

Exam Questions FCP_FMG_AD-7.6

FCP - FortiManager 7.6 Administrator

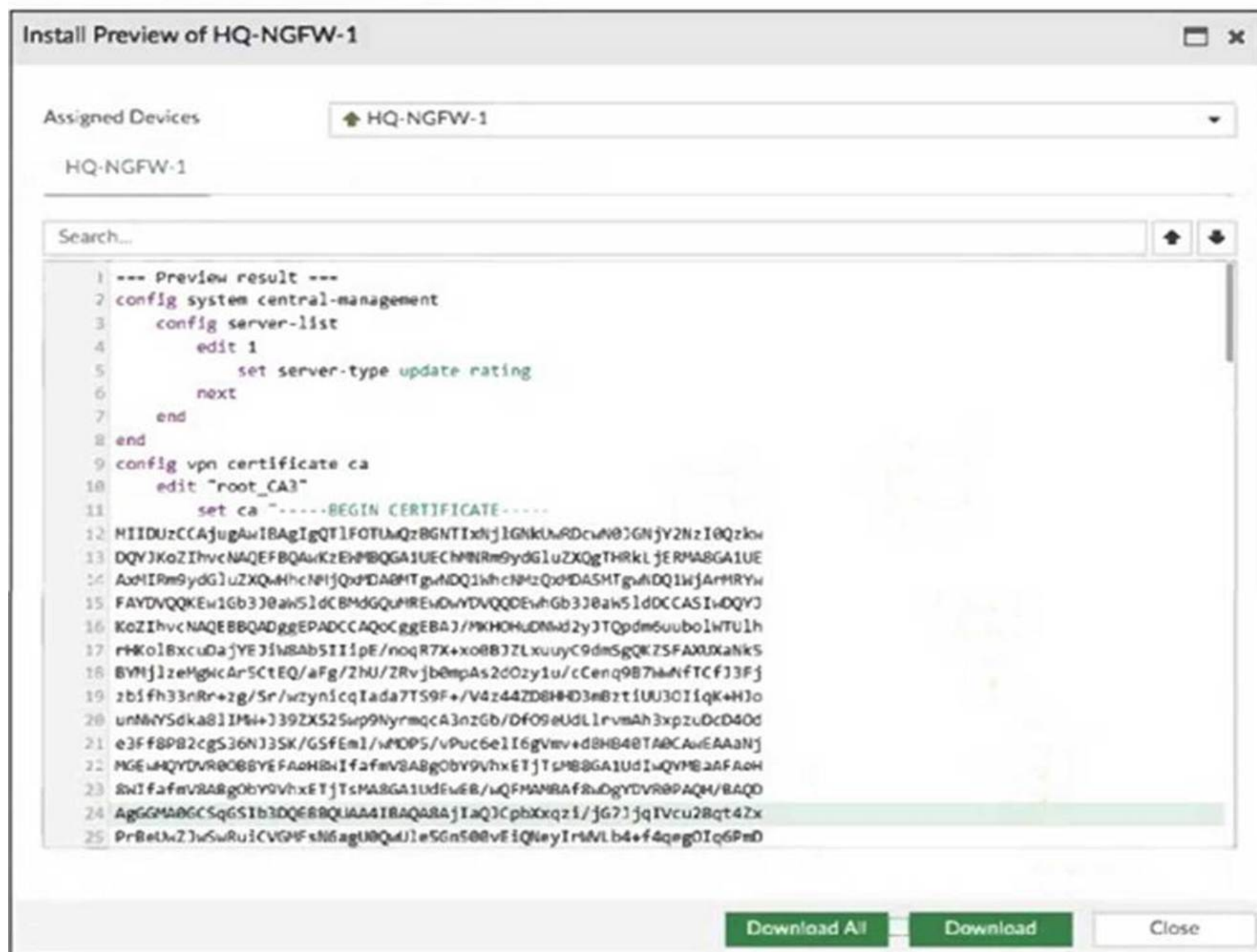
https://www.2passeasy.com/dumps/FCP_FMG_AD-7.6/



NEW QUESTION 1

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 2

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 3

An administrator has assigned a global policy package to a new ADOM named ADOM1.
 What will happen if the administrator tries to create a new policy package in ADOM1?

- A. The administrator will be able to select the option to assign the global policy package to the new policy package.
- B. FortiManager will automatically assign the global policy package to the new policy package.
- C. FortiManager will automatically install policies on the policy package in ADOM1.
- D. The administrator will have to assign the global policy package from the global ADOM.

Answer: A

Explanation:

When a global policy package is assigned to an ADOM, administrators creating new policy packages within that ADOM have the option to select and assign the global policy package to the new policy package if desired.

NEW QUESTION 4

Refer to the exhibit.

FortiManager cluster settings

FortiManager

Cluster Settings

Failover Mode: Manual VRRP

Operation Mode: Standalone Primary Secondary

Peer IP and Peer SN	IP Type	Peer IP	Peer SN	Action
	IPv4	10.0.1.242	FMG-VM0A169	✕ +

Cluster ID: (1-64)

Group Password:

File Quota: MB (2048-20480)

Heart Beat Interval: Seconds

Failover Threshold: (1-255)

VIP:

VRRP Interface:

Priority: (1-253)

Unicast: ☐

Monitored IP	IP	Interface	Action
	10.0.1.241	port2	✕ +

Download Debug Log: Download

If the monitored interface for the primary FortiManager device fails, what must you do to maintain high availability (HA)?

