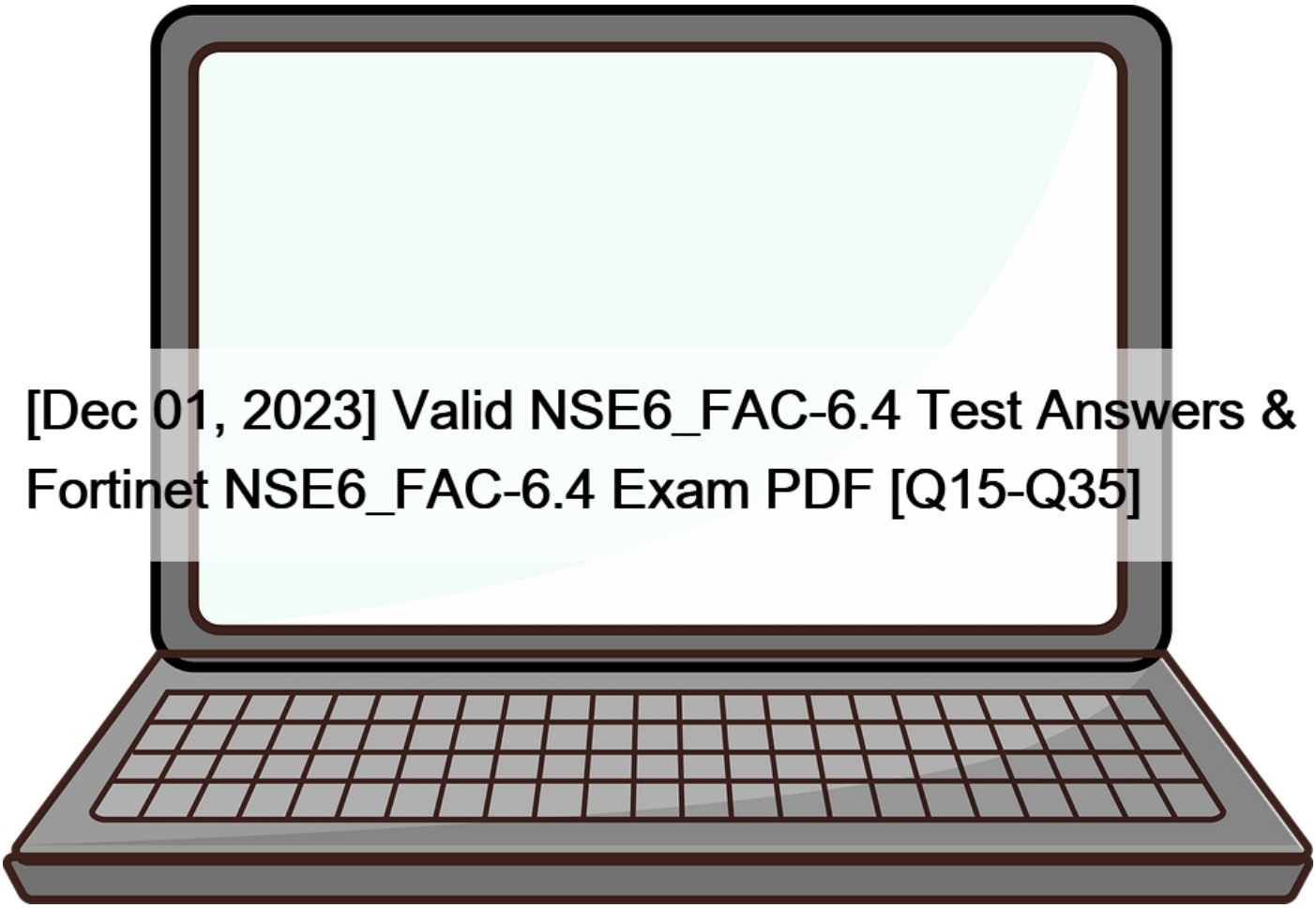
[Dec 01, 2023 Valid NSE6_FAC-6.4 Test Answers & Fortinet NSE6_FAC-6.4 Exam PDF [Q15-Q35



