Exam Questions FCP_FMG_AD-7.4

FCP - FortiManager 7.4 Administrator

https://www.2passeasy.com/dumps/FCP_FMG_AD-7.4/

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
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 4
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.

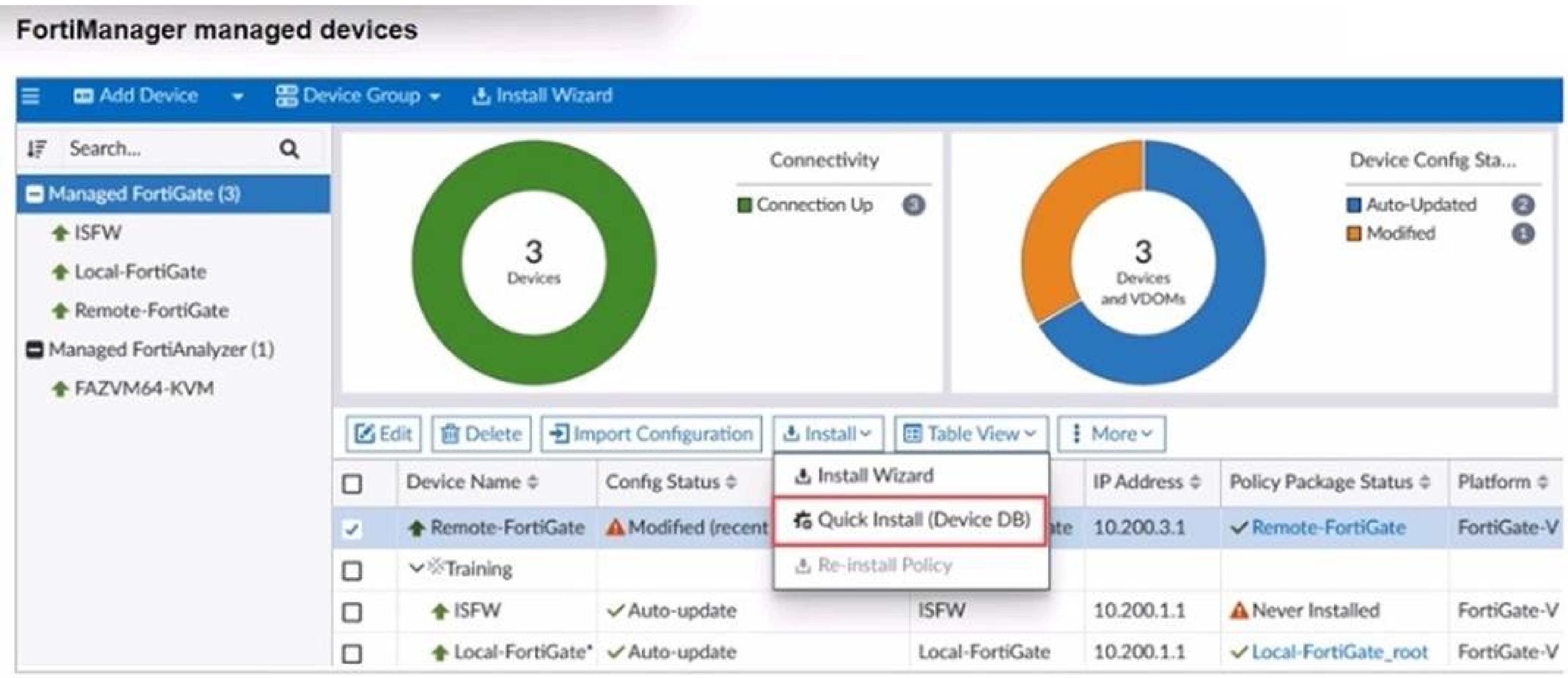
NEW QUESTION 5
Which statement about the policy lock feature on FortiManager is true?

