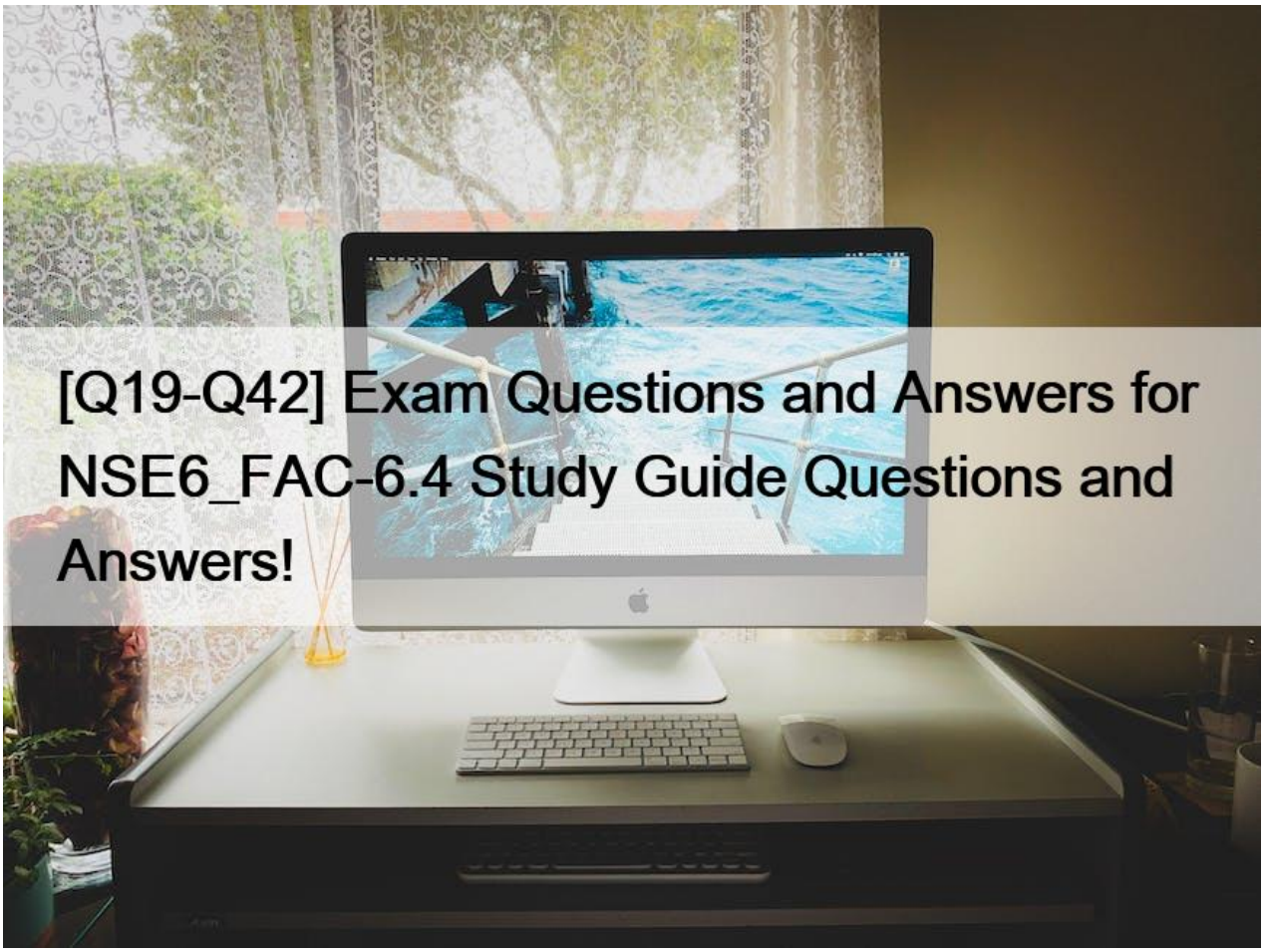
[Q19-Q42 Exam Questions and Answers for NSE6_FAC-6.4 Study Guide Questions and Answers!



