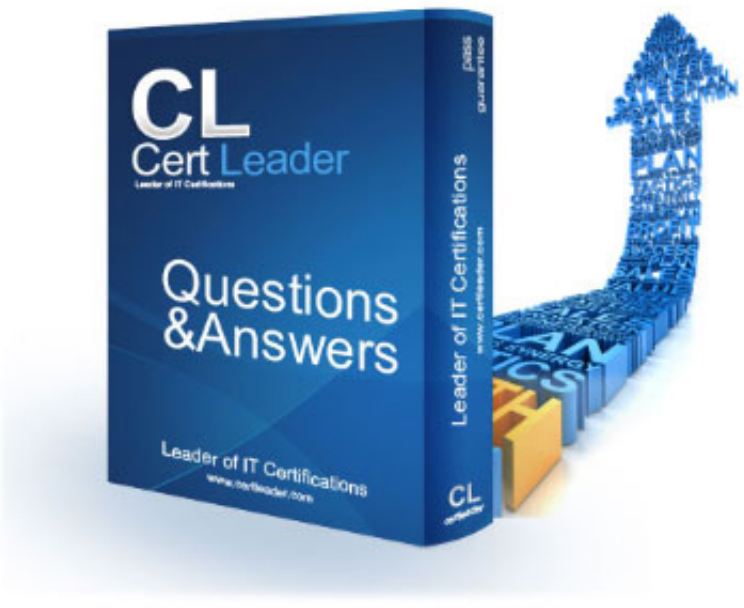
FCP_FMG_AD-7.4 Dumps

FCP - FortiManager 7.4 Administrator

https://www.certleader.com/FCP_FMG_AD-7.4-dumps.html



NEW QUESTION 1
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 override server IP address is set on FortiManager and the NAT device
B. That the external IP address on the NAT device is set to DHCP and configured with the virtual IP
C. That the NAT device IP address and correct ports are configured on FortiManager
D. That the virtual IP address and correct ports are set on the NAT device

Answer: AD

Explanation:
When push updates are failing on a FortiGate device behind a NAT device, the administrator should check:
? A.That the override server IP address is set on FortiManager and the NAT device.
? D.That the virtual IP address and correct ports are set on the NAT device. Options B and C are incorrect because:
? Bsuggests setting the external IP on the NAT device to DHCP, which is not relevant to solving the push update issue.
? Cimplies configuring NAT device IP and ports on FortiManager, which is less likely needed compared to configuring the correct VIP and ports.
FortiManager References:
? Refer to FortiManager 7.4 Administrator Guide: Device Management and NAT Configuration.

NEW QUESTION 2
Which two statements about Security Fabric integration with FortiManager are true? (Choose two.)

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

Answer: AC

Explanation:
Two statements about Security Fabric integration with FortiManager that are true are:
? A. The Fabric View module enables you to generate the Security Fabric ratings for
Security Fabric devices.
? C. The Fabric View module enables you to view the Security Fabric ratings for Security Fabric devices.
Options B and D are incorrect because:
? Bis misleading as the Security Fabric settings are generally configured and managed separately from other device-level settings.
? Dis incorrect as there is no specific requirement for a Security Fabric license, group name, and password solely for FortiManager integration.
FortiManager References:
? Refer to FortiManager 7.4 Security Fabric Integration Guide: Managing Security Fabric and Generating Security Fabric Ratings.

NEW QUESTION 3
An administrator configures a new OSPF area on FortiManager and has not yet pushed the changes to the managed FortiGate device. In which database will the configuration be saved?

A. Device-level database
B. ADOM-level database
C. Configuration-level database
D. Revision history database

Answer: A

Explanation:
When an administrator configures a new OSPF area on FortiManager but has not yet pushed the changes to the managed FortiGate device, the configuration is saved in the Device-level database.
Explanation of Options:
? A. Device-level database:
? B. ADOM-level database:
? C. Configuration-level database:
? D. Revision history database:

NEW QUESTION 4
In the event that one of the secondary FortiManager devices fails, which action must be performed to return the FortiManager HA manual mode to a working state?

A. The FortiManager HA state transition is transparent to administrators and does not require any reconfiguration.
B. Reboot the failed device to remove its IP from the primary device.
C. Manually promote one of the working secondary devices to the primary role, and reboot the old primary device to remove the peer IP of the failed device.
D. Reconfigure the primary device to remove the peer IP of the failed device.