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 6
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

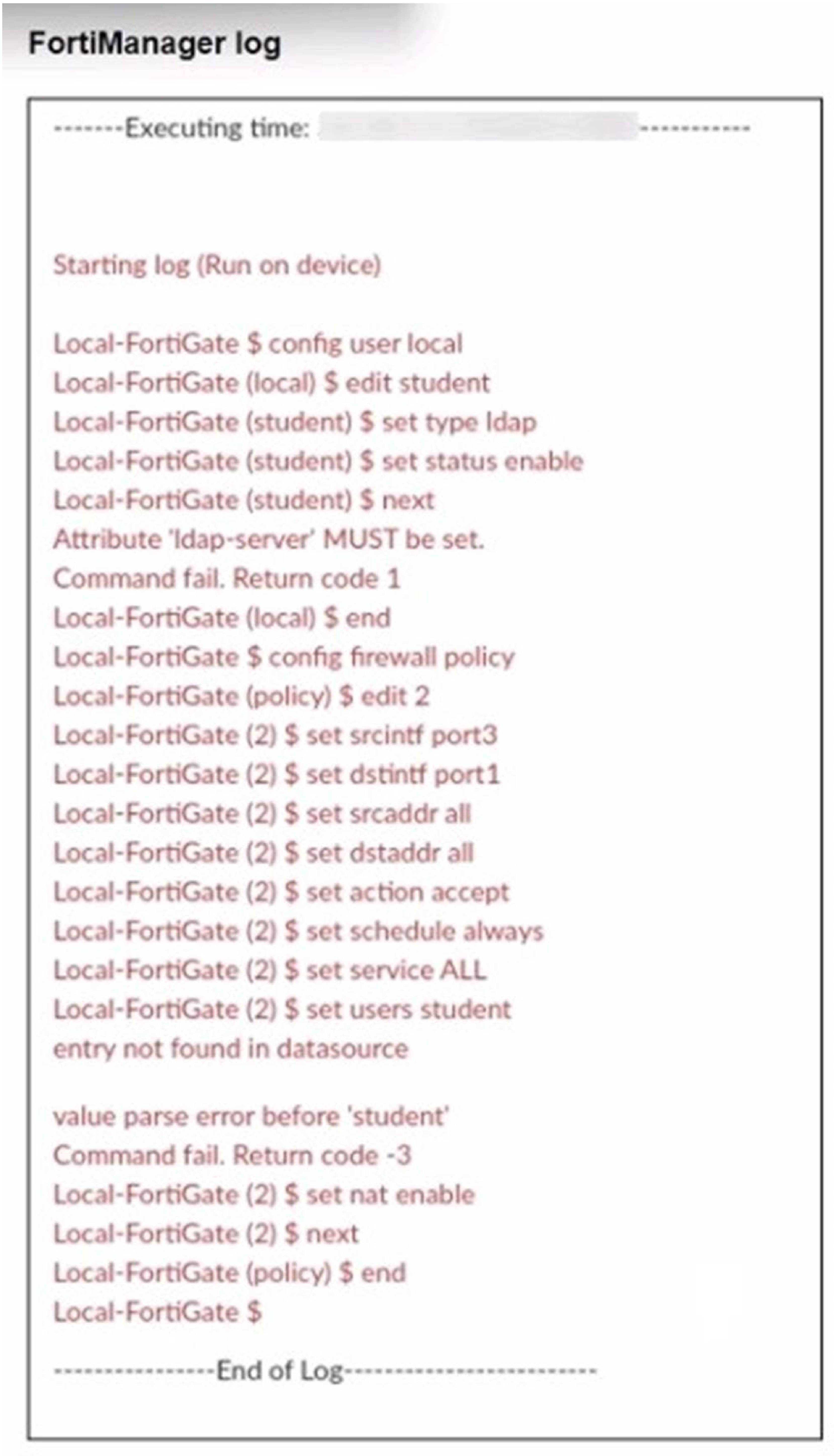
You are using the Quick Install option to install configuration changes on the managed FortiGate.
Which two statements correctly describe the result? (Choose two.)

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 7
Refer to the exhibit.



