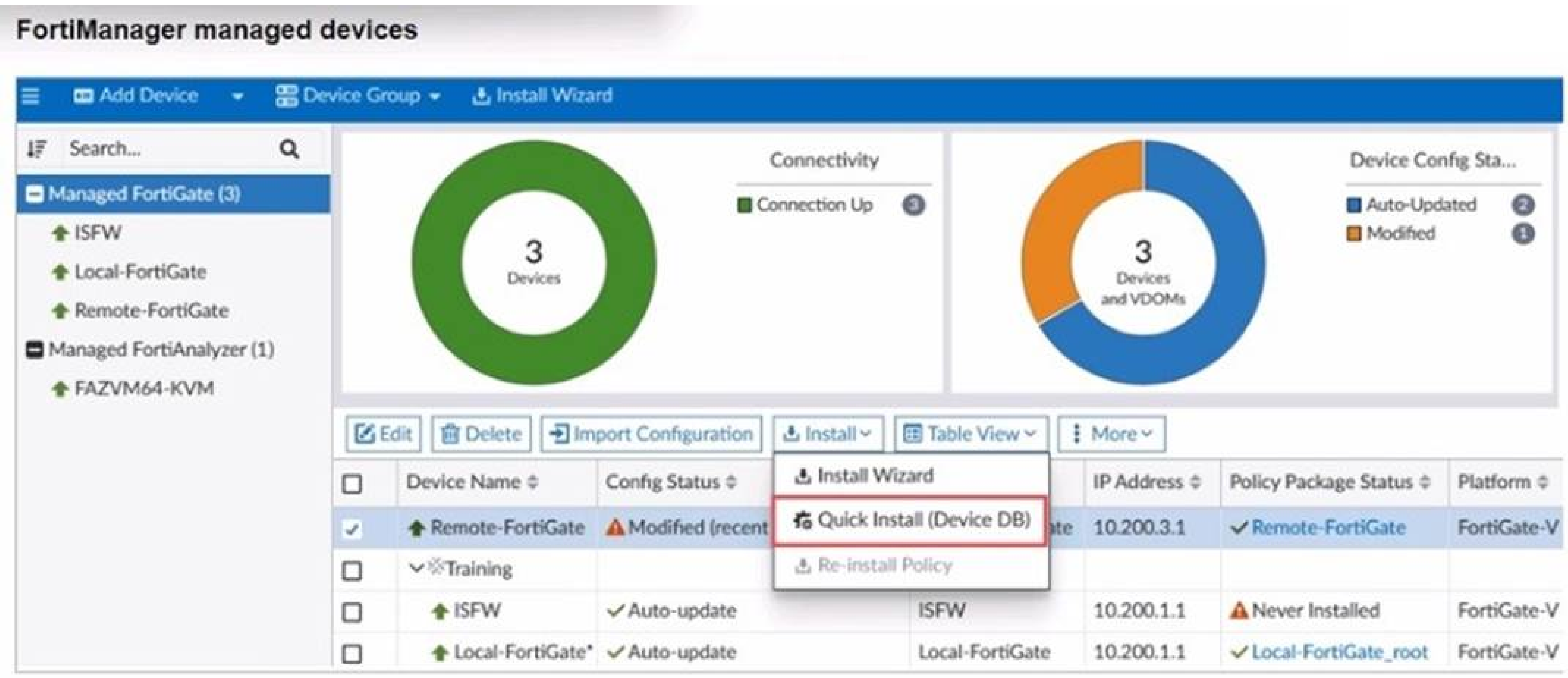
NEW QUESTION 7
Which statement about the policy lock feature on FortiManager is true?

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 8
Refer to the exhibit.


