

Fortinet

Exam Questions NSE5_FMG-7.0

Fortinet NSE 5 - FortiManager 7.0



NEW QUESTION 1

- (Topic 1)

View the following exhibit, which shows the Download Import Report:

```
Start to import config from devices(Remote-FortiGate) vdom (root)to adom (MyADOM),  
  
Package(Remote-FortiGate)  
  
"firewall address", SUCCESS,"(name=REMOTE_SUBNET,oid=580, new object)"  
  
"firewall policy",SUCCESS,"(name=1, oid=990,new object)"  
  
"firewall policy",FAIL,"(name=ID:2(#2), oid=991, reason=interface(interface binding  
Contradiction.detail:any<-port6)binding fail)"
```

Why it is failing to import firewall policy ID 2?

- A. The address object used in policy ID 2 already exist in ADON database with any as interface association and conflicts with address object interface association locally on the FortiGate
- B. Policy ID 2 is configured from interface any to port6 FortiManager rejects to import this policy because any interface does not exist on FortiManager
- C. Policy ID 2 does not have ADOM Interface mapping configured on FortiManager
- D. Policy ID 2 for this managed FortiGate already exists on FortiManager in policy package named Remote-FortiGate.

Answer: A

Explanation:

FortiManager_6.4_Study_Guide-Online – page 331 & 332

NEW QUESTION 2

- (Topic 1)

An administrator run the reload failure command: diagnose test deploymanager reload config <deviceid> on FortiManager. What does this command do?

- A. It downloads the latest configuration from the specified FortiGate and performs a reload operation on the device database.
- B. It installs the latest configuration on the specified FortiGate and update the revision history database.
- C. It compares and provides differences in configuration on FortiManager with the current runningconfiguration of the specified FortiGate.
- D. It installs the provisioning template configuration on the specified FortiGate.

Answer: A

Explanation:

Reference: <https://community.fortinet.com/t5/FortiManager/Technical-Note-Retrieve-configuration-file-using-CLI-from-a/ta-p/191000?externalID=FD36387>

NEW QUESTION 3

- (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 4

- (Topic 1)

An administrator with the Super_User profile is unable to log in to FortiManager because of an authentication failure message. Which troubleshooting step should you take to resolve the issue?

- A. Make sure FortiManager Access is enabled in the administrator profile
- B. Make sure Offline Mode is disabled
- C. Make sure the administrator IP address is part of the trusted hosts.
- D. Make sure ADOMs are enabled and the administrator has access to the Global ADOM

Answer: C

Explanation:

Even if a user entered the correct userid/password, the FMG denies access if a user is logging in from an untrusted source IP subnets.

Reference: <https://docs.fortinet.com/document/fortimanager/6.0.3/administration-guide/107347/trusted-hosts>

NEW QUESTION 5

- (Topic 2)

An administrator is replacing a device on FortiManager by running the following command: execute device replace sn <devname> <serialnum>.

What device name and serial number must the administrator use?

- A. Device name and serial number of the original device.
- B. Device name and serial number of the replacement device.
- C. Device name of the replacement device and serial number of the original device.
- D. Device name of the original device and serial number of the replacement device.

Answer: D

NEW QUESTION 6

- (Topic 2)

