EXAMTOPICS
- Expert Verified, Online, **Free**.

CERTIFICATION TEST
- CertificationTest.net - Cheap & Quality Resources With Best Support

Question #1 *Topic 1*

You want to let multiple administrators work in the same ADOM without creating configuration conflicts.
What is the best and the most effective solution to apply?

A. Configure RADIUS authentication to assign ADOM roles to each user.

B. Enable workflow mode, which is the only way to prevent concurrent configuration conflicts.

C. Assign administrators with JSON API access to the FortiManager.

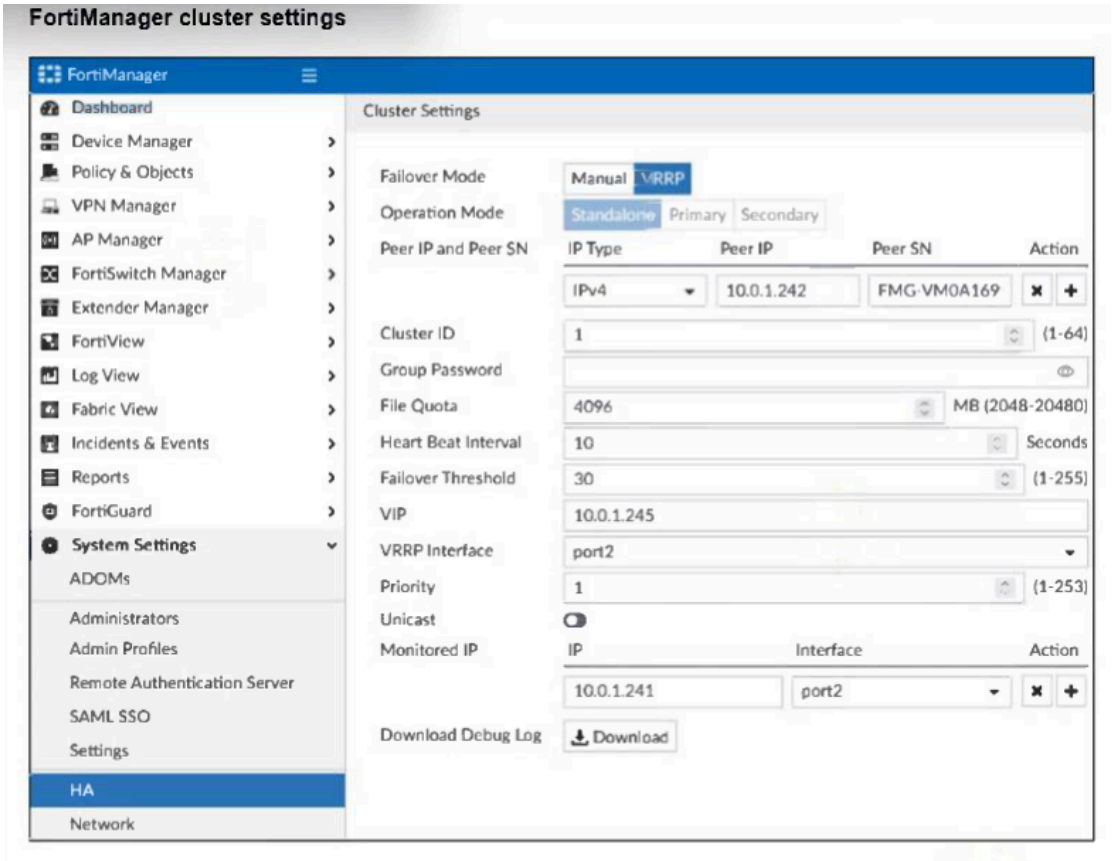
D. Activate workspace mode in the ADOM settings.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 1*

Refer to the exhibit.



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.