Exam Questions and Answers for NSE6_FAC-6.4 Study Guide Questions and Answers! Fortinet NSE 6 - FortiAuthenticator 6.4 Certification Sample Questions and Practice Exam QUESTION 19

A system administrator wants to integrate FortiAuthenticator with an existing identity management system with the goal of authenticating and deauthenticating users into FSSO.

What feature does FortiAuthenticator offer for this type of integration?
* The ability to import and export users from CSV files
* RADIUS learning mode for migrating users
* REST API
* SNMP monitoring and traps

REST API is a feature that allows FortiAuthenticator to integrate with an existing identity management system with the goal of authenticating and deauthenticating users into FSSO. REST API stands for Representational State Transfer Application Programming Interface, which is a method of exchanging data between different systems using HTTP requests and responses. FortiAuthenticator provides a REST API that can be used by external systems to perform various actions, such as creating, updating, deleting, or querying users and groups, or sending FSSO logon or logoff events.

QUESTION 20

You want to monitor FortiAuthenticator system information and receive FortiAuthenticator traps through SNMP.

Which two configurations must be performed after enabling SNMP access on the FortiAuthenticator interface? (Choose two)
* Enable logging services
* Set the tresholds to trigger SNMP traps
* Upload management information base (MIB) files to SNMP server
* Associate an ASN, 1 mapping rule to the receiving host

To monitor FortiAuthenticator system information and receive FortiAuthenticator traps through SNMP, two configurations must be performed after enabling SNMP access on the FortiAuthenticator interface:

Set the thresholds to trigger SNMP traps for various system events, such as CPU usage, disk usage, memory usage, or temperature.

Upload management information base (MIB) files to SNMP server to enable the server to interpret the SNMP traps sent by FortiAuthenticator.

QUESTION 21

You are a Wi-Fi provider and host multiple domains.

How do you delegate user accounts, user groups and permissions per domain when they are authenticating on a single FortiAuthenticator device?
* Create realms.
* Create user groups
* Create multiple directory trees on FortiAuthenticator
* Automatically import hosts from each domain as they authenticate.

Realms are a way to delegate user accounts, user groups and permissions per domain when they are authenticating on a single FortiAuthenticator device. A realm is a logical grouping of users and groups based on a common attribute, such as a domain name or an IP address range. Realms allow administrators to apply different authentication policies and settings to different groups of users based on their realm membership.

QUESTION 22

An administrator is integrating FortiAuthenticator with an existing RADIUS server with the intent of eventually replacing the RADIUS server with FortiAuthenticator.

How can FortiAuthenticator help facilitate this process?
* By configuring the RADIUS accounting proxy
* By enabling automatic REST API calls from the RADIUS server
* By enabling learning mode in the RADIUS server configuration
* By importing the RADIUS user records

FortiAuthenticator can help facilitate the process of replacing an existing RADIUS server by enabling learning mode in the RADIUS server configuration. This allows FortiAuthenticator to learn user credentials from the existing RADIUS server and store them locally for future authentication requests2. This way, FortiAuthenticator can gradually take over the role of the RADIUS server without disrupting the user experience.

QUESTION 23

Which option correctly describes an SP-initiated SSO SAML packet flow for a host without a SAML assertion?
* Service provider contacts idendity provider, idendity provider validates principal for service provider, service provider establishes communication with principal
* Principal contacts idendity provider and is redirected to service provider, principal establishes connection with service provider, service provider validates authentication with identify provider
* Principal contacts service provider, service provider redirects principal to idendity provider, after succesfull authentication identify provider redirects principal to service provider
* Principal contacts idendity provider and authenticates, identity provider relays principal to service provider after valid authentication
SP-initiated SSO SAML packet flow for a host without a SAML assertion is as follows:

Principal contacts service provider, requesting access to a protected resource.

Service provider redirects principal to identity provider, sending a SAML authentication request.

Principal authenticates with identity provider using their credentials.

After successful authentication, identity provider redirects principal back to service provider, sending a SAML response with a SAML assertion containing the principal’s attributes.

Service provider validates the SAML response and assertion, and grants access to the principal.

