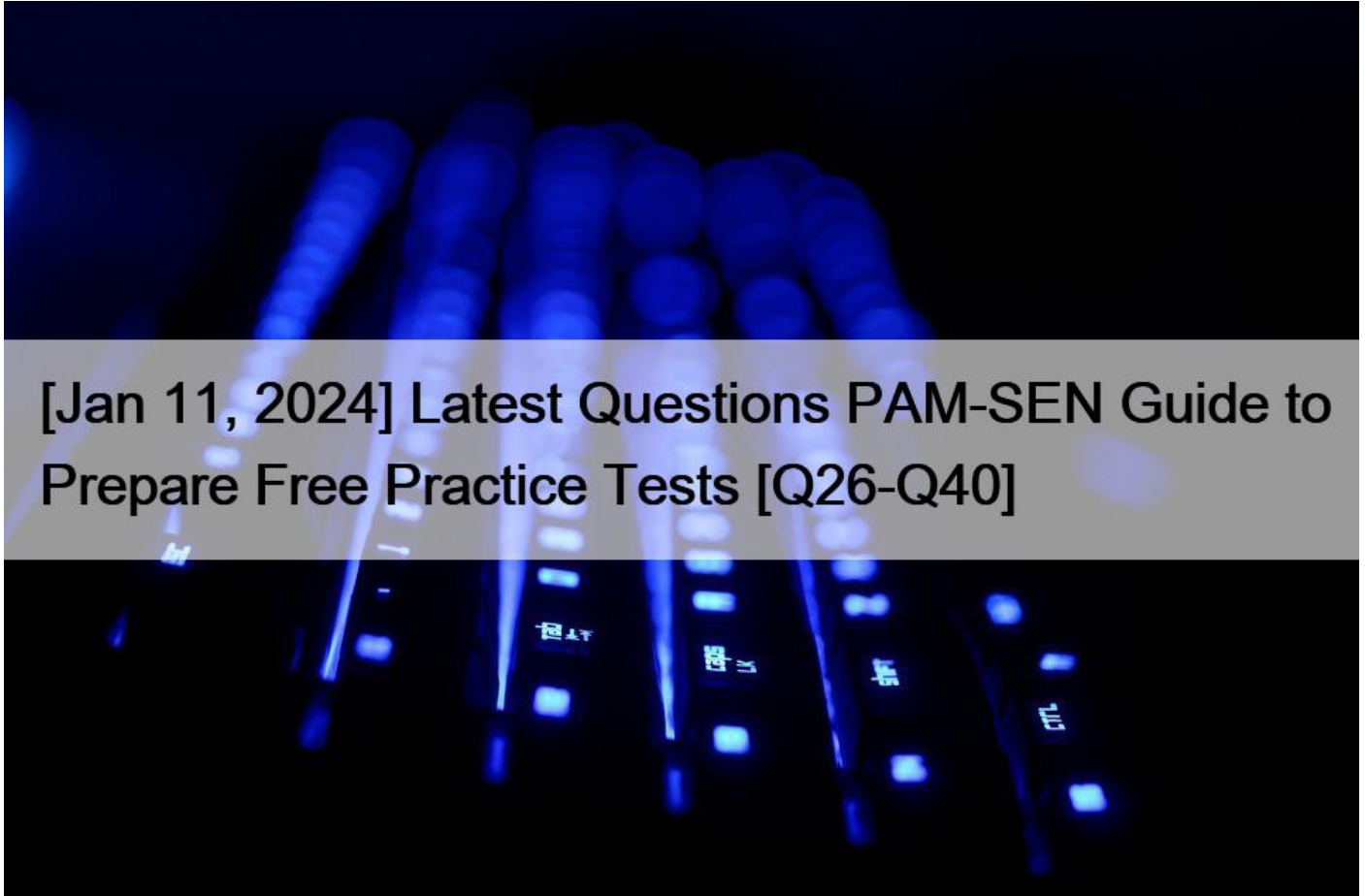


[Jan 11, 2024 Latest Questions PAM-SEN Guide to Prepare Free Practice Tests [Q26-Q40]



[Jan 11, 2024] Latest Questions PAM-SEN Guide to Prepare Free Practice Tests [Q26-Q40]

[Jan 11, 2024 Latest Questions PAM-SEN Guide to Prepare Free Practice Tests Reliable PAM-SEN Dumps Questions Available as Web-Based Practice Test Engine

The CyberArk PAM-SEN exam covers a range of topics related to PAM, including the CyberArk platform architecture, deployment and configuration, user and group management, policy creation and enforcement, session monitoring and recording, and reporting and analytics. Successful completion of the exam demonstrates a deep understanding of PAM best practices and the ability to effectively manage privileged accounts and access across an organization.

CyberArk PAM-SEN Certification Exam is a rigorous and comprehensive program that includes both theoretical and practical components. PAM-SEN exam consists of multiple-choice questions and hands-on exercises that test the candidate's knowledge and proficiency in using the CyberArk PAM solution. The program is designed to help IT professionals gain a deep understanding of the CyberArk PAM solution and its capabilities, which can be applied in real-world scenarios.

