



Fortinet

Exam Questions FCP_FMG_AD-7.6

FCP - FortiManager 7.6 Administrator

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

An administrator has a FortiGate-HQ device with VDOMs—root, HR and Facilities, currently managed under the FortiManager ADOM—Site1. They try to move VDOM HR to the FortiManager ADOM—Site2, but it does not work.

Why is the administrator not able to move FortiGate-HQ VDOM HR to FortiManager ADOM—Site2?

- A. The FortiGate-HQ must be managed under the FortiManager ADOM—root to allow moving its VDOMs to different ADOMs.
- B. The administrator must have full access in the device layer of FortiGate-HQ VDOM-root before they can VDOMs to different ADOMs.
- C. FortiManager must be in ADOM normal mode, which does not allow VDOMs to be managed separately.
- D. The administrator must delete the FortiGate-HQ device from FortiManager and add it again using the Add Device wizard before moving the VDOM.

Answer: A

Explanation:

FortiGate devices must be managed under the FortiManager ADOM corresponding to the root VDOM to allow their individual VDOMs to be moved and managed in different ADOMs. Managing the root VDOM in a different ADOM prevents moving subordinate VDOMs across ADOMs.

NEW QUESTION 3

Which is recommended when you are managing a high volume of logs in your network?

- A. Store logs on FortiManager and use FortiView.
- B. Add and manage FortiAnalyzer from FortiManager.
- C. Enable advanced ADOM mode on FortiManager.
- D. Forward logs from FortiAnalyzer to FortiManager daily.

Answer: B

Explanation:

Adding and managing FortiAnalyzer from FortiManager is recommended for handling a high volume of logs, as FortiAnalyzer is designed specifically for centralized log management, analysis, and reporting, which offloads this workload from FortiManager.

NEW QUESTION 4

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 5

An administrator must create a policy and install it on a FortiGate device within an ADOM in backup mode. How can the administrator perform this task?

- A. Use the Install Wizard located on the device manager.
- B. Enable workflow mode to allow policy creation and approval.
- C. Make sure the ADOM and FortiGate firmware versions match and use the ADOM policy package.
- D. Use a FortiManager script to apply the configuration changes.

Answer: D

Explanation:

In backup mode, FortiManager does not directly manage policy installation via the usual ADOM policy packages; instead, administrators use FortiManager scripts to push configuration changes, including policies, to FortiGate devices.

NEW QUESTION 6

An administrator wants to configure and manage multiple objects in the FortiManager database and give access to other users who work in the same database. To stay in control of the changes made to firewall policies by other team members, the administrator needs a setup where all modifications go through a central check before they can be installed. How can the administrator create this setup?

- A. Enable the prompt asking the administrator to accept firewall policies changes before saving.
- B. Enable the workspace (for all ADOMs) to control all changes made by any administrator.
- C. Enable device lock and the advanced mode feature in the ADOM.
- D. Enable workflow mode and the ADOM lock feature.

Answer: D

Explanation:

Enabling workflow mode along with the ADOM lock feature ensures that all configuration changes go through a centralized review and approval process before installation, allowing controlled and coordinated management of firewall policies by multiple administrators.

NEW QUESTION 7

An administrator has assigned a global policy package to a new ADOM named ADOM1. What will happen if the administrator tries to create a new policy package in ADOM1?

- A. The administrator will be able to select the option to assign the global policy package to the new policy package.
- B. FortiManager will automatically assign the global policy package to the new policy package.
- C. FortiManager will automatically install policies on the policy package in ADOM1.
- D. The administrator will have to assign the global policy package from the global ADOM.

Answer: A

Explanation:

When a global policy package is assigned to an ADOM, administrators creating new policy packages within that ADOM have the option to select and assign the global policy package to the new policy package if desired.

NEW QUESTION 8

What is the best explanation of how FortiManager helps with mass provisioning?

- A. It upgrades the OS of each FortiGate device.
- B. It provides local FortiGuard Distribution Server (FDS) services to the network.
- C. It uses templates to configure the same settings on many devices simultaneously.
- D. It sends email alerts when new devices connect.

Answer: C

Explanation:

FortiManager helps with mass provisioning by using templates that allow administrators to configure the same settings on multiple FortiGate devices simultaneously, streamlining deployment and management.

