

# CyberArk

## Exam Questions CPC-SEN

CyberArk Sentry - Privilege Cloud



#### NEW QUESTION 1

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:

When installing the PSM and CPM components on the same Privilege Cloud Connector and considering the hardening process, it's important to note that PSM settings override the CPM settings when referring to the same parameter. This hierarchy is crucial in ensuring that the more stringent security settings required by PSM, which typically handles direct interaction with end-user sessions, take precedence over CPM settings. This setup helps maintain robust security practices by applying the most restrictive configuration where conflicts occur.

#### NEW QUESTION 2

A support team has asked you to provide the previous password for an account that had its password recently changed by the CPM. In which tab within the account's overview page can you retrieve this information?

- A. Activities
- B. Details
- C. Versions

**Answer:** D

#### Explanation:

To retrieve the previous password for an account that had its password changed by the CPM, you should look under the Versions tab within the account's overview page. This tab maintains a history of password changes, including previous passwords, along with other historical data points that allow for tracking changes over time. This feature is critical for auditing and rollback purposes in environments where knowing past credentials is necessary for troubleshooting or compliance.

#### NEW QUESTION 3

What is the correct CyberArk user to use when installing the Privilege Cloud Connector software?

- A. installeruser@<suffix>
- B. Administrator
- C. <subdomain>\_admin
- D. Installer

**Answer:** C

#### Explanation:

The correct CyberArk user to use when installing the Privilege Cloud Connector software is typically formatted as <subdomain>\_admin. This username format indicates a privileged administrative account associated with the specific subdomain of the CyberArk Privilege Cloud installation. It ensures that the user has sufficient permissions to perform installation tasks across the environment, which are crucial for setting up and configuring the connectors correctly. Details about user roles and permissions can be found in the CyberArk Privilege Cloud installation and configuration guide.

#### 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

When installing the first CPM within Privilege Cloud using the Connector Management Agent, what should you set the Installation Mode to in the CPM section?

- A. Active
- B. Passive
- C. Default
- D. Primary

**Answer:** A

#### Explanation:

When installing the first CyberArk Privilege Management (CPM) instance in the Privilege Cloud using the Connector Management Agent, the installation mode should be set to "Active". This configuration sets the CPM to be actively involved in password management and task processing without being in a standby or passive mode. Here are the step-by-step details:

? Download the Connector Management Agent: Obtain the installer from the CyberArk Marketplace or your installation kit.

? Run the Installer: Start the setup and select the CPM component to install.

? Choose Installation Mode: When prompted, select "Active" as the installation mode. This sets up the CPM as the primary node responsible for handling password management operations.

This setup ensures that the CPM is immediately active and capable of handling requests without waiting for manual intervention or failover.

Reference: CyberArk's official documentation provides guidance on setting up the CPM, where it specifies the modes and their purposes.

#### NEW QUESTION 6

You are planning to configure Multi-Factor Authentication (MFA) for your CyberArk Privilege Cloud Shared Service. What are the available authentication methods?

- A. LDAR RADIUS
- B. SAML OpenID Connect (OIDC)
- C. Window
- D. PK
- E. RADIUS
- F. CyberArk, LDA
- G. SAM
- H. OpenID Connect (OIDC)
- I. Privilege Cloud Shared Services fully utilize CyberArk Identity and its MFA options.
- J. Only RADIUS can be used to achieve MFA across all components, such as PSM for RDP and PSM for SSH.

**Answer: B**

#### Explanation:

In CyberArk Privilege Cloud, Multi-Factor Authentication (MFA) can be configured to enhance security by requiring multiple methods of authentication from independent categories of credentials to verify the user's identity. The available authentication methods include:

? Windows Authentication: Leverages the user's Windows credentials.

? PKI (Public Key Infrastructure): Utilizes certificates to authenticate.

? RADIUS (Remote Authentication Dial-In User Service): A networking protocol that provides centralized Authentication, Authorization, and Accounting management.

? CyberArk: Uses CyberArk's own authentication methods.

? LDAP (Lightweight Directory Access Protocol): Protocol for accessing and maintaining distributed directory information services.

? SAML (Security Assertion Markup Language): An open standard that allows identity providers to pass authorization credentials to service providers.

