



Fortinet

Exam Questions FCP_FMG_AD-7.6

FCP - FortiManager 7.6 Administrator

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

Refer to the exhibits.

Diagnose output

```
FortiManager # get system status
Platform Type           : FMG-VM64-KVM
Platform Full Name      : FortiManager-VM64-KVM
Version                 : v7.6.1-build3344 241023 (GA.M)
Serial Number           : FMG-VMTM24012945
BIOS version            : 04000002
```

Diagnose output

```
FortiManager # diagnose dvm device list
--- There are currently 5 devices/vdoms managed ---
--- There are currently 5 devices/vdoms count for license ---
```

TYPE	OID	SN	HA	IP	NAME	ADOM	IPS	FIRMWARE
fmgfaz-managed	230	FGVM02TM24013423	-	10.0.13.254	FGVM02TM24013423	root	7.0 MR6 (3401)	N/A
- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; conn: up								
- vdom:[3]root flags:0 adom:root pkg:[never-installed]								
unregistered	167	FGVM02TM24013501	-	192.168.1.3	FGVM02TM24013501	root	7.0 MR6 (3401)	N/A
- STATUS: dev-db: unknown; conf: out of sync; cond: unregistered; dm: none; conn: unknown								
- vdom:[3]root flags:0 adom:root pkg:[never-installed]								
unregistered	209	FGVM02TM24013502	-	192.168.1.101	FGVM02TM24013502	root	7.0 MR6 (3401)	N/A
- STATUS: dev-db: unknown; conf: out of sync; cond: unregistered; dm: none; conn: unknown								
- vdom:[3]root flags:0 adom:root pkg:[never-installed]								
unregistered	188	FGVM02TM24013504	-	192.168.1.111	FGVM02TM24013504	root	7.0 MR6 (3401)	N/A
- STATUS: dev-db: unknown; conf: out of sync; cond: unregistered; dm: none; conn: unknown								
- vdom:[3]root flags:0 adom:root pkg:[never-installed]								
fmgfaz-model	262	-	-	-	HQ-NGFW	My_ADOM	7.0 MR6 (3401)	N/A
- STATUS: dev-db: unknown; conf: unknown; cond: unknown; dm: unknown; conn: unknown								
- vdom:[3]root flags:0 adom:My_ADOM pkg:[never-installed]								

```
FortiManager # diagnose test deploymanager reloadconf 262
Retrieving configuration file from FGT...
Error: Configuration file import error.
```

An administrator runs the reload failure command `diagnose test deploymanager reloadconf 262` on FortiManager. Why does the administrator receive an error message?

- A. The administrator must use the FortiGate name instead of the ID number.
- B. The administrator just recently added FortiGate HQ-NGFW as a model device.
- C. FortiManager requires the FortiGate serial number instead of the ID number.
- D. FortiManager does not support FortiOS version 7.0.

Answer: B

Explanation:

The error occurs because the FortiGate HQ-NGFW device with ID 262 is a newly added model device and has not yet been fully synchronized or installed with a configuration package, which causes the reload configuration command to fail.

NEW QUESTION 2

Refer to the exhibit.

```
FortiManager # diagnose dvm device list
--- There are currently 6 devices/vdoms managed ---
--- There are currently 6 devices/vdoms count for license ---
```

TYPE	OID	SN	HA	IP	NAME	ADOM	IPS	FIRMWARE	HW_GenX
fmgfaz-managed	188	FGVM02TM24013504	-	100.65.1.111	BR1-FGT-1	My_ADOM	7.0 MR6 (3401)	N/A	
- STATUS: dev-db: not modified; conf: in sync; cond: pending; dm: installed; conn: up; template:[modified]default									
- vdom:[3]root flags:0 adom:My_ADOM pkg:[imported]BR1-FGT-1									

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

- A. The latest revision history for the managed FortiGate does not match the device-level database.
- B. Configuration changes have been installed on FortiGate, updating policy and device-level database.
- C. The latest revision history for the managed FortiGate does match the FortiManager policy database.
- D. The system template default will override device-level database configurations.

Answer: AD

Explanation:

The status "pending" indicates the latest revision history does not match the device-level database, meaning there are unapplied changes. The template is marked as [modified], so the system template default will override device-level database configurations when installed.

NEW QUESTION 3

Refer to the exhibit.

