Fortinet

Exam Questions NSE6_FAC-6.4

Fortinet NSE 6 - FortiAuthenticator 6.4

NEW QUESTION 1
Why would you configure an OCSP responder URL in an end-entity certificate?

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

NEW QUESTION 2
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 3
When configuring syslog SSO, which three actions must you take, in addition to enabling the syslog SSO method? (Choose three.)

A. Enable syslog on the FortiAuthenticator interface.
B. Define a syslog source.
C. Select a syslog rule for message parsing.
D. Set the same password on both the FortiAuthenticator and the syslog server.
E. Set the syslog UDP port on FortiAuthenticator.

Answer: BCE

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

NEW QUESTION 4
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 5

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

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: AB

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.
References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/user-management#self-
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/user-management#real

NEW QUESTION 6
......

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

100% Actual & Verified — Instant Download, Please Click
[Order The NSE6_FAC-6.4 Practice Test Here](https://www.surepassexam.com/NSE6_FAC-6.4-exam-dumps.html)