

# Exam Questions CPC-SEN

CyberArk Sentry - Privilege Cloud

<https://www.2passeasy.com/dumps/CPC-SEN/>



#### NEW QUESTION 1

Which statement is correct about using the AllowedSafes platform parameter?

- A. It allows users to access accounts in specific safes.
- B. It prevents the CPM from scanning all safes, restricting it to scan only safes that match the AllowedSafes configuration.
- C. It allows the CPM to access PSM safes to monitor platform configuration and connection component changes.
- D. It prevents the CPM from processing pending items in the Discovery safes enforcing manual intervention to complete the onboarding process.

**Answer: B**

#### Explanation:

The correct statement about using the AllowedSafes platform parameter is that it prevents the Central Policy Manager (CPM) from scanning all safes, restricting it to scan only safes that match the AllowedSafes configuration. This parameter is crucial in large-scale deployments where efficiency and resource management are key. By specifying which safes the CPM should manage, unnecessary scanning of irrelevant safes is avoided, thus optimizing the CPM's performance and reducing the load on the CyberArk environment. This configuration can be found in the platform management section of the CyberArk documentation.

#### NEW QUESTION 2

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: AD**

#### Explanation:

During the Central Policy Manager (CPM) hardening process, the locally created users that are granted 'Logon as a Service' rights in the local group policy are typically PasswordManager and PasswordManagerUser. These accounts are crucial for the CPM's operation as they handle password management tasks and require the ability to log on as a service to perform their functions effectively. This configuration is established to ensure that these service accounts can operate under service control manager without interruption, which is critical for automated password rotations and other security processes managed by the CPM. This detail is typically outlined in the CyberArk CPM installation and configuration guide.

#### NEW QUESTION 3

How can a platform be configured to work with load-balanced PSMs?

- A. Remove all entries from configured PSM Servers except for the ID of the PSMs with load balancing.
- B. Create a new PSM definition that targets the load balancer IP address and assign to the platform.
- C. Include details of the PSMs with load balancing in the Basic\_psm.ini file on each PSM server.
- D. Use the Privilege Cloud Portal to update the Session Management settings for the platform in the Master Policy.

**Answer: B**

#### Explanation:

To configure a platform to work with load-balanced Privileged Session Managers (PSMs), you should:

? Create a new PSM definition that targets the load balancer IP address and assign

it to the platform (Option B). This approach involves configuring the platform settings to direct session traffic through a load balancer that distributes the load across multiple PSM servers. This is effective in environments where high availability and fault tolerance are priorities.

Reference: CyberArk's setup guidelines for high-availability environments typically recommend configuring platforms to utilize load balancers to ensure continuous availability and optimal distribution of session management tasks.

#### NEW QUESTION 4

You plan to install Privilege Cloud Connectors on your AWS and Azure environments.

What is the maximum number of concurrent RDP/SSH sessions that each connector can handle for Large Implementations?

- A. 1-10
- B. 31-60
- C. 100
- D. 200

**Answer: B**

#### Explanation:

For large implementations of CyberArk Privilege Cloud Connectors in AWS and Azure environments, each connector can handle between 31-60 concurrent RDP/SSH sessions.

This capacity is specified in the CyberArk documentation concerning Privilege Cloud Connectors and their scalability options. It is designed to support a higher volume of concurrent sessions to meet the needs of larger enterprise environments, ensuring that multiple users can securely access resources without significant performance degradation.

#### NEW QUESTION 5

You are creating a PSM Load Balanced Virtual Server Configuration.

What are the default service ports / protocols used for RDS and the PSM Health Check service?

- A. RDP/389 HTTP/443
- B. RDP/3389 HTTPS/443
- C. UDP/53 HTTPS/389

D. RDP/636 HTTPS/443

Answer: B

Explanation:

In a PSM Load Balanced Virtual Server Configuration, the default service ports/protocols used are RDP/3389 and HTTPS/443. RDP (Remote Desktop Protocol) typically uses port 3389 for remote desktop services, which is essential for PSM functionalities involving remote sessions. HTTPS, which utilizes port 443, is used for the PSM Health Check service to ensure secure and encrypted communication during the monitoring and health verification processes of the PSM services.

