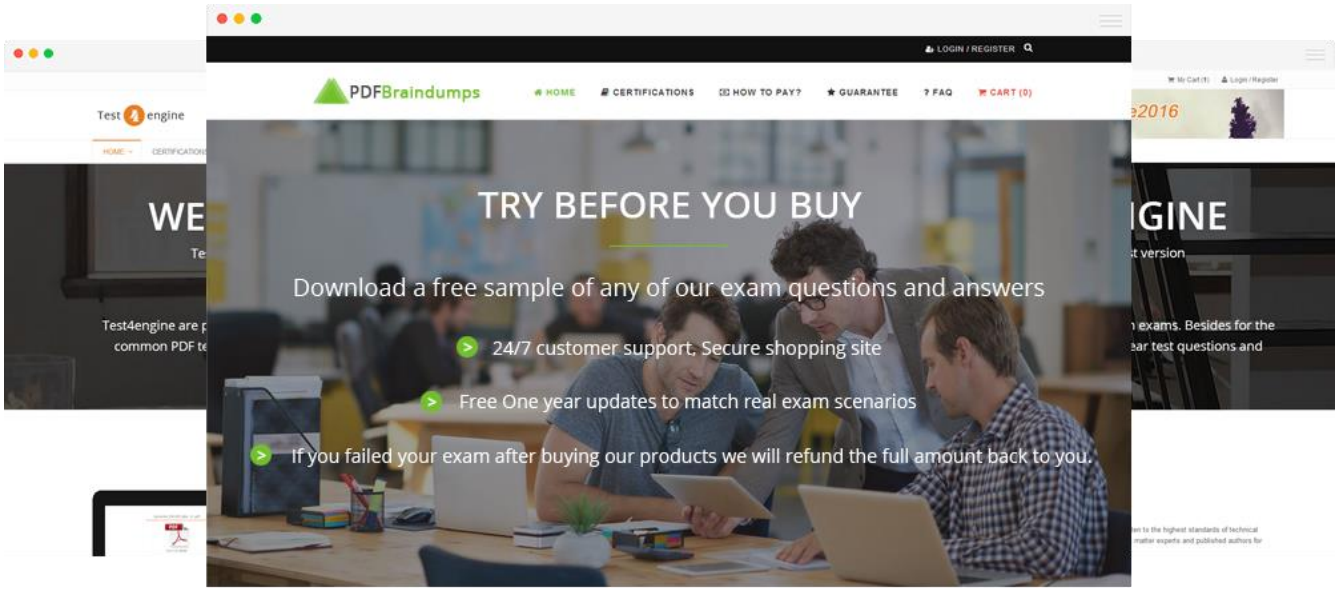
PDFBraindumps



Latest Pdf Braindumps

- LRP-614
- C-SRM-72
- BCABA
- ACMP-6.3
- JN0-740
- 1z0-100
- 250-405
- FM0-308
- DS-200
- C_SRM_72
- SDM_2002001040
- ACMP_6.3
- ST0-250
- 1z0-062
- H12-221
- A4120-784
- M2180-716

Top Certifications

- ISEB Certification
- HCNP
- OCE
- IFPUG Certifications
- NVIDIA Certifications
- dotMobi Certification
- Network+
- SCMA
- IBM Certified Integrat
- MCSD
- CCDH
- NCLP
- IBM Certified Advanc
- XMLMaster Certificat
- eserver Certified Spe
- CS5
- SAP-Certifications
- CHA
- Network Appliance N

Top Vendors

- ISEB
- Fortinet
- ASTQB
- Ericsson
- Aruba
- Liferay
- Data Center Universit
- Novell
- HRCI
- Huawei
- CIW
- RSA
- Patchlink
- MYSQL
- International Consorti
- ISM
- Acme-Packet
- CheckPoint

http://www.pdfbraindumps.com

Latest pdf braindumps provider, high pass rate

Exam : **NSE6_FAZ-7.2**

Title : Fortinet NSE 6 - FortiAnalyzer 7.2 Administrator

Vendor : Fortinet

Version : DEMO

NO.1 Which two methods can you use to restrict administrative access on FortiAnalyzer? (Choose two.)

A. Use administrator profiles.

B. Configure trusted hosts.

C. Fabric connectors to external LDAP servers.

D. Limit access to specific virtual domains.

Answer: A B

Explanation:

To restrict administrative access on FortiAnalyzer, two effective methods are using administrator profiles and configuring trusted hosts. Administrator profiles allow for defining the level of access and permissions for different administrators, controlling what each administrator can seeand do within the FortiAnalyzer unit.

Configuring trusted hosts enhances security by limiting administrative access to specified IP addresses, ensuring that administrators can only connect from approved locations or networks, thus preventing unauthorized access from outside specified subnets or IP addresses.References:FortiAnalyzer 7.4.1 Administration Guide, "Administrators" and "Trusted hosts" sections.

NO.2 Which statement is true about ADOMs?

A. When a FortiAnalyzer Fabric is implemented, the default ADOM mode is set to advanced.

B. A fabric ADOM can include all the device types supported by FortiAnalyzer.

C. You can change the ADOM mode only through the GUI.

D. In normal mode, you cannot change the disk quota of the ADOM after its creation.

Answer: B

Explanation:

Regarding ADOMs (Administrative Domains) in FortiAnalyzer, a fabric ADOM is capable of including all device types that FortiAnalyzer supports. This is part of the flexibility offered by ADOMs to manage and report on logs from various devices within a Fortinet security fabric. ADOMs can be enabled to support non-FortiGate devices as well, and the root ADOM in Fabric ADOMs provides visibility into all Security Fabric devices. Additionally, it should be noted that in normal mode, you cannot assign different FortiGate VDOMs to different ADOMs, while in advanced mode, you can, which provides a more granular control over the log data from individual VDOMs.References:FortiAnalyzer 7.4.1 Administration Guide, "ADOMs" and
"ADOM device modes" sections.

NO.3 Which two of the available registration methods place the device automatically in its assigned ADOM?
(Choose two.)

A. Request from the device

B. Serial number

C. Fabric Authorization

D. Pre-shared key

Answer: B C

Explanation:

The registration methods that automatically place a device in its assigned ADOM are using the serial number and fabric authorization. When devices are added to FortiAnalyzer using these methods, they are automatically placed in the appropriate ADOM, which could be a defaultADOM based on the device type or a predefined ADOM based on the serial number or fabric authorization. This simplifies the management of devices and their logs by organizing them into their respective ADOMs from the moment they are registered.References:FortiAnalyzer 7.4.1 Administration Guide, "Default device type ADOMs" and
"Assigning devices to an ADOM" sections.

NO.4 Which statement is true about the communication between FortiGate high availability (HA) clusters and FortiAnalyzer?

A. Each cluster member sends its logs directly to FortiAnalyzer.

B. You must add the device lo the cluster first, and thenregistersthe cluster with FortiAnalyzer.

C. FortiAnalyzer distinguishes each cluster member by its MAC address.

D. Only the primary device in the cluster communicates with FortiAnalyzer.

Answer: D

Explanation:
In a FortiGate high availability (HA) cluster, only the primary device sends its logs to the FortiAnalyzer. This is to ensure that logs are not duplicated between the primary and secondary devices in the cluster. The configuration of the FortiAnalyzer server on the FortiGate is such that the HA primary device is set as the server that forwards the logs.References:FortiAnalyzer 7.4.1 Administration Guide, sections mentioning HA cluster configuration and log forwarding.