Free Questions for NSE6_FAC-6.4 by ebraindumps

Shared by Rocha on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

How can a SAML metada file be used?

Options:

A- To defined a list of trusted user names

B- To import the required IDP configuration

C- To correlate the IDP address to its hostname

D- To resolve the IDP realm for authentication

Answer:

B

Explanation:

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.

Question 2

Question Type: MultipleChoice

Which two features of FortiAuthenticator are used for EAP deployment? (Choose two)

Options:

A- Certificate authority

B- LDAP server

C- MAC authentication bypass

D- RADIUS server

Answer:

A, D

Explanation:

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.

Question 3

Question Type: MultipleChoice

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)

Options:

A- Enable logging services

B- Set the tresholds to trigger SNMP traps

C- Upload management information base (MIB) files to SNMP server

D- Associate an ASN, 1 mapping rule to the receiving host

Answer:

B, C

Explanation:

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 4

Question Type: MultipleChoice

Which EAP method is known as the outer authentication method?

Options:

A- PEAP

B- EAP-GTC

C- EAP-TLS

D- MSCHAPV2

Answer:

A

Explanation:

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 5

Question Type: **MultipleChoice**

Which two types of digital certificates can you create in Fortiauthenticator? (Choose two)

Options:

A- User certificate

B- Organization validation certificate

C- Third-party root certificate

D- Local service certificate

Answer:

A, D

Explanation:

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.

Question 6

Question Type: **MultipleChoice**

Which option correctly describes an SP-initiated SSO SAML packet flow for a host without a SAML assertion?

Options:

A- Service provider contacts idendity provider, idendity provider validates principal for service provider, service provider establishes communication with principal

B- Principal contacts idendity provider and is redirected to service provider, principal establishes connection with service provider, service provider validates authentication with identify provider

C- Principal contacts service provider, service provider redirects principal to idendity provider, after succesfull authentication identify provider redirects principal to service provider

D- Principal contacts idendity provider and authenticates, identity provider relays principal to service provider after valid authentication

Answer:

C

Explanation:

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 7

Question Type: **MultipleChoice**

An administrator wants to keep local CA cryptographic keys stored in a central location.

Which FortiAuthenticator feature would provide this functionality?

Options:

A- SCEP support

B- REST API

C- Network HSM

D- SFTP server

Answer:

C

Explanation:

Network HSM is a feature that allows FortiAuthenticator to keep local CA cryptographic keys stored in a central location. HSM stands for Hardware Security Module, which is a physical device that provides secure storage and generation of cryptographic keys. Network HSM allows FortiAuthenticator to use an external HSM device to store and manage the private keys of its local CAs, instead of storing them locally on the FortiAuthenticator device.

Question 8

Question Type: MultipleChoice

Why would you configure an OCSP responder URL in an end-entity certificate?

Options:

A- To designate the SCEP server to use for CRL updates for that certificate

B- To identify the end point that a certificate has been assigned to

C- To designate a server for certificate status checking

D- To provide the CRL location for the certificate

Answer:

C

Explanation:

An OCSP responder URL in an end-entity certificate is used to designate a server for certificate status checking. OCSP stands for Online Certificate Status Protocol, which is a method of verifying whether a certificate is valid or revoked in real time. An OCSP responder is a server that responds to OCSP requests from clients with the status of the certificate in question. The OCSP responder URL in an end-entity certificate points to the location of the OCSP responder that can provide the status of that certificate.

Question 9

Question Type: **MultipleChoice**

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?

Options:

A- FortiToken 200 license has expired

B- One of the FortiAuthenticator devices in the active-active cluster has failed

C- Time drift between FortiAuthenticator and hardware tokens

D- FortiAuthenticator has lost contact with the FortiToken Cloud servers

Answer:

C

Explanation:

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.