

NSE5_FMG-7.2 Dumps

Fortinet NSE 5 - FortiManager 7.2

https://www.certleader.com/NSE5_FMG-7.2-dumps.html



NEW QUESTION 1

- (Topic 1)

An administrator would like to review, approve, or reject all the firewall policy changes made by the junior administrators.

How should the Workspace mode be configured on FortiManager?

- A. Set to workflow and use the ADOM locking feature
- B. Set to read/write and use the policy locking feature
- C. Set to normal and use the policy locking feature
- D. Set to disable and use the policy locking feature

Answer: A

Explanation:

Reference: https://help.fortinet.com/fmgr/50hlp/52/5-2-0/FMG_520_Online_Help/200_What's-New.03.03.html

NEW QUESTION 2

- (Topic 1)

In the event that the primary FortiManager fails, which of the following actions must be performed to return the FortiManager HA to a working state?

- A. Secondary device with highest priority will automatically be promoted to the primary role, and manually reconfigure all other secondary devices to point to the new primary device
- B. Reboot one of the secondary devices to promote it automatically to the primary role, and reconfigure all other secondary devices to point to the new primary device.
- C. Manually promote one of the secondary devices to the primary role, and reconfigure all other secondary devices to point to the new primary device.
- D. FortiManager HA state transition is transparent to administrators and does not require any reconfiguration.

Answer: C

Explanation:

FortiManager_6.4_Study_Guide-Online – page 346

FortiManager HA doesn't support IP takeover where an HA state transition is transparent to administrators. If a failure of the primary occurs, the administrator must take corrective action to resolve the problem that may include invoking the state transition. If the primary device fails, the administrator must do the following in order to return the FortiManager HA to a working state:

- * 1. Manually reconfigure one of the secondary devices to become the primary device
- * 2. Reconfigure all other secondary devices to point to the new primary device

NEW QUESTION 3

- (Topic 1)

An administrator would like to create an SD-WAN using central management in the Training ADOM.

To create an SD-WAN using central management, which two steps must be completed? (Choose two.)

- A. Specify a gateway address when you create a default SD-WAN static route
- B. Enable SD-WAN central management in the Training ADOM
- C. Configure and install the SD-WAN firewall policy and SD-WAN static route before installing the SD-WAN template settings
- D. Remove all the interface references such as routes or policies that will be a part of SD-WAN member interfaces

Answer: BD

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/676493/removing-existing-configuration-references-to-interfaces>

NEW QUESTION 4

- (Topic 1)

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

- A. When configuration revision is reverted to previous revision in the revision history
- B. When FortiManager installs device-level changes to a managed device
- C. When FortiManager is auto-updated with configuration changes made directly on a managed device
- D. When changes to device-level database is made on FortiManager

Answer: BC

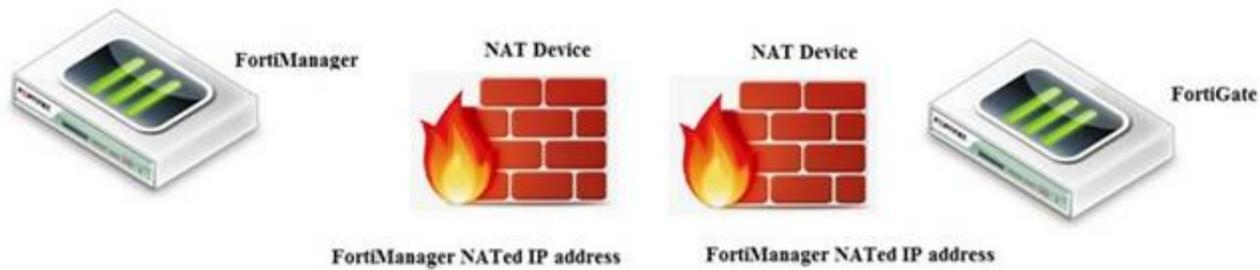
Explanation:

Reference: https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FortiManager_Admin_Guide/1000_Device%20Manager/1500_Manage_device_configs/0600_Manage%20config%20rev%20history.htm

NEW QUESTION 5

- (Topic 1)

View the following exhibit.