FortiManager log

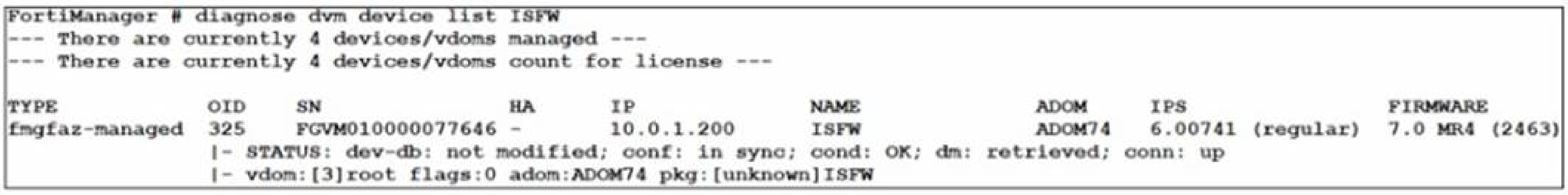
```
-------Executing time: [redacted]-----------



Starting log (Run on device)

Local-FortiGate $ config user local
Local-FortiGate (local) $ edit student
Local-FortiGate (student) $ set type ldap
Local-FortiGate (student) $ set status enable
Local-FortiGate (student) $ next
Attribute 'ldap-server' MUST be set.
Command fail. Return code 1
Local-FortiGate (local) $ end
Local-FortiGate $ config firewall policy
Local-FortiGate (policy) $ edit 2
Local-FortiGate (2) $ set srcintf port3
Local-FortiGate (2) $ set dstintf port1
Local-FortiGate (2) $ set srcaddr all
Local-FortiGate (2) $ set dstaddr all
Local-FortiGate (2) $ set action accept
Local-FortiGate (2) $ set schedule always
Local-FortiGate (2) $ set service ALL
Local-FortiGate (2) $ set users student
entry not found in datasource

value parse error before 'student'
Command fail. Return code -3
Local-FortiGate (2) $ set nat enable
Local-FortiGate (2) $ next
Local-FortiGate (policy) $ end
Local-FortiGate $

---------------End of Log-----------------------
```

A. Policy ID 2 is installed in the disabled state.
B. Policy ID 2 is installed without the remote user student.
C. Policy ID 2 will not be installed.
D. Policy ID 2 is installed without a source address.

Answer: B

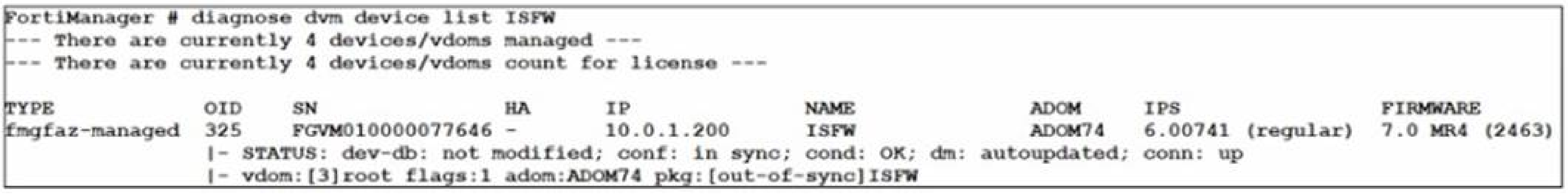
Explanation:
From the log provided in the exhibit, several conclusions can be drawn regarding the installation of Policy ID 2:
? The installation process fails when attempting to set theLDAP user "student". The log shows:
Because of these errors, while other configuration elements (such as source and destination interfaces, actions, and services) are properly set, the user configuration for "student"isnot applied.
Evaluation of the answer options:
? A. Policy ID 2 is installed in the disabled state.
? B. Policy ID 2 is installed without the remote user student.
? C. Policy ID 2 will not be installed.
? D. Policy ID 2 is installed without a source address.
From the log exhibit, we see errors related to the "ldap-server" attribute not being set and an error with the entry "student" not being found in the datasource. This indicates that Policy ID 2 will not be installed due to missing or incorrect data required for successful installation. The "Command fail. Return code -3" confirms the installation failure, so the correct answer is C.
Options A, B, and D are incorrect because:
? A suggests the policy is installed in a disabled state, which isn't supported by the log.
? B and D suggest partial installation, but the error messages indicate a complete failure to install Policy ID 2.
FortiManager References:
? Refer to FortiManager 7.4 Troubleshooting Guide: Common Errors and Log Interpretation.

