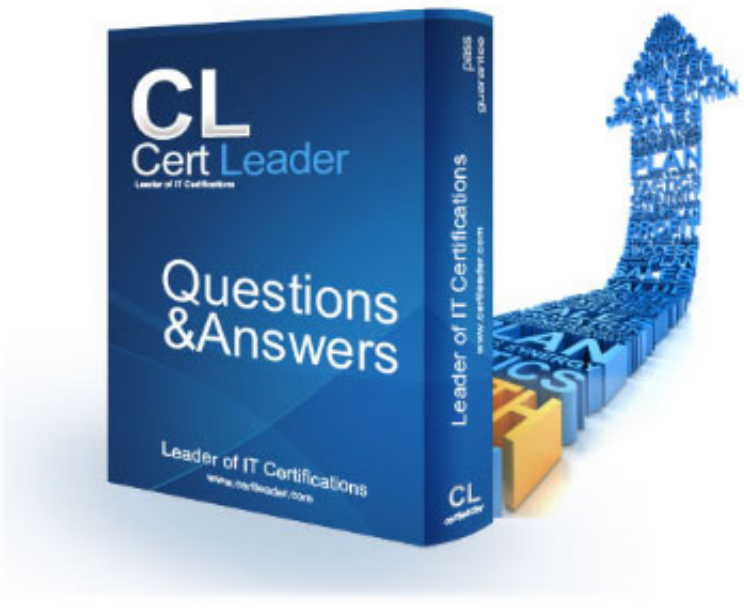
FCP_FMG_AD-7.4 Dumps

FCP - FortiManager 7.4 Administrator

https://www.certleader.com/FCP_FMG_AD-7.4-dumps.html



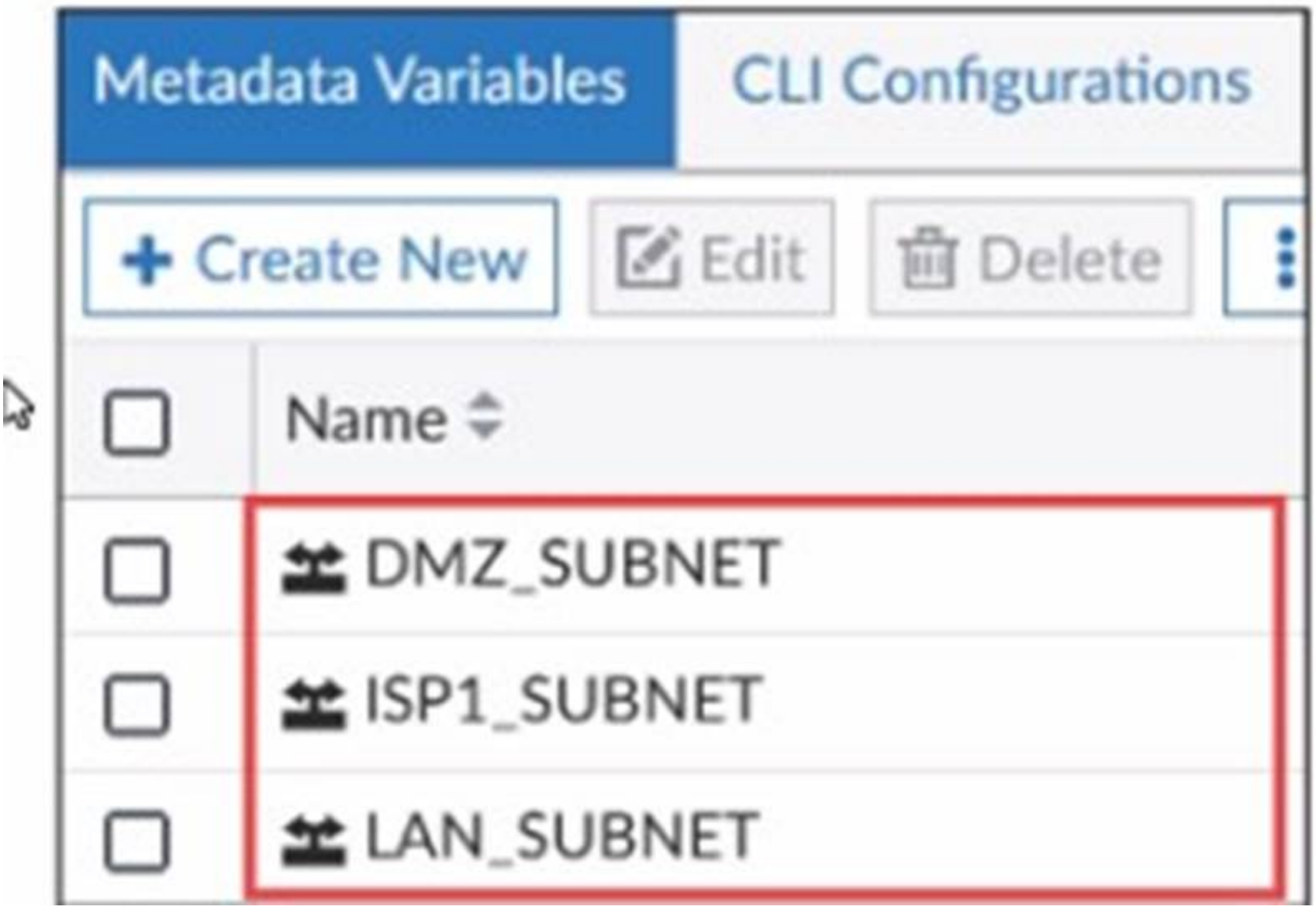
NEW QUESTION 1
Which two statements about Security Fabric integration with FortiManager are true? (Choose two.)