If both FortiManager and FortiGate are behind the NAT devices, what are the two expected results? (Choose two.)

- A. FortiGate is discovered by FortiManager through the FortiGate NATed IP address.
- B. FortiGate can announce itself to FortiManager only if the FortiManager IP address is configured on FortiGate under central management.
- C. During discovery, the FortiManager NATed IP address is not set by default on FortiGate.
- D. If the FCFM tunnel is torn down, FortiManager will try to re-establish the FGFM tunnel.

Answer: AC

Explanation:

Fortimanager can discover FortiGate through a NATed FortiGate IP address. If a FortiManager NATed IP address is configured on FortiGate, then FortiGate can announce itself to FortiManager. FortiManager will not attempt to re-establish the FGFM tunnel to the FortiGate NATed IP address, if the FGFM tunnel is interrupted. Just like it was in the NATed FortiManager scenario, the FortiManager NATed IP address in this scenario is not configured under FortiGate central management configuration.

NEW QUESTION 6

- (Topic 1)

Which three settings are the factory default settings on FortiManager? (Choose three.)

- A. Username is admin
- B. Password is fortinet
- C. FortiAnalyzer features are disabled
- D. Reports and Event Monitor panes are enabled
- E. port1 interface IP address is 192.168.1.99/24

Answer: ACE

NEW QUESTION 7

- (Topic 1)

Which two items does an FGFM keepalive message include? (Choose two.)

- A. FortiGate uptime
- B. FortiGate license information
- C. FortiGate IPS version
- D. FortiGate configuration checksum

Answer: CD

Explanation:

Reference: <https://docs.fortinet.com/document/fortimanager/6.2.0/fortigate-fortimanager-communications-protocol-guide/579138/keep-alive-messages>

NEW QUESTION 8

- (Topic 1)

View the following exhibit.

Import Device - Local-FortiGate [root]

Create a new policy package for import.

Policy Package Name

Folder

Policy Selection

Import All(3)

Select Policies and Profile Groups to Import

Object Selection

Import only policy dependent objects

Import all objects

An administrator is importing a new device to FortiManager and has selected the shown options. What will happen if the administrator makes the changes and installs the modified policy package on this managed FortiGate?

- A. The unused objects that are not tied to the firewall policies will be installed on FortiGate
- B. The unused objects that are not tied to the firewall policies will remain as read-only locally on FortiGate
- C. The unused objects that are not tied to the firewall policies locally on FortiGate will be deleted
- D. The unused objects that are not tied to the firewall policies in policy package will be deleted from the FortiManager database

Answer: C

Explanation:

Reference: <https://community.fortinet.com/t5/FortiManager/Import-all-objects-Versus-Import-only-policy-dependent-objects/ta-p/193259?externalID=FD40392>

NEW QUESTION 9

- (Topic 1)

In addition to the default ADOMs, an administrator has created a new ADOM named Training for FortiGate devices. The administrator sent a device registration to FortiManager from a remote FortiGate. Which one of the following statements is true?

- A. The FortiGate will be added automatically to the default ADOM named FortiGate.
- B. The FortiGate will be automatically added to the Training ADOM.
- C. By default, the unregistered FortiGate will appear in the root ADOM.
- D. The FortiManager administrator must add the unregistered device manually to the unregistered device manually to the Training ADOM using the Add Device wizard

Answer: C

Explanation:

Reference: <https://docs.fortinet.com/document/fortimanager/7.0.0/administration-guide/718923/root-adom>

NEW QUESTION 10

- (Topic 2)

Refer to the exhibit.

