

FCP_FMG_AD-7.6 Dumps

FCP - FortiManager 7.6 Administrator

https://www.certleader.com/FCP_FMG_AD-7.6-dumps.html



NEW QUESTION 1

Company policy dictates that any time a change is made to a policy package on FortiManager an ADOM revision is created before the change installed, and that revision is held for a minimum of 90 days. Over the past three months, each installed change has resulted in several unused policies and duplicate objects. The FortiManager administrator plans to upgrade the FortiGate devices and then upgrade the FortiManager ADOM from version 7.4 to 7.6. Which action can the administrator take to avoid slow ADOM upgrades?

- A. Check and repair the global configuration database before upgrading.
- B. Export firewall policies to Excel, delete them on the ADO
- C. then reimport them after upgrading the ADOM.
- D. Find unused firmware templates, then delete them before upgrading.
- E. Limit ADOM revisions before upgrading.

Answer: D

Explanation:

Limiting ADOM revisions reduces the number of stored historical configurations, which helps avoid performance degradation and slow ADOM upgrades caused by a large volume of revisions.

NEW QUESTION 2

Refer to the exhibits.

Diagnose output

```
FortiManager # get system status
Platform Type           : FMG-VM64-KVM
Platform Full Name      : FortiManager-VM64-KVM
Version                 : v7.6.1-build3344 241023 (GA.M)
Serial Number           : FMG-VMTM24012945
BIOS version            : 04000002
```

Diagnose output

```
FortiManager # diagnose dvm device list
--- There are currently 5 devices/vdoms managed ---
--- There are currently 5 devices/vdoms count for license ---

TYPE          OID   SN              HA   IP           NAME              ADOM   IPS              FIRMWARE
fmgfaz-managed 230  FGVM02TM24013423 -    10.0.13.254  FGVM02TM24013423 root    7.0 MR6 (3401)  N/A
|- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; conn: up
|- vdom:[3]root flags:0 adom:root pkg:[never-installed]
unregistered   167  FGVM02TM24013501 -    192.168.1.3  FGVM02TM24013501 root    7.0 MR6 (3401)  N/A
|- STATUS: dev-db: unknown; conf: out of sync; cond: unregistered; dm: none; conn: unknown
|- vdom:[3]root flags:0 adom:root pkg:[never-installed]
unregistered   209  FGVM02TM24013502 -    192.168.1.101 FGVM02TM24013502 root    7.0 MR6 (3401)  N/A
|- STATUS: dev-db: unknown; conf: out of sync; cond: unregistered; dm: none; conn: unknown
|- vdom:[3]root flags:0 adom:root pkg:[never-installed]
unregistered   188  FGVM02TM24013504 -    192.168.1.111 FGVM02TM24013504 root    7.0 MR6 (3401)  N/A
|- STATUS: dev-db: unknown; conf: out of sync; cond: unregistered; dm: none; conn: unknown
|- vdom:[3]root flags:0 adom:root pkg:[never-installed]
fmgfaz-model   262  -              -    -            HQ-NGFW           My_ADOM 7.0 MR6 (3401)  N/A
|- STATUS: dev-db: unknown; conf: unknown; cond: unknown; dm: unknown; conn: unknown
|- vdom:[3]root flags:0 adom:My_ADOM pkg:[never-installed]

FortiManager # diagnose test deploymanager reloadconf 262
Retriving configuration file from FGT...
Error: Configuration file import error.
```

An administrator runs the reload failure command `diagnose test deploymanager reloadconf 262` on FortiManager. Why does the administrator receive an error message?

- A. The administrator must use the FortiGate name instead of the ID number.
- B. The administrator just recently added FortiGate HQ-NGFW as a model device.
- C. FortiManager requires the FortiGate serial number instead of the ID number.
- D. FortiManager does not support FortiOS version 7.0.

Answer: B

Explanation:

The error occurs because the FortiGate HQ-NGFW device with ID 262 is a newly added model device and has not yet been fully synchronized or installed with a configuration package, which causes the reload configuration command to fail.