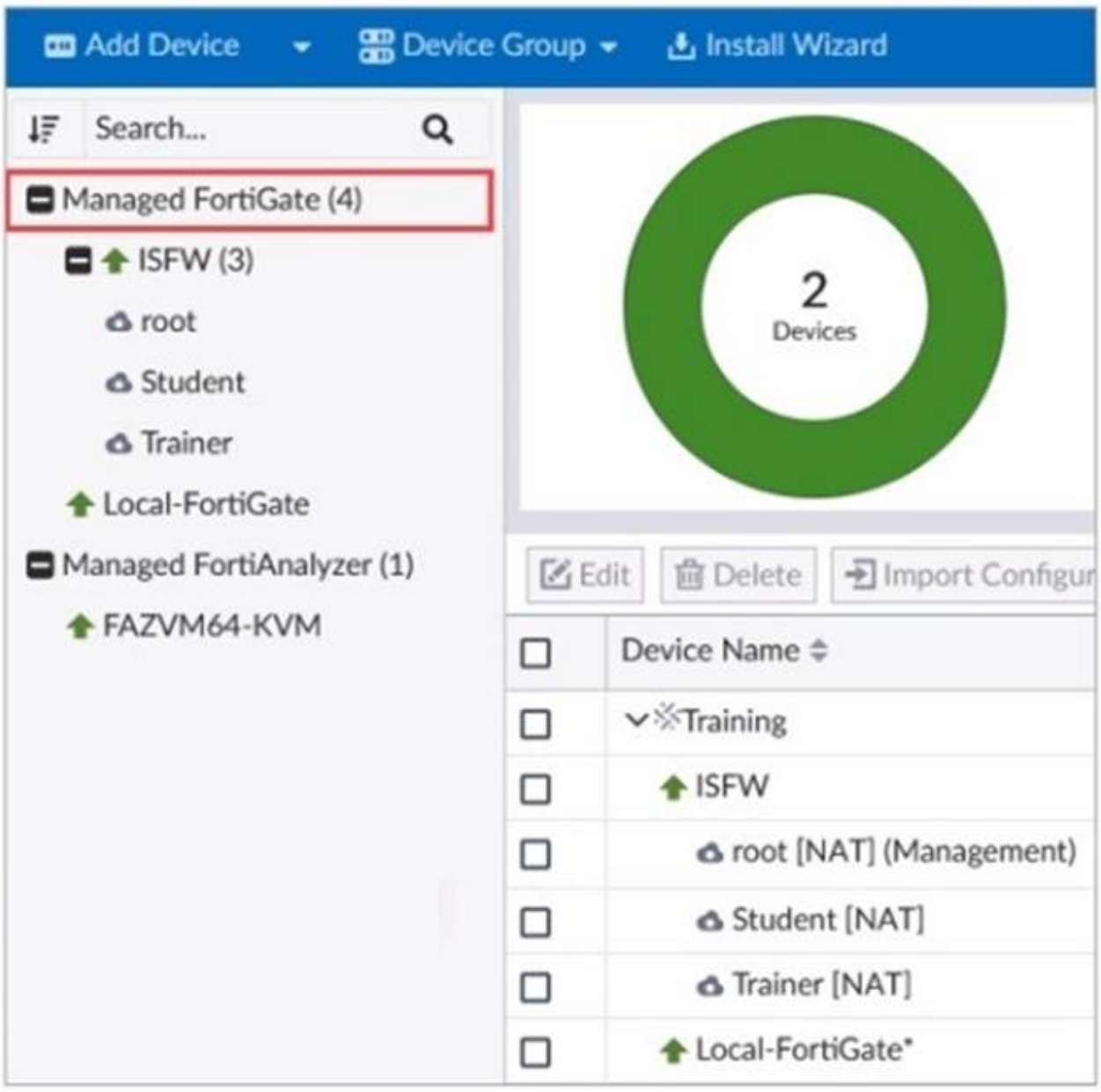
Answer: C

Explanation:
When a secondary FortiManager device fails in HA manual mode, an administrator must manually promote one of the working secondary devices to the primary role and reboot the old primary device to remove the peer IP of the failed device. This ensures the HA configuration is updated correctly, and the network remains resilient.
Options A, B, and D are incorrect because:
? A suggests the transition is transparent, which is true only in automatic mode, not in manual mode.
? B and D imply simpler steps that do not fully address the HA reconfiguration process in manual mode.
FortiManager References:

