PassQueen
a.k.a dumpsqueen.com

CyberArk Sentry - Privilege Cloud

CyberArk CPC-SEN

Version Demo

Total Demo Questions: 7

Total Premium Questions: 70

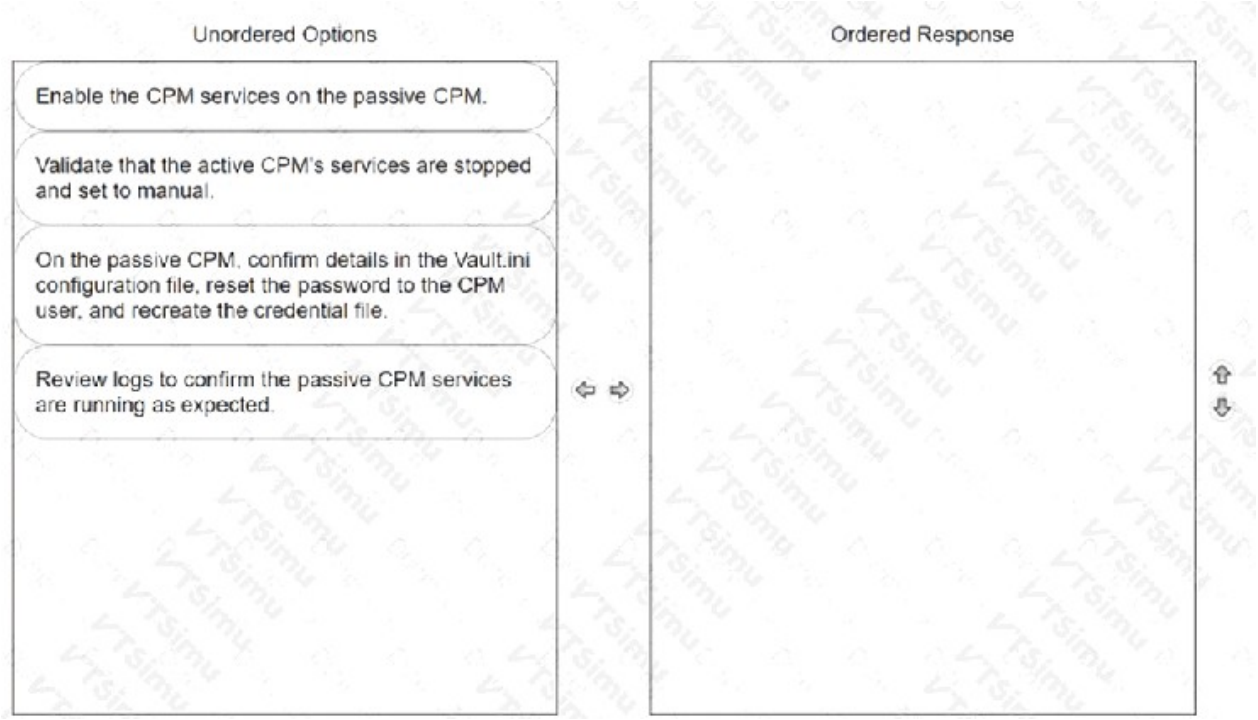
Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1 - (SIMULATION)

Arrange the steps to failover to the passive CPM in the correct sequence.



ANSWER: Check the explanation for the answer

Explanation:

Correct failover sequence:

This sequence prevents two CPMs from operating concurrently, prepares the passive CPM credentials and Vault connection configuration, starts the newly active CPM, and then verifies successful operation through its logs.

QUESTION NO: 2

Following the installation of the PSM for SSH server, which additional tasks should be performed? (Choose 2.)

A. Delete the user.cred file used during installation.

B. Delete the vault.ini you used during installation.

C. Delete the psmpparms file you used during installation.

D. Package all installation log files for upload to CyberArk.

ANSWER: A C

Explanation:

After PSM for SSH installation is complete, delete the user.cred file used during installation and delete the psmpparms file used during installation. These are installation-time artifacts rather than files needed for normal PSM for SSH operation. The credential file is created to supply the installation process with the authorized Vault user credentials needed to register and configure the component. It must be removed once that process has finished so that sensitive credential material is not retained on the host. The parameter file contains the values supplied to the installer, including environment-specific configuration details. Removing it reduces unnecessary exposure of deployment information and follows the post-installation

cleanup procedure. This cleanup should be performed only after confirming that installation completed successfully and that the PSM for SSH service and its Vault connectivity are operational. CyberArk's documentation portal provides the current Privilege Cloud installation and PSM for SSH deployment guidance at CyberArk Documentation. For product and implementation resources, see CyberArk Resources.

QUESTION NO: 3

To disable the PSM default Support for Browser Sessions, which option should be set to 'No* before running Hardening?