FortiManager managed devices

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

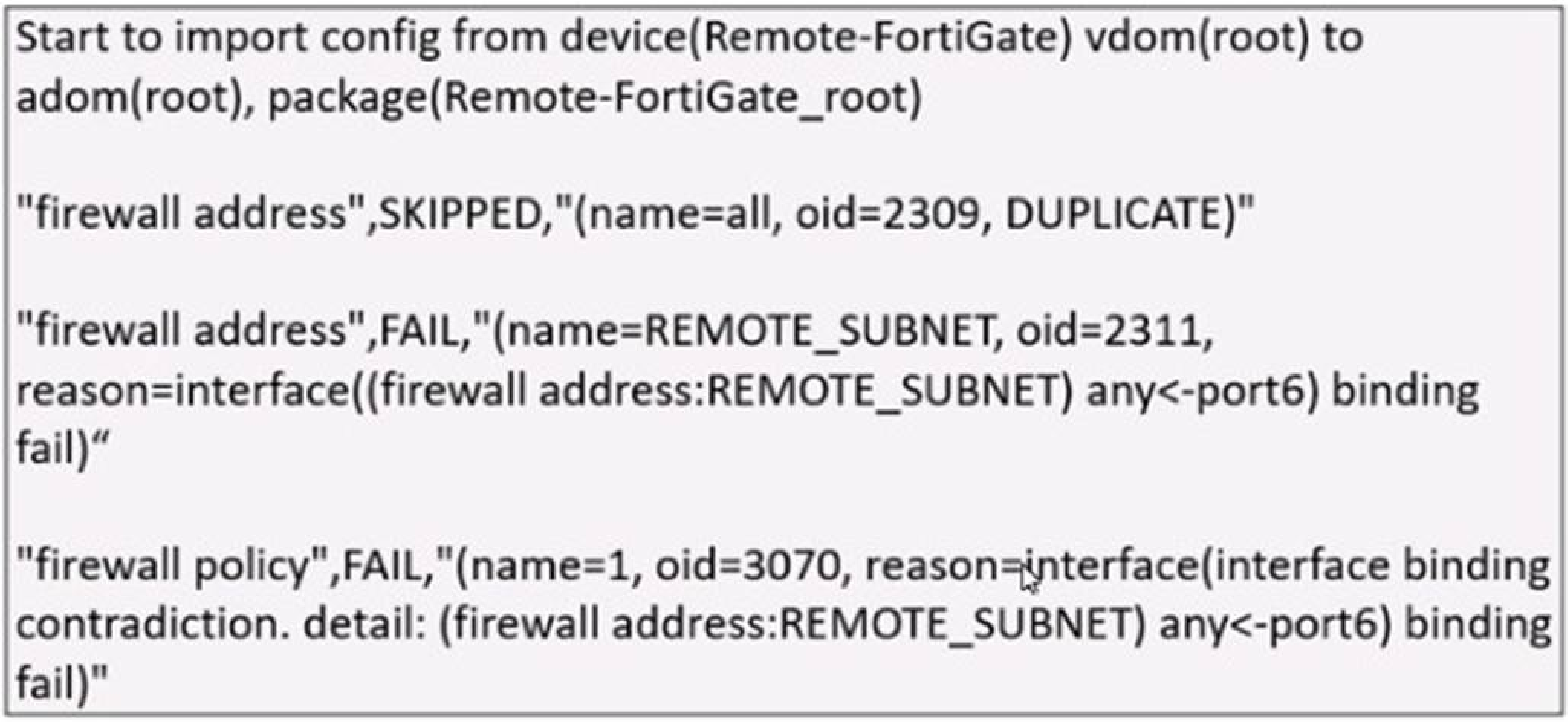
You are using the Quick Install option to install configuration changes on the managed FortiGate.
Which two statements correctly describe the result? (Choose two.)

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 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 9
Refer to the exhibit which shows the Download Import Report.



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

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

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

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

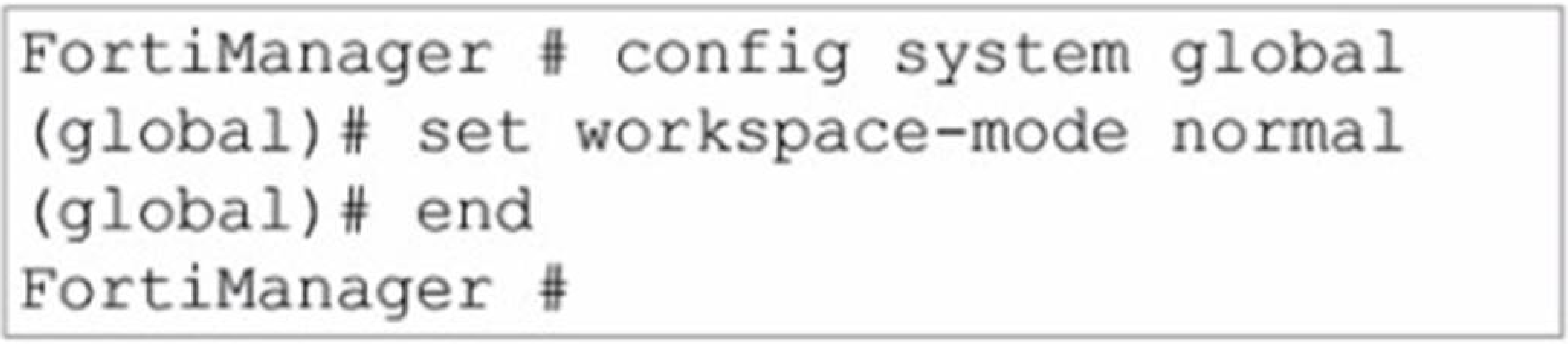
Why is FortiManager failing to import firewall policy ID 1?