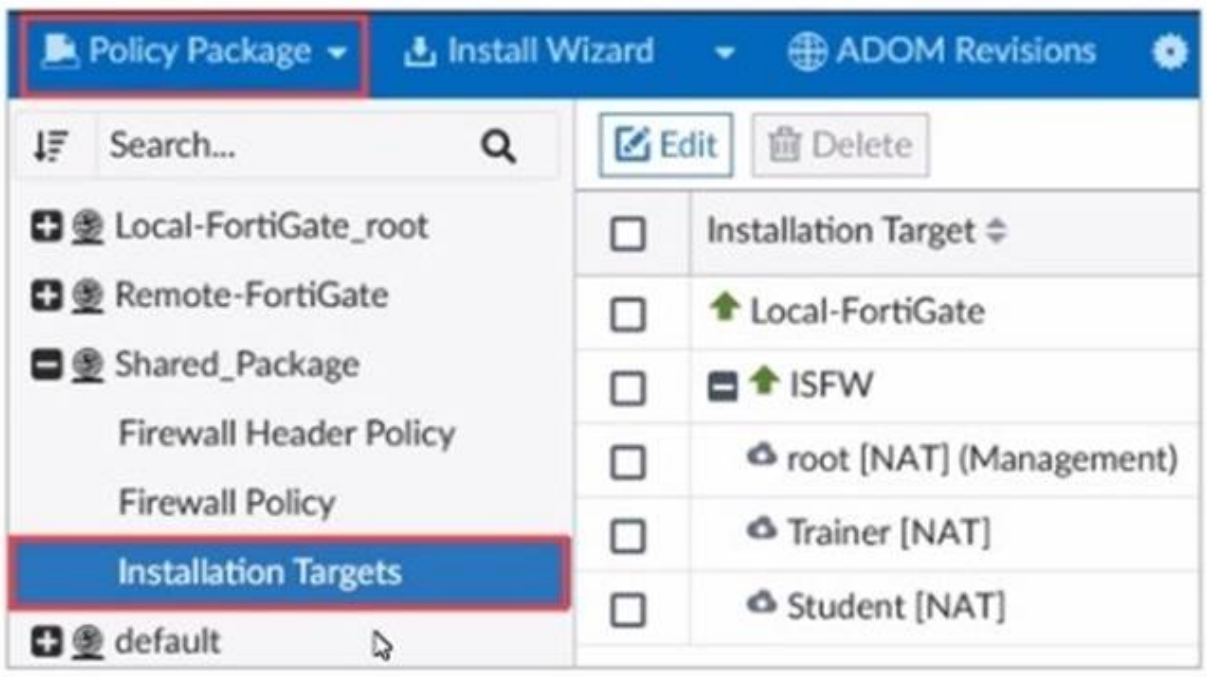
? Refer to FortiManager 7.4 High Availability (HA) Configuration Guide: Manual Mode Configuration and Failover Procedures.

NEW QUESTION 5
Refer to the exhibit.