NEW QUESTION 3

The administrator uses FortiManager to push a CLI script using the Remote FortiGate Directly (via CLI) option to configure an IPsec VPN. However, when running the script, the administrator receives the following error:

config vpn ipsec phase2-interface [parameter(s) invalid. detail: object mismatch]

What must the administrator do to resolve the script error and successfully apply the IPsec configuration?

- A. Add the end command after finishing the IPsec phase 1-interface configuration block.
- B. Use IPsec templates to deploy provisioning templates.
- C. Add a second config vpn ipsec phase2-interface block without linking it to phase1.
- D. Run the script using the policy package or ADOM database method.

Answer: D

Explanation:

Running the script through the policy package or ADOM database method allows FortiManager to properly interpret object relationships and dependencies in the IPsec configuration, preventing object mismatch errors when pushing complex VPN settings directly via CLI.

NEW QUESTION 4

Which is recommended when you are managing a high volume of logs in your network?

- A. Store logs on FortiManager and use FortiView.
- B. Add and manage FortiAnalyzer from FortiManager.
- C. Enable advanced ADOM mode on FortiManager.
- D. Forward logs from FortiAnalyzer to FortiManager daily.

Answer: B

Explanation:

Adding and managing FortiAnalyzer from FortiManager is recommended for handling a high volume of logs, as FortiAnalyzer is designed specifically for centralized log management, analysis, and reporting, which offloads this workload from FortiManager.

NEW QUESTION 5

Refer to the exhibit.

FortiManager policy package

Import Device - HQ-NGFW-1 - Interface Mapping & Policy (2/5)

Create a new policy package for import.

Policy Package Name: HQ-NGFW-1

Folder: root

Policy Selection: **Import All (6)** Select Policies to Import

Object Selection: **Import only policy dependent objects** Import all objects

Device Interface	Mapping Type	Normalized Interface
<input checked="" type="checkbox"/> port2	Per-Device Per-Platform	LAN
<input checked="" type="checkbox"/> port4	Per-Device Per-Platform	Port4
<input checked="" type="checkbox"/> port6	Per-Device Per-Platform	port6

3

Add mappings for all unused device interfaces

Next > Cancel

An administrator added a FortiGate device to FortiManager with the default object settings at the ADOM layer. What can you conclude from the import policy package process of the HQ-NGFW- 1 device?

- A. The administrator must select Per Platform for all interfaces to correctly detect all interfaces from HQ- NGFW-1.
- B. The administrator must manually create the port4 interface on the ADOM layer to avoid import policy errors.
- C. FortiManager will create LAN, port4, and port6 as normalized interfaces at the ADOM layer.
- D. FortiGate may not work as expected when the administrator does not import all objects.

