Free Questions for NSE6_FAC-6.4 by certsinside

Shared by Cervantes on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

When you are setting up two FortiAuthenticator devices in active-passive HA, which HA role must you select on the master FortiAuthenticator?

Options:

A- Active-passive master

B- Standalone master

C- Cluster member

D- Load balancing master

Answer:

A

Explanation:

When you are setting up two FortiAuthenticator devices in active-passive HA, you need to select the active-passive master role on the master FortiAuthenticator device. This role means that the device will handle all requests and synchronize data with the slave device

until a failover occurs. The slave device must be configured as an active-passive slave role. The other roles are used for different HA modes, such as standalone (no HA), cluster (active-active), or load balancing (active-active with load balancing). Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372411/high-availability

Question 2

Question Type: MultipleChoice

Which statement about the guest portal policies is true?

Options:

A- Guest portal policies apply only to authentication requests coming from unknown RADIUS clients

B- Guest portal policies can be used only for BYODs

C- Conditions in the policy apply only to guest wireless users

D- All conditions in the policy must match before a user is presented with the guest portal

Answer:

D

Explanation:

Guest portal policies are rules that determine when and how to present the guest portal to users who want to access the network. Each policy has a set of conditions that can be based on various factors, such as the source IP address, MAC address, RADIUS client, user agent, or SSID. All conditions in the policy must match before a user is presented with the guest portal. Guest portal policies can apply to any authentication request coming from any RADIUS client, not just unknown ones. They can also be used for any type of device, not just BYODs. They can also apply to wired or VPN users, not just wireless users. Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372404/guest-management/372406/portal-policies

Question 3

Question Type: MultipleChoice

Which two capabilities does FortiAuthenticator offer when acting as a self-signed or local CA? (Choose two)

Options:

A- Validating other CA CRLs using OSCP

B- Importing other CA certificates and CRLs

C- Merging local and remote CRLs using SCEP

D- Creating, signing, and revoking of X.509 certificates

Answer:

B, D

Explanation:

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

Question 4

Question Type: MultipleChoice

Which three of the following can be used as SSO sources? (Choose three)

Options:

A- FortiClient SSO Mobility Agent

B- SSH Sessions

C- FortiAuthenticator in SAML SP role

D- Fortigate

E- RADIUS accounting

Answer:

A, D, E

Explanation:

FortiAuthenticator supports various SSO sources that can provide user identity information to other devices in the network, such as FortiGate firewalls or FortiAnalyzer log servers. Some of the supported SSO sources are:

FortiClient SSO Mobility Agent: A software agent that runs on Windows devices and sends user login information to FortiAuthenticator.

FortiGate: A firewall device that can send user login information from various sources, such as FSSO agents, captive portals, VPNs, or LDAP servers, to FortiAuthenticator.

RADIUS accounting: A protocol that can send user login information from RADIUS servers or clients, such as wireless access points or VPN concentrators, to FortiAuthenticator.

SSH sessions and FortiAuthenticator in SAML SP role are not valid SSO sources because they do not provide user identity information to other devices in the network. Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372410/single-sign-on

Question 5

Question Type: MultipleChoice

You are the administrator of a large network that includes a large local user datadabase on the current Fortiauthenticatior. You want to import all the local users into a new Fortiauthenticator device.

Which method should you use to migrate the local users?

Options:

A- Import users using RADIUS accounting updates.

B- Import the current directory structure.

C- Import users from RADUIS.

D- Import users using a CSV file.

Answer:

D

Explanation:

The best method to migrate local users from one FortiAuthenticator device to another is to export the users from the current device as a CSV file and then import the CSV file into the new device. This method preserves all the user attributes and settings and allows you to modify them if needed before importing. The other methods are not suitable for migrating local users because they either require an external RADIUS server or do not transfer all the user information. Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372409/user-management

Question 6

Question Type: MultipleChoice

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

Options:

A- Revoked certificates cannot be reinstated for any reason

B- All certificates signed by a revoked CA certificate are automatically revoked

C- Revoked certificates are automatically added to the CRL

D- External CAs will priodically query Fortiauthenticator and automatically download revoked certificates

Answer:

B, C

Explanation:

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

Question 7

Question Type: MultipleChoice

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

Options:

A- Idendity provider

B- Principal

C- Assertion server

D- Service provider

Answer:

A, D

Explanation:

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 8

Question Type: MultipleChoice

A device or user identity cannot be established transparently, such as with non-domain BYOD devices, and allow users to create their own credentialis.

In this case, which user idendity discovery method can Fortiauthenticator use?

Options:

A- Syslog messaging or SAML IDP

B- Kerberos-base authentication

C- Radius accounting

D- Portal authentication

Answer:

D

Explanation:

Portal authentication is a user identity discovery method that can be used when a device or user identity cannot be established transparently, such as with non-domain BYOD devices, and allow users to create their own credentials. Portal authentication requires users to enter their credentials on a web page before accessing network resources. The other methods are used for transparent identification of domain devices or users. Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372406/user-identity-discovery

Question 9

Question Type: MultipleChoice

Which two are supported captive or guest portal authentication methods? (Choose two)

Options:

A- LinkedIn

B- Apple ID

C- Instagram

D- Email

Answer:

A, D

Explanation:

FortiAuthenticator supports various captive or guest portal authentication methods, including social media login with LinkedIn, Facebook, Twitter, Google+, or WeChat; email verification; SMS verification; voucher code; username and password; and MAC address bypass. Apple ID and Instagram are not supported as authentication methods. Reference: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372404/guest-management/372405/authentication-methods

Question 10

Question Type: MultipleChoice

A digital certificate, also known as an X.509 certificate, contains which two pieces of information? (Choose two.)

Options:

A- Issuer

B- Shared secret

C- Public key

D- Private key

Answer:

A, C

Explanation:

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 11

Question Type: MultipleChoice

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

Options:

A- Self-registration information can be sent to the user through email or SMS

B- Realms can be used to configure which seld-registered users or groups can authenticate on the network

C- Administrator approval is required for all self-registration

D- Authenticating users must specify domain name along with username

Answer:

A, B

Explanation:

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 12

Question Type: MultipleChoice

Which two statement about the RADIUS service on FortiAuthenticator are true? (Choose two)

Options:

A- Two-factor authentication cannot be enforced when using RADIUS authentication

B- RADIUS users can migrated to LDAP users

C- Only local users can be authenticated through RADIUS

D- FortiAuthenticator answers only to RADIUS client that are registered with FortiAuthenticator

Answer:

B, D

Explanation:

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.