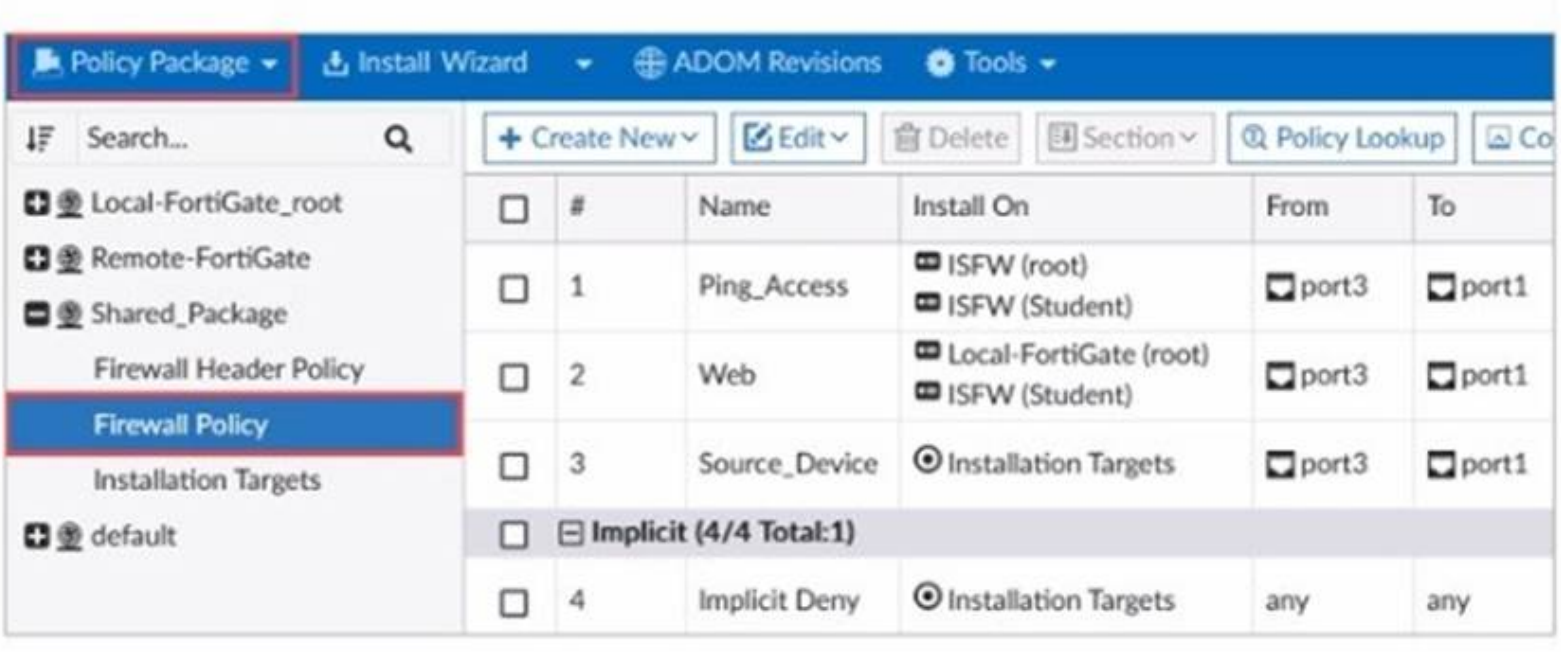
Managed FortiGate devices



FortiManager policy package



FortiManager policy package



Given the configuration shown in the exhibit, which two conclusions can you draw from the installation targets in the Install On column? (Choose two.)

A. Policy seq.S will be installed on all managed devices and VDOMs that are listed under Installation Targets
B. Policy seq.# 3 will be skipped because no installation targets are specified.
C. Policy seq.# 2 will not be installed on the Local-FortiGate root VDOM because there is no root VDOM in the Installation Target
D. Policy seq.# 1 will be installed on the ISFW device root[NAT] and Student[NAT] VDOMs only.

Answer: AD

Explanation:
? Option A: Policy seq.S will be installed on all managed devices and VDOMs that are listed under Installation Targets.This is correct. The "Install On" column indicates that the policy is targeted for installation on all listed managed devices and VDOMs under Installation Targets.
? Option D: Policy seq.# 1 will be installed on the ISFW device root[NAT] and Student[NAT] VDOMs only.This is correct. Policy sequence #1 specifies that it will be installed only on the ISFW device and the VDOMs 'root[NAT]' and 'Student[NAT]' as indicated by the "Install On" column.
Explanation of Incorrect Options:
? Option B: Policy seq.# 3 will be skipped because no installation targets are specifiedis incorrect because it is clearly listed under "Installation Targets," which means it will be installed according to the specified configuration.
? Option C: Policy seq.# 2 will not be installed on the Local-FortiGate root VDOM because there is no root VDOM in the Installation Targetis incorrect as the exhibit does not show any specific exclusion for seq.# 2 on the Local-FortiGate root VDOM.
FortiManager References:
? Refer to the FortiManager Administration Guide sections on "Policy Packages" and "Policy Installation Targets" for more details.

NEW QUESTION 6
What must you consider before deciding to use FortiManager to manage a FortiAnalyzer device?

A. Confirm that FortiManager has enough storage capacity for the expected logs.
B. Ensure that FortiAnalyzer features are installed in advance.
C. Check whether FortiManager is part of a high availability (HA) cluster.
D. Determine whether the VDOMs of the same FortiGate will be assigned to different ADOMs.

Answer: B

Explanation:
When deciding to use FortiManager to manage a FortiAnalyzer device, you must ensure certain conditions are met so that the integration works seamlessly. One key aspect to consider is whether the necessary FortiAnalyzer features are enabled on FortiManager.
Explanation of Options:
? A. Confirm that FortiManager has enough storage capacity for the expected logs.
? B. Ensure that FortiAnalyzer features are installed in advance.
? C. Check whether FortiManager is part of a high availability (HA) cluster.
? D. Determine whether the VDOMs of the same FortiGate will be assigned to different ADOMs.