[Dec 01, 2023] Valid NSE6_FAC-6.4 Test Answers & Fortinet NSE6_FAC-6.4 Exam PDF
Realistic NSE6_FAC-6.4 Exam Dumps with Accurate & Updated Questions

NEW QUESTION 15

How can a SAML metada file be used?
* To defined a list of trusted user names
* To import the required IDP configuration
* To correlate the IDP address to its hostname
* To resolve the IDP realm for authentication

A SAML metadata file can be used to import the required IDP configuration for SAML service provider mode. A SAML metadata file is an XML file that contains information about the identity provider (IDP) and the service provider (SP), such as their entity IDs, endpoints, certificates, and attributes. By importing a SAML metadata file from the IDP, FortiAuthenticator can automatically configure the necessary settings for SAML service provider mode.

NEW QUESTION 16

An administrator has an active directory (AD) server integrated with FortiAuthenticator. They want members of only specific AD groups to participate in FSSO with their corporate FortiGate firewalls.

How does the administrator accomplish this goal?
* Configure a FortiGate filter on FortiAuthenticatoc
* Configure a domain groupings list to identify the desired AD groups.
* Configure fine-grained controls on FortiAuthenticator to designate AD groups.
* Configure SSO groups and assign them to FortiGate groups.

To allow members of only specific AD groups to participate in FSSO with their corporate FortiGate firewalls, the administrator can configure SSO groups and assign them to FortiGate groups. SSO groups are groups of users or devices that are defined on FortiAuthenticator based on various criteria, such as user group membership, source IP address, MAC address, or device type. FortiGate groups are groups of users or devices that are defined on FortiGate based on various criteria, such as user group membership, firewall policy, or authentication method. By mapping SSO groups to FortiGate groups, the administrator can control which users or devices can access the network resources protected by FortiGate.

NEW QUESTION 17

You are a FortiAuthenticator administrator for a large organization. Users who are configured to use FortiToken 200 for two-factor authentication can no longer authenticate. You have verified that only the users with two-factor authentication are experiencing the issue.

What can cause this issue?
* FortiToken 200 license has expired
* One of the FortiAuthenticator devices in the active-active cluster has failed
* Time drift between FortiAuthenticator and hardware tokens
* FortiAuthenticator has lost contact with the FortiToken Cloud servers

One possible cause of the issue is time drift between FortiAuthenticator and hardware tokens. Time drift occurs when the internal clocks of FortiAuthenticator and hardware tokens are not synchronized. This can result in mismatched one-time passwords (OTPs) generated by the hardware tokens and expected by FortiAuthenticator. To prevent this issue, FortiAuthenticator provides a time drift tolerance option that allows a certain number of seconds of difference between the clocks.

NEW QUESTION 18

Which statement about the assignment of permissions for sponsor and administrator accounts is true?
* Only administrator accounts permissions are assigned using admin profiles.
* Sponsor permissions are assigned using group settings.
* Administrator capabilities are assigned by applying permission sets to admin groups.
* Both sponsor and administrator account permissions are assigned using admin profiles.

Both sponsor and administrator account permissions are assigned using admin profiles. An admin profile is a set of permissions that defines what actions an administrator or a sponsor can perform on FortiAuthenticator. An admin profile can be assigned to an admin group or an individual admin user. A sponsor is a special type of admin user who can create and manage guest accounts on behalf of other users.

NEW QUESTION 19

Which two capabilities does FortiAuthenticator offer when acting as a self-signed or local CA? (Choose two)
* Validating other CA CRLs using OSCP
* Importing other CA certificates and CRLs
* Merging local and remote CRLs using SCEP

* Creating, signing, and revoking of X.509 certificates

FortiAuthenticator can act as a self-signed or local CA that can issue certificates to users, devices, or other CAs. It can also import other CA certificates and CRLs to trust them and validate their certificates. It can also create, sign, and revoke X.509 certificates for various purposes, such as VPN authentication, web server encryption, or wireless security. It cannot validate other CA CRLs using OCSP or merge local and remote CRLs using SCEP because these are protocols that require communication with external CAs. Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372408/certificate-management

NEW QUESTION 20

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.

