Fortinet

Exam Questions FCP_FMG_AD-7.4

FCP - FortiManager 7.4 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!

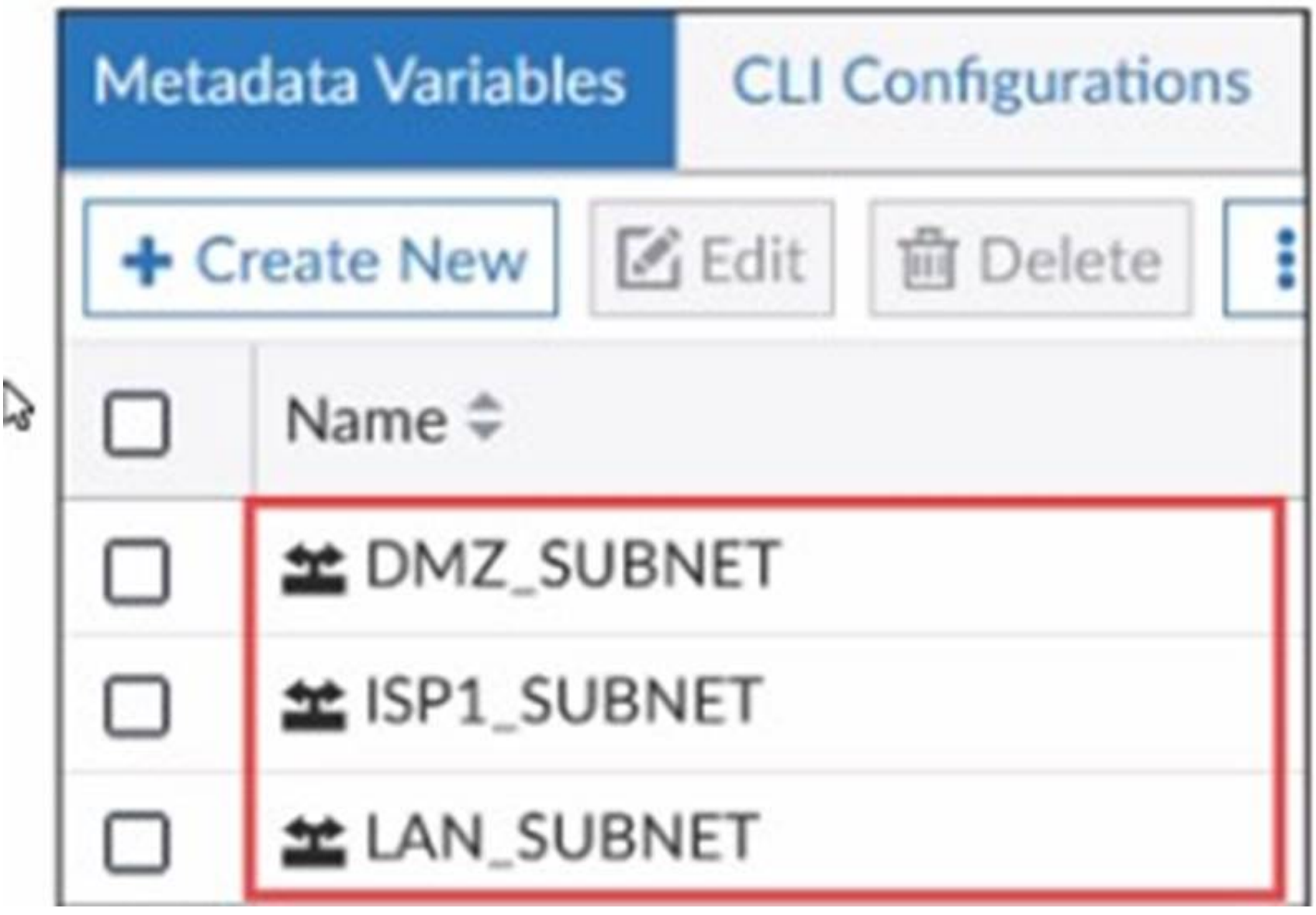
NEW QUESTION 1
What is a characteristic of the FortiManager high availability (HA) feature?

A. When a secondary unit is removed, FortiManager updates the managed devices using TCP port 5199.
B. The primary unit synchronizes all configuration revision with the seconday units.
C. All secondary units must be in the same network as the primary unit.
D. Each cluster member must be upgraded manually, starting with the primary unit.