A. SupportWebApplications

B. SupportBrowsers

C. SupportWebBrowsers

D. SupportHTML5Content

ANSWER: A

Explanation:

SupportWebApplications is the PSM hardening configuration parameter that controls whether PSM is prepared to support web-application, including browser-based, sessions. Before executing the PSM hardening process, setting this parameter to **No** directs the hardening process not to enable the components and configuration required for browser-session support. This must be decided before hardening because the hardening workflow applies the selected configuration to the PSM host, including the relevant application-support settings and security controls. CyberArk's PSM deployment and hardening guidance describes selecting the web-application support setting in the PSM hardening configuration before the hardening script is run. Using **SupportWebApplications** accurately reflects CyberArk's parameter naming and its broader scope: it governs support for web applications rather than referring only to a particular browser executable or to HTML content. Administrators should retain the associated hardening configuration as part of their PSM build documentation so that a later change in required session types can be implemented through the documented configuration and hardening procedure. See CyberArk's PSM hardening documentation and PSM installation guidance.

QUESTION NO: 4

In the directory lookup order, which directory service is always looked up first for the CyberArk Privilege Cloud solution?

A. Active Directory

B. LDAP

C. Federated Directory

D. CyberArk Cloud Directory

ANSWER: D

Explanation:

CyberArk Cloud Directory is correct because it is the cloud-hosted directory built into the CyberArk Privilege Cloud service and is given priority during directory lookup. When Privilege Cloud must resolve a user or group for authentication, authorization, or directory mapping, it first checks the CyberArk Cloud Directory before proceeding through any configured external directory sources. This priority enables CyberArk-managed cloud identities and groups to be recognized consistently, including identities used to administer and access the Privilege Cloud service. The lookup sequence is important because it determines where Privilege Cloud first attempts to find the requested identity and its associated directory information. Organizations can integrate external identity sources and use federation as part of their access design, but the built-in Cloud Directory remains the first directory service queried in the Privilege Cloud lookup order. This behavior supports the service's cloud-native identity foundation while allowing customers to extend access through their connected enterprise identity environment. CyberArk describes Privilege Cloud as a SaaS privileged-access-management offering at

CyberArk Privilege Cloud; product documentation and configuration guidance are available through the CyberArk Documentation Portal.

QUESTION NO: 5

A PSM for SSH server has been installed successfully by using installation-time credential and parameter files. A security review requires removal of files that are no longer needed for normal operation. Which files should be removed? (Choose 2.)

A. user.cred

B. vault.ini

C. psmpparms

D. sshd_config

E. PSM for SSH service log files

ANSWER: A C

Explanation:

The **user.cred** file and the **psmpparms** file are installation-time artifacts that should be deleted after a successful PSM for SSH installation. The credential file can contain protected authentication material used by the installer, while the parameter file contains deployment-specific installation values.

The SSH daemon configuration and Vault configuration are required by the installed service and must not be removed as post-installation cleanup.

QUESTION NO: 6

When installing the PSM and CPM components on the same Privilege Cloud Connector, what should you consider when hardening?

A. PSM settings override the CPM settings when referring to the same parameter.

B. CPM settings override the PSM settings when referring to the same parameter

C. They can only be installed on the same Privilege Cloud Connector when installed ' in Domain ' .

D. They can only be installed on the same Privilege Cloud Connector when installed ' out of Domain ' .

ANSWER: A

Explanation:

PSM settings override the CPM settings when referring to the same parameter. When Privileged Session Manager and Central Policy Manager are co-located on one Privilege Cloud Connector, both component-hardening procedures can configure overlapping Windows security settings. CyberArk documents that, where the PSM and CPM hardening configuration addresses the same parameter, the PSM configuration takes precedence. Administrators should therefore plan and validate the final server configuration with that precedence in mind, rather than assuming that applying CPM hardening last will control a shared setting. This is especially important when reviewing local security policy, service-related settings, firewall rules, or other host-level controls affected by component installation and hardening. Applying the supported hardening process and recognizing PSM's precedence helps ensure the connector remains in a supported, secure configuration while it performs both password-management and session-management responsibilities. Before placing both services on the same connector, confirm that the sizing, installation, and hardening guidance for the deployed Privilege Cloud offering supports the combined role, then validate the resulting effective policies after installation. CyberArk's product documentation is available through the CyberArk Documentation Portal; see also CyberArk's Privileged Access Manager product information for the roles performed by CPM and PSM.

QUESTION NO: 7

During CPM hardening, which locally created users are granted Logon as a Service rights in the local group policy? (Choose 2.)

A. PasswordManager

B. PluginManagerUser

C. ScannerUser

D. PasswordManagerUser

E. CPMServiceAccount

ANSWER: A D

Explanation:

PasswordManager and **PasswordManagerUser** are the locally created CPM-related accounts assigned the Windows *Log on as a service* user right during CPM hardening. CPM depends on its hardened local service identities being able to start and continue under the Windows Service Control Manager without requiring an interactive desktop logon. Assigning this right enables the CPM components operating under these identities to perform their automated password-management workload, including scheduled verification, reconciliation, and change activities, while retaining the separation of service execution from ordinary interactive user access. The hardening configuration is therefore part of establishing the intended CPM operating context and should be preserved when local security policy, Group Policy Objects, or account-rights baselines are applied to the CPM server. CyberArk documentation should be consulted for the applicable Privilege Cloud CPM installation and hardening procedures for the deployed version: CyberArk Documentation. The Windows meaning and management of this specific user right are described by Microsoft in Log on as a service.