Prepare Smart for Success Free Fortinet NSE6_FSR_AN-7.6 Exam Questions and Answers

Ready to pass faster? Grab free and updated Fortinet NSE 6 - FortiSOAR 7.6 Analyst exam PDF questions now. Get authentic NSE6_FSR_AN-7.6 dumps packed with verified answers and secure your certification success with PrepBolt NSE6_FSR_AN-7.6 exam pdf questions and answers.

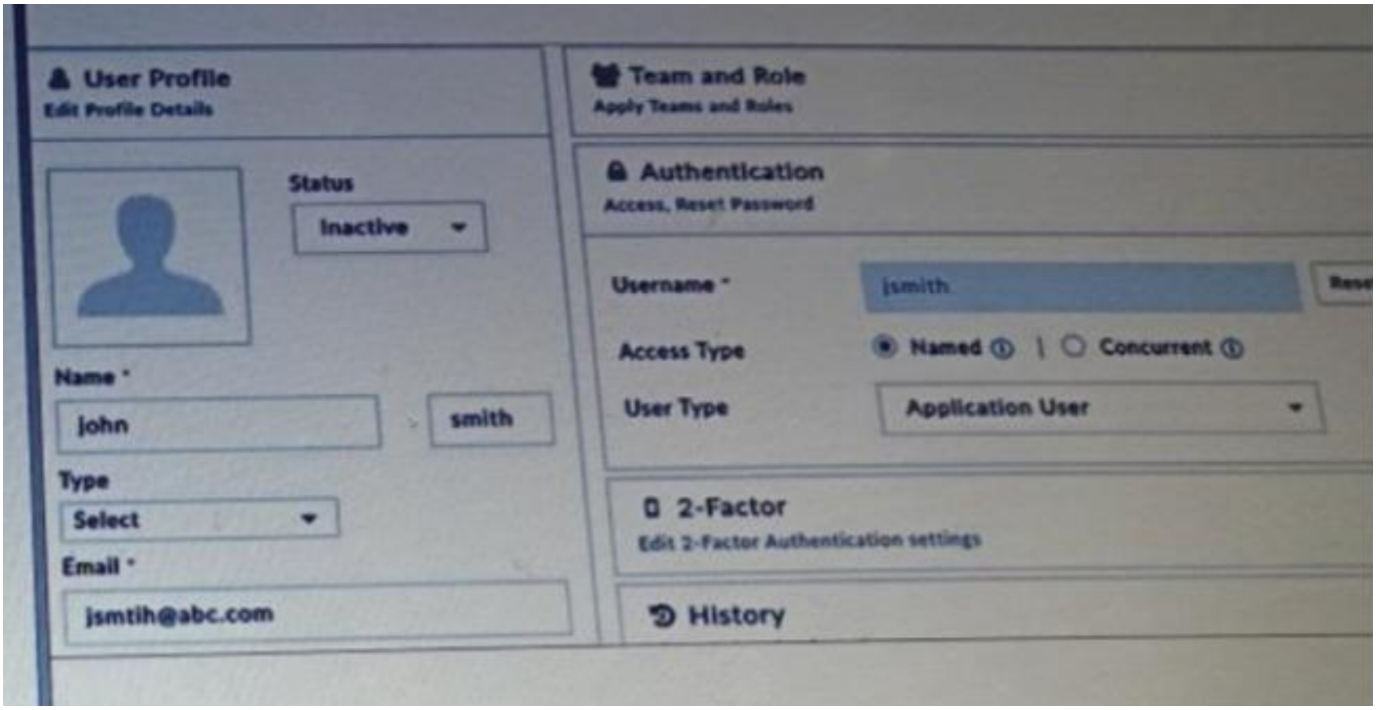
Thank you for Downloading NSE6_FSR_AN-7.6 exam PDF Demo

https://prepbolt.com/NSE6_FSR_AN-7.6.html

Question 1

Question Type: MultipleChoice

Refer to the exhibit.



Why is this user's account inactive? (Choose one answer)

Options:

A- The user has exceeded the maximum number of authentication tries for a one-hour period.
B- The user does not have a valid email ID for the account.
C- The user has not reset the password for the account.
D- The user has exceeded the maximum number of allowed user accounts.

Answer:

D

Explanation:

Comprehensive and Detailed Explanation From FortiSOAR 7.3 Exact Extract study guide:

According to the FortiSOAR 7.3 Administration and Deployment Guides, specifically in the 'Licensing FortiSOAR' and 'Security Management' sections:

Licensing Enforcement: FortiSOAR strictly enforces the number of active users based on the installed license. The license specifies the maximum number of active users allowed in the system at any given

point in time.