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

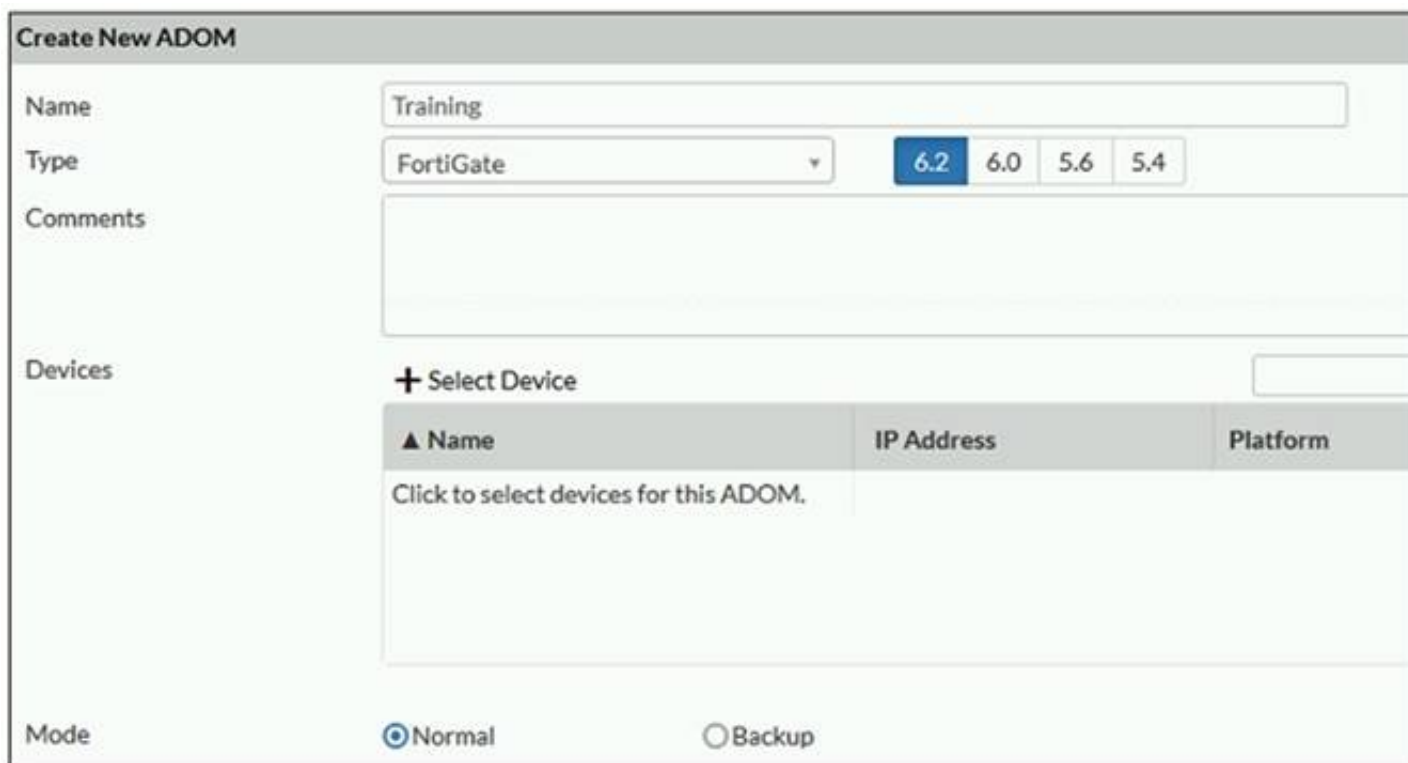
- A. FortiGate devices in HA cluster devices are counted as a single device.
- B. FortiGate in transparent mode configurations are not counted toward the device count on FortiManager.
- C. FortiGate devices in an HA cluster that has five VDOMs are counted as five separate devices.
- D. The maximum number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

Answer: AC

NEW QUESTION 7

- (Topic 2)

Refer to the exhibit.



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 8

- (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 9

- (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 as Super_User in 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 10

- (Topic 2)

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

- A. The Security Fabric license, group name and password are required for the FortiManager Security Fabric integration
- B. The Fabric View module enables you to generate the Security Fabric ratings for Security Fabric devices
- C. The Security Fabric settings are part of the device level settings
- D. The Fabric View module enables you to view the Security Fabric ratings for Security Fabric devices

Answer: CD

NEW QUESTION 10

- (Topic 2)

Refer to the exhibit.



An administrator logs into the FortiManager GUI and sees the panes shown in the exhibit. Which two reasons can explain why the FortiAnalyzer feature panes do not appear? (Choose two.)

- A. The administrator logged in using the unsecure protocol HTTP, so the view is restricted.
- B. The administrator profile does not have full access privileges like the Super_User profile.
- C. The administrator IP address is not a part of the trusted hosts configured on FortiManager interfaces.
- D. FortiAnalyzer features are not enabled on FortiManager.

Answer: BD

NEW QUESTION 13

- (Topic 3)

View the following exhibit.

Edit Address

Address Name

Training

Type

IP/Netmask

IP/Network

192.168.1.0/255.255.255.255.0

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"/>	Local-FortiGate	root	IP/Netmask10.0.10/255.255.255.0

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

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

Answer: A

NEW QUESTION 16

- (Topic 3)

What does a policy package status of Modified indicate?

- A. FortiManager is unable to determine the policy package status
- B. The policy package was never imported after a device was registered on FortiManager
- C. The Policy configuration has been changed on a managed device and changes have not yet been imported into FortiManager
- D. The Policy package configuration has been changed on FortiManager and changes have not yet been installed on the managed device.