NEW QUESTION 8
Which output is displayed right after moving the ISFW device from one ADOM to another?
A)



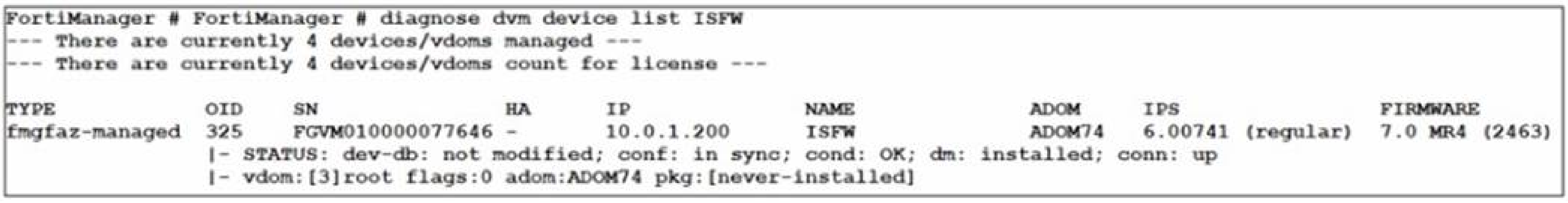
```
FortiManager # diagnose dvm device list ISFW
--- There are currently 4 devices/vdoms managed ---
--- There are currently 4 devices/vdoms count for license ---

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)



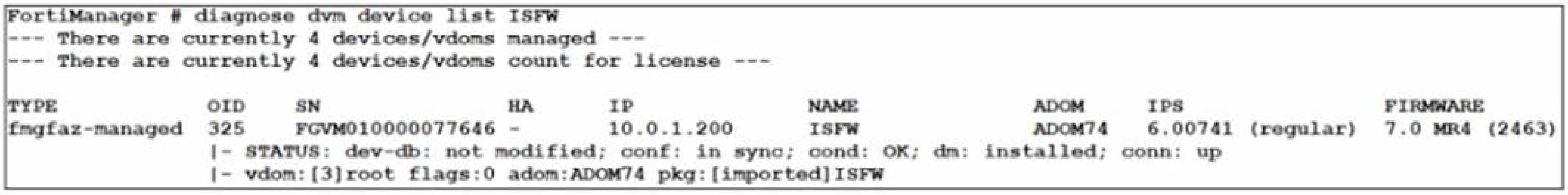
```
FortiManager # diagnose dvm device list ISFW
--- There are currently 4 devices/vdoms managed ---
--- There are currently 4 devices/vdoms count for license ---

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 9
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.

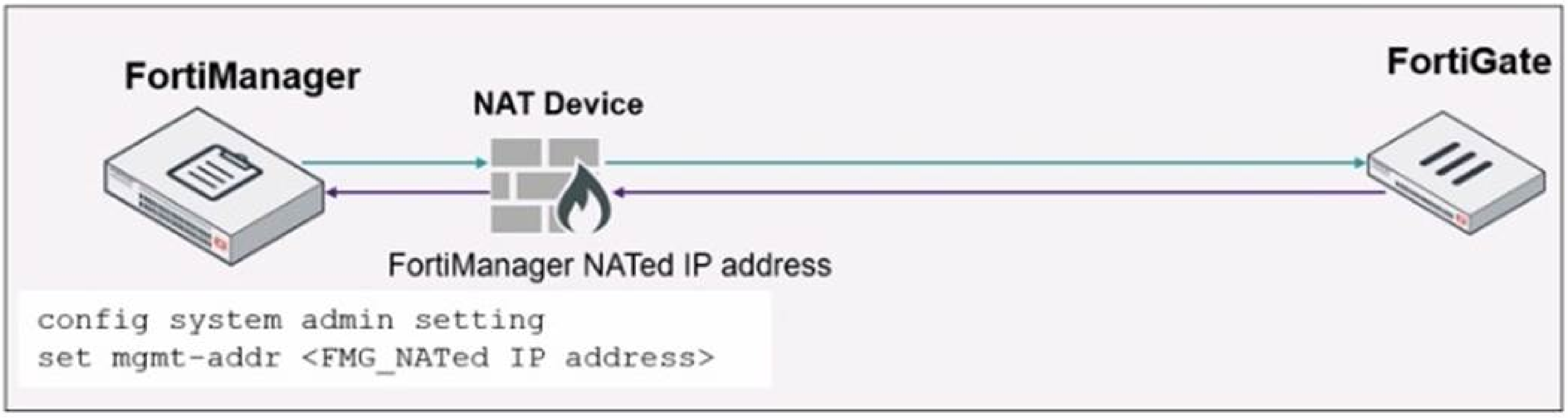
NEW QUESTION 10
What will be the result of reverting to a previous revision version in the revision history?