QUESTION 26

A customer has five PVWA servers. Three are located at the primary data center and the remaining two are at a satellite data center.

What is important to consider about the load balancer? (Choose two.)

- * It must not alter page content, or should include a mechanism to prevent pages from being altered. Most Voted
- * It must support “sticky sessions”. Most Voted
- * It must be able to digitally sign and issue certificates for PVWA servers.
- * It must be able to connect to all Vault and PVWA servers through Port TCP 443.
- * It must be configured with high-availability (HA) enabled.

QUESTION 27

Which SMTP address can be set on the Notification Settings page to re-invoke the ENE setup wizard after the initial Vault installation?

- * 255.255.255.255
- * 8.8.8.8
- * 192.168.1.1
- * 1.1.1.1

QUESTION 28

What are the basic network requirements to deploy a CPM server?

- * Port 1858 to Vault and Port 443 to PVWA
- * Port 1858 only
- * all ports to the Vault
- * Port UDP/1858 to Vault and all required ports to targets and Port 389 to the PSM

QUESTION 29

The account used to install a PVWA must have ownership of which safes? (Choose two.)

- * VaultInternal
- * PVWAConfig
- * System
- * Notification Engine
- * PVWAReports

QUESTION 30

Which statement is correct about a post-install hardening?

- * The Vault must be hardened during the Vault installation process. Most Voted
- * After the Vault server is installed, you must join the server to the Enterprise Domain and reboot the host.
- * It is executed after Vault installation by running CAVaultHarden.exe and hardening options can be edited by changing the Hardening.ini file. Most Voted
- * If it is mandated by an organization's IT governance, you do not have to execute Vault hardening; however, server hardening cannot be reversed.

QUESTION 31

For redundancy, you want to add a secondary RADIUS server.

What must you do to accomplish this?

- * Add to the application settings of the PVWA web.config file.
- * In the PVWA vault.ini file, list each RADIUS server host address in the “Addresses” attribute separated by commas.
- * Open the DBParm.ini on the Vault server. Add the second RADIUS server configuration settings after the first one, separated by a comma. Most Voted
- * In the PVWA web.config file, add the location element at the end of the config file. Set the path value to “Default Web Site/PasswordVault/api/auth/pkipn/logon”.

QUESTION 32

What must you do to synchronize a new Vault server with an organization’s NTP server?

- * Configure an AllowNonStandardFWAddresses rule for the organization’s NTP server in DBParm.ini on the Vault server.
- * Use the Windows Firewall console to configure a rule on the Vault server which allows communication with the organization’s NTP server.
- * Ensure the organization’s NTP server is installed in the same location as the Vault server requiring synchronization.
- * Update the AutoSyncExternalObjects configuration in DBParm.ini on the Vault server to schedule regular synchronization.

QUESTION 33

When a DR vault server becomes an active vault, it will automatically fail back to the original state once the primary vault comes back online.

- * True, this is the default behavior.
- * False, this is not possible.
- * True, if the ‘AllowFailback’ setting is set to yes in the PADR.ini file.
- * True, if the ‘AllowFailback’ setting is set to yes in the dbparm.ini file.

QUESTION 34

You are installing a CPM.

In addition to Add Safes, Add/Update Users, Reset Users’ Passwords and Manage Server File Categories, which Vault authorization(s) does a CyberArk user need to install the CPM?

- * Manage Directory Mapping
- * Activate Users
- * Backup All Safes, Restore All Safes
- * Audit Users, Add Network Areas

QUESTION 35

When integrating a Vault with HSM, which file is uploaded to the HSM device?

- * server.key
- * recpub.key
- * recprv.key
- * mdbase.dat

QUESTION 36

What is required before the first CPM can be installed?

- * The environment must have at least one Vault and one PVWA installed.
- * The Vault environment must have at least one account stored in a safe.
- * Custom platforms must be downloaded from the CyberArk Marketplace.
- * The PSM component must be installed and proper functionality validated.

QUESTION 37

Which user is enabled when replicating data between active and stand-by Vaults?

- * DR
- * Backup
- * Operator
- * Auditor

QUESTION 38

Which components can connect to a satellite Vault in a distributed Vault architecture?

- * CPM, EPM, PTA
- * PVWA, PSM
- * CPM, PVWA, PSM
- * CPM, PSM

QUESTION 39

When configuring RADIUS authentication, which utility is used to create a file containing an encrypted version of the RADIUS secret?

- * CAVaultManager
- * CACert
- * CreateAuthFile
- * CreateCredFile

QUESTION 40

How should you configure PSM for SSH to support load balancing?

- * by using a network load balancer Most Voted
- * in PVWA > Options > PSM for SSH Proxy > Servers
- * in PVWA > Options > PSM for SSH Proxy > Servers > VIP
- * by editing sshd.config on the all the PSM for SSH servers

Correct and Up-to-date CyberArk PAM-SEN BrainDumps:

https://www.test4engine.com/PAM-SEN_exam-latest-braindumps.html