Fortinet

Exam Questions FCP_FMG_AD-7.4

FCP - FortiManager 7.4 Administrator

NEW QUESTION 1
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 2
What is a characteristic of the FortiManager high availability (HA) feature?

A. When a secondary unit is removed, FortiManager updates the managed devices using TCP port 5199.
B. The primary unit synchronizes all configuration revision with the seconday units.
C. All secondary units must be in the same network as the primary unit.
D. Each cluster member must be upgraded manually, starting with the primary unit.

Answer: B

Explanation:
The characteristic of the FortiManager high availability (HA) feature is that the primary unit synchronizes all configuration revisions with the secondary units. This ensures that all devices in the HA cluster are up-to-date with the same configurations, providing redundancy and failover capabilities.
Options A, C, and D are incorrect because:
? Arefers to a specific port number (5199), but FortiManager does not specifically use TCP port 5199 to update managed devices when a secondary unit is removed.
? Cis incorrect as secondary units do not necessarily have to be in the same network as the primary unit; they just need to be able to communicate with each other.
? Dis incorrect because HA upgrades can be automated and do not require manual upgrading, starting with the primary unit.
FortiManager References:
? Refer to FortiManager 7.4 High Availability (HA) Guide: HA Synchronization and Configuration.

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?

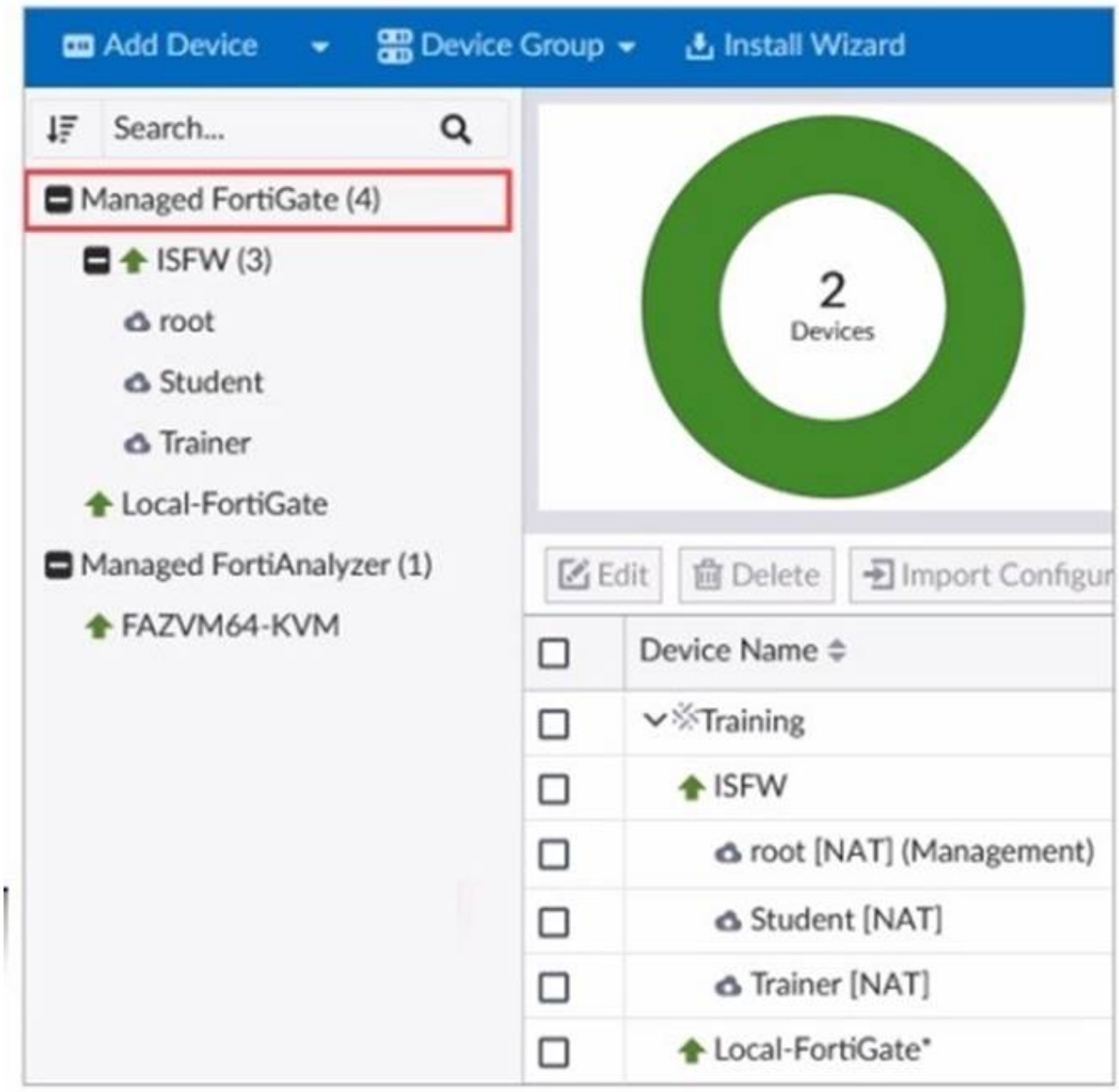
A. FortiManager file system
B. ADOM2 object database
C. ADOM2 device database
D. Source ADOM policy database