Edit Address

Address Name: LAN

Type: IP/Netmask

IP/Netmask: 192.168.1.0/255.255.255.0

Interface: any

Static Route Configuration: OFF

Comments: 0/255

Add to Groups: Click to add ...

Advanced Options >

Per-Device Mapping: ON

+ Add Edit Delete

<input type="checkbox"/>	Name	VDOM	Details
<input type="checkbox"/>	Remote-FortiGate	root	IP/Netmask:10.200.1.0/255.255.255.0

An administrator has created a firewall address object, Training which is used in the Local- FortiGate policy package. When the installation operation is performed, which IP/Netmask will be installed on the Local-FortiGate, for the Training firewall address object?

- A. 192.168.0.1/24
- B. 10.200.1.0/24
- C. It will create a firewall address group on Local-FortiGate with 192.168.0.1/24 and 10.0.1.0/24 object values.
- D. Local-FortiGate will automatically choose an IP/Netmask based on its network interface settings.

Answer: A

NEW QUESTION 10

- (Topic 2)

Refer to the exhibit.

```
config system global
set workspace-mode normal
end
```

Given the configuration shown in the exhibit, which two statements are true? (Choose two.)

- A. It allows two or more administrators to make configuration changes at the same time, in the same ADOM.
- B. It disables concurrent read-write access to an ADOM.
- C. It allows the same administrator to lock more than one ADOM at the same time.
- D. It is used to validate administrator login attempts through external servers.

Answer: BC

Explanation:

Reference: <https://docs.fortinet.com/document/fortimanager/6.0.4/administration-guide/86456/concurrentadom-access>

NEW QUESTION 13

- (Topic 2)

Refer to the exhibit.

Create New ADOM

Name: Training

Type: FortiGate (6.2, 6.0, 5.6, 5.4)

Comments:

Devices:

Name	IP Address	Platform
Click to select devices for this ADOM.		

Mode: Normal Backup

Which two statements about an ADOM set in Normal mode on FortiManager are true? (Choose two.)

- A. It supports the FortiManager script feature
- B. It allows making configuration changes for managed devices on FortiManager panes
- C. FortiManager automatically installs the configuration difference in revisions on the managed FortiGate
- D. You cannot assign the same ADOM to multiple administrators

Answer: AB

Explanation:

"FortiGate units in the ADOM will query their own configuration every 5 seconds. If there has been a configuration change, the FortiGate unit will send a diff revision on the change to the FortiManager using the FGFM protocol."

NEW QUESTION 18

- (Topic 2)

An administrator has enabled Service Access on FortiManager.

What is the purpose of Service Access on the FortiManager interface?

- A. Allows FortiManager to download IPS packages
- B. Allows FortiManager to respond to request for FortiGuard services from FortiGate devices
- C. Allows FortiManager to run real-time debugs on the managed devices
- D. Allows FortiManager to automatically configure a default route

Answer: B

Explanation:

FortiManager 6.2 Study guide page 350

NEW QUESTION 23

- (Topic 2)

Which two statements regarding device management on FortiManager are true? (Choose two.)

- A. FortiGate devices in HA cluster devices are counted as a single device.
- B. FortiGate in transparent mode configurations are not counted toward the device count on FortiManager.
- C. FortiGate devices in an HA cluster that has five VDOMs are counted as five separate devices.
- D. The maximum number of managed devices for each ADOM is 500.

Answer: AC

NEW QUESTION 28

- (Topic 2)

Which two items are included in the FortiManager backup? (Choose two.)

- A. FortiGuard database
- B. Global database
- C. Logs
- D. All devices

Answer: BD

Explanation:

Reference: <https://kb.fortinet.com/kb/viewContent.do?externalId=FD34549>

NEW QUESTION 33

- (Topic 2)

An administrator's PC crashes before the administrator can submit a workflow session for approval. After the PC is restarted, the administrator notices that the

ADOM was locked from the session before the crash.
How can the administrator unlock the ADOM?

