PassQueen
a.k.a dumpsqueen.com

Fortinet NSE 5 - FortiManager 7.6 Administrator

Fortinet FCP_FMG_AD-7.6

Version Demo

Total Demo Questions: 8

Total Premium Questions: 83

Buy Premium PDF

https://passqueen.com

support@passqueen.com

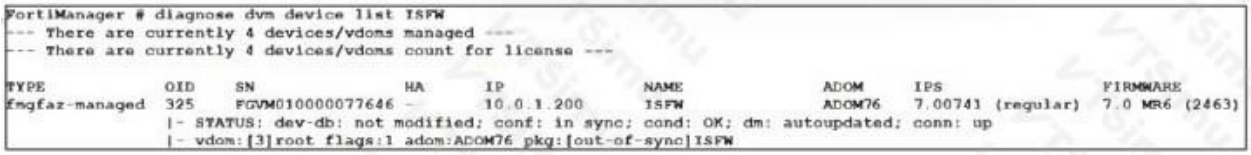
Topic Break Down

Topic	No. of Questions
Topic 1, Administration	15
Topic 2, Device registration	9
Topic 3, Device-level configuration and installation	7
Topic 4, Provisioning templates	5
Topic 5, Policy and objects	20
Topic 6, Global policy and ADOM policy packages	5
Topic 7, Scripts	8
Topic 8, FortiGuard services	3
Topic 9, Troubleshooting	4
Topic 10, High availability	5
Topic 11, Mix Questions	2
Total	83

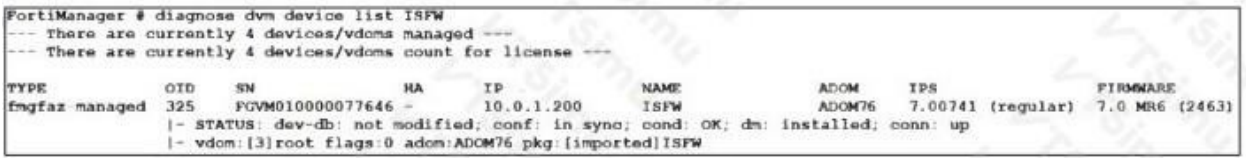
QUESTION NO: 1

Which output is displayed right after moving the ISFW device from one ADOM to another?

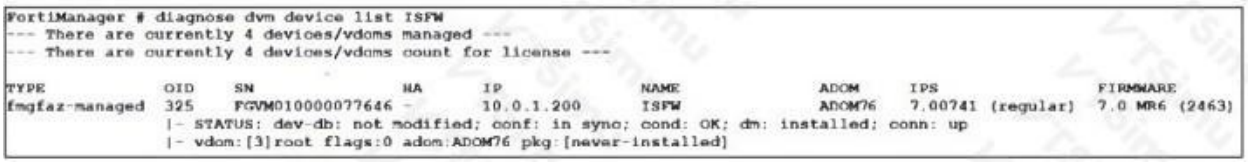
A)



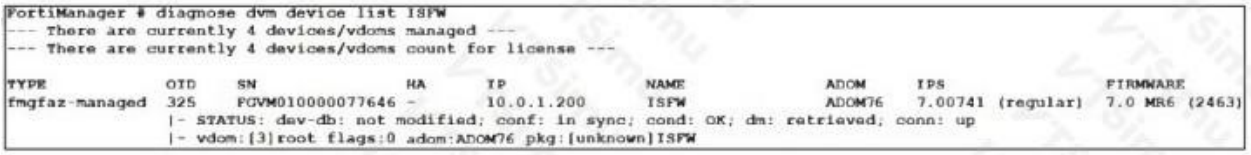
B)



C)



D)