Answer: D

Explanation:

Reference: http://help.fortinet.com/fmgr/50hlp/56/5-6-1/FortiManager_Admin_Guide/1200_Policy%20and%20Objects/0800_Managing%20policy%20packages/2200_Policy%20Package%20Installation%20targets.htm

NEW QUESTION 18

- (Topic 3)

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

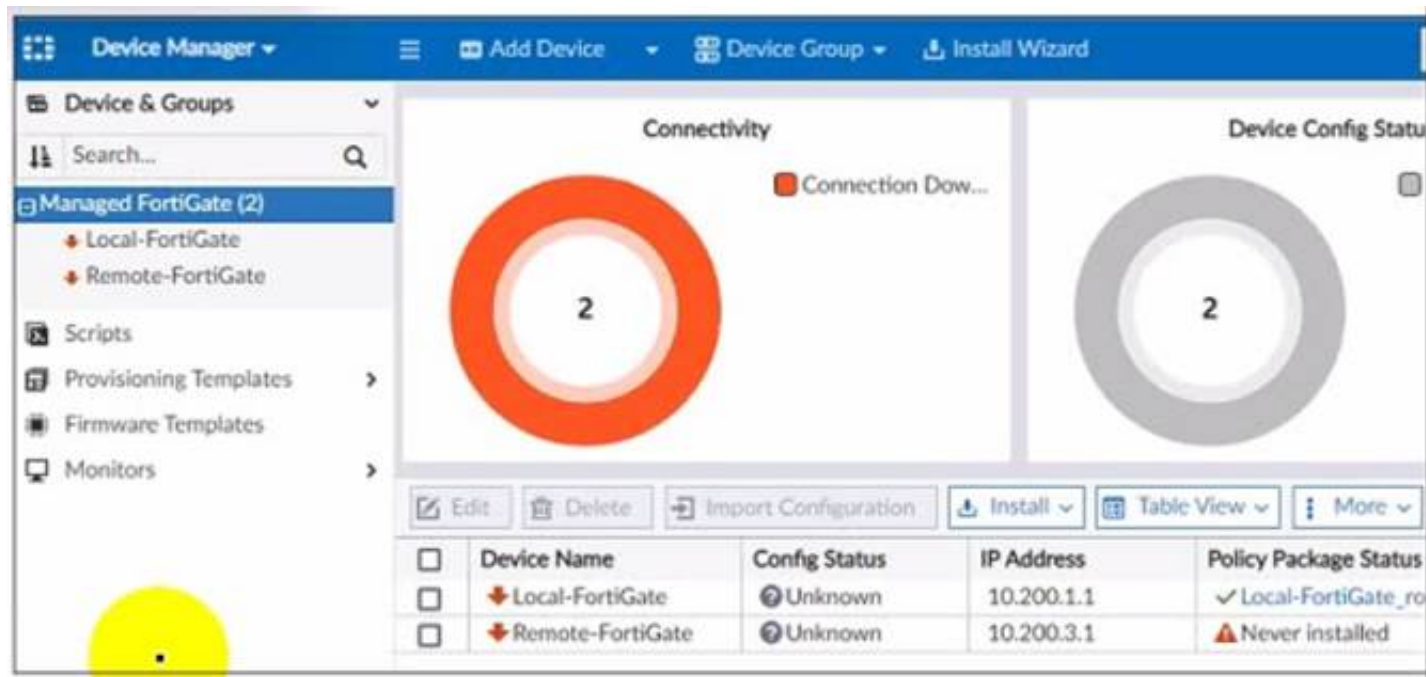
- A. NSX-T Service Template
- B. Security profiles
- C. SNMP
- D. Routing

Answer: D

NEW QUESTION 22

- (Topic 3)

Refer to the exhibit.



A junior administrator is troubleshooting a FortiManager connectivity issue that is occurring with managed FortiGate devices. Given the FortiManager device manager settings shown in the exhibit, what can you conclude from the exhibit?

- A. The administrator had restored the FortiManager configuration file
- B. The administrator must refresh both devices to restore connectivity
- C. FortiManager test internet connectivity therefore, both devices appear to be down
- D. The administrator can reclaim the FGFM tunnel to get both devices online

Answer: C

NEW QUESTION 26

- (Topic 3)

Which of the following statements are true regarding schedule backup of FortiManager? (Choose two.)

- A. Backs up all devices and the FortiGuard database.
- B. Does not back up firmware images saved on FortiManager
- C. Supports FTP, SCP, and SFTP
- D. Can be configured from the CLI and GUI

Answer: BC

NEW QUESTION 29

- (Topic 3)

Push updates are failing on a FortiGate device that is located behind a NAT device. Which two settings should the administrator check? (Choose two.)

- A. That the virtual IP address and correct ports are set on the NAT device
- B. That the NAT device IP address and correct ports are configured on FortiManager
- C. That the external IP address on the NAT device is set to DHCP and configured with the virtual IP
- D. That the override server IP address is set on FortiManager and the NAT device

Answer: BC

NEW QUESTION 33

.....

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

NSE5_FMG-7.0 Practice Exam Features:

- * NSE5_FMG-7.0 Questions and Answers Updated Frequently
- * NSE5_FMG-7.0 Practice Questions Verified by Expert Senior Certified Staff
- * NSE5_FMG-7.0 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * NSE5_FMG-7.0 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE5_FMG-7.0 Practice Test Here](#)