- A. Restore the configuration from a previous backup.
- B. Log in asSuper_Userin order to unlock the ADOM.
- C. Log in using the same administrator account to unlock the ADOM.
- D. Delete the previous admin session manually through the FortiManager GUI or CLI.

Answer: D

NEW QUESTION 35

- (Topic 2)

Refer to the exhibit.

Create New CLI Script

Script Name: [\[View Sample Script\]](#)

Comments: 0/255

Type:

Run script on:

Script details:

```
config router prefix-list
edit public
config rule
edit 1
set prefix 0.0.0.0/0
set action permit
next
edit 2
set prefix 8.8.8.8/32
set action deny
end
```

[Advanced Device Filters >](#)

Which two statements are true if the script is executed using theDevice Databaseoption? (Choose two.)

- A. You must install these changes using theInstall Wizardto a managed device
- B. The successful execution of a script on theDevice Databasewill create a new revision history
- C. The script history will show successful installation of the script on the remote FortiGate
- D. TheDevice Settings Statuswill be tagged asModified

Answer: AD

NEW QUESTION 37

- (Topic 2)

An administrator has assigned a global policy package to custom ADOM1. Then the administrator creates a new policy package, Fortinet, in the custom ADOM1. Which statement about the global policy package assignment to the newly-created policy package Fortinetis true?

- A. When a new policy package is created, it automatically assigns the global policies to the new package.
- B. When a new policy package is created, you need to assign the global policy package from the globalADOM.
- C. When a new policy package is created, you need to reapply the global policy package to the ADOM.
- D. When a new policy package is created, you can select the option to assign the global policies to the new package.

Answer: A

Explanation:

Global Policy Package is applied at the ADOM level and you have the option to choose which ADOM policy packages you want to exclude (there is no option to choose Policy Packages to include).

NEW QUESTION 39

- (Topic 3)

An administrator is in the process of moving the system template profile between ADOMs by running the following command: execute improfile import-profile ADOM2 3547 /tmp/myfile Where does the administrator import the file from?

- A. File system
- B. ADOM1
- C. ADOM2 object database
- D. ADOM2

Answer: A

NEW QUESTION 41

- (Topic 3)

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

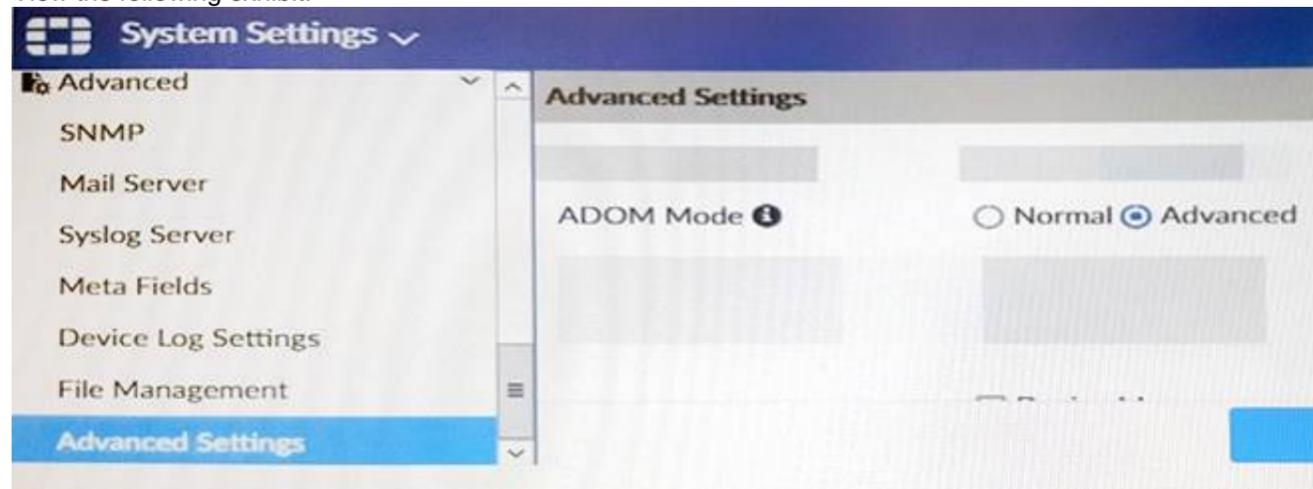
- A. When FortiManager is auto-updated with configuration changes made directly on a managed device
- B. When changes to the device-level database are made on FortiManager
- C. When FortiManager installs device-level changes on a managed device
- D. When a configuration revision is reverted to a previous revision in the revision history