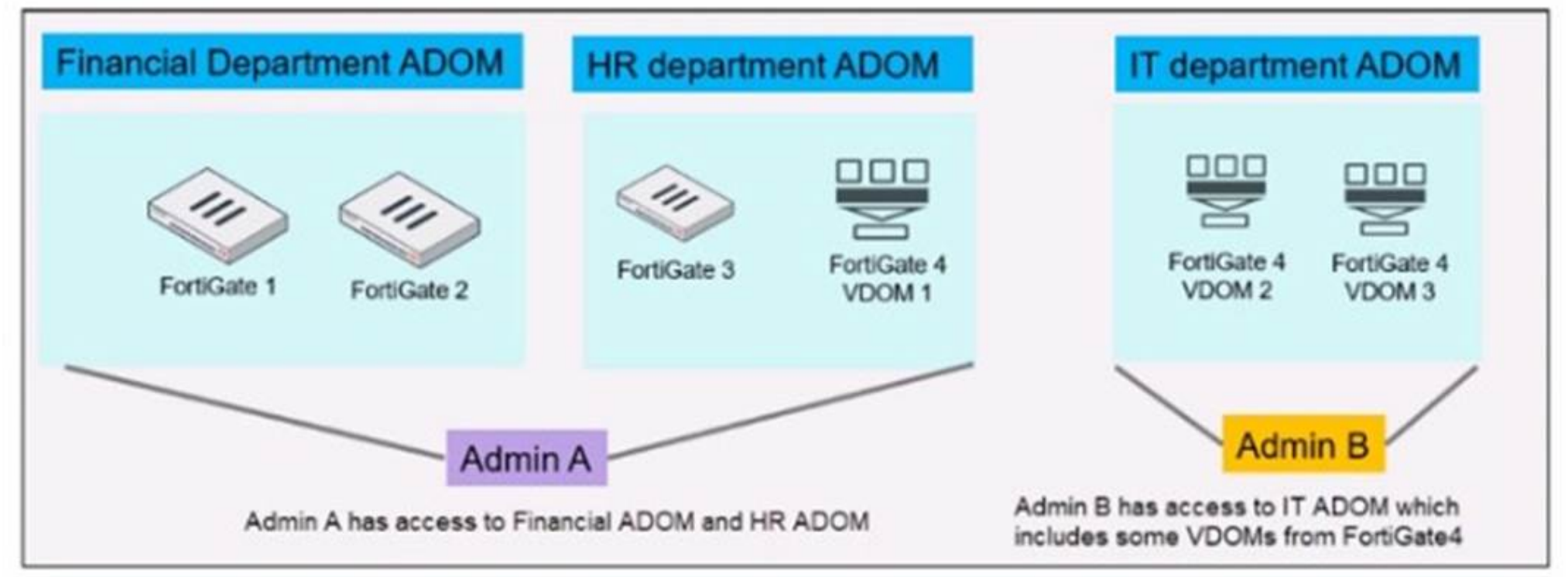
NEW QUESTION 7
Which configuration setting for FortiGate is part o an ADOM-level database on FortiManager?

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

Answer: B

Explanation:
? Option B: Routingis the correct answer. The ADOM-level database in FortiManager stores configuration settings such as routing, firewall policies, and objects that are shared across multiple devices in the ADOM.
Explanation of Incorrect Options:
? Option A: NSX-T Service Templateis incorrect as it is not a FortiGate-specific setting managed at the ADOM level.
? Option C: SNMPis incorrect because SNMP settings are typically managed on a per-device basis.
? Option D: Security profilesis incorrect because security profiles are generally device-level configurations, not ADOM-level.
FortiManager References:
? Refer to "FortiManager Administration Guide" for further details on ADOM-level and device-level configurations.

NEW QUESTION 8
Exhibit.



An administrator would like to create three ADOMs on FortiManager with different access levels based on departments. What two conclusions can you draw from the design shown in the exhibit? (Choose two.)

A. The FortiManager administrator must set the ADOM device mode to Advanced
B. Policies and objects databases can be shared between the Financial and HR ADOMs.
C. An administrator with the super user profile can access all the VDOMs.
D. The administrator must configure FortiManager in workspace normal mode.