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

"firewall address",SKIPPED,"(name=all, oid=2309, DUPLICATE)"

"firewall address",FAIL,"(name=REMOTE_SUBNET, oid=2311,
reason=interface((firewall address:REMOTE_SUBNET) any<-port6) binding
fail)"

"firewall policy",FAIL,"(name=1, oid=3070, reason=interface(interface binding
contradiction. detail: (firewall address:REMOTE_SUBNET) any<-port6) binding
fail)"
```

What can you conclude from the downloaded import report?

- A. FortiManager does not support per-device mapping for firewall addresses.
- B. The administrator will see a new policy package named Remote-FortiGate_root in the FortiManager ADOM database.
- C. FortiManager will change the configuration of REMOTE_SUBNET to match the interface mapping coming in from Remote-FortiGate.
- D. As a result of this policy import process, FortiManager will create a new firewall address called REMOTE_SUBNET in the ADOM database.

Answer: B

Explanation:

The import report shows that a new policy package named Remote-FortiGate_root will be created in the FortiManager ADOM database, but some firewall addresses and policies failed to import due to interface binding conflicts.

NEW QUESTION 4

Refer to the exhibit.

FortiManager cluster settings

FortiManager

Dashboard

Device Manager

Policy & Objects

VPN Manager

AP Manager

FortiSwitch Manager

Extender Manager

FortiView

Log View

Fabric View

Incidents & Events

Reports

FortiGuard

System Settings

ADOMs

Administrators

Admin Profiles

Remote Authentication Server

SAML SSO

Settings

HA

Network

Cluster Settings

Fallover 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

(1-64)

Group Password

File Quota

4096

MB (2048-20480)

Heart Beat Interval

10

Seconds

Fallover Threshold

30

(1-255)

VIP

10.0.1.245

VRRP Interface

port2

Priority

1

(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

While attempting to push a NetFlow configuration script through the FortiManager policy package: an administrator encounters an error stating that an object is unrecognized in line 4.

```
Starting log (Run on database)
config vdom
edit AGEUSR
[line 4] > config sys interface [parameter(s) invalid. detail: object unrecognized]
Failed to commit to DB, reason([line 4] > config sys interface [parameter(s) invalid. detail: object unrecognized])

