Fortinet

Exam Questions NSE6_FAC-6.4

Fortinet NSE 6 - FortiAuthenticator 6.4

NEW QUESTION 1
Which two protocols are the default management access protocols for administrative access for FortiAuthenticator? (Choose two)

A. Telnet
B. HTTPS
C. SSH
D. SNMP

Answer: BC

Explanation:
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.
References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/system-settings#manag

NEW QUESTION 2
Which FSSO discovery method transparently detects logged off users without having to rely on external features such as WMI polling?

A. Windows AD polling
B. FortiClient SSO Mobility Agent
C. Radius Accounting
D. DC Polling

Answer: B

Explanation:
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.
References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/single-sign-on#forticlie

NEW QUESTION 3
How can a SAML metada file be used?

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.
References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/saml-service-provider#

NEW QUESTION 4
When you are setting up two FortiAuthenticator devices in active-passive HA, which HA role must you select on the master FortiAuthenticator?

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). References:
https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372411/high-availability

NEW QUESTION 5
Which two are supported captive or guest portal authentication methods? (Choose two)

A. LinkedIn
B. Apple ID
C. Instagram
D. Email

Answer:

AD

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. References:
https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372404/guest-management/37240

NEW QUESTION 6
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?

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. References:
https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372409/user-management

NEW QUESTION 7
Which statement about the guest portal policies is true?

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. References:
https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372404/guest-management/37240

NEW QUESTION 8
What are three key features of FortiAuthenticator? (Choose three)

A. Identity management device
B. Log server
C. Certificate authority
D. Portal services
E. RSSO Server

Answer: ACD

Explanation:
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. References:
https://docs.fortinet.com/document/fortiauthenticator/6.4/release-notes

NEW QUESTION 9
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?

A. One standalone and two load balancersB One standalone primary, one cluster member, and one load balancer
B. Two cluster members and one backup
C. Two cluster members and one load balancer

Answer: B

Explanation:
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

References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/high-availability#ha-an

NEW QUESTION 10
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?

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.
References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/two-factor-authenticati

NEW QUESTION 10
An administrator wants to keep local CA cryptographic keys stored in a central location.
Which FortiAuthenticator feature would provide this functionality?

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.
References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/certificate-management

NEW QUESTION 15
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

NSE6_FAC-6.4 Practice Exam Features:

* NSE6_FAC-6.4 Questions and Answers Updated Frequently

* NSE6_FAC-6.4 Practice Questions Verified by Expert Senior Certified Staff

* NSE6_FAC-6.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE6_FAC-6.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year