Answer: AC

Explanation:
Based on the exhibit, the FortiManager administrator is setting up three ADOMs (Administrative Domains) that correspond to different departments (Financial, HR, and IT). Each ADOM has specificFortiGate devices or VDOMs (Virtual Domains) assigned to it, with different administrators managing the ADOMs.
Explanation of Options:
? A. The FortiManager administrator must set the ADOM device mode to Advanced.
? B. Policies and objects databases can be shared between the Financial and HR ADOMs.
? C. An administrator with the super user profile can access all the VDOMs.
? D. The administrator must configure FortiManager in workspace normal mode.
Conclusion:
? Ais correct becauseAdvanced modeis necessary for managing VDOMs within ADOMs.
? Cis correct because asuper usercan access all VDOMs and ADOMs without restrictions.

NEW QUESTION 9
Which statement about the upgrade of ADOMs on FortiManager is true?

A. To ensure database consistency, you must upgrade an ADOM before you upgrade the devices in it.
B. Upgrading the FortiManager version upgrades all existing ADOMs automatically.
C. You cannot import policies from a device until its FortiOS version matches the ADOM version.
D. ADOMs using global objects can be upgraded before or after upgrading the global database ADOM.

Answer: A

Explanation:
? Option A: To ensure database consistency, you must upgrade an ADOM before you upgrade the devices in it.This is the correct answer. When upgrading ADOMs on FortiManager, the ADOM must be upgraded first to match the FortiOS version of the devices it manages. This is necessary to ensure compatibility and consistency between the ADOM's database schema and the FortiGate's configuration.
Explanation of Incorrect Options:
? Option B: Upgrading the FortiManager version upgrades all existing ADOMs automaticallyis incorrect because the ADOMs must be upgraded manually or individually after upgrading the FortiManager.
? Option C: You cannot import policies from a device until its FortiOS version matches the ADOM versionis incorrect because while version matching is important, it is not strictly necessary for policy import.
? Option D: ADOMs using global objects can be upgraded before or after upgrading the global database ADOMis incorrect as the order of upgrade matters to maintain compatibility.
FortiManager References:
? Refer to "FortiManager Upgrade Guide" for detailed procedures on upgrading ADOMs and devices.

NEW QUESTION 10
Refer to the exhibit which shows the Download Import Report.

```
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)"
```

Why is FortiManager failing to import firewall policy ID 1?

A. Policy ID 1 is configured from the interface any to port6. FortiManager rejects the request to import this policy because the any interface does not exist on FortiManager
B. Policy ID 1 for this managed FortiGate already exists on FortiManager in the policy package named Remote-FortlGate.
C. Policy ID 1 has an address object that already exists in the ADOM database with any as the interface association, and conflicts with the address object interface association locally on FortiGate.
D. Policy ID 1 does not have the ADOM Interface mapping configured on FortiManager.

Answer: A

Explanation:
? Option A: Policy ID 1 is configured from the interface any to port6. FortiManager rejects the request to import this policy because the any interface does not exist on FortiManager.This is the correct answer. FortiManager fails to import firewall policy ID 1 because it cannot map the "any" interface to a valid interface in its ADOM database. The error indicates that there is a binding failure due to an interface mismatch.
Explanation of Incorrect Options:
? Option B: Policy ID 1 for this managed FortiGate already exists on FortiManager in the policy package named Remote-FortiGateis incorrect because the error is related to interface mapping, not a duplicate policy ID.
? Option C: Policy ID 1 has an address object that already exists in the ADOM database with any as the interface association and conflicts with the address object interface association locally on FortiGateis incorrect because the error specifies an interface issue, not an address object conflict.
? Option D: Policy ID 1 does not have the ADOM Interface mapping configured on FortiManageris incorrect because the error directly mentions a binding failure due to the "any" interface.
FortiManager References:
? For more information, refer to the "Device Manager" section and "Configuration Import and Mapping" in the FortiManager Administration Guide.

NEW QUESTION 10
Which output is displayed right after moving the ISFW device from one ADOM to another?
A)

```
FortiManager # diagnose dvm device list ISFW
--- There are currently 4 devices/vdoms managed ---
--- There are currently 4 devices/vdoms count for license ---

TYPE            OID   SN               HA   IP           NAME   ADOM    IPS              FIRMWARE
fmgfaz-managed  325   FGVM010000077646 -    10.0.1.200   ISFW   ADOM74  6.00741 (regular) 7.0 MR4 (2463)
                |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; conn: up
                |- vdom:[3]root flags:0 adom:ADOM74 pkg:[unknown]ISFW
```