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 10
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?

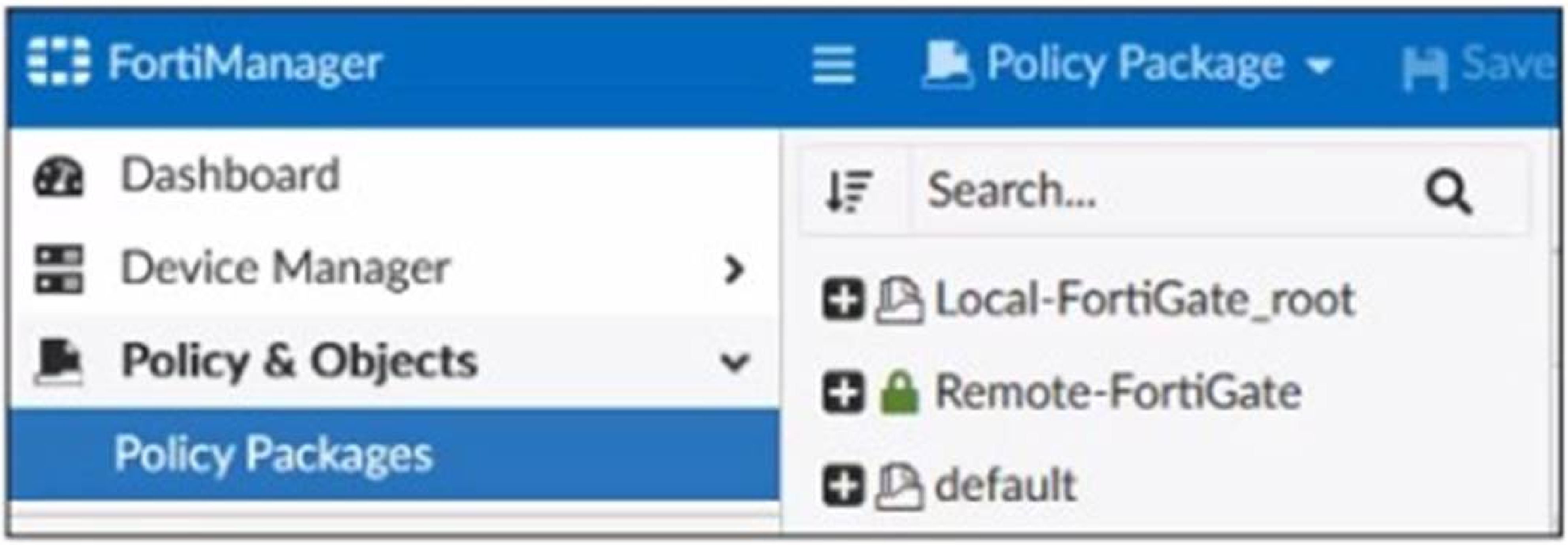
A. During discover
B. FortiManager uses only the FortiGate serial number to establish the
C. During discovery, FortiManager sets both the FortiManager NATed IP address and NAT device IP address on FortiGate.
D. During discover
E. FortiManager sets the NATed device IP address on FortiGate.
F. During discovery, FortiManager sets the FortiManager NATed IP address on FortiGate.

Answer: D

Explanation:

When adding a FortiGate device to FortiManager that is operating behind a NAT device, and the FortiManager NATed IP address is configured under the system administration settings, FortiManager will set the FortiManager NATed IP address on the FortiGate device during the discovery process. This ensures that the FortiGate knows how to reach the FortiManager through the NAT device.
Options A, B, and C are incorrect because:
? Ais incorrect because the discovery process also requires knowing the NATed IP to establish a connection, not just the serial number.
? Bis incorrect because FortiManager does not set the NAT device's IP address on the FortiGate.
? Cis incorrect because it implies that the NAT device IP is set on FortiGate, which is not the expected outcome.
FortiManager References:
? Refer to FortiManager 7.4 Administrator Guide: Device Discovery and Management with NAT.

