

Practice Exam Questions

FORTINET



Fortinet NSE 5 - FortiManager 7.0



EXAMKILLER

Help Pass Your Exam At First Try

Fortinet

Exam NSE5_FMG-7.0

Fortinet NSE 5 - FortiManager 7.0

Version: 4.0

[Total Questions: 72]

Topic break down

Topic	No. of Questions
Topic 1: Main Questions Pool A	33
Topic 2: Main Questions Pool B	17
Topic 3: Main Questions Pool C	22

Topic 1, Main Questions Pool A

Question No : 1 - (Topic 1)

You are moving managed FortiGate devices from one ADOM to a new ADOM.

Which statement correctly describes the expected result?

- A. Any pending device settings will be installed automatically
- B. Any unused objects from a previous ADOM are moved to the new ADOM automatically
- C. The shared policy package will not be moved to the new ADOM
- D. Policy packages will be imported into the new ADOM automatically

Answer: C

Reference: <https://community.fortinet.com/t5/FortiManager/Technical-Note-How-to-move-objects-to-new-ADOM-on-FortiManager/ta-p/198342>

Question No : 2 - (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: C,D

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

Question No : 3 - (Topic 1)

Refer to the exhibit.

Start to import config from device(Local-FortiGate) vdom(root) to
 adom(My_ADOM), package(Local-FortiGate_root)

"firewall service category",SKIPPED,"(name=General, oid=697, DUPLICATE)"

"firewall address",SUCCESS,"(name=LOCAL_SUBNET, oid=684, new object)"

"firewall service custom",SUCCESS,"(name=ALL, oid=863, update previous
 object)"

"firewall policy",SUCCESS,"(name=1, oid = 1090, new object)"

Which statement about the object named ALL is true?

- A. FortiManager updated the object ALL using the FortiGate value in its database.
- B. FortiManager installed the object ALL with the updated value.
- C. FortiManager created the object ALL as a unique entity in its database, which can be only used by this managed FortiGate.
- D. FortiManager updated the object ALL using the FortiManager value in its database.

Answer: A

Question No : 4 - (Topic 1)

An administrator, Trainer, who is assigned the Super_User profile, is trying to approve a workflow session that was submitted by another administrator, Student. However, Trainer is unable to approve the workflow session.

What can prevent an admin account that has Super_User rights over the device from approving a workflow session?

Session List

View Diff					
<input type="checkbox"/>	ID	Name	User	Date Submitt...	Approved/To... Comments
<input checked="" type="checkbox"/>	1	Firewall p..	Student	2017-06-01...	0/1 firewall policies

+ Add Comment

[Student] - 2017-06-01
 13:31:35
 firewall policies
 [Student] - 2017-06-01
 16:29:27

- A. Trainer is not a part of workflow approval group
- B. Trainer does not have full rights over this ADOM

- C. Trainer must close Student's workflow session before approving the request
 D. Student, who submitted the workflow session, must first self-approve the request

Answer: A

Reference: https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMG-FAZ/0800_ADOMs/1800_Workflow/0600_Workflow%20sessions.htm

Question No : 5 - (Topic 1)

View the following exhibit.

The screenshot displays the Fortinet FortiManager interface. The top navigation bar includes 'Device Manager', 'Device & Groups', 'Firmware', and 'License'. The 'Device Manager' tab is active, showing a list of devices under 'Managed FortiGate'. The list includes 'Local-FortiGate', 'Remote-FortiGate', 'root [NAT] (Management)', 'Student[NAT]', and 'Trainer [NAT]'. A red box labeled 'Managed FortiGate devices' highlights this list.

The bottom section shows the 'Policy Packages' configuration. The 'Install' tab is active, displaying a table of installation targets. The table has columns: 'Seq.#', 'Install On', 'Name', 'From', and 'To'. The 'Install On' column shows the target devices for each policy package. A red box labeled 'Installation targets' highlights the table.

Seq.#	Install On	Name	From	To
1	Remote-FortiGate(Student) Local-FortiGate(root)	Ping_Access	port3	port1
2	Remote-FortiGate(Student)	Web	port3	port1
3	Installation Targets	Source_Device	port3	port1

A red box labeled 'Policy Package' highlights the table.