- A. The FortiManager HA failover is transparent to administrators and does not require any additional action.
- B. Manually promote one of the working secondary devices to the primary role: and reboot the original primary device to remove the peer IP address of the failed device.
- C. Reconfigure the primary device to remove the peer IP address of the failed device from its configuration.
- D. Check the integrity database of the primary device to force a secondary device to become the new primary with all active interfaces.

Answer: A

Explanation:

In a FortiManager HA cluster configured with VRRP failover, the failover process is automatic and transparent to administrators. If the monitored interface on the primary device fails, the secondary device takes over without requiring manual intervention to maintain HA.

NEW QUESTION 5

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 6

A service provider administrator has assigned a global policy package to a managed customer ADOM named My_ADOM. The customer administrator has access only to My_ADOM.

How can the customer administrator edit the global header policy of the global policy package?

- A. The customer administrator can edit the header policy by using workspace mode on the global ADOM.
- B. The customer administrator can edit the header policy by using workflow mode on the global ADOM and My_ADOM.
- C. The service provider administrator can unlock the global policy from the global ADOM to authorize changes to the customer administrator.
- D. The customer administrator cannot edit the global header policy; only the service provider administrator can make changes from the global ADOM.

Answer: D

Explanation:

The global policy package is managed only from the global ADOM by the service provider administrator. Customer administrators with access solely to their ADOM (My_ADOM) cannot edit the global header policy; such changes must be made by the service provider administrator in the global ADOM.

NEW QUESTION 7

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.

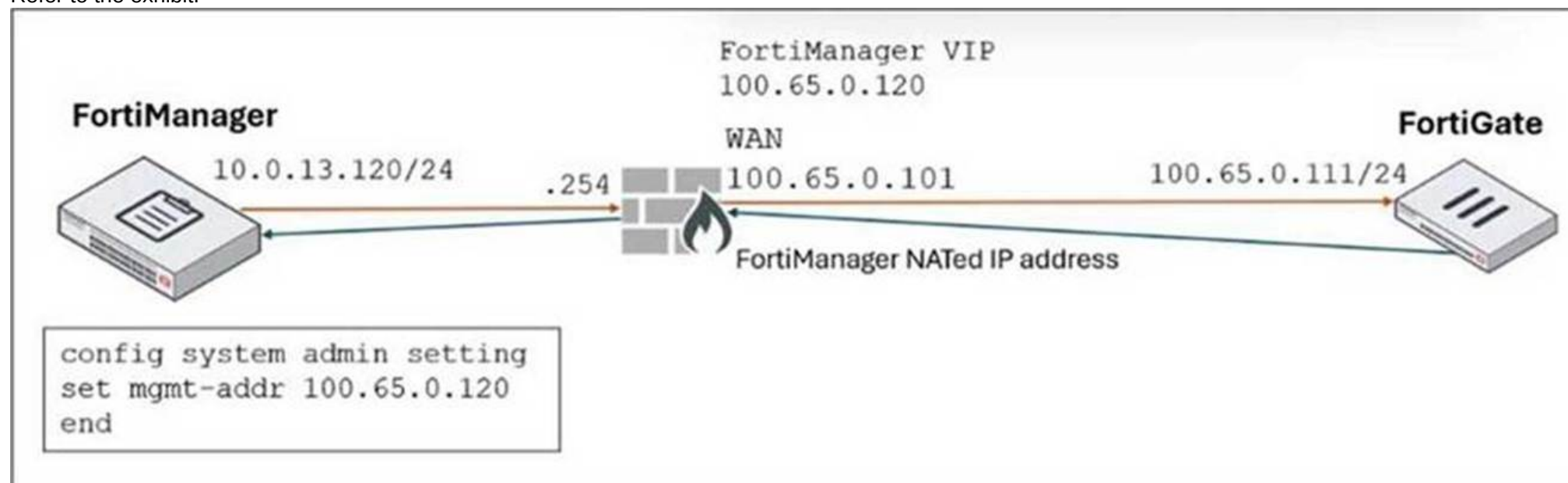
Answer: AD

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 8

Refer to the exhibit.



FortiManager is operating behind a network address translation (NAT) device, and the administrator configured the FortiManager NATed IP address under the FortiManager system administration settings.

What is the expected result during discovery?

- A. FortiManager sets both the 100.65.0.120 IP address and 10.0.13.120 IP address on FortiGate.
- B. FortiManager sets both the 100.65.0.120 IP address and 100.65.0.101 IP address on FortiGate.
- C. FortiManager sets the 100.65.0.101 IP address on FortiGate.
- D. FortiManager sets the 100.65.0.120 IP address on FortiGate.

Answer: D

Explanation:

When FortiManager is behind a NAT device, setting the NATed IP address (100.65.0.120) in the system admin settings causes FortiManager to use that NATed IP address for communication and configuration with FortiGate during discovery and management operations.

NEW QUESTION 10

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual FCP_FMG_AD-7.6 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the FCP_FMG_AD-7.6 Product From:

https://www.2passeasy.com/dumps/FCP_FMG_AD-7.6/

Money Back Guarantee

FCP_FMG_AD-7.6 Practice Exam Features:

- * FCP_FMG_AD-7.6 Questions and Answers Updated Frequently
- * FCP_FMG_AD-7.6 Practice Questions Verified by Expert Senior Certified Staff
- * FCP_FMG_AD-7.6 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * FCP_FMG_AD-7.6 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year