Vendor: Fortinet

Exam Code: NSE6_FSR-7.3

Exam Name: Fortinet NSE 6 - FortiSOAR 7.3 Administrator

Version: DEMO

QUESTION 1
An administrator is issuing the following command on a node trying to join a FortiSOAR duster as a standby:

csadm ha join-cluster --status active --role secondary --primary-node 10.0.1.160

The node fails to join the cluster. What is the issue?

A. The role value should be worker.
B. The primary node needs to be resolvable via FQDN.
C. The IP address should be for secondary-node Instead of primary-node.
D. The status value should be passive.

Answer: D
Explanation:
When joining a FortiSOAR cluster as a standby node, the correct status value should be passive. Using active would imply that the node is trying to join as an active node, which could cause conflicts in the cluster setup. In FortiSOAR, standby nodes must be set as passive to ensure they are recognized correctly and to avoid conflicts with the primary node or other active nodes within the cluster. Therefore, setting the status to passive will resolve the issue and allow the node to join the cluster as intended.

QUESTION 2
When deleting a user account on FortiSOAR, you must enter the user ID in which file on FortiSOAR?

A. userDelete.txt.
B. config_yml
C. scripts
D. usersToDelete.txt

Answer: D
Explanation:
When deleting a user account in FortiSOAR, the user ID must be entered into the usersToDelete.txt file. This file is specifically used to list users that are marked for deletion. Once the user IDs are listed in this file, the system can process the deletion of these accounts as part of its user management operations. This method ensures that only specified users are deleted, as referenced in FortiSOAR's administrative controls.

QUESTION 3
Which two statements about upgrading a FortiSOAR HA cluster are true7 (Choose two.)

A. Nodes can be upgraded while the primary node or secondary node are in the HA cluster.
B. Upgrading a FortiSOAR HA cluster requires no downtime.
C. The upgrade procedure for an active-active cluster and an active-passive cluster are the same.
D. It is recommended that the passive secondary node be upgraded first, and then the active primary node.

Answer: CD
Explanation:
Upgrading a FortiSOAR HA cluster follows the same procedure regardless of whether it is configured in an active-active or active-passive setup. The process generally involves upgrading

one node at a time to minimize service disruption. Best practices recommend upgrading the passive secondary node first before moving to the active primary node. This sequence helps maintain cluster stability and ensures that at least one node remains operational during the upgrade.

QUESTION 4
Which SMS vendor does FortiSOAR support for two-factor authentication?

A. Twilio
B. Google Authenticator
C. 2factor
D. Telesign

Answer: D
Explanation:
For two-factor authentication (2FA) via SMS, FortiSOAR supports integration with Telesign. This vendor provides SMS-based 2FA services, enabling FortiSOAR to leverage Telesign's API for sending verification codes as part of its security features. Telesign's service is compatible with FortiSOAR, ensuring secure user authentication when accessing the platform or certain features.

QUESTION 5
Which three actions can be performed from within the war room? (Choose three)

A. View graphical representation of all records linked to an incident in the Artifacts lab
B. Change the room's status to Escalated to enforce hourly updates.
C. Investigate issues by tagging results as evidence.
D. Use the Task Manager tab to create, manage, assign, and track tasks.
E. Integrate a third-party instant messenger directly into the collaboration workspace.

Answer: ACD
Explanation:
In FortiSOAR's War Room, users can perform several actions to manage incidents effectively. They can view a graphical representation of records linked to an incident in the Artifacts lab, which helps visualize connections and dependencies. Additionally, the War Room supports tagging investigation results as evidence, allowing for a structured approach to incident documentation. Users can also manage tasks via the Task Manager tab, facilitating task creation, assignment, and tracking within the incident response workflow.

QUESTION 6
Which two statements about appliance users are true? (Choose two.)

A. Appliance users do not have a login ID and do not add to the license count.
B. Appliance users represent non-human users.
C. Appliance users use two-factor authentication for messages sent to the API.
D. Appliance users use time-expiring tokens for primary authentication.

Answer: AB
Explanation:
In FortiSOAR, appliance users are accounts that represent non-human entities, such as system processes or integrations. These users do not require login IDs and therefore do not contribute to the licensing user count. Appliance users are configured for backend tasks or to interact with

external systems, enabling automated processes without consuming standard user licenses. This approach optimizes system resources and keeps licensing costs manageable.

QUESTION 7
Which two statements about Elasticsearch are true? (Choose two.)

A. Elasticsearch allows you to store, search, and analyze huge volumes of data quickly. In near real time, and return answers in milliseconds.
B. To change the location of your Elasticsearch instance from the local instance to a remote location, you must update the falcon. conf file.
C. The minimum version of the Elasticsearch cluster must be 6.0.2. if you want to externalize the Elasticsearch data.
D. The global search mechanism in FortiSOAR leverages an Elasticsearch database to achieve rapid, efficient searches across the entire record system.

Answer: AD
Explanation:
Elasticsearch in FortiSOAR is used for its robust data handling capabilities, allowing rapid storage, searching, and analysis of vast amounts of data in near real-time. Its integration with FortiSOAR's global search enables efficient querying across all records, providing quick response times and a seamless user experience. The Elasticsearch database is crucial for handling extensive datasets and delivering swift search results, making it integral to FortiSOAR's performance and data management capabilities.

QUESTION 8
Which CLI command will not work when the PostgreSQL database on FortiSOAR is externalized?

A. csada ha firedrill
B. csadmin ha show-health --all-nodes
C. csadm ha takeover
D. csadm ha export-conf

Answer: A
Explanation:
When the PostgreSQL database is externalized in FortiSOAR, certain HA-related CLI commands become inapplicable. Specifically, the csada ha firedrill command, which is used to test the integrity of the HA cluster by simulating failures, is not applicable in scenarios where the database is managed outside FortiSOAR. Externalizing the database changes how FortiSOAR manages database connections, making some internal commands like firedrill redundant.

Thank You for Trying Our Product

Passleader Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.passleader.com/all-products.html

10% Discount Coupon Code: **ASTR14**