Answer: A

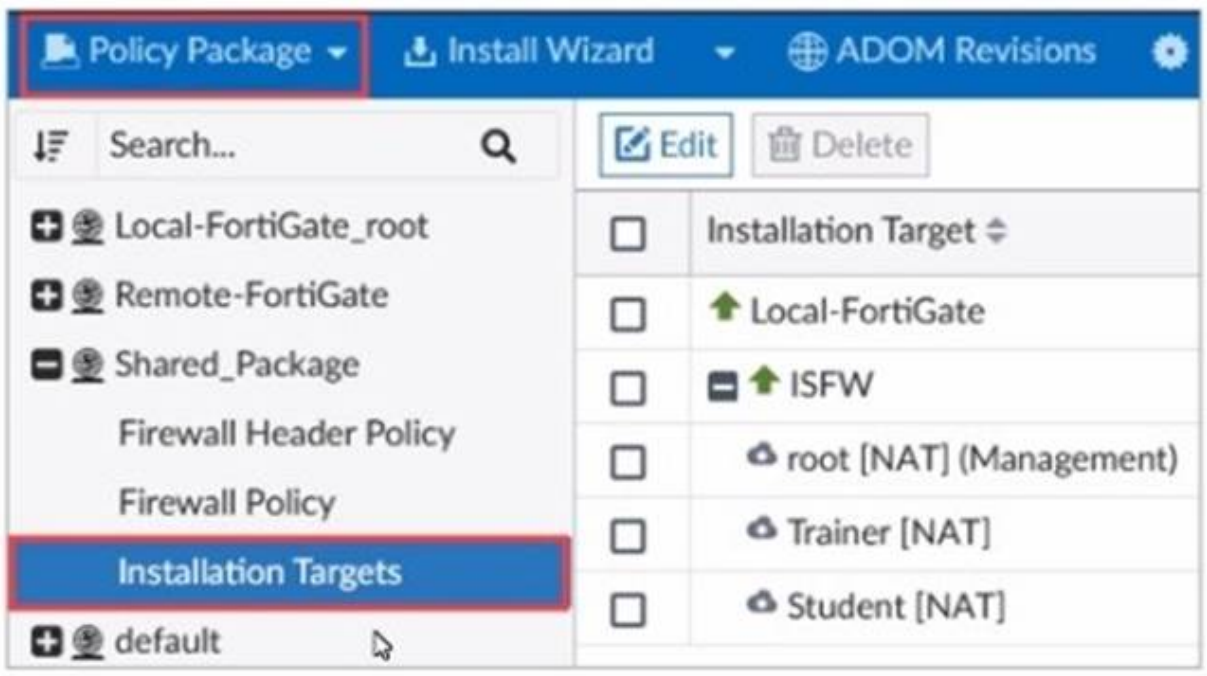
Explanation:
The commandexecute fmprofile import-profile ADOM2 3547 /tmp/myfileis used to import a system template profile from the FortiManager file system. The path/tmp/myfileindicates a location in the FortiManager's local file system, from which the profile will be imported into the specified ADOM.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