NEW QUESTION 9

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 10

Refer to the exhibits.

FortiManager device database

Device Name	Config Status	Provisioning Templates	Policy Package Status
BR1-FGT-1	✓ Synchronized	✓ default	⚠ BR1-FGT-1
HQ-NGFW-1	⚠ Modified	⚠ default	✓ HQ-NGFW-1
Local-Firewall	⚠ Modified	⚠ default	⚠ Central
Remote-Firewall	⚠ Modified	⚠ default	⚠ Central

Installation Targets Central policy package

Installation Target	Config Status	Policy Package Status
<input type="checkbox"/> BR1-FGT-1	✓ Synchronized	● BR1-FGT-1
<input type="checkbox"/> Local-Firewall	⊙ Unknown	▲ Central
<input type="checkbox"/> Remote-Firewall	⊙ Unknown	▲ Central

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 10

What is the purpose of ADOM revisions?

- A. ADOM revisions find unused, duplicate, and unnecessary firewall policies and objects.
- B. ADOM revisions show specific changes in a policy package when it is installed.
- C. ADOM revisions compare previous snapshots of the Policy Package and ADOM-level objects with the device-level database.
- D. ADOM revisions save the current state of all policy packages and objects for an ADOM.

Answer: D

Explanation:

ADOM revisions save the current state of all policy packages and objects within an ADOM, allowing administrators to track changes over time and revert to previous configurations if needed.

NEW QUESTION 11

Refer to the exhibit.

Workspace	Mail Server	Syslog Server	Meta Fields	Misc Settings
<div style="display: flex; justify-content: space-between;"> + Create New Edit Delete Collapse All Expand All </div>				
<input type="checkbox"/>	Meta Fields			
Firewall Address (2)				
<input type="checkbox"/>	ExternalSubnet			
<input type="checkbox"/>	InternalSubnet			

An administrator created two new meta fields in FortiManager. Which operation can you perform with these parameters?

- A. You can add them to objects as custom attributes.
- B. You can export them to be used in other ADOMs.
- C. You can use them as variables in scripts.
- D. You can invoke them using the \$ character.

Answer: A

Explanation:

Meta fields in FortiManager can be added to objects as custom attributes, allowing administrators to categorize and add additional information to firewall objects for

easier management and identification.

NEW QUESTION 12

An administrator is copying a system template profile between ADOMs by running the following command:

execute fmpfile export-profile ADOM 3547 /tmp/Backup_File

output dump to file: [/tmp/Backup_File]

Where does this command export the system template profile from?

- A. FortiManager /tmp/Backup_File folder
- B. FortiManager ADOM policy database
- C. ADOM device database
- D. FortiManager configuration backup file

Answer: B

Explanation:

The command exports the system template profile from the FortiManager ADOM policy database, which stores the configuration templates for devices within that ADOM.

NEW QUESTION 15

Refer to the exhibits.

Device Revision Diff wizard

Revision ID: 11		Revision ID: 9	
Total	12696	Total	12704
Deleted	0	Added	8
Modified	0	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"
    
```

Buttons: 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 17

An administrator configures a new BGP peer in the FortiManager device-level database of FortiGate. They reinstall the policy package to the managed FortiGate device without any errors. However, when the administrator logs in to FortiGate, they do not see the BGP configuration changes.

What is the most likely reason why FortiManager did not push the BGP peer changes to FortiGate?

- A. The administrator must run a sanity check on FortiManager to make sure the database is not corrupted.
- B. Fortigate has a BGP template assigned on the FortiManager database.
- C. The administrator must use the Install Wizard and select Install device settings only to push BGP settings
- D. The FortiGate firmware version is different from the FortiManager ADOM version.

Answer: B

Explanation:

If a BGP template is assigned to the FortiGate device on FortiManager, device-level BGP configurations made directly in the device-level database are overridden by the template settings, so the changes do not get pushed to the device.

NEW QUESTION 20

.....

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

FCP_FMG_AD-7.6 Practice Exam Features:

- * FCP_FMG_AD-7.6 Questions and Answers Updated Frequently
- * FCP_FMG_AD-7.6 Practice Questions Verified by Expert Senior Certified Staff
- * FCP_FMG_AD-7.6 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * FCP_FMG_AD-7.6 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The FCP_FMG_AD-7.6 Practice Test Here](#)