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

Answer: A

Explanation:
? Option A: Policy ID 1 is configured from the interface any to port6. FortiManager rejects the request to import this policy because the any interface does not exist on FortiManager.This is the correct answer. FortiManager fails to import firewall policy ID 1 because it cannot map the "any" interface to a valid interface in its ADOM database. The error indicates that there is a binding failure due to an interface mismatch.
Explanation of Incorrect Options:
? Option B: Policy ID 1 for this managed FortiGate already exists on FortiManager in the policy package named Remote-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
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 10
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.

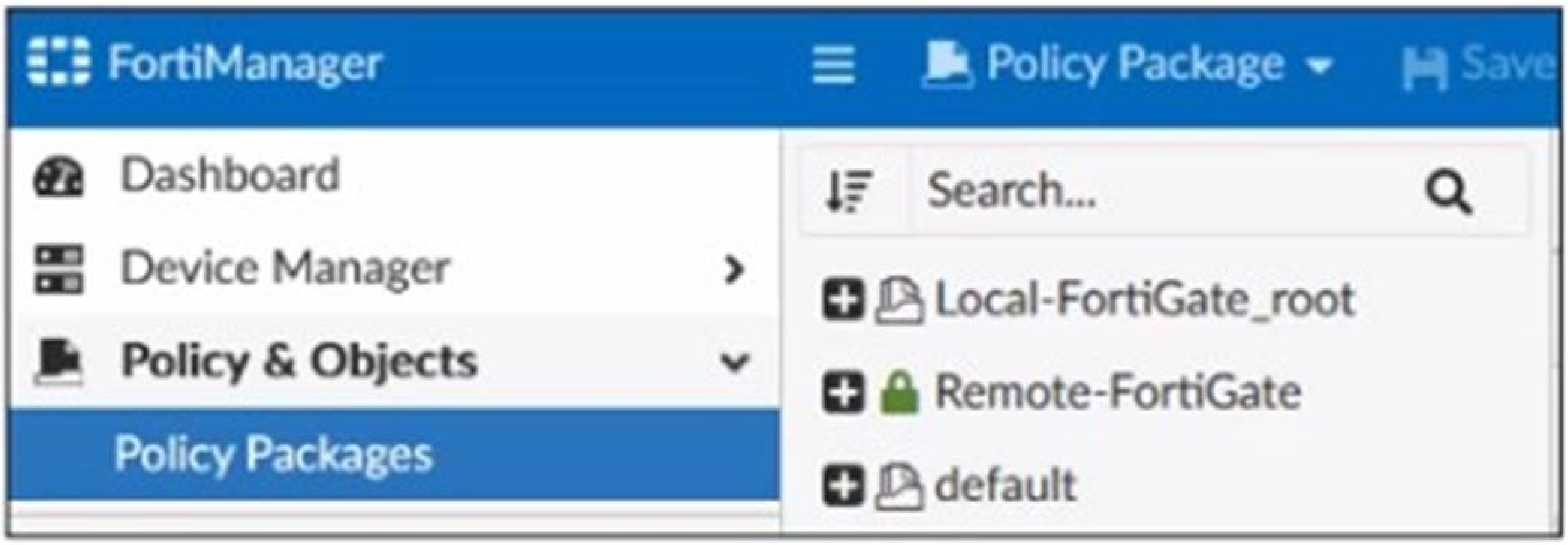
NEW QUESTION 13
What will be the result of reverting to a previous revision version in the revision history?

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 17
Exhibit.