Answer: BC

NEW QUESTION 44

- (Topic 3)

View the following exhibit.



Which of the following statements are true based on this configuration setting? (Choose two.)

- A. This setting will enable the ADOMs feature on FortiManager.
- B. This setting is applied globally to all ADOMs.
- C. This setting will allow assigning different VDOMs from the same FortiGate to different ADOMs.
- D. This setting will allow automatic updates to the policy package configuration for a managed device.

Answer: BC

NEW QUESTION 47

- (Topic 3)

In the event that one of the secondary FortiManager devices fails, which action must be performed to return the FortiManager HA manual mode to a working state?

- A. The FortiManager HA state transition is transparent to administrators and does not require any reconfiguration.
- B. Manually promote one of the working secondary devices to the primary role, and reboot the old primary device to remove the peer IP of the failed device.
- C. Reconfigure the primary device to remove the peer IP of the failed device.
- D. Reboot the failed device to remove its IP from the primary device.

Answer: C

NEW QUESTION 52

- (Topic 3)

In addition to the default ADOMs, an administrator has created a new ADOM named Training for FortiGate devices. The administrator authorized the FortiGate device on FortiManager using the Fortinet Security Fabric.

Given the administrator's actions, which statement correctly describes the expected result?

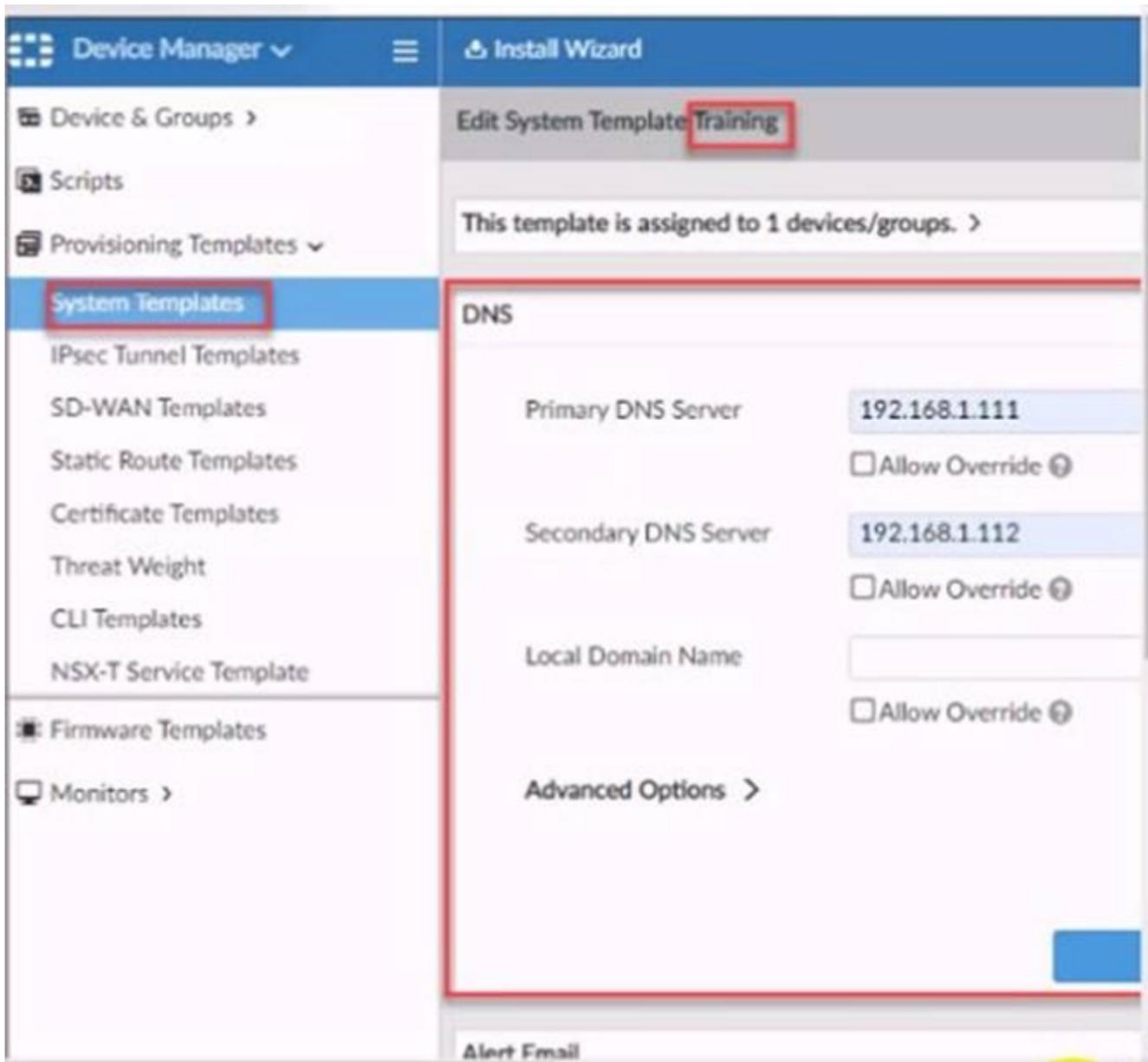
- A. The FortiManager administrator must add the authorized device to the Training ADOM using the Add Device wizard only.
- B. The authorized FortiGate will be automatically added to the Training ADOM.
- C. The authorized FortiGate will appear in the root ADOM.
- D. The authorized FortiGate can be added to the Training ADOM using FortiGate Fabric Connectors.

