TestpassportQ&A

Higher Quality Better Service!

We offer free update service for one year

Http://www.testpassport.com

Exam : **NSE6_FMG_AD-7.6**

Title : Fortinet NSE 6 - FortiManager 7.6 Administrator

Version : DEMO

1.Scenario-based Analysis (FortiManager with FortiAnalyzer Features)
Scenario: An administrator has enabled FortiAnalyzer features on a FortiManager device to provide centralized logging. A new Administrative Domain (ADOM) named 'Branch_Security' is created to manage a group of branch FortiGate devices.
What specific storage configuration must the administrator perform for this new ADOM that is not required when FortiManager operates strictly as a management-only platform?
A. The administrator must manually synchronize the centralized device revision history database with the newly allocated logging storage volume.
B. The administrator must provision a dedicated offline model device to temporarily buffer the incoming traffic logs during periods of high network congestion.
C. The administrator must strictly configure dedicated disk quotas for analytical and archive logs and define a specific log retention data policy.
D. The administrator must carefully configure a dedicated management tunnel exclusively for securely transmitting the syslog traffic from branch devices.
Answer: C
Explanation:
This scenario tests your understanding of FortiManager features as outlined in the blueprint. When FortiManager has FortiAnalyzer features enabled, it acts as a syslog receiver and log analyzer. This natively requires the administrator to configure data policies and allocate specific disk space quotas (divided into Analytical and Archive storage) for every newly created ADOM to manage log retention. This specific storage allocation step is entirely not applicable when the FortiManager is utilized purely for centralized configuration management without the logging features enabled.

2.Multiple Choice (API HTTP Response Codes)
A DevSecOps team is testing a Python automation script that utilizes the FortiManager REST API to automatically deploy firewall policy packages. During execution, the script receives an HTTP 403 response code directly from the FortiManager appliance.
Which two statements accurately describe the potential causes for this specific HTTP response code? (Choose two.)
A. The requested API endpoint URL is formatted incorrectly, or the specified target resource does not exist in the active database.
B. The provided authentication session token is missing from the request payload or has already expired due to session timeout.
C. The targeted administrative domain is currently locked by another administrator utilizing the standard workspace mode feature.
D. The administrative profile assigned to the API user lacks the required read and write permissions for the requested endpoint.
Answer: B, D
Explanation:
This question evaluates your knowledge of the FortiManager API integration tasks. The FortiManager JSON-RPC API relies heavily on standard HTTP status codes. An HTTP 403 (Forbidden) code strictly indicates an authentication or authorization failure. The FortiManager understood the request, but it refuses to authorize the specific action. This occurs when the session token is missing or expired (Option B), or when the authenticated user profile does not have sufficient privileges to execute the action on the

requested endpoint (Option D). An incorrect URL or missing resource would generate a 404 Not Found (Option A). A workspace lock typically returns a 200 OK accompanied by an internal JSON error code indicating the locked status, not an HTTP 403 (Option C).

3.Scenario-based Analysis (Concurrent ADOM Access - Workspace Mode)
Scenario: A FortiManager appliance is configured with standard workspace mode enabled globally to control concurrent access. Administrator A logs in and locks the 'DataCenter' ADOM to implement complex firewall policy modifications. At the same time, Administrator B logs in and attempts to access the identical 'DataCenter' ADOM to investigate an urgent routing issue.
How does FortiManager handle Administrator B's access attempt in this specific concurrent scenario?
A. Administrator B is successfully permitted to enter the ADOM and view configurations, but their session is strictly limited to a read-only state.
B. Administrator B is completely denied entry into the ADOM and receives an error message indicating that the domain is currently locked.
C. Administrator B is prompted to enter super_admin credentials to forcefully override the lock and merge their pending configuration changes.
D. Administrator B can successfully access the ADOM and modify the routing table because the workspace lock strictly applies to firewall policies.
Answer: A
Explanation:
This scenario explores the concurrency controls of standard workspace mode. The primary purpose of standard workspace mode is to prevent concurrent configuration changes that could corrupt the management database. When an administrator locks an ADOM, they acquire exclusive read-write access to that entire domain, which includes both the Policy & Objects database and the Device Manager database. However, FortiManager does not completely block other administrators from entering the locked ADOM. Administrator B can enter the 'DataCenter' ADOM and view configurations, but their access is restricted to read-only until the lock is formally released by Administrator.
A. Therefore, they cannot modify the routing table or any other settings.

4.Single Choice (ADOM Upgrades)
A FortiManager administrator needs to upgrade an Administrative Domain (ADOM) from version 7.2 to version 7.4. The target ADOM currently manages a mix of devices: fifteen FortiGate appliances running FortiOS 7.2 and five newer appliances running FortiOS 7.4.
What is the mandatory operational prerequisite to successfully execute this ADOM database version upgrade?
A. The administrator must downgrade the system-level global ADOM to version 7.2 to properly maintain backward compatibility during the upgrade.
B. The FortiManager must temporarily place all assigned devices into an offline state to completely prevent configuration synchronization errors.
C. The administrator must manually execute a database rebuild script via CLI to convert all legacy configuration objects to the new 7.4 format.
D. The firmware versions of all assigned managed devices must already be successfully upgraded to a version equal to or higher than version 7.4.
Answer: D

Explanation:
This question tests the fundamental logic of ADOM upgrades. An ADOM database version strictly defines the configuration syntax and features that FortiManager utilizes to compile and push policies to managed devices. FortiManager inherently enforces a strict dependency rule: an ADOM cannot be upgraded to a higher version if any registered device within that ADOM is running a firmware version lower than the target ADOM version. If the ADOM were upgraded first, FortiManager would attempt to push 7.4 syntax to 7.2 devices, causing critical installation failures and database corruption. Therefore, all physical devices must be upgraded to at least 7.4 before the ADOM upgrade operation is permitted.

5.Single Choice (External Validation of Nonlocal Logins)
An enterprise integrates FortiManager with a centralized RADIUS server for administrator authentication. The security team wants to dynamically assign specific administrative privileges to remote users based on their RADIUS group, avoiding the need to manually create individual local accounts on the FortiManager appliance.
Which specific configuration component is strictly required on FortiManager to successfully implement this authentication architecture?
A. The administrator must explicitly disable local authentication and configure FortiManager to strictly synchronize its database with the RADIUS server.
B. The administrator must manually execute a CLI script to permanently bind the default super_admin profile to all incoming RADIUS authentication requests.
C. The administrator must correctly configure a wildcard administrator account and properly map the RADIUS vendor-specific attribute to a local access profile.
D. The administrator must import the RADIUS server digital certificate into FortiManager and enable Single Sign-On utilizing the standard SAML identity provider.
Answer: C
Explanation:
This evaluates the "External validation of nonlocal administrator logins" blueprint topic. When utilizing external authentication servers (like RADIUS or TACACS+) and actively avoiding the creation of local accounts for every single user, FortiManager utilizes a "Wildcard" administrator account (often denoted by a *). The wildcard account is configured to systematically query the external server. To assign the correct privileges dynamically, the RADIUS server must be configured to return a Vendor-Specific Attribute (VSA) upon successful authentication. FortiManager reads this exact VSA string and matches it to a predefined local Administrator Profile (e.g., 'Super_Admin' or 'Read_Only'), instantly granting the remote user the appropriate level of access.
Practice Set 1: Administration (Continued)