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

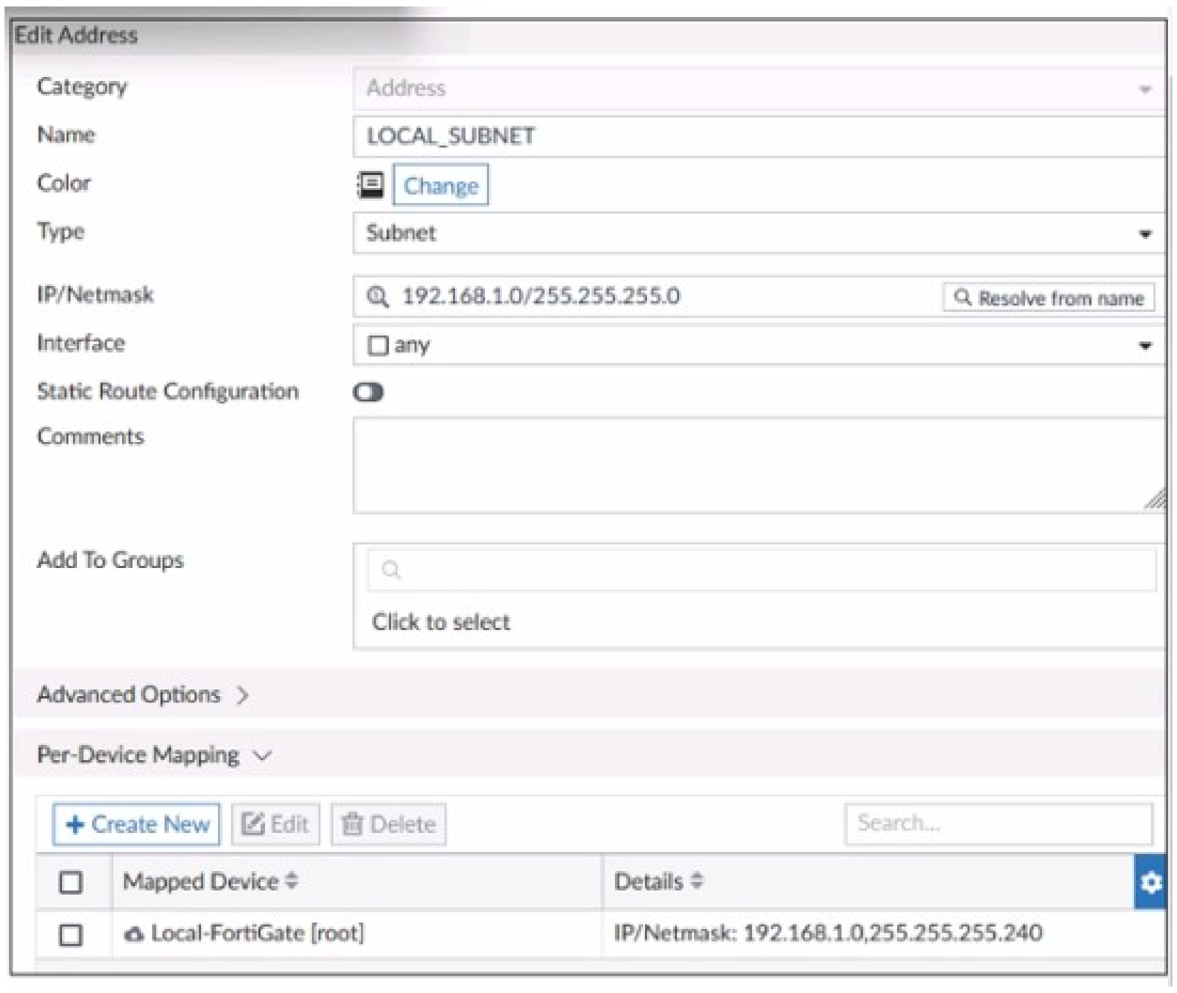
A. An administrator can also lock the Local-FortiGate_root policy package.
B. FortiManager is in workflow mode.

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 22
Refer to the exhibit.



Edit Address

Category: Address
Name: LOCAL_SUBNET
Color: Change
Type: Subnet
IP/Netmask: 192.168.1.0/255.255.255.0 — Resolve from name
Interface: □ any
Static Route Configuration: ○
Comments:
Add To Groups: Click to select
Advanced Options >
Per-Device Mapping ∨

+ Create New | Edit | Delete | Search...

□	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 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 26
......