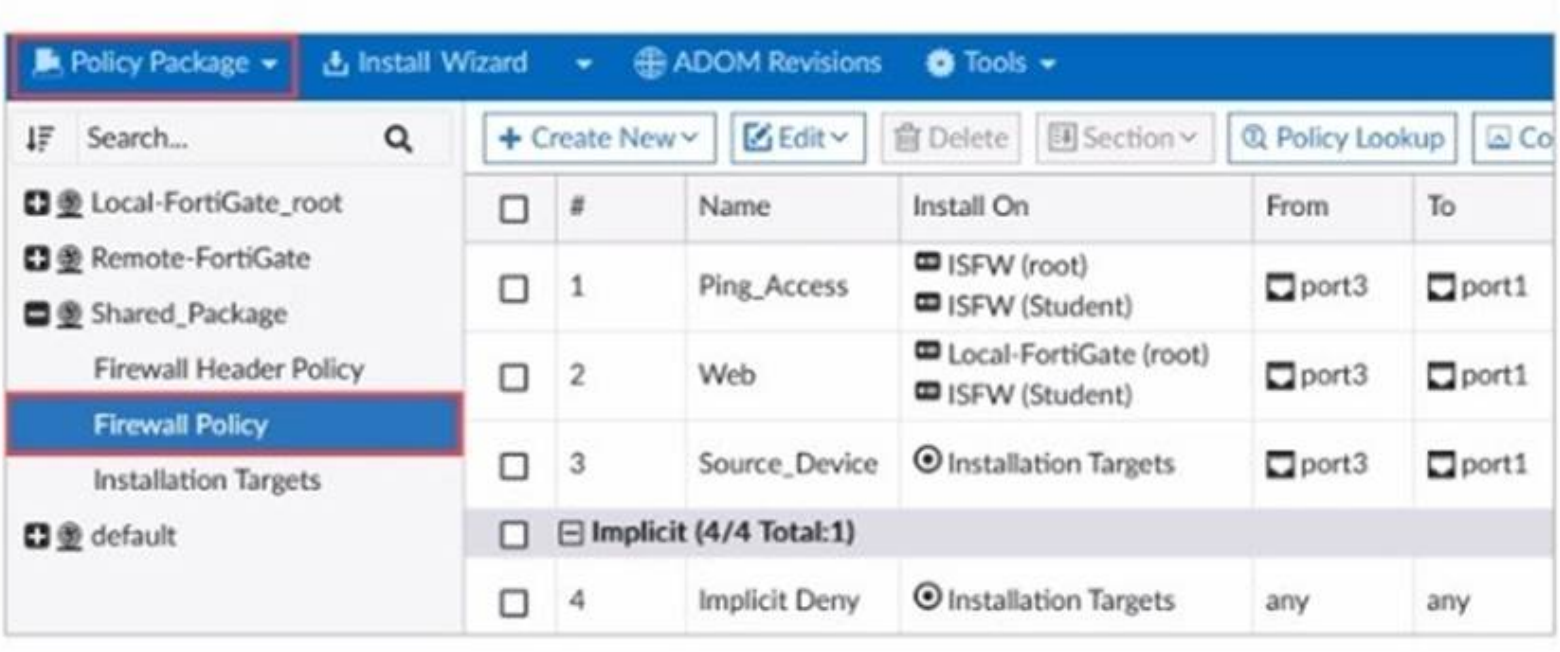
Managed FortiGate devices



FortiManager policy package



FortiManager policy package



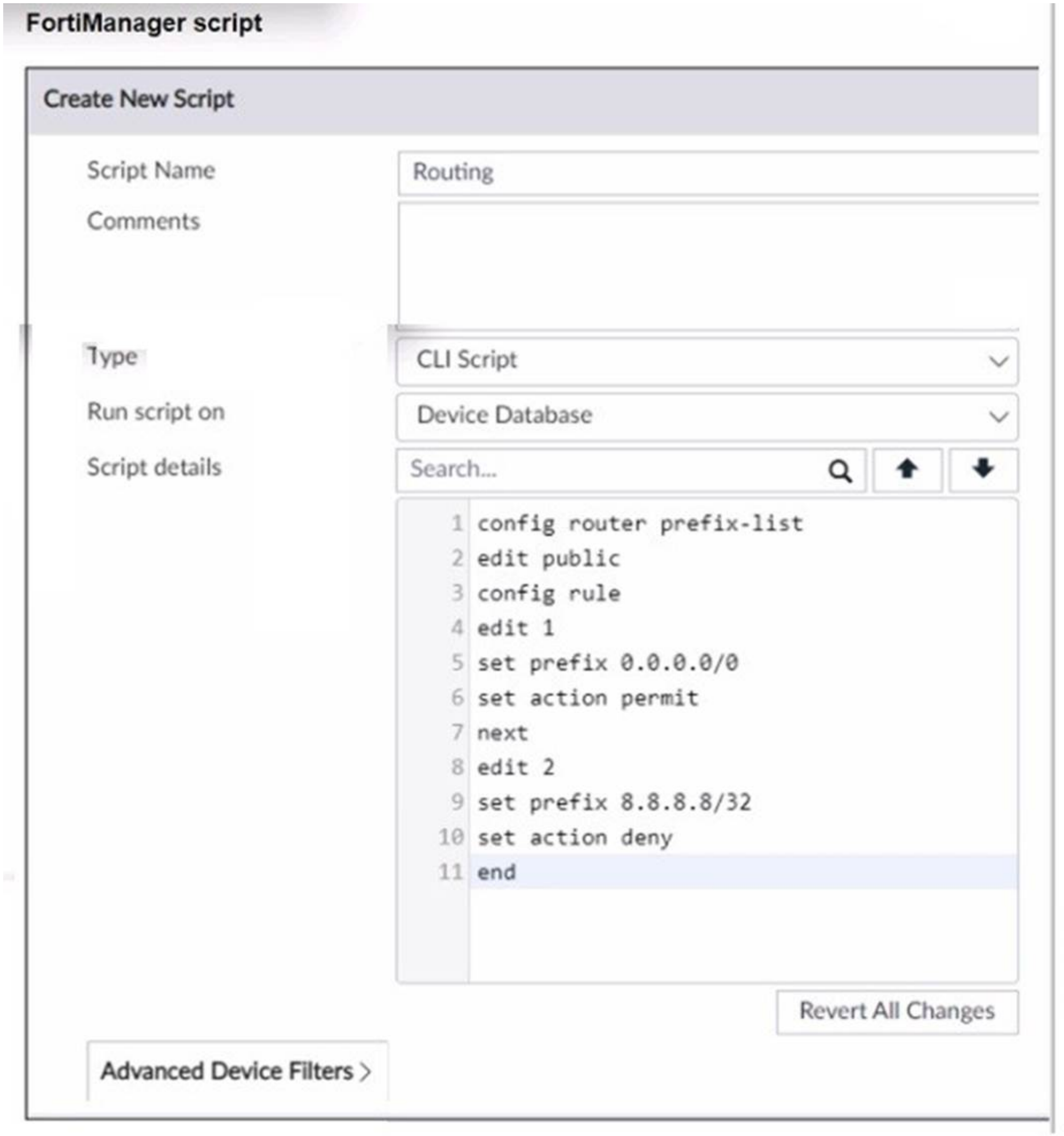
Given the configuration shown in the exhibit, which two conclusions can you draw from the installation targets in the Install On column? (Choose two.)

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
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 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
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 8
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 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
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.