User Status (Active vs. Inactive): When the number of active users reaches the limit defined by the license, any additional users created or imported will be set to an Inactive status by default. An administrator cannot change their status to 'Active' until an existing active user is deactivated or deleted, or the license is upgraded to support more users.

Locked Status (Option A): It is important to distinguish between 'Inactive' and 'Locked.' Users become temporarily locked out of FortiSOAR when they exceed the configured number of authentication attempts (defaulting to 5 times) within a specific period. A locked user profile will typically display a 'Locked' indicator or a checkbox to 'Unlock' rather than a simple 'Inactive' status.

Other Options: While an email ID is required for account creation, its validity does not automatically trigger an 'Inactive' status (Option B). Similarly, a required password reset (Option C) forces a password change upon login but does not disable the account.

Question 2

Question Type: MultipleChoice

Which three features are installed with the FortiSOAR Incidence Response Content Pack? (Choose three answers)

Options:

A- System monitoring connectors1
B- Sample data for playbooks
C- Sample alerts and incidents
D- System playbooks2
E- SLA template module

Answer:

B, C, D

Explanation:

Comprehensive and Detailed Explanation From FortiSOAR 7.3 Exact Extract study guide:

The FortiSOAR Incidence Response Content Pack (which is essentially the predecessor or foundational component of the SOAR Framework Solution Pack in version 7.3) is designed to provide users with an immediate, functional environment. According to the FortiSOAR 7.3 Administration Guide and Content Hub documentation:

Sample Alerts and Incidents (C): The content pack includes a set of demo records.3 Upon installation and clicking the 'Demo IR Records' button, the system populates the Alerts and Incidents modules with pre-configured samples, including associated indicators and assets, to demonstrate how records are handled.4

System Playbooks (D): It installs a comprehensive collection of 'out-of-the-box' (OOB) playbooks. These include system-level playbooks used for triaging, indicator extraction, and managing standard record lifecycles (such as auto-populating dates when a record is closed).5

Sample Data for Playbooks (B): Along with the records themselves, the pack includes simulation and training data (often referred to as 'Playbook Samples' or 'Mock Data').6 This allows administrators to test playbook logic and workflows without requiring live feeds from third-party security tools.

Why other options are incorrect:

System monitoring connectors (A): While the pack may configure some basic internal connectors (like the Code Snippet connector), 'system monitoring connectors' are generally standalone integrations or part of specific device solution packs rather than the core IR pack.

SLA template module (E): Although the pack includes playbooks that manage SLAs (calculating response and resolution times), the 'SLA Management' or 'SLA Template' capability is often categorized as an additional module or handled via the Module Editor, rather than being a specific 'feature' installed solely by the IR pack.

Question 3

Question Type: MultipleChoice

Which statement about licensing on FortiSOAR is true? (Choose one answer)

Options:

A- A FortiSOAR VM with a perpetual license needs access to update.fortiguard.net.1
B- The subscription license requires connectivity to globalupdate.fortinet.net to retrieve information.
C- The perpetual trial license has a limit on actions per day but no limit on user count.2
D- The evaluation license has an expiry date but no limit on user count.3

Answer:

B

Explanation:

Comprehensive and Detailed Explanation From FortiSOAR 7.3 Exact Extract study guide:

According to the FortiSOAR 7.3 Deployment and Administration Guide under the 'Licensing FortiSOAR' section:

Connectivity Requirements: For the FortiSOAR license deployment and validation process to succeed, the instance must have outbound connectivity to https://globalupdate.fortinet.net. This URL is specifically used by the FortiSOAR license manager to fetch entitlements, verify the subscription status, and retrieve product information from the Fortinet licensing servers. If this connectivity is blocked (and a FortiManager is not being used as a local FDN proxy), the license deployment will fail.4

License Limits: Every FortiSOAR license---whether Perpetual, Subscription, or Trial---strictly enforces a maximum number of active users (concurrent or named) and often a limit on the number of automation actions per day.5

Perpetual Trial Licenses (often called 'Free Trial') are restricted to a specific user count (typically 2 or 3) and a daily action limit (e.g., 200 or 1000 actions). Therefore, options C and D are incorrect as they suggest 'no limit on user count.'

URL Clarification: While update.fortiguard.net is a common Fortinet endpoint for security signatures (IPS/AV), FortiSOAR's specific licensing and entitlement communication is directed to the globalupdate.fortinet.net service.