Answer: C

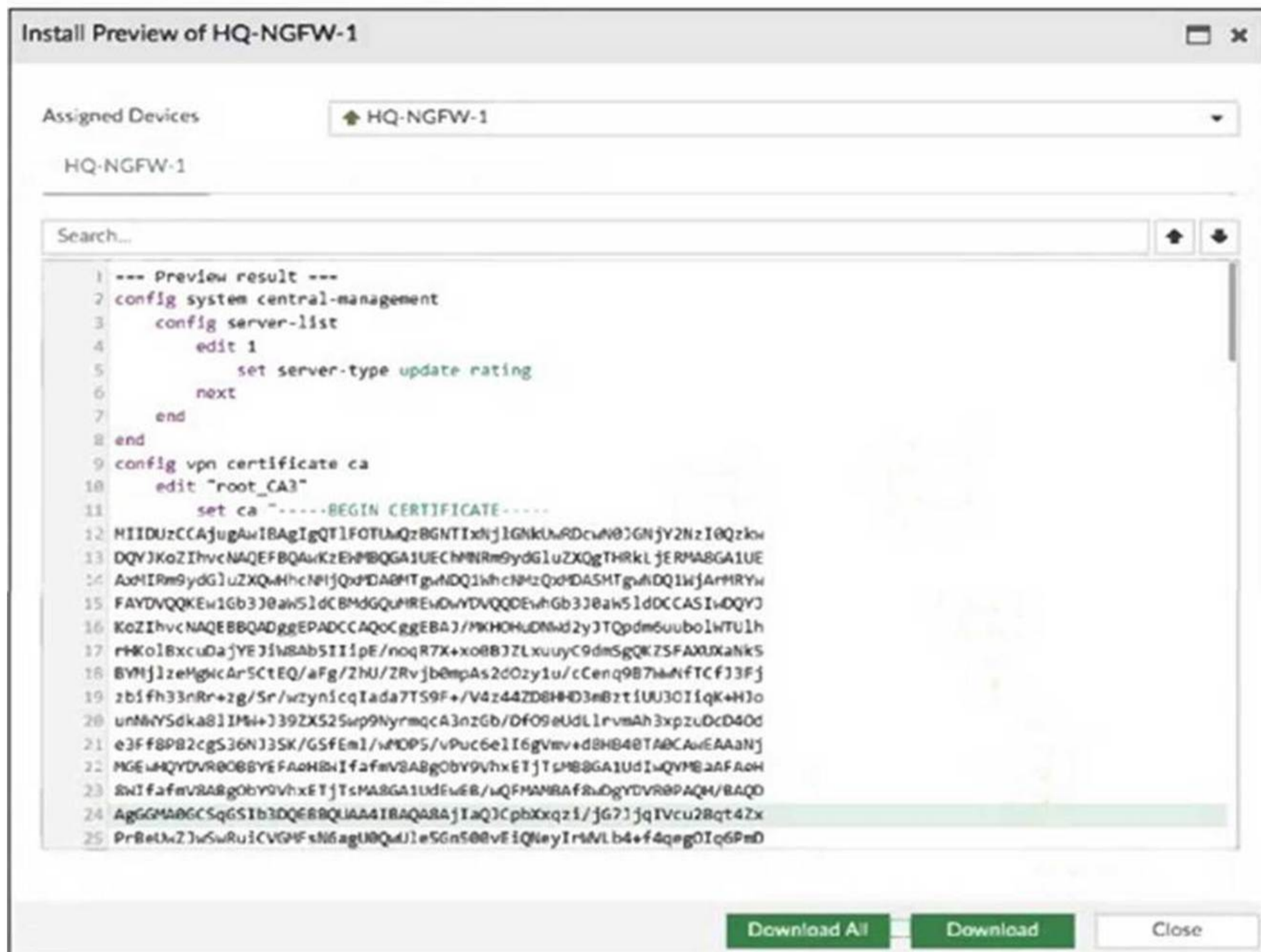
Explanation:

The import process shows that FortiManager will create normalized interfaces named LAN, port4, and port6 at the ADOM layer, mapping them to the corresponding device interfaces based on the import settings.

NEW QUESTION 6

Refer to the exhibit.

FortiManager—HQ-NGFW-1 install preview



An administrator assigned a new policy package to FortiGate HQ-NGFW-1. In the installation preview, they noticed some settings they did not modify and are unsure about the changes.

Based on the exhibit, which two things will happen if they continue with the installation? (Choose two.)

- A. FortiGate HQ-NGFW-1 can use FortiManager firmware templates to upgrade firmware and ratings.
- B. FortiGate HQ-NGFW-1 can contact the FortiManager acting as FortiGuard Distribution Server (FDS) to download FortiGuard updates.
- C. FortiGate HQ-NGFW-1 will use the root_CA3 certificate in firewall address objects or policies.
- D. FortiManager will install the CA certificate named root_CA3 to authenticate FortiGate-to-FortiManager communication protocol (FGFM) tunnel connections with FortiGate HQ-NGFW-1.

Answer: BD

Explanation:

The configuration includes a server-list with server-type set to "update rating," which enables FortiGate HQ-NGFW-1 to contact FortiManager as a FortiGuard Distribution Server (FDS) for FortiGuard updates.