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
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.

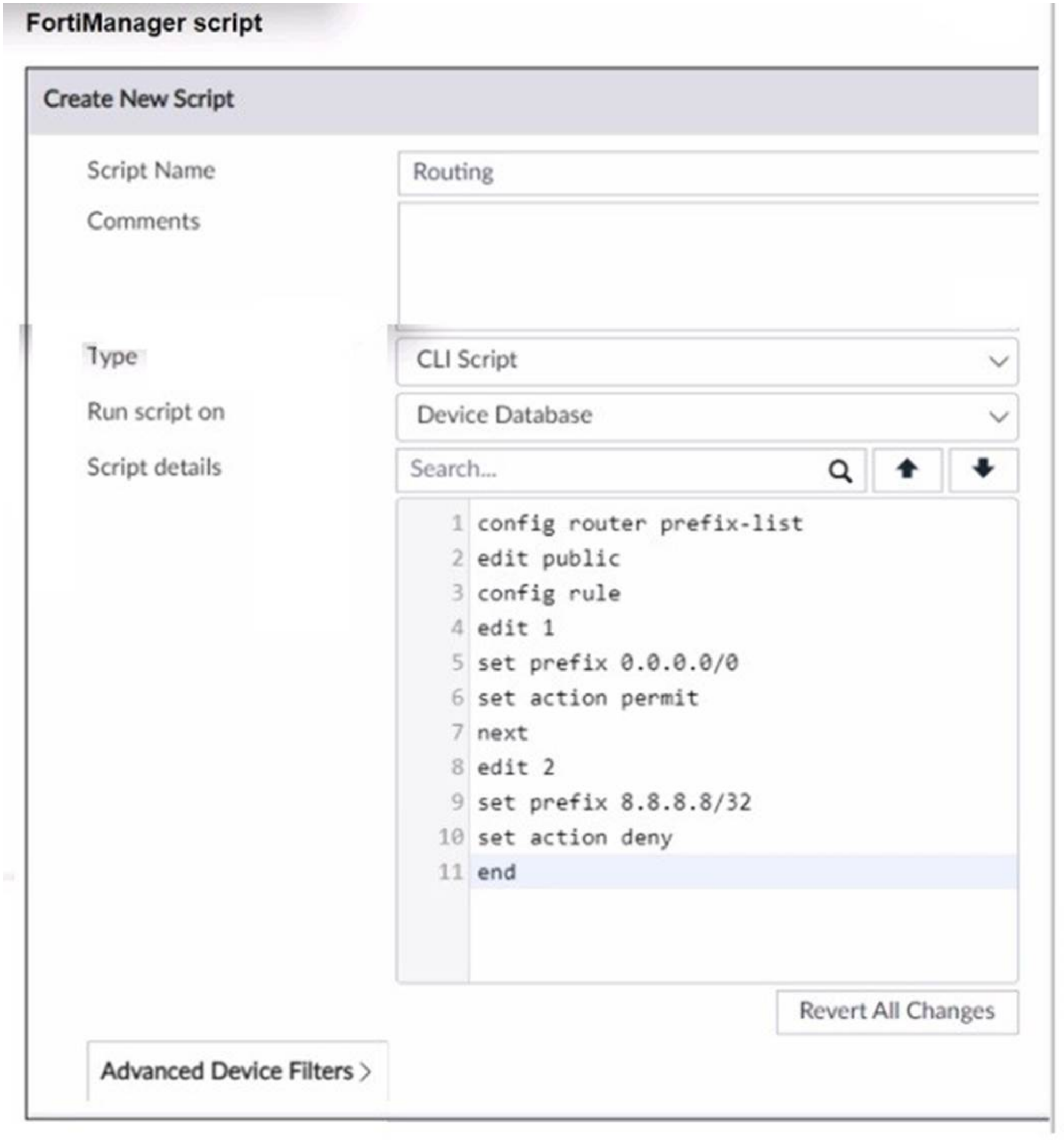
NEW QUESTION 3
An administrator has enabled Service Access on FortiManager. What is the purpose of Service Access on the FortiManager interface?