B)

```
FortiManager # diagnose dvm device list ISFW
--- There are currently 4 devices/vdoms managed ---
--- There are currently 4 devices/vdoms count for license ---

TYPE            OID   SN               HA   IP           NAME   ADOM    IPS              FIRMWARE
fmgfaz-managed  325   FGVM010000077646 -    10.0.1.200   ISFW   ADOM74  6.00741 (regular) 7.0 MR4 (2463)
                |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: autoupdated; conn: up
                |- vdom:[3]root flags:1 adom:ADOM74 pkg:[out-of-sync]ISFW
```

C)

```
FortiManager # FortiManager # diagnose dvm device list ISFW
--- There are currently 4 devices/vdoms managed ---
--- There are currently 4 devices/vdoms count for license ---

TYPE            OID   SN               HA   IP           NAME   ADOM    IPS              FIRMWARE
fmgfaz-managed  325   FGVM010000077646 -    10.0.1.200   ISFW   ADOM74  6.00741 (regular) 7.0 MR4 (2463)
                |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: installed; conn: up
                |- vdom:[3]root flags:0 adom:ADOM74 pkg:[never-installed]
```

D)

```
FortiManager # diagnose dvm device list ISFW
--- There are currently 4 devices/vdoms managed ---
--- There are currently 4 devices/vdoms count for license ---

TYPE            OID    SN                HA      IP              NAME            ADOM     IPS                FIRMWARE
fmgfaz-managed  325    FGVM010000077646  -       10.0.1.200      ISFW            ADOM74   6.00741 (regular)  7.0 MR4 (2463)
                |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: installed; conn: up
                |- vdom:[3]root flags:0 adom:ADOM74 pkg:[imported]ISFW
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

Explanation:
When a FortiGate device, like the ISFW (Internal Segmentation Firewall), is moved from one ADOM to another in FortiManager, the status of the device in the new ADOM will temporarily show some level of inconsistency or unknown state until the ADOM fully syncs and integrates the device.
In the provided options, we are analyzing the FortiManager diagnose dvm device list output for the ISFW device.
Explanation of the Outputs:
? Option A:
? Option B:
? Option C:
? Option D:
Conclusion:
The output that is displayedimmediately after movingthe ISFW device from one ADOM to another isOption A, where the package status is still unknown (pkg: [unknown]) because FortiManager has not yet fully synchronized the device's configuration in the new ADOM.

NEW QUESTION 12
Exhibit.