A. Option A

B. Option B

C. Option C

D. Option D

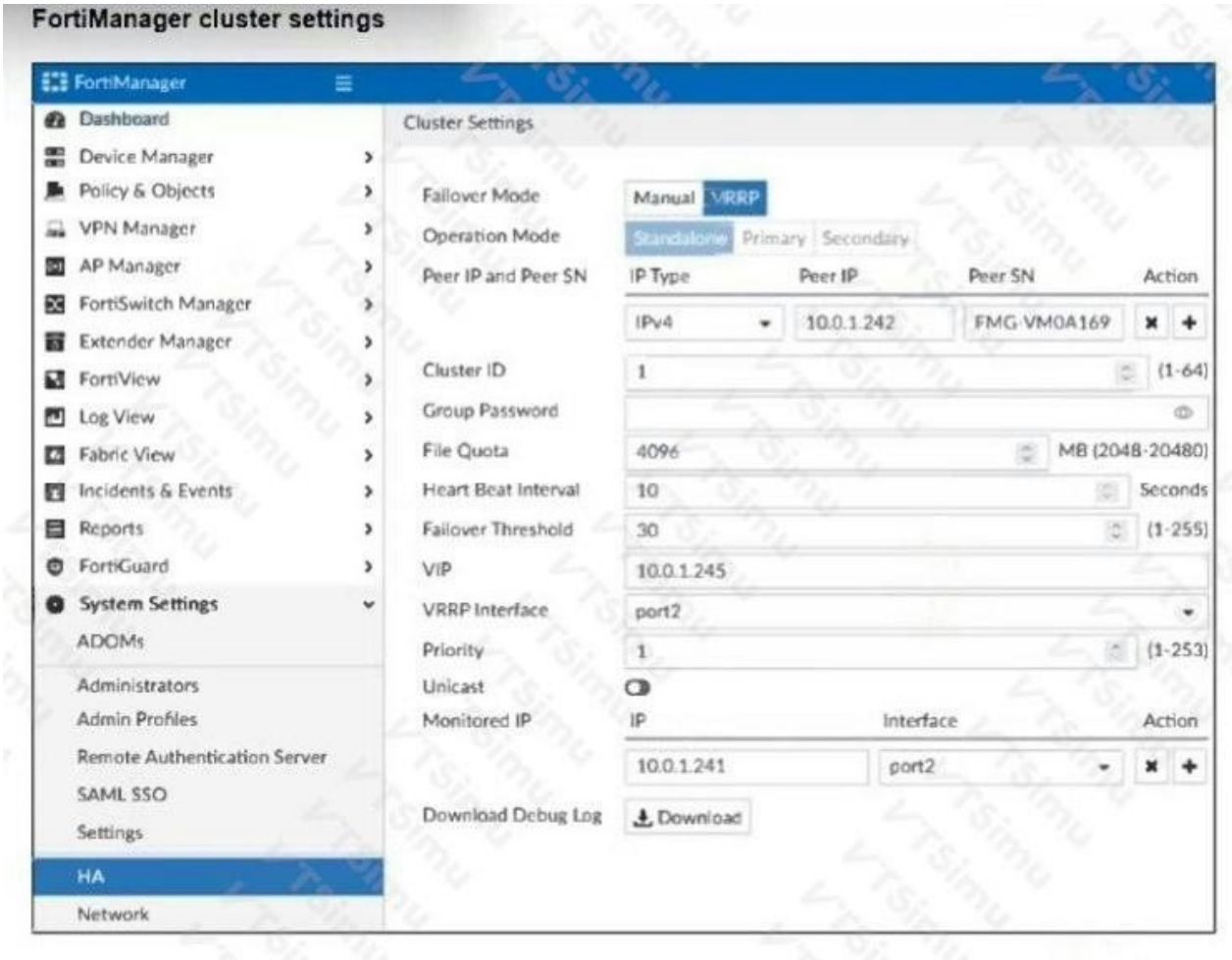
ANSWER: A D

Explanation:

The outputs represented by “Option A” and “Option D” are displayed immediately after the ISFW is moved because a FortiManager ADOM move changes the administrative domain that owns the device record and its associated management data. FortiManager must place the device into the destination ADOM context and reconcile the device configuration, policy-package assignment, and database state for that new ADOM. Consequently, the immediate post-move view can show the device under its newly selected ADOM while also indicating that further synchronization, configuration retrieval, or installation activity is required before the FortiManager database and the FortiGate are fully aligned.