NEW QUESTION 6

DRAG DROP

Arrange the steps to install passive CPM using Connector Management in the correct sequence

Unordered Options

Run the Connector Management Connector installer.

When prompted to select the CPM mode, select Passive.

When prompted to select the components to install, select CPM.

Install the CPM and optionally PSM, if required.

Ordered Response

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To correctly arrange the steps for installing a passive CPM using Connector Management, you should follow this order:  
? Run the Connector Management Connector installer.Begin the installation process by running the installer for the Connector Management Connector. This is the initial step where you set up the basic environment and prerequisites needed for the CPM installation.  
? When prompted to select the components to install, select CPM.During the installation process, you'll be asked to choose which components to install. Here, you should select the CPM (Central Policy Manager) to proceed with setting it up specifically for your needs.  
? When prompted to select the CPM mode, select Passive.After selecting the CPM component, the installer will ask for the mode in which the CPM should operate. Choose 'Passive' to configure the CPM in a passive mode, which is typically used for failover or load balancing purposes.  
? Install the CPM and optionally PSM, if required.Complete the installation of the CPM and, if necessary, the Privileged Session Manager (PSM). This step finalizes the installation process, setting up the CPM to function in the specified passive mode and integrating PSM if it's part of your deployment plan.  
These steps ensure that the CPM is installed correctly in the passive mode, providing a robust setup for high availability or disaster recovery configurations.

NEW QUESTION 7

After correctly configuring reconciliation parameters in the Prod-AIX-Root-Accounts Platform, this error message appears in the CPM log: CACPM410E Ending password policy Prod-AIX-Root-Accounts since the reconciliation task is active but the AllowedSafes parameter was not updated What caused this situation?

- A. The reconciliation account defined in the Platform is in a locked state and is not accessible.
- B. The CPM is currently configured to use to an unsigned engine.
- C. The AllowedSafes parameter does not include the safe containing the reconciliation account defined in the Platform.
- D. A second CPM is incorrectly configured to manage the reconciliation account's safe which is causing a deadlock situation between the two CPMs.

Answer: C

Explanation:

The error message "CACPM410E Ending password policy Prod-AIX-Root-Accounts since the reconciliation task is active but the AllowedSafes parameter was not updated" suggests an issue with configuration parameters. The likely cause is:

? The AllowedSafes parameter does not include the safe containing the reconciliation account defined in the Platform (Option C). This parameter must accurately reflect all safes where the reconciliation account operates to ensure proper management and access by the Central Policy Manager (CPM). If the safe containing the reconciliation account is not listed, the CPM cannot perform its tasks, leading to this error.

Reference: CyberArk??s error codes and troubleshooting guides detail how specific configuration mismatches, like an incomplete AllowedSafes parameter, can disrupt normal operations, especially in reconciliation processes.

#### NEW QUESTION 8

Which tool configures the user object that will be used during the installation of the PSM for SSH component?

- A. CreateUserPass
- B. CreateCredFile
- C. ConfigureCredFile
- D. ConfigureUserPass

**Answer: B**

#### Explanation:

The tool used to configure the user object for the installation of the PSM for SSH component is CreateCredFile. This tool is responsible for creating a credentials file that stores the necessary user details required during the installation process, ensuring secure and correct authentication.

References:

? CyberArk Privilege Cloud Introduction

#### NEW QUESTION 9

A CyberArk Privileged Cloud Shared Services customer asks you how to find recent failed login events for all users. Where can you do this without generating reports?

- A. Privileged Cloud Portal
- B. Identity Administration Portal
- C. both Identity Administration and Identity User Portals
- D. Identity User Portal

**Answer: A**

#### Explanation:

To find recent failed login events for all users in CyberArk Privileged Cloud Shared Services without generating reports, you can use the Privileged Cloud Portal. This portal provides administrators with direct access to security and audit logs, including failed login attempts. It offers a real-time view and monitoring capabilities that allow for immediate visibility into authentication activities and potential security issues. This feature is crucial for maintaining the security and integrity of privileged accounts, enabling administrators to quickly respond to and investigate authentication failures.

#### NEW QUESTION 10

Your customer is using Privilege Cloud Shared Services. What is the correct CyberArk Vault address for this customer?