Running script(NetFlow_Configuration) on DB failed
```

What must the administrator do to successfully apply the NetFlow configuration script and avoid the object unrecognized error?

- A. Make sure the user running the script has full access to the VDOM—AGEUSR.
- B. Run the script on the device database.
- C. Use metadata variables if they use VDOMs in the script.
- D. Create a normalized interface on the policy layer before running the script.

Answer: C

Explanation:

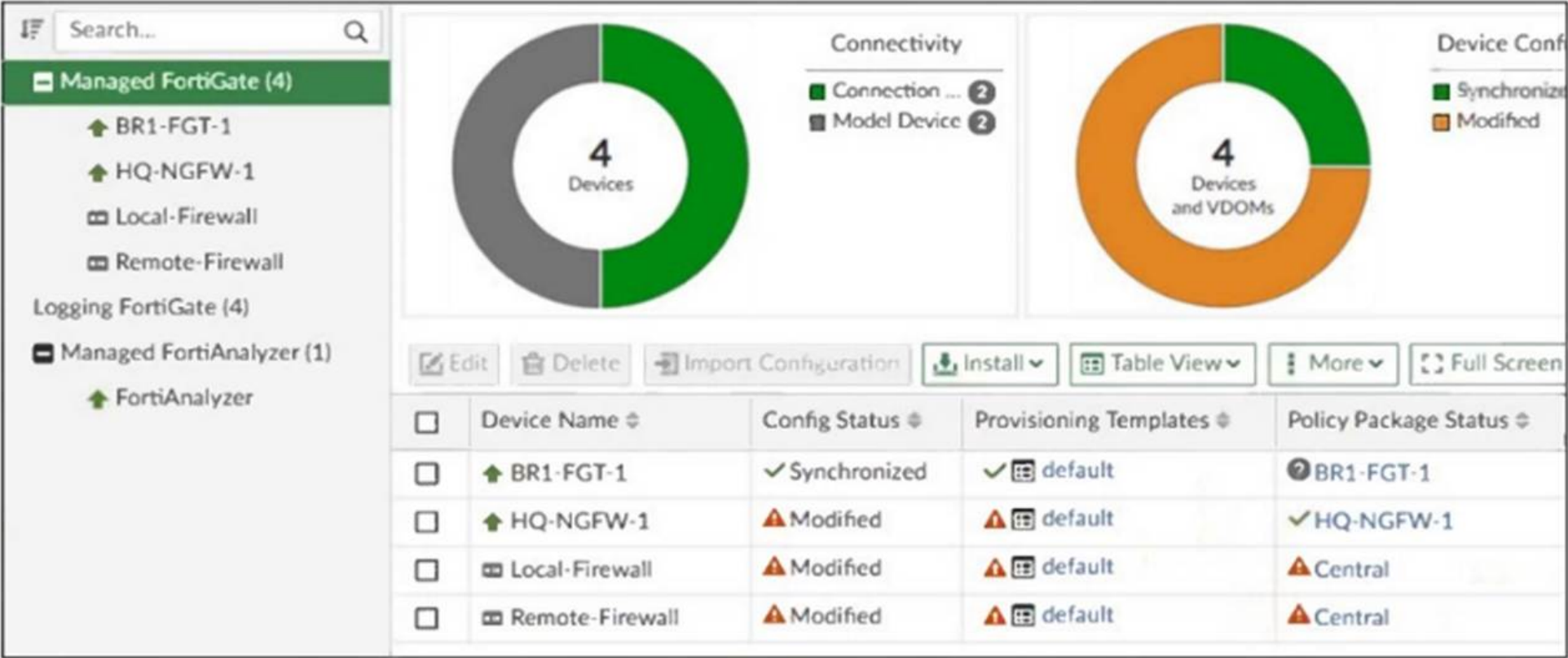
When using scripts that reference VDOM-specific objects, such as interfaces, in FortiManager, metadata variables must be used to correctly map those objects per

VDOM. This prevents "object unrecognized" errors during script execution.

NEW QUESTION 6

Refer to the exhibits.

FortiManager device database



Installation Targets Central policy package

BR1-FGT-1	Installation Target	Config Status	Policy Package Status
Central	BR1-FGT-1	Synchronized	BR1-FGT-1
Firewall Policy	Local-Firewall	Unknown	Central
Installation Targets	Remote-Firewall	Unknown	Central
HQ-NGFW-1			
default			

An administrator has been asked to install the same policies from a central policy package onto the BR1-FGT- 1 firewall. The administrator added BR1-FGT-1 as a target in the central policy package installation. What should the administrator do when reinstalling the central policy package on the BR1-FGT-1 firewall?

- A. Assign only one policy package to the firewall because FortiManager does not allow more than one policy package assigned per device at the same time.
- B. Import the policy package to change the unknown status and synchronize the policy package.
- C. Use the install wizard to install the central policy package on the BR1-FGT-1 firewall.
- D. First resolve the modified status in the configuration and provisioning templates to allow a smooth installation.

Answer: C

Explanation:

Using the Install Wizard is the recommended method to reinstall the central policy package on the BR1-FGT- 1 firewall, ensuring all settings, installation targets, and dependencies are correctly processed during installation.

NEW QUESTION 7

Push updates are failing on a FortiGate device located behind a network address translation (NAT) device? Which two settings should the administrator check to correct this problem? (Choose two.)

- A. Make sure the NAT device IP address and the correct ports are configured on FortiManager.
- B. Make sure FortiGuard updates and web service are enabled on the FortiGuard service interface.
- C. Make sure the virtual IP address and the correct ports are configured on the NAT device.
- D. Make sure the Bind to IP address option on the FortiGuard service interface is set to the virtual IP address from the NAT device.

Answer: AC

Explanation:

FortiManager must have the NAT device's IP address and correct ports configured to communicate properly with the FortiGate behind NAT. The NAT device must have the correct virtual IP address and ports configured to allow push updates to reach the FortiGate device.

NEW QUESTION 8

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

- A. When FortiManager installs device-level changes on a managed device

- B. When changes to the device-level database are made on FortiManager
- C. When FortiManager is auto-updated with configuration changes made directly on a managed device
- D. When a provisioning template is assigned to a managed device on the device-level database

Answer: BC

Explanation:

FortiManager creates a new revision history entry whenever changes are made to the device-level database on FortiManager.
FortiManager also creates a new revision when it auto-updates its database with configuration changes detected directly on a managed device.

NEW QUESTION 9

Refer to the exhibits.

Device Revision Diff wizard

Device Revision Diff

Revision ID: 11

Total

12696

Deleted

0

Modified

0

Revision ID: 9

Total

12704

Added

8

Modified

0

8500

(...)

end

8501

config user group

(...)

12154

set service "ALL"

12155

set comments "test"

(...)

8500

(...)

end

8501

config user local

8502

edit "Support"

8503

set type password

8504

set two-factor email

8505

set email-to "support@mail.com"

8506

next

8507

end

8508

config user group

(...)

12161

set service "ALL"

12162

set users "Support"

12163

set comments "test"

(...)

Save Diff as Script

Show Full Diff

Cancel

An administrator needed to recover all the configurations related to the user, Support. The configurations were saved in configuration revision ID 9. The administrator reverted the configuration using the Configuration Revision History window and received the CLI output shown in the exhibit. What can you conclude from the CLI output?

- A. The administrator set the flag to 0 to prevent configuration overrides.
- B. The administrator reinstalled the policy package.
- C. The administrator needs to retrieve the device to correctly detect the FortiGate firmware version.
- D. The administrator installed only the device-level configuration.

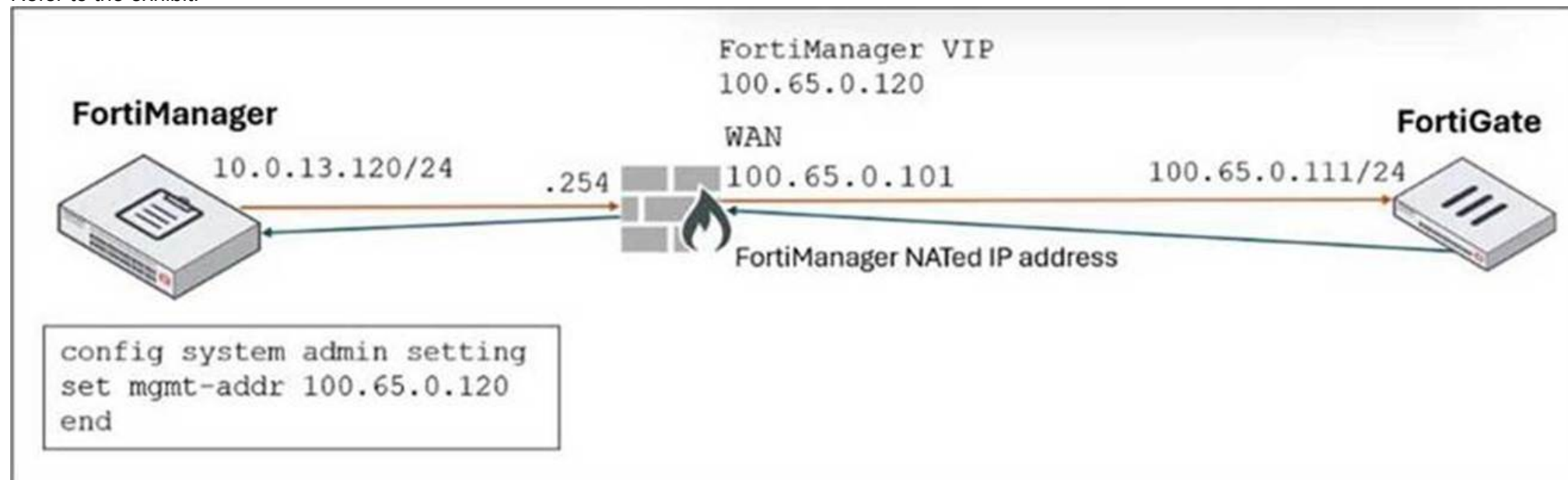
Answer: C

Explanation:

The CLI output shows the status "dev-db: not modified; conf: in sync; cond: OK; dm: installed," but the firmware version for the device is listed as "[unknown]." This indicates that FortiManager has not properly detected the FortiGate firmware version, likely because the device needs to be retrieved to update its information.

NEW QUESTION 10

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

.....

Relate Links

100% Pass Your FCP_FMG_AD-7.6 Exam with Examible Prep Materials

https://www.exambible.com/FCP_FMG_AD-7.6-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>