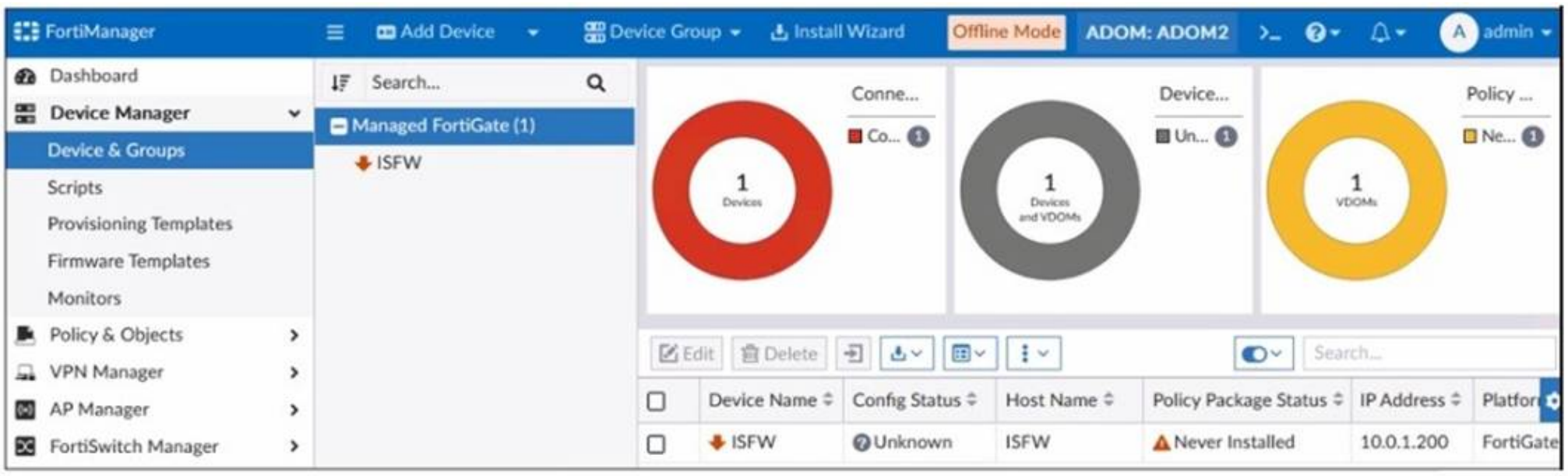
NEW QUESTION 10
What is the purpose of ADOM revisions?

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
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
Which two items are included in the FortiManager backup? (Choose two.)

A. All devices
B. Firmware images
C. FortiGuard database
D. Flash configuration

Answer: AD

Explanation:
FortiManager backups include:
? A. All devices— This includes all device configurations managed by FortiManager, such as firewall policies, objects, and other settings.
? D. Flash configuration— This consists of local FortiManager configurations stored
in flash memory, such as system settings, scripts, and other locally-stored configurations.
Options B and C are incorrect because:
? B (Firmware images)are not typically included in a FortiManager backup. Firmware images are usually stored separately and managed through a different process.
? C (FortiGuard database)is incorrect as the FortiGuard database, which contains threat intelligence and security signatures, is not part of the standard FortiManager backup.
FortiManager References:
? Refer to FortiManager 7.4 Administrator Guide: Backup and Restore Processes.

NEW QUESTION 17
An administrator wants to create a policy on an ADOM that is in backup mode and install it on a FortiGate device in the same ADOM. How can the administrator perform this task?

A. The administrator must use the Policy & Objects section to create a policy first.
B. The administrator must use a FortiManager script.
C. The administrator must disable the FortiManager offline mode first.
D. The administrator must change the ADOM mode to Advanced to bring the FortiManager online.

Answer: B

Explanation:
To create and install a policy on a FortiGate device in an ADOM (Administrative Domain) that is in backup mode, the administrator must use a FortiManager script. This is because backup mode restricts direct configuration changes, and scripts can be used to push specific configuration changes without altering the ADOM mode.
Options A, C, and D are incorrect because:
? A requires the ADOM to be in normal or advanced mode to create policies directly in the Policy & Objects section.
? C suggests disabling offline mode, which is irrelevant to the backup mode configuration.
? D implies changing the ADOM mode, which is unnecessary if using a script to perform the task.
FortiManager References:
? Refer to FortiManager 7.4 Administrator Guide: Working with ADOMs and Using Scripts for managing policies in backup mode.

NEW QUESTION 18
.....

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