Answer: C

NEW QUESTION 57

- (Topic 3)

Refer to the exhibit.



According to the error message why is FortiManager failing to add the FortiAnalyzer device?

- A. The administrator must turn off the Use Legacy Device login and add the FortiAnalyzer device to the same network as Forti-Manager
- B. The administrator must select the Forti-Manager administrative access checkbox on the FortiAnalyzer management interface
- C. The administrator must use the Add Model Device section and discover the FortiAnalyzer device
- D. The administrator must use the correct user name and password of the FortiAnalyzer device

Answer: A

NEW QUESTION 60

- (Topic 3)
Refer to the exhibit.

```
Request
POST http://localhost:8080/fpc/api/customers/1/policytabs

Headers
accept: application/json
content-type: application/json
fpc-sid: $FPCSID
Cookie: JSESSIONID=$FPCSID

Payload
{
  "centralNat": true,
  "interfacePolicy6": false,
  "dosPolicy6": false,
  "policy64": false,
  "interfacePolicy": true,
  "policy6": false,
  "dosPolicy": false,
  "policy46": false,
  "id": 1,
  "customerId": 1
}

Response
Status 200 OK
```

Which statement is true about the FortiManager ADOM policy tab based on the API request?

- A. The API command has enabled both central NAT and interface policy on the policy tab.
- B. The API command has requested the policy tab permissions information only.
- C. The API command has failed when requesting policy tab permissions information.
- D. The API command has applied to customer with ID: 200.

Answer: A

NEW QUESTION 62

- (Topic 3)

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

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

Answer: B

NEW QUESTION 64

.....

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 NSE5_FMG-7.2 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE5_FMG-7.2-dumps.html