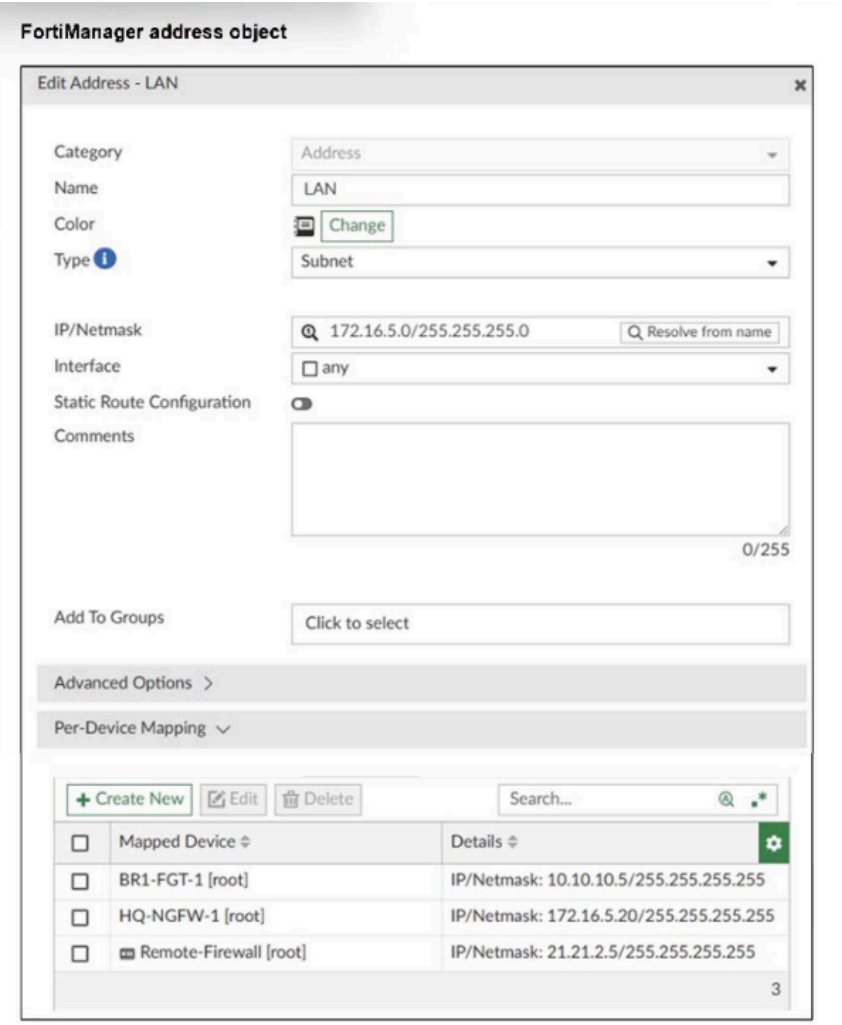
D. Check the integrity database of the primary device to force a secondary device to become the new primary with all active interfaces.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 1*

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 will be installed on Remote-Firewall [VDOM1] for the LAN firewall address object?

A. 21.21.2.5/255.255.255.255

B. 172.16.5.20/255.255.255.255

C. 172.16.5.0/255.255.255.0

D. 10.10.10.5/255.255.255.255

Suggested Answer: *A*

Community vote distribution

C (100%)