NEW QUESTION 21

What happens when a certificate is revoked? (Choose two)

* Revoked certificates cannot be reinstated for any reason
* All certificates signed by a revoked CA certificate are automatically revoked
* Revoked certificates are automatically added to the CRL
* External CAs will priodically query Fortiauthenticator and automatically download revoked certificates

When a certificate is revoked, it means that it is no longer valid and should not be trusted by any entity. Revoked certificates are automatically added to the certificate revocation list (CRL) which is published by the issuing CA and can be checked by other parties. If a CA certificate is revoked, all certificates signed by that CA are also revoked and added to the CRL. Revoked certificates can be reinstated if the reason for revocation is resolved, such as a compromised private key being recovered or a misissued certificate being corrected. External CAs do not query FortiAuthenticator for revoked certificates, but they can use protocols such as SCEP or OCSP to exchange certificate information with FortiAuthenticator. Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372408/certificate-management

NEW QUESTION 22

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

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

NEW QUESTION 23

Which two features of FortiAuthenticator are used for EAP deployment? (Choose two)
* Certificate authority
* LDAP server
* MAC authentication bypass
* RADIUS server

Two features of FortiAuthenticator that are used for EAP deployment are certificate authority and RADIUS server. Certificate authority allows FortiAuthenticator to issue and manage digital certificates for EAP methods that require certificate-based authentication, such as EAP-TLS or PEAP-EAP-TLS. RADIUS server allows FortiAuthenticator to act as an authentication server for EAP methods that use RADIUS as a transport protocol, such as EAP-GTC or PEAP-MSCHAPV2.

NEW QUESTION 24

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.

NEW QUESTION 25

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.

NEW QUESTION 26

Which FSSO discovery method transparently detects logged off users without having to rely on external features such as WMI polling?

* Windows AD polling
* FortiClient SSO Mobility Agent
* Radius Accounting
* DC Polling

FortiClient SSO Mobility Agent is a FSSO discovery method that transparently detects logged off users without having to rely on external features such as WMI polling. FortiClient SSO Mobility Agent is a software agent that runs on Windows devices and communicates with FortiAuthenticator to provide FSSO information. The agent can detect user logon and logoff events without using WMI polling, which can reduce network traffic and improve performance.

NEW QUESTION 27

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.

NEW QUESTION 28

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.

NEW QUESTION 29

Which network configuration is required when deploying FortiAuthenticator for portal services?

* FortiAuthenticator must have the REST API access enable on port1
* One of the DNS servers must be a FortiGuard DNS server
* Fortigate must be setup as default gateway for FortiAuthenticator
* Policies must have specific ports open between FortiAuthenticator and the authentication clients

When deploying FortiAuthenticator for portal services, such as guest portal, sponsor portal, user portal or FortiToken activation

portal, the network configuration must allow specific ports to be open between FortiAuthenticator and the authentication clients. These ports are:

TCP 80 for HTTP access

TCP 443 for HTTPS access

TCP 389 for LDAP access

TCP 636 for LDAPS access

UDP 1812 for RADIUS authentication

UDP 1813 for RADIUS accounting

NEW QUESTION 30

Which two types of digital certificates can you create in Fortiauthenticator? (Choose two)
* User certificate
* Organization validation certificate
* Third-party root certificate
* Local service certificate

FortiAuthenticator can create two types of digital certificates: user certificates and local service certificates. User certificates are issued to users or devices for authentication purposes, such as VPN, wireless, or web access. Local service certificates are issued to FortiAuthenticator itself for securing its own services, such as HTTPS, RADIUS, or LDAP.

NEW QUESTION 31

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

NEW QUESTION 32

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 FortiAuthenticator serial number
* Time and seed
* Time and mobile location

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.

NEW QUESTION 33

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