QUESTION 24

What are three key features of FortiAuthenticator? (Choose three)
* Identity management device
* Log server
* Certificate authority
* Portal services
* RSSO Server
FortiAuthenticator is a user and identity management solution that provides strong authentication, wireless 802.1X authentication, certificate management, RADIUS AAA (authentication, authorization, and accounting), and Fortinet Single Sign-On (FSSO). It also offers portal services for guest management, self-service password reset, and device registration. It is not a log server or an RSSO server. Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4/release-notes

QUESTION 25

A digital certificate, also known as an X.509 certificate, contains which two pieces of information? (Choose two.)
* Issuer
* Shared secret
* Public key
* Private key
A digital certificate, also known as an X.509 certificate, contains two pieces of information:

Issuer, which is the identity of the certificate authority (CA) that issued the certificate Public key, which is the public part of the asymmetric key pair that is associated with the certificate subject

QUESTION 26

At a minimum, which two configurations are required to enable guest portal services on FortiAuthenticator? (Choose two)

* Configuring a portal policy
* Configuring at least on post-login service
* Configuring a RADIUS client
* Configuring an external authentication portal

To enable guest portal services on FortiAuthenticator, you need to configure a portal policy that defines the conditions for presenting the guest portal to users and the authentication methods to use. You also need to configure at least one post-login service that defines what actions to take after a user logs in successfully, such as sending an email confirmation, assigning a VLAN, or creating a user account. Configuring a RADIUS client or an external authentication portal are optional steps that depend on your network setup and requirements. Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372404/guest-management

QUESTION 27

You are the administrator of a global enterprise with three FortiAuthenticator devices. You would like to deploy them to provide active-passive HA at headquarters, with geographically distributed load balancing.

What would the role settings be?

* One standalone and two load balancers
* One standalone primary, one cluster member, and one load balancer
* Two cluster members and one backup
* Two cluster members and one load balancer

To deploy three FortiAuthenticator devices to provide active-passive HA at headquarters, with geographically distributed load balancing, the role settings would be:

One standalone primary, which acts as the master device for HA and load balancing One cluster member, which acts as the backup device for HA and load balancing One load balancer, which acts as a remote device that forwards authentication requests to the primary or cluster member device

QUESTION 28

Which two statements about the self-service portal are true? (Choose two)

* Self-registration information can be sent to the user through email or SMS
* Realms can be used to configure which seld-registered users or groups can authenticate on the network
* Administrator approval is required for all self-registration
* Authenticating users must specify domain name along with username

Two statements about the self-service portal are true:

Self-registration information can be sent to the user through email or SMS using the notification templates feature. This feature allows administrators to customize the messages that are sent to users when they register or perform other actions on the self-service portal.

Realms can be used to configure which self-registered users or groups can authenticate on the network using the realm-based authentication feature. This feature allows administrators to apply different authentication policies and settings to different groups of users based on their realm membership.

QUESTION 29

When configuring syslog SSO, which three actions must you take, in addition to enabling the syslog SSO method? (Choose three.)

* Enable syslog on the FortiAuthenticator interface.
* Define a syslog source.
* Select a syslog rule for message parsing.

* Set the same password on both the FortiAuthenticator and the syslog server.
* Set the syslog UDP port on FortiAuthenticator.

To configure syslog SSO, three actions must be taken, in addition to enabling the syslog SSO method:

Define a syslog source, which is a device that sends syslog messages to FortiAuthenticator containing user logon or logoff information.

Select a syslog rule for message parsing, which is a predefined or custom rule that defines how to extract the user name, IP address, and logon or logoff action from the syslog message.

Set the syslog UDP port on FortiAuthenticator, which is the port number that FortiAuthenticator listens on for incoming syslog messages.

QUESTION 30

You have implemented two-factor authentication to enhance security to sensitive enterprise systems.

How could you bypass the need for two-factor authentication for users accessing form specific secured networks?

* Create an admin realm in the authentication policy
* Specify the appropriate RADIUS clients in the authentication policy
* Enable Adaptive Authentication in the portal policy
* Enable the Resolve user geolocation from their IP address option in the authentication policy.

Adaptive Authentication is a feature that allows administrators to bypass the need for two-factor authentication for users accessing from specific secured networks. Adaptive Authentication uses geolocation information from IP addresses to determine whether a user is accessing from a trusted network or not. If the user is accessing from a trusted network, FortiAuthenticator can skip the second factor of authentication and grant access based on the first factor only.

