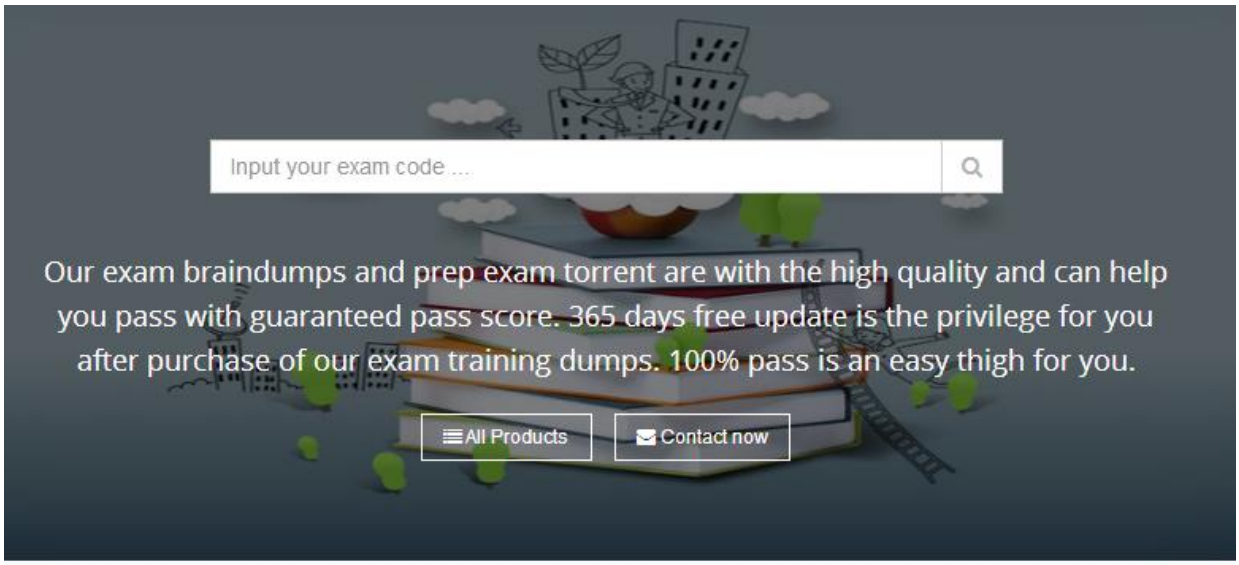
BraindumpsPrep



QUALITY AND VALUE

BraindumpsPrep Practice Exams are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development - no all dumps.

TESTED AND APPROVED

We are committed to the process of vendor and third party approvals. We believe professionals and executives alike deserve the confidence of quality coverage these authorizations provide.

EASY TO PASS

If you prepare for the exams using our BraindumpsPrep testing engine, It is easy to succeed for all certifications in the first attempt. You don't have to deal with all dumps or any free torrent / rapidshare all stuff.

TRY BEFORE BUY

BraindumpsPrep offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

http://www.braindumpsprep.com

Prep your actual exam test with our valid braindumps for successful pass

Exam : **NSE6_FAC-6.4**

Title : Fortinet NSE 6 - FortiAuthenticator 6.4

Vendor : Fortinet

Version : DEMO

NO.1 Which two SAML roles can Fortiauthenticator be configured as? (Choose two)

A. Principal

B. Service provider

C. Assertion server

D. Idendity provider

Answer: B,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

NO.2 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)

A. Upload management information base (MIB) files to SNMP server

B. Associate an ASN, 1 mapping rule to the receiving host

C. Enable logging services

D. Set the tresholds to trigger SNMP traps

Answer: A,D

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.

NO.3 When you are setting up two FortiAuthenticator devices in active-passive HA, which HA role must you select on the master FortiAuthenticator?

A. Load balancing master

B. Active-passive master

C. Standalone master

D. Cluster member

Answer: B

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

NO.4 Which two statements about the self-service portal are true? (Choose two)

A. Administrator approval is required for all self-registration

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

C. Authenticating users must specify domain name along with username

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

Answer: B,D

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.

NO.5 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 provide the CRL location for the certificate

C. To designate a server for certificate status checking

D. To identify the end point that a certificate has been assigned to

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.