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 4
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 5

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 6
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 7
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 8
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.

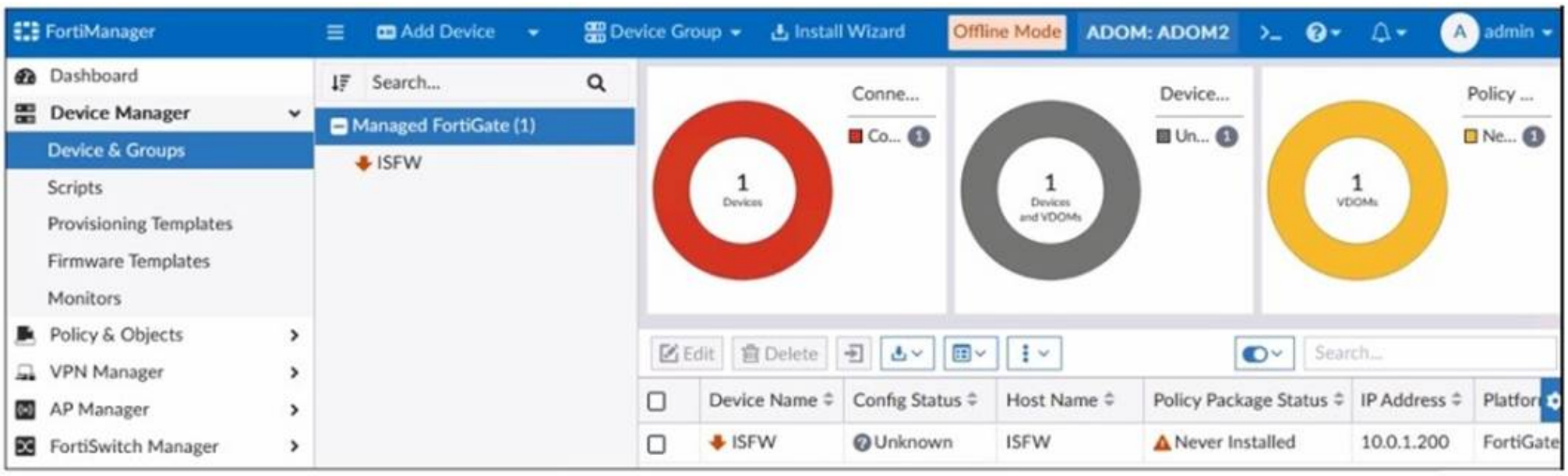
NEW QUESTION 9
What will be the result of reverting to a previous revision version in the revision history?

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.



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 10

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 15
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

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your FCP_FMG_AD-7.4 Exam with Our Prep Materials Via below:

https://www.certleader.com/FCP_FMG_AD-7.4-dumps.html