QUESTION 31

You are an administrator for a large enterprise and you want to delegate the creation and management of guest users to a group of sponsors.

How would you associate the guest accounts with individual sponsors?

* As an administrator, you can assign guest groups to individual sponsors.
* Guest accounts are associated with the sponsor that creates the guest account.
* You can automatically add guest accounts to groups associated with specific sponsors.
* Select the sponsor on the guest portal, during registration.

Guest accounts are associated with the sponsor that creates the guest account. A sponsor is a user who has permission to create and manage guest accounts on behalf of other users3. A sponsor can create guest accounts using the sponsor portal or the REST API3. The sponsor’s username is recorded as a field in the guest account’s profile3.

QUESTION 32

Which two SAML roles can Fortiauthenticator be configured as? (Choose two)

* Idendity provider
* Principal
* Assertion server
* Service provider

FortiAuthenticator can be configured as a SAML identity provider (IdP) or a SAML service provider (SP). As an IdP, FortiAuthenticator authenticates users and issues SAML assertions to SPs. As an SP, FortiAuthenticator receives SAML assertions

from IdPs and grants access to users based on the attributes in the assertions. Principal and assertion server are not valid SAML roles. Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372407/saml

QUESTION 33

Which two statement about the RADIUS service on FortiAuthenticator are true? (Choose two)
* Two-factor authentication cannot be enforced when using RADIUS authentication
* RADIUS users can migrated to LDAP users
* Only local users can be authenticated through RADIUS
* FortiAuthenticator answers only to RADIUS client that are registered with FortiAuthenticator
Two statements about the RADIUS service on FortiAuthenticator are true:

RADIUS users can be migrated to LDAP users using the RADIUS learning mode feature. This feature allows FortiAuthenticator to learn user credentials from an existing RADIUS server and store them locally as LDAP users for future authentication requests.

FortiAuthenticator answers only to RADIUS clients that are registered with FortiAuthenticator. A RADIUS client is a device that sends RADIUS authentication or accounting requests to FortiAuthenticator. A RADIUS client must be added and configured on FortiAuthenticator before it can communicate with it.

QUESTION 34

Which of the following is an OATH-based standard to generate event-based, one-time password tokens?
* HOTP
* SOTP
* TOTP
* OLTP
Reference:

HOTP stands for HMAC-based One-time Password, which is an OATH-based standard to generate event-based OTP tokens. HOTP uses a cryptographic hash function called HMAC (Hash-based Message Authentication Code) to generate OTPs based on two pieces of information: a secret key and a counter. The counter is incremented by one after each OTP generation, creating an event-based sequence of OTPs.

QUESTION 35

When generating a TOTP for two-factor authentication, what two pieces of information are used by the algorithm to generate the TOTP?
* UUID and time
* Time and seed
* Time and mobile location
* Time and FortiAuthenticator serial number
TOTP stands for Time-based One-time Password, which is a type of OTP that is generated based on two pieces of information: time and seed. The time is the current timestamp that is synchronized between the client and the server. The seed is a secret key that is shared between the client and the server. The TOTP algorithm combines the time and the seed to generate a unique and short-lived OTP that can be used for two-factor authentication.

QUESTION 36

Which EAP method is known as the outer authentication method?
* PEAP

* EAP-GTC
* EAP-TLS
* MSCHAPV2

PEAP is known as the outer authentication method because it establishes a secure tunnel between the client and the server using TLS. The inner authentication method, such as EAP-GTC, EAP-TLS, or MSCHAPV2, is then used to authenticate the client within the tunnel.

QUESTION 37

Which two protocols are the default management access protocols for administrative access for FortiAuthenticator? (Choose two)

* Telnet
* HTTPS
* SSH
* SNMP

HTTPS and SSH are the default management access protocols for administrative access for FortiAuthenticator. HTTPS allows administrators to access the web-based GUI of FortiAuthenticator using a web browser and a secure connection. SSH allows administrators to access the CLI of FortiAuthenticator using an SSH client and an encrypted connection. Both protocols require the administrator to enter a valid username and password to log in.