Ghaleb 4 days, 4 hours ago

Selected Answer: C

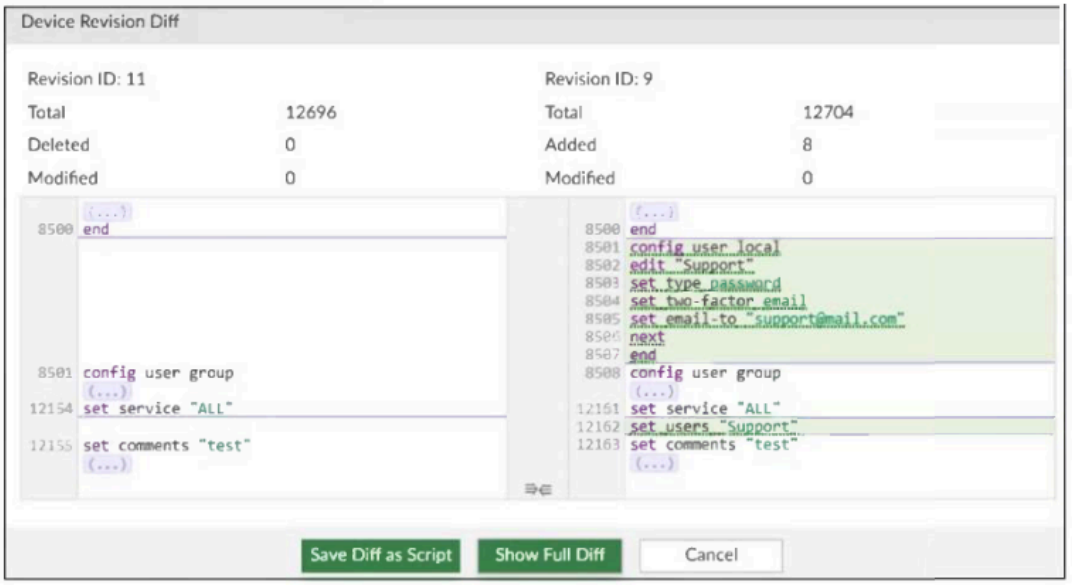
VDOM1 is not in the pre-device mapping

upvoted 1 times

Question #4 *Topic 1*

Refer to the exhibits.

Device Revision Diff wizard



CLI output

```
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: OK; dm: installed; conn: up; template:[installed]default
                |- vdom:[3]root flags:0 adom:My_ADOM pkg:[unknown]BR1-FGT-1
```

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.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

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.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 1*

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

Suggested Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 1*

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.

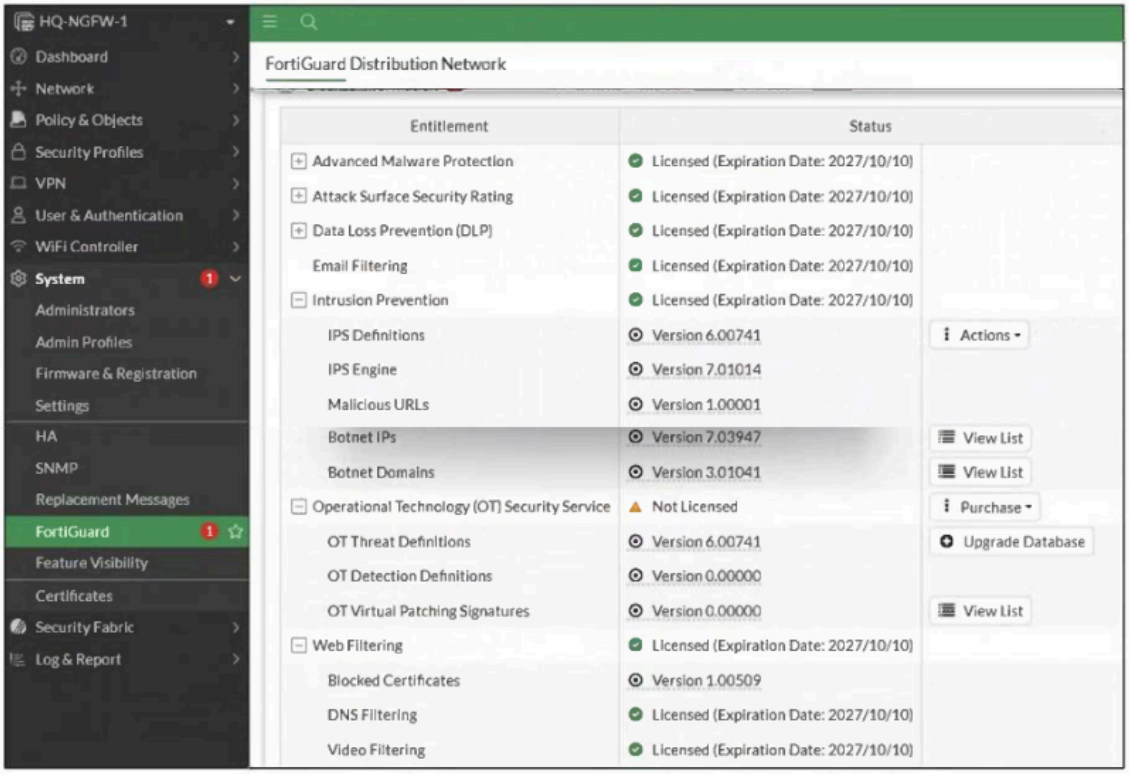
D. The administrator will have to assign the global policy package from the global ADOM.

