Exam Questions NSE5_FMG-7.0

Fortinet NSE 5 - FortiManager 7.0

https://www.2passeasy.com/dumps/NSE5_FMG-7.0/

NEW QUESTION 1
- (Exam 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-WANtemplate 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-reference

NEW QUESTION 2
- (Exam Topic 1)
Refer to the exhibit.

```
FortiManager # diagnose dvm device list
--- There are currently 1 devices/vdoms managed ---

TYPE            OID    SN      HA    IP             NAME            ADOM      IPS              FIRMWARE
fmg/faz enabled 157    FGVM01.. -    10.200.1.1     Local-FortiGate My_ADOM   14.00641 (regular) 6.0 MR2 (866)
                |- STATUS: dev-db: modified; conf: in sync; cond: pending; dm: retrieved; conn: up

                |- vdom:[3]root flags:0 adom:My_ADOM pkg:[imported]Local-FortiGate
```

Which two statements about the output are true? (Choose two.)

A. The latest revision history for the managed FortiGate does match with the FortiGate running configuration
B. Configuration changes have been installed to FortiGate and represents FortiGate configuration has been changed
C. The latest history for the managed FortiGate does not match with the device-level database
D. Configuration changes directly made on the FortiGate have been automatically updated to device-leveldatabase

Answer: AC

Explanation:
STATUS: dev-db: modified; conf: in sync; cond: pending; dm: retrieved; conn: up– dev-db: modified –
This is the device setting status which indicates that configuration changes were made on FortiManager.
– conf: in sync – This is the sync status which shows that the latest revision history is in sync with Fortigate's configuration.– cond: pending – This is the configuration status which says that configuration changes need to be installed.
Most probably a retrieve was done in the past (dm: retrieved) updating the revision history DB (conf: in sync) and FortiManager device level DB, now there is a new modification on FortiManager device level DB (dev-db: modified) which wasn't installed to FortiGate (cond: pending), hence; revision history DB is not aware of that modification and doesn't match device DB.
Conclusion:– Revision DB does match FortiGate.– No changes were installed to FortiGate yet.– Device DB doesn't match Revision DB.– No changes were done on FortiGate (auto-update) but configuration was retrieved instead
After an Auto-Update or Retrieve:device database = latest revision = FGT
Then after a manual change on FMG end (but no install yet):latest revision = FGT (still) but now device database has been modified (is different).
After reverting to a previous revision in revision history:device database = reverted revision != FGT

NEW QUESTION 3
- (Exam 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

NEW QUESTION 4
- (Exam 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 5
- (Exam 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 6
- (Exam 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

	ID	Name	User	Date Submitt...	Approved/To...	Comments
☑	1	Firewall p..	Student	2017-06-01...	0/1	firewall policies

View Diff

+ 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

Explanation:
Reference:

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

NEW QUESTION 7
- (Exam 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
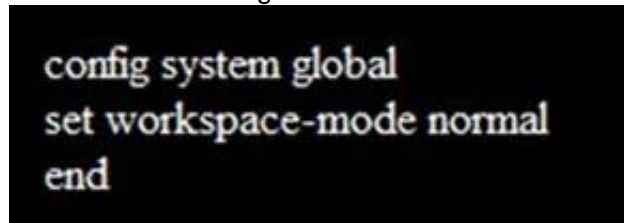
Answer: A

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 8
- (Exam Topic 1)
Refer to the following exhibit:


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

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

A. The same administrator can lock more than one ADOM at the same time
B. Ungraceful closed sessions will keep the ADOM in a locked state until the administrator session times out
C. Unlocking an ADOM will submit configuration changes automatically to the approval administrator
D. Unlocking an ADOM will install configuration automatically on managed devices

Answer: AB

Explanation:
Reference: http://help.fortinet.com/fmgr/cli/5-6-2/Document/0800_AD0Ms/200_Configuring+.htm

NEW QUESTION 9
- (Exam 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 referencedfirewall policy
D. FortiManager will replace the deleted address object with all address object in the referenced firewall policy

Answer: C

Explanation:
Reference:
https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FortiManager_Admin_Guide/1200_Policy%20and%20Objects/12

NEW QUESTION 10
- (Exam 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 10
- (Exam 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 12
- (Exam Topic 2)
Refer to the exhibit.

```
config system dm
set rollback-allow-reboot enable
end
```

An administrator has configured the command shown in the exhibit on FortiManager. A configuration change has been installed from FortiManager to the managed FortiGate that causes the FGFM tunnel to go down for more than 15 minutes.
What is the purpose of this command?

A. It allows FortiGate to unset central management settings.
B. It allows FortiGate to reboot and recover the previous configuration from its configuration file.
C. It allows the FortiManager to revert and install a previous configuration revision on the managed FortiGate.
D. It allows FortiGate to reboot and restore a previously working firmware image.

Answer: B

Explanation:
Reference:
https://docs.fortinet.com/document/fortimanager/6.2.0/fortigate-fortimanager-communicationsprotocol-guide/14

NEW QUESTION 17
- (Exam 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 18
- (Exam Topic 3)
An administrator has added all the devices in a Security Fabric group to FortiManager. How does the administrator identify the root FortiGate?

A. By a dollar symbol ($) at the end of the device name
B. By an at symbol (@) at the end of the device name
C. By a QUESTION NO: mark(?) at the end of the device name
D. By an Asterisk (*) at the end of the device name

Answer: D

NEW QUESTION 23
- (Exam Topic 3)
Which of the following statements are true regarding VPN Manager? (Choose three.)

A. VPN Manager must be enabled on a per ADOM basis.
B. VPN Manager automatically adds newly-registered devices to a VPN community.
C. VPN Manager can install common IPsec VPN settings on multiple FortiGate devices at the same time.
D. Common IPsec settings need to be configured only once in a VPN Community for all managed gateways.
E. VPN Manager automatically creates all the necessary firewall policies for traffic to be tunneled by IPsec.

Answer: ACD

NEW QUESTION 26
- (Exam 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%20Packag

NEW QUESTION 30
- (Exam 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 33
- (Exam Topic 3)
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)"
```

Given the configuration shown in the exhibit, how did FortiManager handle the service category named General?

A. FortiManager ignored the firewall service category General but created a new service category in its database.
B. FortiManager ignored the firewall service category general and deleted the duplicate value In Its database
C. FortiManager ignored the firewall service category General and updated the FortiGate duplicate value in the FortiGate database.
D. FortiManager ignored the firewall service category General and did not update Its database with the value

Answer: C

NEW QUESTION 38
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE5_FMG-7.0 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE5_FMG-7.0 Product From:

https://www.2passeasy.com/dumps/NSE5_FMG-7.0/

Money Back Guarantee

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 FirstTry

* NSE5_FMG-7.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year