Answer: B

Explanation:
The characteristic of the FortiManager high availability (HA) feature is that the primary unit synchronizes all configuration revisions with the secondary units. This ensures that all devices in the HA cluster are up-to-date with the same configurations, providing redundancy and failover capabilities.
Options A, C, and D are incorrect because:
? Arefers to a specific port number (5199), but FortiManager does not specifically use TCP port 5199 to update managed devices when a secondary unit is removed.
? Cis incorrect as secondary units do not necessarily have to be in the same network as the primary unit; they just need to be able to communicate with each other.
? Dis incorrect because HA upgrades can be automated and do not require manual upgrading, starting with the primary unit.
FortiManager References:
? Refer to FortiManager 7.4 High Availability (HA) Guide: HA Synchronization and Configuration.

NEW QUESTION 2
Exhibit.



What is true about the objects highlighted in the image?

A. They can be set to optional or required.
B. They are available across all ADOMs by default.
C. They can be used as variables in scripts.
D. They cannot be created in the global database ADOM.

Answer: C

Explanation:
The objects highlighted in the image (DMZ_SUBNET, ISP1_SUBNET, LAN_SUBNET) aremetadata variables.
? C.They can be used as variables in scripts.
Options A, B, and D are incorrect because:
? Asuggests optional or required settings, which do not apply to metadata variables.
? Bimplies they are available across all ADOMs by default, which is not always the case.
? Dstates they cannot be created in the global database ADOM, but metadata variables are typically managed within ADOMs and can be utilized globally based on specific configurations.
FortiManager References:
? Refer to FortiManager 7.4 Administrator Guide: Using Metadata Variables and Script Management.

NEW QUESTION 3
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 4
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 5
An administrator created a new global policy package that includes header and footer policies and then assigned it to an ADOM. What are two outcomes of this action? (Choose two.)

A. To assign another global policy package later to the same ADO
B. you must unassign this policy first.
C. After you assign the global policy package to an ADO
D. the impacted policy packages become hidden in that ADOM.
E. You can edit or delete all the global objects in the global ADOM.
F. You must manually move the header and footer policies after the policy assignment.

Answer: AC

Explanation:
? Option A: To assign another global policy package later to the same ADOM, you must unassign this policy first.This is correct. FortiManager does not allow multiple global policy packages to be assigned to a single ADOM simultaneously. If you want to assign a different global policy package, the existing one must be unassigned first.
? Option C: You can edit or delete all the global objects in the global ADOM.This is correct. Once a global policy package is assigned, you have the flexibility to edit or delete global objects in the global ADOM, affecting all ADOMs to which this package is assigned.
Explanation of Incorrect Options:
? Option B: After you assign the global policy package to an ADOM, the impacted policy packages become hidden in that ADOMis incorrect because the policy packages do not become hidden; they are modified according to the global
policies.
? Option D: You must manually move the header and footer policies after the policy assignmentis incorrect because header and footer policies are automatically applied when assigned.
FortiManager References:
? See the "Global Policy and ADOM Management" section in the FortiManager Administration Guide.

NEW QUESTION 6
Refer to the exhibit.

FortiManager log

```
-------Executing time: [redacted]----------

Starting log (Run on device)

Local-FortiGate $ config user local
Local-FortiGate (local) $ edit student
Local-FortiGate (student) $ set type ldap
Local-FortiGate (student) $ set status enable
Local-FortiGate (student) $ next
Attribute 'ldap-server' MUST be set.
Command fail. Return code 1
Local-FortiGate (local) $ end
Local-FortiGate $ config firewall policy
Local-FortiGate (policy) $ edit 2
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 users student
entry not found in datasource

value parse error before 'student'
Command fail. Return code -3
Local-FortiGate (2) $ set nat enable
Local-FortiGate (2) $ next
Local-FortiGate (policy) $ end
Local-FortiGate $

----------------End of Log----------------------------
```

A. Policy ID 2 is installed in the disabled state.
B. Policy ID 2 is installed without the remote user student.
C. Policy ID 2 will not be installed.
D. Policy ID 2 is installed without a source address.

Answer: B

Explanation:
From the log provided in the exhibit, several conclusions can be drawn regarding the installation of Policy ID 2:
? The installation process fails when attempting to set theLDAP user "student". The log shows:
Because of these errors, while other configuration elements (such as source and destination interfaces, actions, and services) are properly set, the user configuration for "student"isnot applied.
Evaluation of the answer options:
? A. Policy ID 2 is installed in the disabled state.
? B. Policy ID 2 is installed without the remote user student.
? C. Policy ID 2 will not be installed.
? D. Policy ID 2 is installed without a source address.
From the log exhibit, we see errors related to the "ldap-server" attribute not being set and an error with the entry "student" not being found in the datasource. This indicates that Policy ID 2 will not be installed due to missing or incorrect data required for successful installation. The "Command fail. Return code -3" confirms the installation failure, so the correct answer is C.
Options A, B, and D are incorrect because:
? A suggests the policy is installed in a disabled state, which isn't supported by the log.
? B and D suggest partial installation, but the error messages indicate a complete failure to install Policy ID 2.
FortiManager References:
? Refer to FortiManager 7.4 Troubleshooting Guide: Common Errors and Log Interpretation.