```
FortiManager # config system global
(global)# set workspace-mode normal
(global)# end
FortiManager #
```

Given the configuration shown in the exhibit, what are two results from this configuration?
{Choose two.)

A. You can validate administrator login attempts through external servers.
B. The same administrator can lock more than one ADOM at the same time.
C. Two or more administrators can make configuration changes at the same time, in the same ADOM.
D. Concurrent read-write access to an ADOM is disabled.

Answer: BD

Explanation:
The configuration shown in the exhibit sets theworkspace-mode to normal. The workspace mode in FortiManager defines how configuration changes and administrative tasks are handled, specifically regarding locking and collaboration in ADOMs (Administrative Domains).
Understanding the workspace modes:
? Normal Mode:In this mode, only one administrator at a time can lock and edit an ADOM. The changes made by one administrator must be completed and saved before another administrator can make changes. It prevents concurrent read-write access within the same ADOM.
? Workflow Mode:This mode allows multiple administrators to work on different tasks within the same ADOM, but changes still need to be approved before being committed.
Explanation of Options:
? A. You can validate administrator login attempts through external servers.
? B. The same administrator can lock more than one ADOM at the same time.
? C. Two or more administrators can make configuration changes at the same time, in the same ADOM.
? D. Concurrent read-write access to an ADOM is disabled.

NEW QUESTION 16
An administrator has assigned a global policy package to custom ADOM1. Then the administrator creates a new policy package. Fortinet. in the custom ADOM1. What happens to the Fortinet policy package when it is created?

A. You must assign the global policy package from the global ADOM.
B. The global policy package is automatically assigned.
C. You must reapply the global policy package to ADOM1.
D. You can select the option to assign the global policies.

Answer: B

Explanation:
When a new policy package is created in a custom ADOM that already has a global policy package assigned, the global policy package is automatically assigned to the
new policy package. This behavior ensures consistent policy enforcement across different ADOMs.
Options A, C, and D are incorrect because:
? A and C incorrectly suggest that manual reassignment or reapplication is needed.
? D implies optional assignment, whereas it is automatically done.
FortiManager References:
? Refer to FortiManager 7.4 Administrator Guide: Working with Global and Custom ADOM Policy Packages

NEW QUESTION 18
What is the purpose of ADOM revisions?

A. To save the current state of the whole ADOM
B. To save the current state of all policy packages and objects for an ADOM
C. To revert individual policy packages and device-level settings for a managed FortiGate
D. To save the FortiManager configuration in the System Checkpoints

Answer: B

Explanation:
? Option B: To save the current state of all policy packages and objects for an ADOMis the correct answer. ADOM (Administrative Domain) revisions in FortiManager are used to create a snapshot of the current state of all policy packages and objects associated with an ADOM. This allows administrators to save a specific configuration state and revert to it if necessary. It helps in managing changes and recovering from configuration errors or unintended changes.
? Explanation of Incorrect Options:
FortiManager References:
? Refer to the FortiManager 7.4 Administration Guide, "ADOM Management" section, which describes the purpose and usage of ADOM revisions for configuration management and restoration.

NEW QUESTION 20
Refer to the exhibit.

An administrator is about to add the FortiGate device to FortiManager using the discovery process.
FortiManager is operating behind a NAT device, and the administrator configured the FortiManager NATed IP address under the FortiManager system administration settings.
What is the expected result?

A. During discover
B. FortiManager uses only the FortiGate serial number to establish the
C. During discovery, FortiManager sets both the FortiManager NATed IP address and NAT device IP address on FortiGate.
D. During discover
E. FortiManager sets the NATed device IP address on FortiGate.
F. During discovery, FortiManager sets the FortiManager NATed IP address on FortiGate.

Answer: D

Explanation:
When adding a FortiGate device to FortiManager that is operating behind a NAT device, and the FortiManager NATed IP address is configured under the system administration settings, FortiManager will set the FortiManager NATed IP address on the FortiGate device during the discovery process. This ensures that the FortiGate knows how to reach the FortiManager through the NAT device.
Options A, B, and C are incorrect because:
? Ais incorrect because the discovery process also requires knowing the NATed IP to establish a connection, not just the serial number.
? Bis incorrect because FortiManager does not set the NAT device's IP address on the FortiGate.
? Cis incorrect because it implies that the NAT device IP is set on FortiGate, which is not the expected outcome.
FortiManager References:
? Refer to FortiManager 7.4 Administrator Guide: Device Discovery and Management with NAT.

NEW QUESTION 24
Which two items are included in the FortiManager backup? (Choose two.)

A. All devices
B. Firmware images
C. FortiGuard database
D. Flash configuration

Answer: AD

Explanation:
FortiManager backups include:
? A. All devices— This includes all device configurations managed by FortiManager, such as firewall policies, objects, and other settings.
? D. Flash configuration— This consists of local FortiManager configurations stored
in flash memory, such as system settings, scripts, and other locally-stored configurations.
Options B and C are incorrect because:
? B (Firmware images)are not typically included in a FortiManager backup. Firmware images are usually stored separately and managed through a different process.
? C (FortiGuard database)is incorrect as the FortiGuard database, which contains threat intelligence and security signatures, is not part of the standard FortiManager backup.
FortiManager References:
? Refer to FortiManager 7.4 Administrator Guide: Backup and Restore Processes.

NEW QUESTION 27
An administrator wants to create a policy on an ADOM that is in backup mode and install it on a FortiGate device in the same ADOM. How can the administrator perform this task?

A. The administrator must use the Policy & Objects section to create a policy first.
B. The administrator must use a FortiManager script.
C. The administrator must disable the FortiManager offline mode first.
D. The administrator must change the ADOM mode to Advanced to bring the FortiManager online.

Answer: B

Explanation:
To create and install a policy on a FortiGate device in an ADOM (Administrative Domain) that is in backup mode, the administrator must use a FortiManager script. This is because backup mode restricts direct configuration changes, and scripts can be used to push specific configuration changes without altering the ADOM mode.
Options A, C, and D are incorrect because:
? A requires the ADOM to be in normal or advanced mode to create policies directly in the Policy & Objects section.
? C suggests disabling offline mode, which is irrelevant to the backup mode configuration.
? D implies changing the ADOM mode, which is unnecessary if using a script to perform the task.
FortiManager References:
? Refer to FortiManager 7.4 Administrator Guide: Working with ADOMs and Using Scripts for managing policies in backup mode.

NEW QUESTION 31
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your FCP_FMG_AD-7.4 Exam with Our Prep Materials Via below:

https://www.certleader.com/FCP_FMG_AD-7.4-dumps.html