- A. carkvault-<subdomain>.privilegecloud.cyberark.cloud
- B. vault-<subdomain>.privilegecloud.cyberark.cloud
- C. v-<subdomain>.privilegecloud.cyberark.cloud
- D. carkvlt-<subdomain> privilegecloud.cyberark.cloud

**Answer: B**

#### Explanation:

For customers using CyberArk Privilege Cloud Shared Services, the correct format for the CyberArk Vault address is:

? vault-<subdomain>.privilegecloud.cyberark.cloud (Option B). This format is used to access the vault services provided by CyberArk in the cloud environment, where <subdomain> is the unique identifier assigned to the customer??s specific instance of the Privilege Cloud.

Reference: CyberArk??s Privilege Cloud documentation provides details on how to access various services, including the vault. The standard naming convention for accessing the vault services in the cloud typically follows this format.

#### NEW QUESTION 10

What is a requirement when installing the PSM on multiple Privileged Cloud Connector servers?

- A. Each PSM must have the same path to the same recordings directory.
- B. All PSMs in the environment must be configured to use load balancing.
- C. Additional Privilege Cloud Connector servers cannot have CPM installed.
- D. In-domain servers cannot be used when deploying multiple PSM servers.

**Answer: A**

#### Explanation:

When installing the Privileged Session Manager (PSM) on multiple servers, it is required that each PSM installation has the same path to the same recordings directory. This is necessary to ensure that session recordings are stored consistently across different PSM instances, which is important for high availability and load balancing implementations, as well as for maintaining a unified audit trail.

References:

? CyberArk documentation on installing multiple PSM servers

#### NEW QUESTION 15

Refer to the exhibit.



You set up your LDAP Directory in CyberArk Identity, but encountered an error during the connection test. Which scenarios could represent a valid misconfiguration? (Choose 2.)

# Test Connection



Cannot contact the LDAP server. Possible causes of this error include: The transport connection to the LDAP server is not secured with SSL, the server running the connector does not trust the LDAP server's SSL certificate or the LDAP server is not reachable on the specified port (636 if not specified).

Close

- A. TCP Port 636 could be blocked by a network firewall, preventing communication between the CyberArk Identity Connector and the LDAP Server.
- B. All required CA Certificates have been installed on the CyberArk Identity Connector but the LDAP Bind credentials provided are incorrect.
- C. 'Verify Server Certificate' is activated but the provided hostname is not listed as a Subject Alternative Name (SAN) in the LDAP server's certificate.
- D. TCP Port 636 could be blocked by a network firewall, preventing communication between the Secure Tunnel and the LDAP Server.

**Answer:** AC

## Explanation:

From the error message provided, two likely scenarios could represent valid misconfigurations:

? TCP Port 636 could be blocked by a network firewall, preventing communication between the CyberArk Identity Connector and the LDAP Server (A). This is a common issue where firewall settings prevent the secure communication port (typically 636 for LDAPS) from transmitting data between the server and the connector, thus blocking the connection attempt.

? 'Verify Server Certificate' is activated but the provided hostname is not listed as a Subject Alternative Name (SAN) in the LDAP server's certificate (C). This scenario occurs when SSL/TLS security measures are stringent, requiring that the hostname used to connect to the LDAP server must match one listed in the server's SSL certificate. If the hostname does not match, the connection will fail due to SSL certificate validation errors.

## NEW QUESTION 16

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:** AC

## Explanation:

Following the installation of the PSM for SSH server, certain security and cleanup tasks are crucial to secure the environment and eliminate potential vulnerabilities:

? Delete the user.cred file used during installation (A): The user.cred file contains sensitive credential information used during the installation process. Deleting this file post-installation ensures that this sensitive data is not left accessible on the system, mitigating the risk of unauthorized access.

? Delete the psmpparms file you used during installation (C): Similar to the user.cred file, the psmpparms file often contains parameters that might include sensitive configuration details. Removing this file after the installation process is completed helps in securing the server by removing potential leakage points of sensitive information.

These actions are part of best practices to secure the installation environment and reduce the risk of sensitive information exposure.

## NEW QUESTION 18

Your customer recently merged with a smaller organization. The customer's connector has no network connectivity to the smaller organization's infrastructure. You need to map LDAP users from both your customer and the smaller organization. How is this achieved?

