Fortinet

NSE6_FSR-7.3 Exam

Fortinet NSE 6 - FortiSOAR 7.3 Administrator

Questions & Answers
Demo

Version: 4.0

Question: 1

Several users have informed you that the FortiSOAR GUI Is not reachable. When troubleshooting, which step should you take first?

A. Enter the csadm license --show-details command to check if there is a duplicate license.
B. Enter the csadm services --restart ngiax command to restart only the Nginx process.
C. Enter the systemct1 status nginx command to gather more information.
D. Review the connecters.log file to see what is happening to the HTTPS connections.

Answer: C

Explanation:

When troubleshooting the issue of the FortiSOAR GUI not being reachable, the first step should be to check the status of the nginx service, which is responsible for managing web requests. Using the command systemctl status nginx will provide information on whether the service is running and any potential issues or errors related to it. This approach is more efficient as it directly addresses the service responsible for the web interface, making it possible to diagnose and resolve common issues such as service failure, configuration errors, or connectivity problems.

Question: 2

What are two system-level logs that can be purged using application configuration? (Choose two.)

A. Connector logs
B. Reporting logs
C. Audit togs
D. Executed Playbook logs

Answer: C, D

Explanation:

In FortiSOAR, system-level logs that can be purged include both "Audit logs" and "Executed Playbook logs." These types of logs can be configured to be purged periodically to free up storage space and ensure that unnecessary logs do not impact system performance. The application configuration allows administrators to schedule automatic purges, which can be especially useful in high-activity environments where log data accumulates quickly. Purging these logs helps maintain a cleaner and more efficient system.

Question: 3

The Create Record and Update Record steps are categorized under which playbook step'

A. Evaluate
B. Execute
C. Core
D. Reference

Answer: C

Explanation:

In FortiSOAR playbooks, the "Create Record" and "Update Record" steps are categorized under the "Core" category of playbook steps. Core steps are essential actions that are frequently used in playbooks to interact with records in the FortiSOAR database. They include fundamental operations such as creating, reading, updating, or deleting records within modules. These steps are crucial for the automation of tasks such as data management, where playbooks need to create new entries or update existing data as part of incident response workflows.

Question: 4

When configuring the system proxy on FortiSOAR. which two URLs should be accessible from the proxy server? (Choose two.)

A. https://fortiguard.coin
B. https: //licensing, fortinet .net
C. https://iepo.fortisoar.fcrtinet.ccm
D. https://globalupdate.fortinet.net

Answer: C, D

Explanation:

When configuring the system proxy for FortiSOAR, it is essential to ensure connectivity to certain URLs to maintain system updates and licensing. For FortiSOAR, access to https://iepo.fortisoar.fortinet.com is required for incident enrichment and analysis, while https://globalupdate.fortinet.net is necessary for global updates to keep the system up-to-date with the latest threat information. These connections allow FortiSOAR to communicate with Fortinet's servers to fetch updated threat intelligence and system updates, which are critical for the operational effectiveness of FortiSOAR.

Question: 5

When configuring an HA cluster with an externalized PostgreSQL database, which two tiles on the database server need to be configured to trust all FortiSOAR nodes' incoming connections? (Choose two.)

A. pg_hba.conf
B. db_external_config.yml.

C. postgreaq1.conf
D. db_config.yml

Answer: A, C

Explanation:

In a FortiSOAR High Availability (HA) cluster setup with an externalized PostgreSQL database, it is necessary to configure the database server to allow incoming connections from all FortiSOAR nodes. This configuration involves modifying the pg_hba.conf file to set up host-based authentication and control which IP addresses can connect. The postgresql.conf file must also be adjusted to enable listening on all necessary IP addresses, which is critical for FortiSOAR nodes to connect to the database server securely and reliably. Together, these configurations ensure that all FortiSOAR nodes can access the database, facilitating effective HA functionality.