Question 4

Question Type: MultipleChoice

What two permissions must you assign to a user to allow the purge of audit logs for all users? (Choose two answers)

Options:

A- Delete permission on the Security module
B- Delete permission on the Audit Log Activities module
C- Delete permission on the People module
D- Delete permission on the Users module

Answer:

A, B

Explanation:

Comprehensive and Detailed Explanation From FortiSOAR 7.3 Exact Extract study guide:

According to the FortiSOAR 7.3 Administration Guide under the 'Audit Logs' and 'Role-Based Access Control (RBAC)' sections, managing the lifecycle of system logs requires elevated administrative privileges.

To perform a manual purge of audit logs, the system validates permissions across two specific areas:

Audit Log Activities Module: The user must have Delete permissions on this specific module because it is the repository where the actual log records are stored. Without 'Delete' rights here, the application cannot remove the database entries.

Security Module: Because the purging of audit logs is a sensitive security operation that affects the system's accountability trail, FortiSOAR requires the Delete permission on the Security module. This acts as a secondary administrative guardrail to ensure only authorized security administrators can permanently remove audit trails.

Permissions on the People or Users modules (Options C and D) are used for managing user profiles and account attributes, but they do not grant the authority to manipulate system-level audit databases.

Question 5

Question Type: MultipleChoice

Which two roles are default roles configured on FortiSOAR? (Choose two answers)

Options:

A- T1 Analyst
B- T3 Analyst
C- FortiSOAR Agent
D- Connector Administrator

Answer:

A, D

Explanation:

Comprehensive and Detailed Explanation From FortiSOAR 7.3 Exact Extract study guide:

FortiSOAR comes with several pre-defined (out-of-the-box) roles designed to align with common Security Operations Center (SOC) functions. According to the FortiSOAR 7.3 Administration Guide

under the 'Security Management' section:

T1 Analyst (Tier 1): This role is a default configuration intended for front-line analysts who perform initial triaging of alerts and basic incident response tasks.

Connector Administrator: This is a specialized default role that grants permissions specifically for configuring, updating, and managing the lifecycle of connectors within the environment.

While FortiSOAR is highly customizable and allows for the creation of T2 or T3 roles, they are not always present as specific 'default' named roles in the same way the T1 Analyst is across all base installations. Furthermore, 'FortiSOAR Agent' refers to a technical component or a deployment architecture rather than a standard user RBAC (Role-Based Access Control) role. Other common default roles include Security Administrator, Application Administrator, and Full Access.

Question 6

Question Type: MultipleChoice

Select two statements that are true about FortiSOAR themes.

(Choose two.)

Options:

A- There are three theme options available: Dark, Light, and Sky.
B- Non-administrator users can change the theme by editing their user profile.
C- FortiSOAR theme can be configured to apply to all users on the system.
D- Selecting Revert Theme allows the user to revert the user profile theme.

Answer:

B, C

Question 7

Question Type: MultipleChoice

View the exhibit:

What does the command output mean?

```
root@fortisoar ~]# csadm db --check-connection
The file db_external_config.yml does not exist. Failed to connect the instance.
[root@fortisoar ~]#
```

Options:

A- The configuration to enable database externalization has not been completed.
B- The local PostgreSQL database is disabled on the FortiSOAR instance.
C- The local PostgreSQL database is configured on the FortiSOAR instance.
D- There is no connectivity between the PostgreSQL databases of the primary and secondary FortiSOAR instances.

Answer:

A

Question 8

Question Type: MultipleChoice

Which two system monitoring reports are available on the System Monitoring widget?

(Choose two.)

Options:

A- RAM Usage
B- CPU Usage
C- Service Status
D- Playbook Health Status

Answer:

B, C

Question 9

Question Type: MultipleChoice

What are two use cases for configuring a FortiSOAR HA cluster?

(Choose two.)

Options:

A- Disaster recovery
B- Multi-tenancy
C- Data externalization
D- Scaling

Answer:

A, D

Thank You for trying NSE6_FSR_AN-7.6 PDF Demo

To try our NSE6_FSR_AN-7.6 practice exam software visit link below

https://prepbolt.com/NSE6_FSR_AN-7.6.html

Start Your NSE6_FSR_AN-7.6 Preparation

Use Coupon “SAVE50” for extra 50% discount on the purchase of Practice Test Software. Test your NSE6_FSR_AN-7.6 preparation with actual exam questions.