The installation includes a root_CA3 certificate, which FortiManager will install on FortiGate HQ-NGFW-1 to authenticate FGFM tunnel connections between the devices.

NEW QUESTION 7

An administrator wants to configure and manage multiple objects in the FortiManager database and give access to other users who work in the same database. To stay in control of the changes made to firewall policies by other team members, the administrator needs a setup where all modifications go through a central check before they can be installed.

How can the administrator create this setup?

- A. Enable the prompt asking the administrator to accept firewall policies changes before saving.
- B. Enable the workspace (for all ADOMs) to control all changes made by any administrator.
- C. Enable device lock and the advanced mode feature in the ADOM.
- D. Enable workflow mode and the ADOM lock feature.

Answer: D

Explanation:

Enabling workflow mode along with the ADOM lock feature ensures that all configuration changes go through a centralized review and approval process before installation, allowing controlled and coordinated management of firewall policies by multiple administrators.

NEW QUESTION 8

Refer to the exhibit.

```
Start to import config from device(Remote-FortiGate) vdom(root) to
adam(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)"
```

What can you conclude from the downloaded import report?

- A. FortiManager does not support per-device mapping for firewall addresses.
- B. The administrator will see a new policy package named Remote-FortiGate_root in the FortiManager ADOM database.
- C. FortiManager will change the configuration of REMOTE_SUBNET to match the interface mapping coming in from Remote-FortiGate.
- D. As a result of this policy import process, FortiManager will create a new firewall address called REMOTE_SUBNET in the ADOM database.

Answer: B

Explanation:

The import report shows that a new policy package named Remote-FortiGate_root will be created in the FortiManager ADOM database, but some firewall addresses and policies failed to import due to interface binding conflicts.

NEW QUESTION 9

While attempting to push a NetFlow configuration script through the FortiManager policy package: an administrator encounters an error stating that an object is unrecognized in line 4.

```
Starting log (Run on database)
config vdom
edit AGEUSR
[line 4] > config sys interface [parameter(s) invalid. detail: object unrecognized]
Failed to commit to DB, reason([line 4] > config sys interface [parameter(s) invalid. detail: object unrecognized]

Running script(NetFlow_Configuration) on DB failed
```

What must the administrator do to successfully apply the NetFlow configuration script and avoid the object unrecognized error?

- A. Make sure the user running the script has full access to the VDOM—AGEUSR.
- B. Run the script on the device database.
- C. Use metadata variables if they use VDOMs in the script.
- D. Create a normalized interface on the policy layer before running the script.

Answer: C

Explanation:

When using scripts that reference VDOM-specific objects, such as interfaces, in FortiManager, metadata variables must be used to correctly map those objects per VDOM. This prevents "object unrecognized" errors during script execution.

NEW QUESTION 10

What is the purpose of ADOM revisions?

- A. ADOM revisions find unused, duplicate, and unnecessary firewall policies and objects.
- B. ADOM revisions show specific changes in a policy package when it is installed.
- C. ADOM revisions compare previous snapshots of the Policy Package and ADOM-level objects with the device-level database.
- D. ADOM revisions save the current state of all policy packages and objects for an ADOM.

Answer: D

Explanation:

ADOM revisions save the current state of all policy packages and objects within an ADOM, allowing administrators to track changes over time and revert to previous configurations if needed.

NEW QUESTION 10

Push updates are failing on a FortiGate device located behind a network address translation (NAT) device? Which two settings should the administrator check to correct this problem? (Choose two.)

- A. Make sure the NAT device IP address and the correct ports are configured on FortiManager.
- B. Make sure FortiGuard updates and web service are enabled on the FortiGuard service interface.
- C. Make sure the virtual IP address and the correct ports are configured on the NAT device.
- D. Make sure the Bind to IP address option on the FortiGuard service interface is set to the virtual IP address from the NAT device.

Answer: AC

Explanation:

FortiManager must have the NAT device's IP address and correct ports configured to communicate properly with the FortiGate behind NAT. The NAT device must have the correct virtual IP address and ports configured to allow push updates to reach the FortiGate device.