Given the configurations shown in the exhibit, what can you conclude from the installation targets in the **Install On** column?

- A. The Install On column value represents successful installation on the managed devices
 B. Policy seq#3 will be installed on all managed devices and VDOMs that are listed under Installation Targets
 C. Policy seq#3 will be installed on the Trainer[NAT] VDOM only
 D. Policy seq#3 will be not installed on any managed device

Answer: B

Question No : 6 - (Topic 1)

Which two settings must be configured for SD-WAN Central Management? (Choose two.)

- A. SD-WAN must be enabled on per-ADOM basis
- B. You can create multiple SD-WAN interfaces per VDOM
- C. When you configure an SD-WAN, you must specify at least two member interfaces.
- D. The first step in creating an SD-WAN using FortiManager is to create two SD-WAN firewall policies.

Answer: A,C

Question No : 7 - (Topic 1)

View the following exhibit.

Import Device - Local-FortiGate [root]

Create a new policy package for import.

Policy Package Name	<input type="text" value="Local-FortiGate"/>
Folder	<input type="text" value="root"/>
Policy Selection	<input checked="" type="radio"/> Import All(3) <input type="radio"/> Select Policies and Profile Groups to Import
Object Selection	<input type="radio"/> Import only policy dependent objects <input checked="" type="radio"/> 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

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

Question No : 8 - (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>

Question No : 9 - (Topic 1)

View the following exhibit.

Starting Log (Run the device)**Start installing****Local-FortiGate \$ config user device****Local-FortiGate (device) \$ edit "mydevice"****new entry 'mydevice' added****Local-FortiGate (mydevice) \$ next****MAC address can not be 0****Node_check_object fail!for mac 00:00:00:00:00:00****Attribute 'mac' value '00:00:00:00:00:00' checkingfail -33****Command fail. Return code 1****Local-FortiGate (device) \$ end****...****Local-FortiGate \$ config firewall policy****Local-FortiGate (policy) \$ edit 2****New entry '2' added****Local-FortiGate (2) \$ set name "Device_policy"****Local-FortiGate (2) \$ set uuid 64...****Local-FortiGate (2) \$ set srcintf "port3"****Local-FortiGate (2) \$ set dstintf "port1"****Local-FortiGate (2) \$ set srcaddr "all"****Local-FortiGate (2) \$ set dstaddr "all"****Local-FortiGate (2) \$ set action accept****Local-FortiGate (2) \$ set schedule "always"****Local-FortiGate (2) \$ set service "ALL"****Local-FortiGate (2) \$ set devices "mydevice"****Entry not found in datasource****Value parse error before 'mydevice'****Command fail. Return code -3****Local-FortiGate (2) \$ set nat enable****Local-FortiGate (2) \$ next****Local-FortiGate (policy) \$ end****...**

Which statement is true regarding this failed installation log?

- A. Policy ID 2 is installed without a source address
- B. Policy ID 2 will not be installed
- C. Policy ID 2 is installed in disabled state
- D. Policy ID 2 is installed without a source device

Answer: D

Question No : 10 - (Topic 1)

An administrator wants to delete an address object that is currently referenced in a firewall policy.

What can the administrator expect to happen?

- A. FortiManager will not allow the administrator to delete a referenced address object
- B. FortiManager will disable the status of the referenced firewall policy
- C. FortiManager will replace the deleted address object with the **none** address object in the referenced firewall policy
- D. FortiManager will replace the deleted address object with **all** address object in the referenced firewall policy

Answer: C

Reference: https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FortiManager_Admin_Guide/1200_Policy%20and%20Objects/1200_Managing%20objects/0800_Remove%20an%20object.htm

Question No : 11 - (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: B,C

Reference: [https://help.fortinet.com/fmgr/50hlp/56/5-6-](https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FortiManager_Admin_Guide/1200_Policy%20and%20Objects/1200_Managing%20objects/0800_Remove%20an%20object.htm)