This behavior is particularly important for an ISFW because the managed device can contain multiple VDOMs and policy objects whose management scope is governed by ADOM membership. Moving the device is therefore an administrative reorganization action, not an automatic confirmation that all managed settings are already synchronized in the destination ADOM. Administrators should verify the device status and perform the required retrieve, revision, and installation workflow from the new ADOM before treating the move as complete. Fortinet documents ADOM-based device management and device configuration synchronization in the FortiManager 7.6 Administration Guide and its FortiManager documentation portal.

QUESTION NO: 2



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: B

Explanation:

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.
is correct because FortiManager HA requires an administrator-directed role change when the active unit remains operational but loses a monitored interface. Interface monitoring detects that the primary no longer has the required network connectivity; however, maintaining service requires a healthy secondary with functional monitored interfaces to be made the active primary. Promoting that device establishes the correct active HA role and restores management availability through the healthy unit.

Rebooting the original primary after the role change lets it leave the active state and rejoin the HA cluster cleanly with updated peer information. This prevents the unit affected by the monitored-interface failure from remaining active or retaining stale HA peer state while the healthy device serves as primary. The process preserves the intended active-passive HA design: a reachable, healthy unit manages the FortiGate devices, while the repaired former primary can subsequently operate as a synchronized secondary.

Fortinet documents HA configuration, monitored interfaces, member roles, and HA recovery behavior in the FortiManager 7.6 Administration Guide. See also Fortinet's HA configuration technical tip for operational HA concepts.

QUESTION NO: 3

Which two statements describe FortiManager management of a FortiGate HA cluster? (Choose two.)

A. FortiManager installs policy package changes on the primary FortiGate unit.

B. The primary FortiGate synchronizes the applicable configuration to secondary units.

C. FortiManager must install the policy package separately on every secondary unit.

D. A secondary FortiGate unit is always the preferred target for device settings installation.

E. FortiManager converts each HA member into a separate ADOM automatically.

ANSWER: A B

Explanation:

FortiManager sends policy and configuration installation operations to the primary FortiGate unit. The primary is the active unit that accepts centralized management changes and maintains the active cluster configuration.

The primary FortiGate synchronizes the applicable configuration to secondary members by using the FortiGate HA synchronization mechanism. FortiManager does not need to independently install the same policy package on each secondary member of the cluster.

See the FortiManager 7.6 Administration Guide for managed-device and HA deployment information.

QUESTION NO: 4

An administrator starts an installation task for several FortiGate devices. The task completes with errors on one device.

Where can the administrator review the task output and the error details for the failed installation?

A. Task Monitor

B. Revision History

C. FortiGuard Distribution Server

D. Global ADOM Object Configurations

ANSWER: A

Explanation:

The administrator should review the task in Task Monitor. Task Monitor records FortiManager operations such as policy installation, device settings installation, script execution, configuration retrieval, and firmware tasks. The task details provide status and output information that can be used to identify the affected device and the reason for failure.

Reviewing the task result is the appropriate first troubleshooting step because it distinguishes device communication failures, validation errors, and FortiOS CLI errors from successful installation activity. See the FortiManager 7.6 Administration Guide for task monitoring and troubleshooting information.

QUESTION NO: 5

An administrator must create a restricted FortiManager account for a team that manages devices only in ADOM1.

Which two configurations are required? (Choose two.)

A. Assign an administrative profile with the required permissions.

B. Assign the administrator access to ADOM1.

C. Enable global ADOM access for the administrator.

D. Assign the administrator a device revision.

E. Create a separate policy package for the administrator.

ANSWER: A B

Explanation:

The administrator must assign an administrative profile that grants the required permissions, such as read-write access to the Policy & Objects and Device Manager areas. Administrative profiles define what functions an administrator can use in FortiManager.