- A. Create the required users in one directory and configure the Identity Connector to read that directory, as there can only be one Identity Connector.
- B. Create mappings for both directories from the original Identity Connector.
- C. Deploy Identity Connectors in the newly acquired infrastructure and create user mappings.
- D. Switch all users to SAML authentication as there can only be one Identity Connector.

**Answer:** C

## Explanation:

To map LDAP users from both your customer and the smaller organization they have merged with, especially when there is no network connectivity between the

two infrastructures, the best approach is to:

? Deploy Identity Connectors in the newly acquired infrastructure and create user mappings (Option C). This involves setting up additional Identity Connectors within the smaller organization's network. These connectors will facilitate the integration of user directories from both organizations into the customer's Privilege Cloud environment.

Reference: CyberArk documentation on Identity Connectors often outlines the capability of deploying multiple connectors to manage different user directories, especially useful in scenarios involving mergers or acquisitions where separate infrastructures need integration.

#### NEW QUESTION 21

Which authentication methods does PSM for SSH support? (Choose 2.)

- A. OIDC
- B. MFA Caching
- C. SAML
- D. RADIUS
- E. Client Authentication Certificate

**Answer:** DE

#### Explanation:

PSM for SSH supports various authentication methods, specifically focusing on secure and verified access mechanisms. The supported methods include:

? RADIUS (D): Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting management for users who connect and use a network service. PSM for SSH utilizes RADIUS to authenticate SSH sessions, which adds an additional layer of security by centralizing authentication requests to a RADIUS server.

? Client Authentication Certificate (E): This method uses certificates for authentication, where a client presents a certificate that the server verifies against known trusted certificates. This type of authentication is highly secure as it ensures that both parties involved in the communication are precisely who they claim to be, making it suitable for environments that require stringent security measures.

These methods provide robust security options for SSH sessions managed through CyberArk's PSM, ensuring that only authorized users can access critical systems.

#### NEW QUESTION 24

Which users are Privilege Cloud Standard built-in users? (Choose 2.)

- A. NASCorp
- B. saascorps
- C. CyberArkAdmin
- D. remoteAccessAppUser
- E. PASReporterUser

**Answer:** CE

#### Explanation:

In CyberArk Privilege Cloud Standard, certain users are predefined as built-in for administrative and operational purposes. The built-in users include:

? CyberArkAdmin (Option C): This user is typically set up as a default administrator with full access to manage and configure the Privilege Cloud environment.

? PASReporterUser (Option E): This user is often configured as a reporting user, designed to generate and access various reports without having broader administrative privileges.

Reference: CyberArk's Privilege Cloud setup and administration guides usually list these users as part of the default configuration to facilitate initial setup and ongoing management of the platform.

#### NEW QUESTION 29

What is the default username for the PSM for SSH maintenance user?

- A. proxymng
- B. psm\_p\_maintenance
- C. psmmaintenanceuser
- D. proxyusr

**Answer:** B

#### Explanation:

The default username for the Privileged Session Manager (PSM) for SSH maintenance user in CyberArk Privilege Cloud is psm\_p\_maintenance. This account is used for maintenance purposes and is integral for administrative tasks and configurations related to SSH sessions managed by the PSM. The username is predefined and standardized across deployments to maintain consistency and ensure security best practices are adhered to. The username is mentioned in the CyberArk official documentation regarding PSM configuration for SSH.

#### NEW QUESTION 30

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:** B

#### Explanation:

To disable the PSM default support for browser sessions, the option SupportBrowsers should be set to 'No' before running the hardening process. This configuration change is made within the PSM's configuration files, typically found in the PSM's administrative interface or directly within specific XML configuration files like PSMHardening.xml. Setting this option to 'No' prevents the PSM from processing session requests that involve web browsers, thereby enhancing security by limiting the session types the PSM will support. This setting is particularly important in environments where web browsing sessions are

deemed unnecessary or too risky.

#### NEW QUESTION 34

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CPC-SEN Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CPC-SEN Product From:

<https://www.2passeasy.com/dumps/CPC-SEN/>

## Money Back Guarantee

### CPC-SEN Practice Exam Features:

- \* CPC-SEN Questions and Answers Updated Frequently
- \* CPC-SEN Practice Questions Verified by Expert Senior Certified Staff
- \* CPC-SEN Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* CPC-SEN Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year