

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:

? B is misleading as the Security Fabric settings are generally configured and managed separately from other device-level settings.

? D is 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

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 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. The keepalive messages are 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 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 command `execute fmprofile import-profile ADOM2 3547 /tmp/myfile` is used to import a system template profile from the FortiManager file system. The path `/tmp/myfile` indicates 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 D suggest 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 5

Refer to the exhibit.

Managed FortiGate devices

Add Device **Device Group** **Install Wizard**

Search...

Managed FortiGate (4)

- ISFW (3)
 - root
 - Student
 - Trainer
- Local-FortiGate

Managed FortiAnalyzer (1)

- FAZVM64-KVM

2 Devices

Edit **Delete** **Import Configur**

<input type="checkbox"/>	Device Name
<input type="checkbox"/>	Training
<input type="checkbox"/>	ISFW
<input type="checkbox"/>	root [NAT] (Management)
<input type="checkbox"/>	Student [NAT]
<input type="checkbox"/>	Trainer [NAT]
<input type="checkbox"/>	Local-FortiGate*

FortiManager policy package

Policy Package **Install Wizard** **ADOM Revisions**

Search...

Local-FortiGate_root

Remote-FortiGate

Shared_Package

- Firewall Header Policy
- Firewall Policy
- Installation Targets**

default

Edit **Delete**

<input type="checkbox"/>	Installation Target
<input type="checkbox"/>	Local-FortiGate
<input type="checkbox"/>	ISFW
<input type="checkbox"/>	root [NAT] (Management)
<input type="checkbox"/>	Trainer [NAT]
<input type="checkbox"/>	Student [NAT]

FortiManager policy package

Policy Package **Install Wizard** **ADOM Revisions** **Tools**

Search...

Local-FortiGate_root

Remote-FortiGate

Shared_Package

- Firewall Header Policy
- Firewall Policy**
- Installation Targets

default

Create New **Edit** **Delete** **Section** **Policy Lookup** **Co**

<input type="checkbox"/>	#	Name	Install On	From	To
<input type="checkbox"/>	1	Ping_Access	ISFW (root) ISFW (Student)	port3	port1
<input type="checkbox"/>	2	Web	Local-FortiGate (root) ISFW (Student)	port3	port1
<input type="checkbox"/>	3	Source_Device	Installation Targets	port3	port1
<input type="checkbox"/>	Implicit (4/4 Total:1)				
<input type="checkbox"/>	4	Implicit Deny	Installation Targets	any	any

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 6

Refer to the exhibit.

FortiManager script

Create New Script

Script Name

Routing

Comments

Type

CLI Script

Run script on

Device Database

Script details

Search...

1 config router prefix-list

2 edit public

3 config rule

4 edit 1

5 set prefix 0.0.0.0/0

6 set action permit

7 next

8 edit 2

9 set prefix 8.8.8.8/32

10 set action deny

11 end

Advanced Device Filters >

Revert All Changes

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 7

Exhibit.

```
FortiManager # diagnose dvm device list
--- There are currently 1 devices/vdoms managed ---
--- There are currently 1 devices/vdoms count for license ---

TYPE              OID    SN              HA    IP              NAME              ADOM    IPS              FIRMWARE
fmgfaz-managed    325    FGVM010000077646 -    10.0.1.200    ISFW              ADOM2    6.00741 (regular)  7.0 MR4 (2463)
|- STATUS: dev-db: modified; conf: in sync; cond: pending; dm: retrieved; conn: up
|- vdom:[3]root flags:1 adom:ADOM2 pkg: [imported]ISFW
```

Which two statements about the output are true? (Choose two.)

- A. The latest revision history for the managed FortiGate does not match the device-level database.
- B. Configuration changes have been installed on FortiGate, which means the FortiGate configuration has been changed.
- C. Configuration changes directly made on FortiGate have been automatically updated to the device-level database.
- D. The latest revision history for the managed FortiGate does match the FortiGate running configuration.

Answer: AB

Explanation:

The output indicates that:

? The device's status is shown as "dev-db: modified" and "conf: in sync," which means that there is a difference between the device-level database on FortiManager and the actual running configuration of the managed FortiGate. Therefore, the latest revision history for the managed FortiGate does not match the device-level database, which confirms statement A as true.

? "dm: retrieved" status indicates that configuration changes have been installed on the FortiGate, confirming statement B as true. It also means that the configuration has been modified, and those changes have been pulled from the FortiGate to the FortiManager.

Statements C and D are incorrect because:

? C is incorrect as it implies an automatic update, whereas "dev-db: modified" indicates changes have been made on the FortiGate device that are not yet reflected in the FortiManager's database.

? D is incorrect because "dev-db: modified" shows that the device-level database and running configuration are not in sync.

FortiManager References:

? Refer to the FortiManager 7.4 Administrator Guide: Device Manager > Device Status to understand the "dev-db" and "conf" status meanings.

NEW QUESTION 8

Which configuration setting for FortiGate is part of an ADOM-level database on FortiManager?

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

Answer: B

Explanation:

? Option B: Routing is 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 Template is incorrect as it is not a FortiGate-specific setting managed at the ADOM level.

? Option C: SNMP is incorrect because SNMP settings are typically managed on a per-device basis.

? Option D: Security profiles is 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 9

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, the `set` method is used to create new objects or overwrite 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 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 ADOM is 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

Refer to the exhibit.



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:

? A is incorrect because the discovery process also requires knowing the NATed IP to establish a connection, not just the serial number.

? B is incorrect because FortiManager does not set the NAT device's IP address on the FortiGate.

? C is 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 11

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 12

An administrator enabled workspace mode and now wants to delete an address object that is currently referenced in a firewall policy. Which two results can the administrator expect? (Choose two.)

- A. FortiManager will temporarily change the status of the referenced firewall policy to disabled.
- B. FortiManager will disable the status of the address object until the changes are installed.
- C. FortiManager will not allow the administrator to delete a referenced address object until they lock the ADOM.
- D. FortiManager will replace the deleted address object with the none address object in the referenced firewall policy.

Answer: CD

Explanation:

When operating in workspace mode on FortiManager 7.4, the administrator must understand how object references and deletions work:

? Option C- "FortiManager will not allow the administrator to delete a referenced address object until they lock the ADOM":In workspace mode, all changes are managed within an Administrative Domain (ADOM) scope. When an object (like an address object) is referenced in a policy, FortiManager prevents its deletion to maintain configuration integrity. The ADOM must be locked by the administrator to make changes to any referenced objects. This locking mechanism ensures that no unintended deletions or changes occur that could disrupt the policies or configuration.

? Option D- "FortiManager will replace the deleted address object with the none address object in the referenced firewall policy":If the administrator attempts to delete an address object that is currently referenced by a firewall policy, FortiManager will replace the deleted object with the 'none' address object. This is done to maintain the policy structure and avoid policy corruption due to a missing reference. This behavior ensures that the firewall policy remains syntactically correct, even though the specific address object is no longer in use.

NEW QUESTION 14

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions 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

100% Actual & Verified — Instant Download, Please Click
[Order The FCP_FMG_AD-7.4 Practice Test Here](#)