NEW QUESTION 7
Which API method is used to create objects or overwrite existing ones?

A. Set
B. Add
C. Exec
D. Update

Answer: A

Explanation:
In the context of the FortiManager JSON API, thesetmethod is used tocreate new objects oroverwrite existing ones. The API allows administrators to manage FortiManager and its associated devices by automating tasks like configuration changes, policy updates, and object creation.
Explanation of Options:
? A. Set:
? B. Add:
? C. Exec:
? D. Update:

NEW QUESTION 8
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 9
What will be the result of reverting to a previous revision version in the revision history?

A. It win install configuration changes to managed device automatically.
B. It will tag the device settings status as Auto-Update.
C. It will modify the device-level database.
D. It will generate a new version ID and remove all other revision history versions.

Answer: C

Explanation:
? Option C: It will modify the device-level database.This is correct. Reverting to a previous revision version in the revision history affects the device-level database by restoring it to the state saved in the selected revision. This ensures that any changes made after the selected revision are discarded, and the device configuration is returned to the earlier state.
Explanation of Incorrect Options:
? Option A: It will install configuration changes to managed devices automaticallyis incorrect because reverting a revision does not automatically push changes to the devices; it merely reverts the configuration on the FortiManager.
? Option B: It will tag the device settings status as Auto-Updateis incorrect because "Auto-Update" is not a status related to the revision history mechanism.
? Option D: It will generate a new version ID and remove all other revision history versionsis incorrect as reverting to a previous revision does not delete all other versions; it creates a new revision point for tracking.
FortiManager References:
? Refer to the "Revision Management" section in the FortiManager Administration Guide, which provides an overview of how revisions are managed and utilized for restoring configurations.

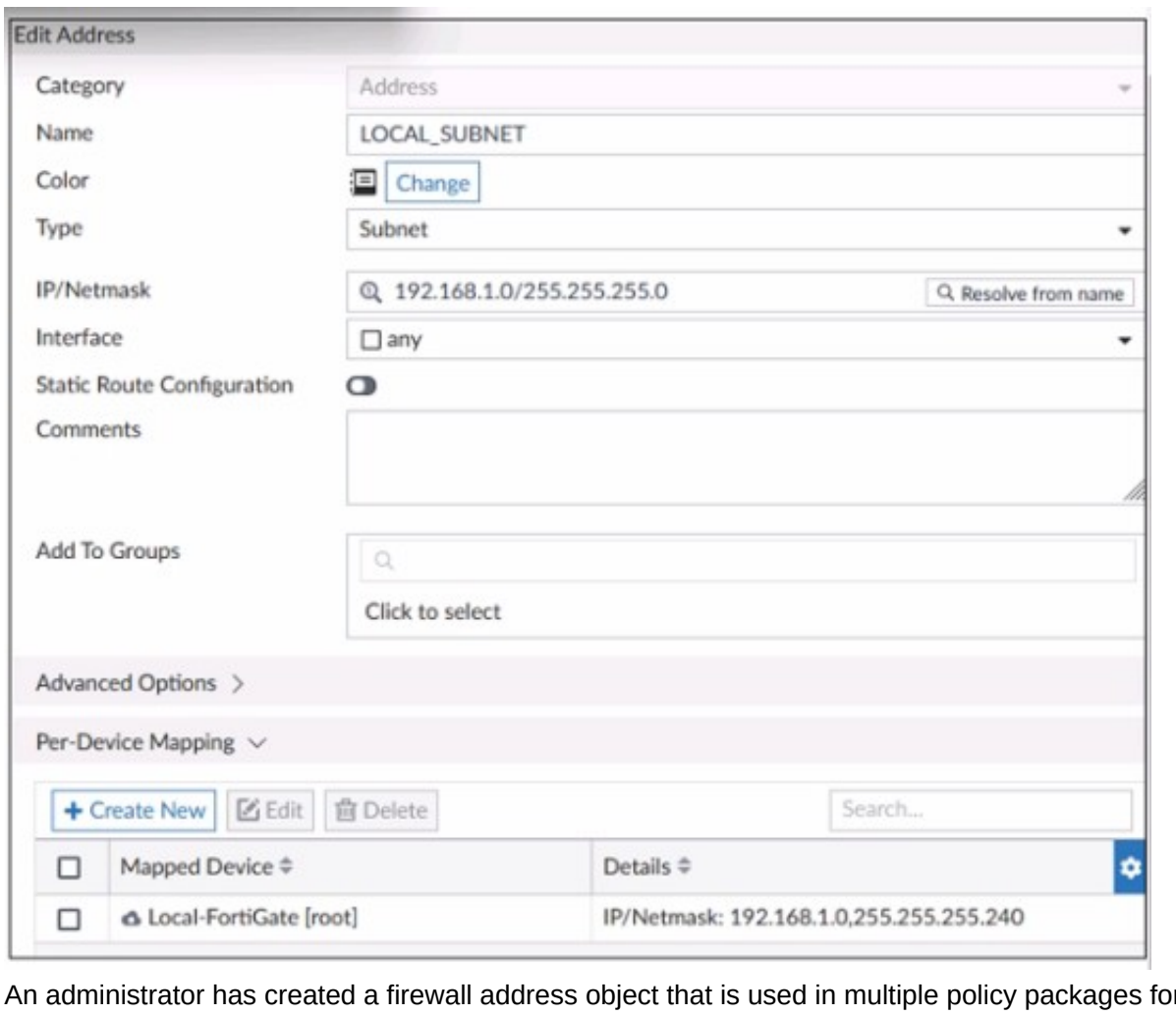
NEW QUESTION 10
Which two items are included in the FortiManager backup? (Choose two.)