NEW QUESTION 11

Which two conditions trigger FortiManager to create a new revision history? (Choose two.)

- A. When FortiManager installs device-level changes on a managed device
- B. When changes to the device-level database are made on FortiManager
- C. When FortiManager is auto-updated with configuration changes made directly on a managed device
- D. When a provisioning template is assigned to a managed device on the device-level database

Answer: BC

Explanation:

FortiManager creates a new revision history entry whenever changes are made to the device-level database on FortiManager. FortiManager also creates a new revision when it auto-updates its database with configuration changes detected directly on a managed device.

NEW QUESTION 12

Refer to the exhibit.

```
FortiManager # config system global
(global) # set workspace-mode normal
(global) # end
FortiManager #
```

What are two results from the configuration shown in the exhibit? (Choose two.)

- A. Ungraceful closed sessions will keep the ADOM in a locked state until the administrator session times out.
- B. The administrator can lock policy blocks and FortiManager global ADOM.
- C. The same administrator can lock more than one ADOM at the same time.
- D. The administrator must have access to the ADOM to approve changes.

Answer: AB

Explanation:

In normal workspace mode, ungraceful session closures will keep the ADOM locked until the session times out, preventing other administrators from editing. Normal workspace mode allows administrators to lock policy blocks and the global ADOM, providing granular locking control.

NEW QUESTION 17

An administrator is copying a system template profile between ADOMs by running the following command:

```
execute fmpfile export-profile ADOM 3547 /tmp/Backup_File
```

```
output dump to file: [/tmp/Backup_File]
```

Where does this command export the system template profile from?

- A. FortiManager /tmp/Backup_File folder
- B. FortiManager ADOM policy database
- C. ADOM device database
- D. FortiManager configuration backup file

Answer: B

Explanation:

The command exports the system template profile from the FortiManager ADOM policy database, which stores the configuration templates for devices within that ADOM.

NEW QUESTION 21

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          ADOM76    7.00741 (regular) 7.0 MR6 (2463)
|- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: autoupdated; conn: up
|- vdom:[3]root flags:1 adom:ADOM76 pkg:[out-of-sync]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          ADOM76    7.00741 (regular) 7.0 MR6 (2463)
|- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: installed; conn: up
|- vdom:[3]root flags:0 adom:ADOM76 pkg:[imported]ISFW
```

C)

```
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          ADOM76    7.00741 (regular) 7.0 MR6 (2463)
|- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: installed; conn: up
|- vdom:[3]root flags:0 adom:ADOM76 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          ADOM76    7.00741 (regular) 7.0 MR6 (2463)
|- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; conn: up
|- vdom:[3]root flags:0 adom:ADOM76 pkg:[unknown]ISFW
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

Explanation:

Right after moving the ISFW device to a new ADOM, the status typically shows the policy package as never-installed, indicating that the device has been assigned to the new ADOM but no policy package has yet been installed in that ADOM.

NEW QUESTION 25

Refer to the exhibit.

FortiManager script

Create New Script
0/225

Type: CLI Script

Run script on: Device Database

Validate on change:

Validation device platform: FortiGate-VM64

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
                
```

Format CLI script
Revert All Changes

Advanced Device Filters >

Which two results occur if you run the script using the Device Database option? (Choose two.)

- A. The device Config Status is tagged as Modified.
- B. The script history shows the successful installation of the script on the remote FortiGate.
- C. The successful execution of a script on the Device Database creates a new revision history.
- D. The administrator must install these changes on a managed device using the Install Wizard.

Answer: AD

Explanation:

Running a script on the Device Database marks the configuration as modified but does not immediately apply changes to the device. The administrator must use the Install Wizard to push and install these changes from the Device Database onto the managed device.

NEW QUESTION 27

.....

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-7.6 Exam with Our Prep Materials Via below:

https://www.certleader.com/FCP_FMG_AD-7.6-dumps.html