NEW QUESTION 14
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 17
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.

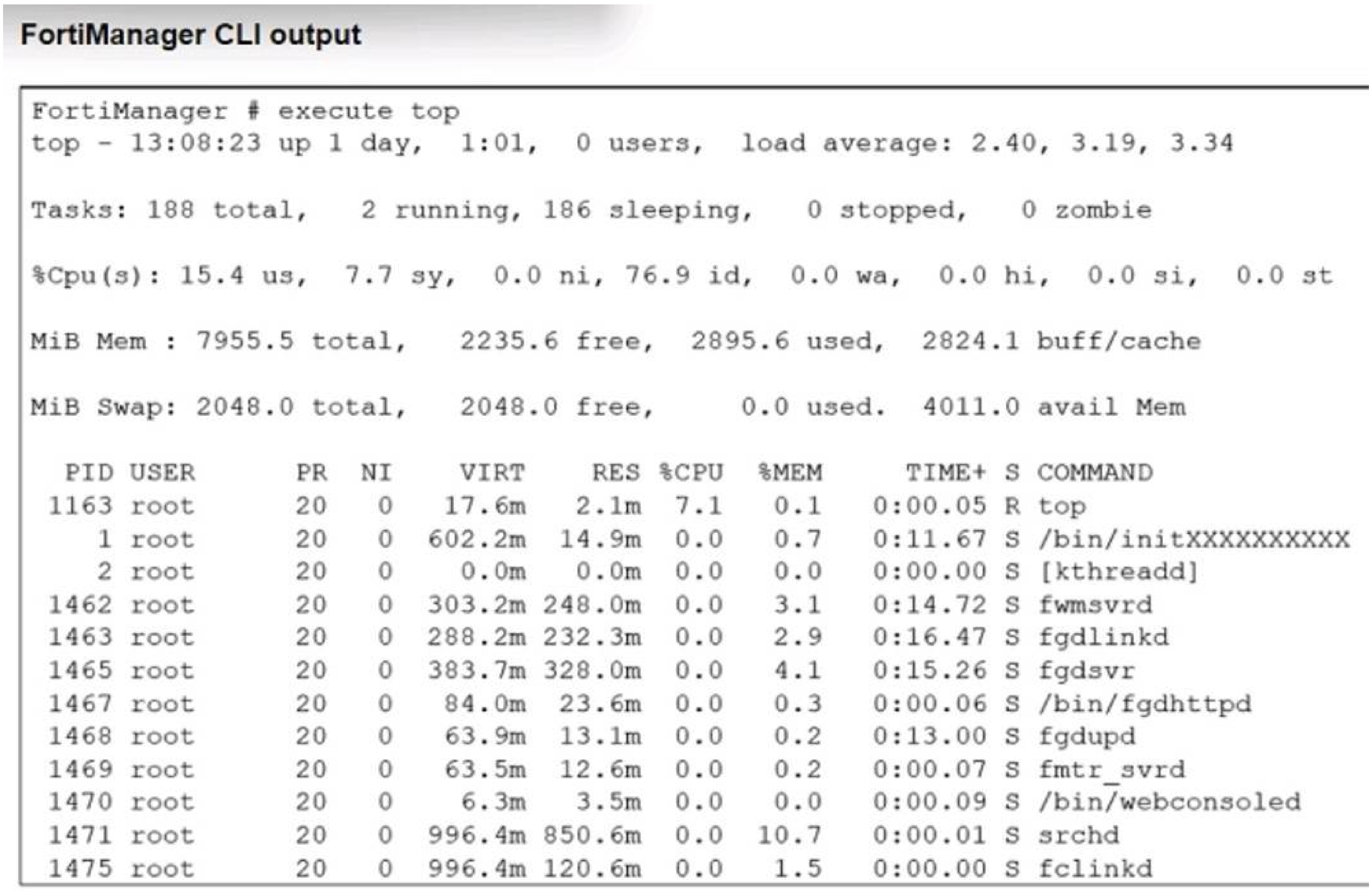
NEW QUESTION 20
An administrator wants to create a policy on an ADOM that is in backup mode and install it on a FortiGate device in the same ADOM. How can the administrator perform this task?

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 24
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
......