Suggested Answer: *A*

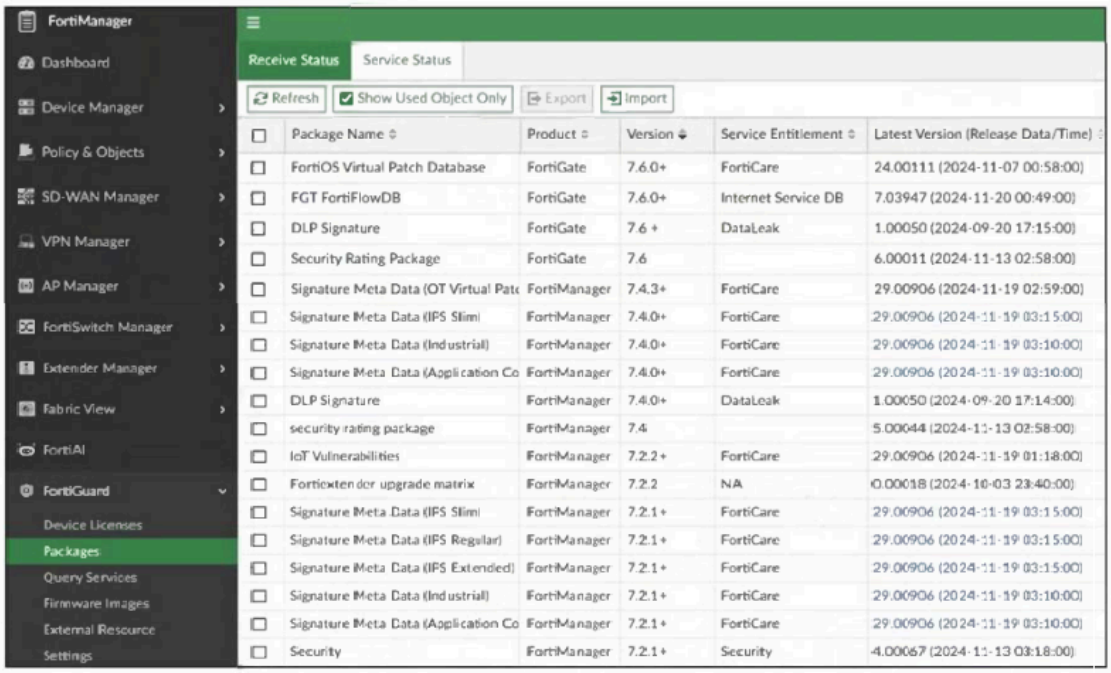
Currently there are no comments in this discussion, be the first to comment!

Refer to the exhibits.

FortiGate GUI—FortiGuard



FortiManager GUI—FortiGuard



FortiGate CLI—Central management

```
HQ-NGFW-1 (central-management) # sh
config system central-management
    set type fortimanager
    set allow-push-firmware disable
    set allow-remote-firmware-upgrade disable
    set serial-number "FMG-VMTM24012945"
    set fmg "::ffff:10.0.13.120"
    config server-list
        edit 1
            set server-type update
            set server-address 192.168.1.120
        next
    end
    set include-default-servers disable
end
```

FortiGate HQ-NGFW-1 downloads and validates FortiGuard databases from FortiManager which acts as a local FortiGuard Distribution Server (FDS) in a closed network. An administrator pushes a new firewall policy with an intrusion prevention system (IPS) profile from FortiManager to FortiGate HQ- NGFW-1 However, FortiGate does not recognize the new IPS signature from FortiManager.
What is the most likely reason why FortiGate HQ-NGFW-1 does not recognize the new IPS signature?

A. FortiGate must enable rating for the FortiManager IP address, 192.168.1.120, in server list 1.

B. FortiManager and FortiGate have different IPS database versions.

C. The administrator must enable IPv6 connections for FortiGuard services on FortiManager.

D. The administrator must enable the fortiguard-anycast option to correctly download all signatures from the local FDS.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

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.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

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.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

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.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

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.