The administrator must also assign the account access to ADOM1. ADOM assignment defines the management scope in which the administrator can perform the actions allowed by the administrative profile. An account with a suitable profile but no ADOM assignment cannot manage ADOM1.

For more information, see the FortiManager 7.6 Administration Guide.

QUESTION NO: 6

What allows FortiManager to run CLI scripts on FortiGate devices without prompting for SSH authentication each time?

A. FortiGate devices using the legacy login method.

B. The secure management tunnel between FortiManager and FortiGate devices.

C. The script using the Remote FortiGate Directly (via CLI) option.

D. The script on the FortiManager device database.

ANSWER: B

Explanation:

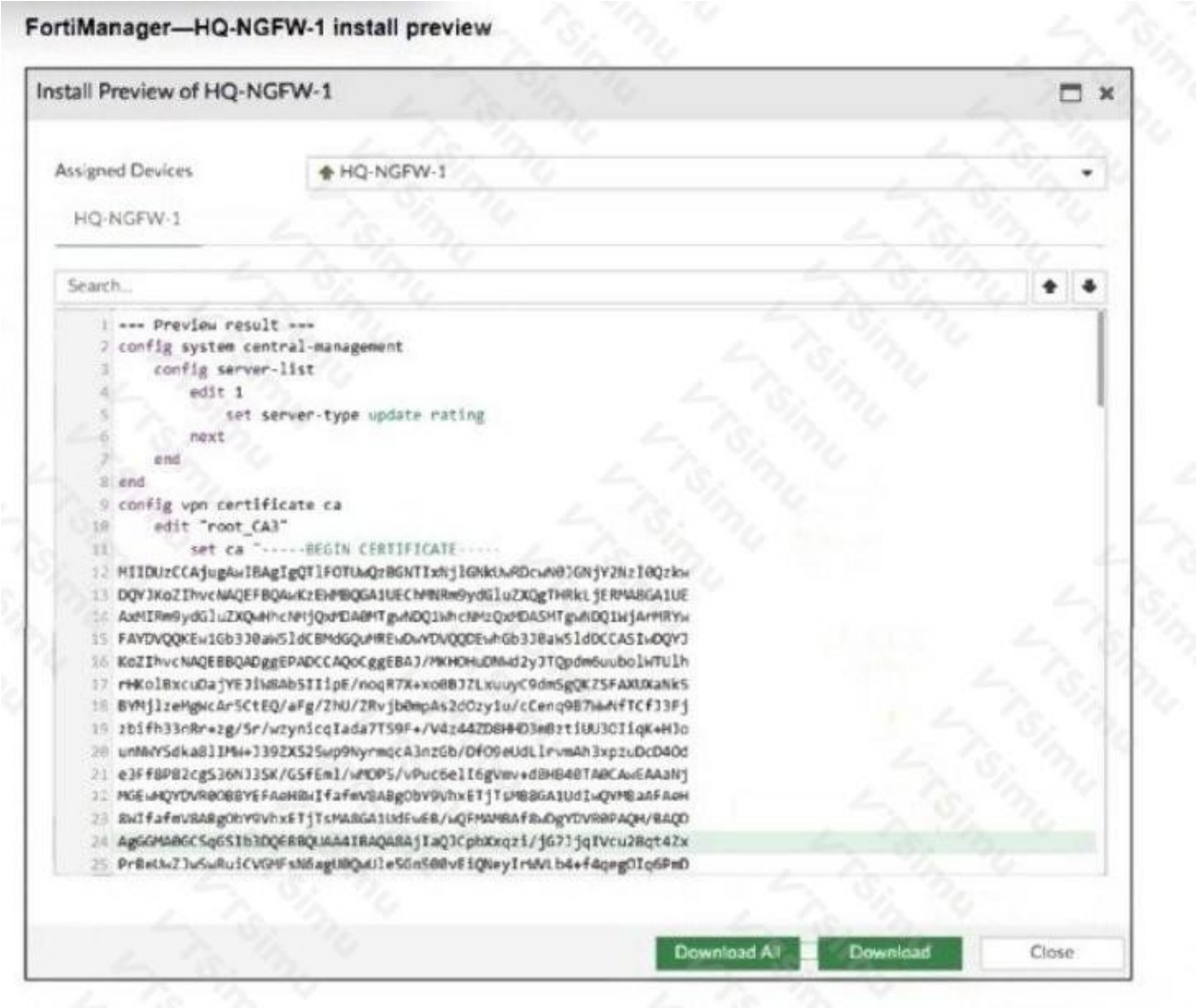
The secure management tunnel between FortiManager and FortiGate devices allows this behavior. After a FortiGate is authorized and managed by FortiManager, the two systems communicate through the Fortinet management protocol connection, commonly called the FGFM tunnel. This authenticated, encrypted management channel is established for centralized device administration and is reused for management operations rather than requiring FortiManager to create a separate interactive SSH connection for every task.