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 10
Refer to the exhibit.



An administrator has created a firewall address object that is used in multiple policy packages for multiple FortiGate devices in an ADOM.
After the installation operation is performed, which IP/netmask is shown on FortiManager for this firewall address object for devices without a Per-Device Mapping set?

A. FortiManager generates an error for each FortiGate without a per-device mappingdefined for that object.
B. 192.168.1.0/24
C. 192.168.1.0/28
D. FortiManager replaces the address object to none.

Answer: B

Explanation:
? Option B: 192.168.1.0/24is the correct answer. In FortiManager, when a firewall address object is defined and used across multiple policy packages without any Per-Device Mapping, the default value configured in the object definition (192.168.1.0/255.255.255.0) is applied to all devices. The exhibit shows that the address objectLOCAL_SUBNEThas a default IP/netmask of192.168.1.0/24. Therefore, FortiManager will use this default value for any FortiGate device that does not have a specific Per-Device Mapping configured.
? Explanation of Incorrect Options:
FortiManager References:
? Refer to the FortiManager 7.4 Administration Guide, specifically in sections related to "Address Object Management" and "Per-Device Mapping," which detail the behavior of address objects without specific device mappings.

NEW QUESTION 14
An administrator enabled workspace mode and now wants to delete an address object that is currently referenced in a firewall policy. Which two results can the administrator expect? (Choose two.)

A. FortiManager will temporarily change the status of the referenced firewall policy to disabled.
B. FortiManager will disable the status of the address object until the changes are installed.
C. FortiManager will not allow the administrator to delete a referenced address object until they lock the ADOM.
D. FortiManager will replace the deleted address object with the none address object in the referenced firewall policy.

Answer: CD

Explanation:
When operating in workspace mode on FortiManager 7.4, the administrator must understand how object references and deletions work:
? Option C- "FortiManager will not allow the administrator to delete a referenced
address object until they lock the ADOM":In workspace mode, all changes are managed within an Administrative Domain (ADOM) scope. When an object (like an address object) is referenced in a policy, FortiManager prevents its deletion to maintain configuration integrity. The ADOM must be locked by the administrator to make changes to any referenced objects. This locking mechanism ensures that no unintended deletions or changes occur that could disrupt the policies or configuration.
? Option D- "FortiManager will replace the deleted address object with the none
address object in the referenced firewall policy":If the administrator attempts to delete an address object that is currently referenced by a firewall policy, FortiManager will replace the deleted object with the 'none' address object. This is done to maintain the policy structure and avoid policy corruption due to a missing reference. This behavior ensures that the firewall policy remains syntactically correct, even though the specific address object is no longer in use.

NEW QUESTION 15
.....

Relate Links

100% Pass Your FCP_FMG_AD-7.4 Exam with Exambible Prep Materials

https://www.exambible.com/FCP_FMG_AD-7.4-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/