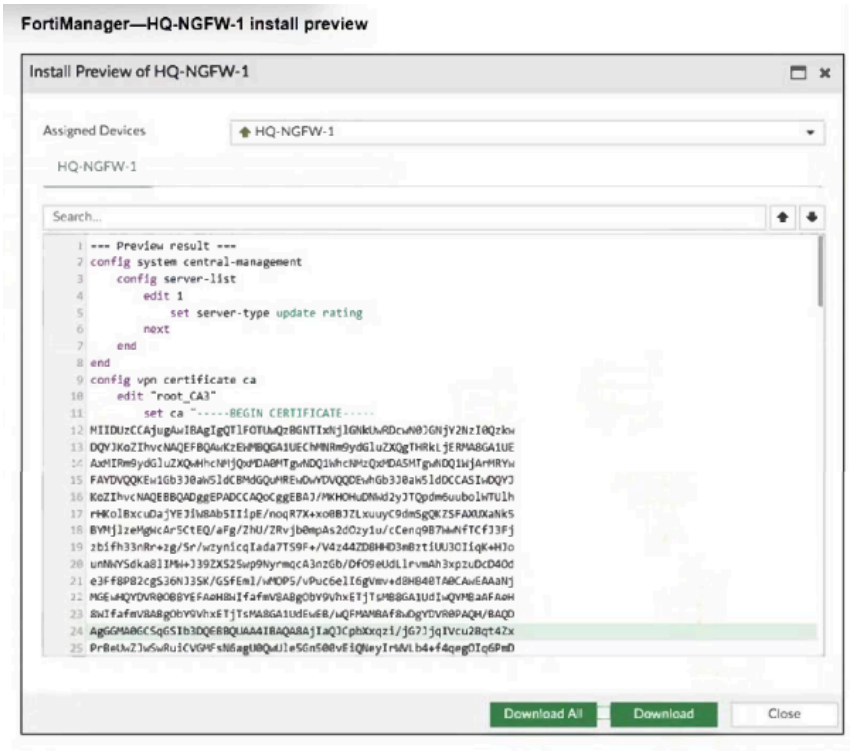
D. ADOM revisions save the current state of all policy packages and objects for an ADOM.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

Refer to the exhibit.



An administrator assigned a new policy package to FortiGate HQ-NGFW-1. In the installation preview, they noticed some settings they did not modify and are unsure about the changes.

Based on the exhibit, which two things will happen if they continue with the installation? (Choose two.)

A. FortiGate HQ-NGFW-1 can use FortiManager firmware templates to upgrade firmware and ratings.

B. FortiGate HQ-NGFW-1 can contact the FortiManager acting as FortiGuard Distribution Server (FDS) to download FortiGuard updates.

C. FortiGate HQ-NGFW-1 will use the root_CA3 certificate in firewall address objects or policies.

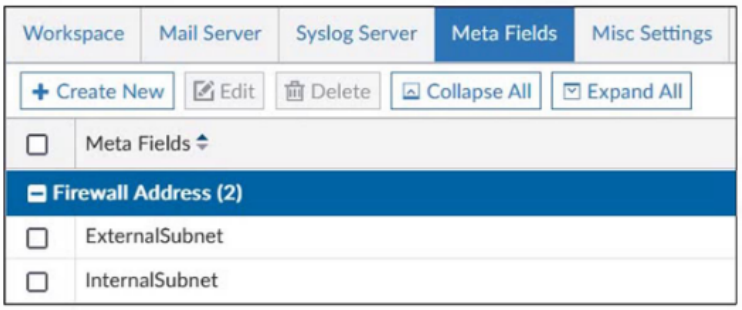
D. FortiManager will install the CA certificate named root_CA3 to authenticate FortiGate-to-FortiManager communication protocol (FGFM) tunnel connections with FortiGate HQ- NGFW-1.

Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

Refer to the exhibit.



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.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 1*

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.

Suggested Answer: *AC*

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 1*

The administrator uses FortiManager to push a CLI script using the Remote FortiGate Directly (via CLI) option to configure an IPsec VPN. However, when running the script, the administrator receives the following error: config vpn ipsec phase2-interface [parameter(s) invalid. detail: object mismatch]
What must the administrator do to resolve the script error and successfully apply the IPsec configuration?

A. Add the end command after finishing the IPsec phase 1-interface configuration block.

B. Use IPsec templates to deploy provisioning templates.

C. Add a second config vpn ipsec phase2-interface block without linking it to phase1.

D. Run the script using the policy package or ADOM database method.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!