Consequently, when an administrator executes a CLI script from FortiManager against a managed FortiGate, FortiManager sends the script through its existing trusted management connection. The managed-device relationship has already established the required authentication and authorization context, enabling FortiManager to perform actions such as configuration installation, policy deployment, device database synchronization, and script execution without asking the administrator to supply FortiGate SSH credentials each time.

Fortinet documents CLI scripts as a FortiManager feature for executing commands on managed devices, and its device-management documentation describes the FortiManager–FortiGate management connection used for centralized administration. See the FortiManager 7.6 Administration Guide and the FortiGate 7.6 Administration Guide.

QUESTION NO: 7

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.

ANSWER: B C

Explanation:

FortiManager can install device-level settings and policy-package dependencies in addition to the firewall-policy rules that an administrator expects to deploy. The previewed FortiGuard configuration causes FortiGate HQ-NGFW-1 to use FortiManager as a FortiGuard Distribution Server (FDS). Consequently, the FortiGate can contact FortiManager for FortiGuard update content, allowing FortiManager to act as the local distribution point for services such as antivirus and IPS updates where that feature is configured.

The preview also includes the CA certificate object named `root_CA3`. Continuing the installation places that CA certificate on the managed FortiGate so it is available to configuration objects delivered with, or referenced by, the policy package. Certificate objects can be required by policy-related security configuration, such as inspection and authentication-related

settings, and FortiManager installs those dependent objects to ensure the package configuration can be used consistently on the FortiGate.

These results follow FortiManager's installation behavior: it calculates and deploys all relevant configuration changes, including policy-package objects and applicable device settings, rather than limiting the install to policy entries alone. See the FortiManager 7.6 Administration Guide and the FortiGate 7.6 Administration Guide.

QUESTION NO: 8

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:

Add and manage FortiAnalyzer from FortiManager. FortiAnalyzer is Fortinet's purpose-built logging, analytics, reporting, and long-term log-storage platform. It is designed to receive and process the high event volumes generated by FortiGate devices, index those events for efficient search and investigation, and retain data according to configured storage and retention policies. Using a dedicated FortiAnalyzer allows logging workloads to be scaled separately from the centralized configuration-management functions performed by FortiManager.

FortiManager can centrally authorize and manage FortiAnalyzer integration, including associating managed FortiGate devices with an appropriate FortiAnalyzer. This provides an operationally efficient division of responsibilities: FortiManager manages devices, policies, objects, and administrative workflows, while FortiAnalyzer handles log ingestion, analysis, FortiView-style visibility, event investigation, and report generation. This architecture is especially appropriate when the environment has many managed devices or substantial traffic and security-event activity, because log processing and retention do not compete with configuration-management resources. Fortinet documents FortiAnalyzer as the centralized logging and reporting component and documents its integration with FortiManager in the respective product documentation: FortiAnalyzer documentation and FortiManager documentation.