? OpenID Connect (OIDC): An authentication layer on top of OAuth 2.0, an authorization framework.

Reference for this can be found in the CyberArk Privilege Cloud documentation, which details the integration and setup of MFA using these methods.

#### NEW QUESTION 7

Which option correctly describes the authentication differences between CyberArk Privilege Cloud and CyberArk PAM Self-Hosted?

- A. CyberArk Privilege Cloud only provides a username and password authentication without third-party IdP integration; CyberArk PAM Self-Hosted uses traditional on-premises methods such as Windows and LDA
- B. but lacks modern protocols such as SAML or OIDC.
- C. CyberArk Privilege Cloud uses cloud-based methods, integrating with CyberArk Identity for MF
- D. and supports SAML and OIDC; CyberArk PAM Self-Hosted depends on on-premises methods such as RADIUS and LDAP, but can adopt SAML or OIDC with additional setups.
- E. CyberArk Privilege Cloud requires on-premises components for all authentication and does not support other cloud-based authentication protocols; CyberArk PAM Self-Hosted offers a wide array of methods, including support for SAM
- F. OID
- G. and other modern protocols, without needing on-premises components.
- H. Both use the same authentication methods.

**Answer: B**

#### Explanation:

The correct description of the authentication differences between CyberArk Privilege Cloud and CyberArk PAM Self-Hosted is that CyberArk Privilege Cloud uses cloud-based methods, integrating with CyberArk Identity for Multi-Factor Authentication (MFA), and supports SAML and OIDC, while CyberArk PAM Self-Hosted relies on on-premises methods such as RADIUS and LDAP, but can adopt SAML or OIDC with additional setups. CyberArk Privilege Cloud is designed to leverage modern cloud-based authentication protocols to enhance security and ease of use, particularly in distributed and diverse IT environments. In contrast, CyberArk PAM Self-Hosted offers flexibility to use traditional on-premises authentication methods but also supports modern protocols if configured to do so.

#### NEW QUESTION 8

Before the hardening process, your customer identified a PSM Universal Connector executable that will be required to run on the PSM. Which file should you update to allow this to run?

- A. PSMConfigureAppLocker.xml
- B. PSMHardening.xml
- C. PSMAAppConfig.xml
- D. PSMConfigureHardening.xml

**Answer: A**

#### Explanation:

To allow a PSM Universal Connector executable to run on the PSM after the hardening process, you should update the PSMConfigureAppLocker.xml file. This file configures AppLocker, which is a feature that controls which apps and files users can run on a system. Including the necessary executable in the PSMConfigureAppLocker.xml ensures it is whitelisted by AppLocker policies, thus permitted to execute even under the hardened security settings of the PSM environment. References to this configuration can be found in the CyberArk Privilege Session Manager implementation documentation,

specifically in sections detailing customization and security hardening of environment configurations.

#### NEW QUESTION 9

You have been tasked with deploying a Privilege Cloud PSM for SSH connector. When the initial installation has successfully completed, you create and permission several maintenance users to be used for administering the connector. Which configuration file must be updated to define these maintenance users?

- A. sshd.config
- B. basic\_psmserver.conf
- C. sshd\_config
- D. psmpparms

**Answer: C**

#### Explanation:

The sshd\_config file is the correct configuration file that must be updated to define maintenance users for administering the Privilege Cloud PSM for SSH connector. This file contains configurations for the SSH daemon, including user permissions and group settings. When adding maintenance users, their user accounts are created on the PSM

server, and then they are added to the AllowGroups parameter within the sshd\_config file to grant them the necessary permissions.

References:

? CyberArk documentation on the PSM for SSH environment<sup>1</sup>.

? CyberArk Sentry guide on how to add maintenance users for SSH PSM

? When deploying a Privilege Cloud PSM for SSH connector, the configuration file that must be updated to define maintenance users is "sshd\_config". This file is used to configure options specific to the SSH daemon, which includes user permissions, authentication methods, and other security-related settings. To add and configure maintenance users for the PSM for SSH, you will need to modify this file to specify allowed users and their respective privileges.

Reference: The configuration of SSH-related components typically involves the "sshd\_config" file, as outlined in SSH and PSM for SSH setup guides. This is a standard practice in systems that utilize SSH for secure communications and management.

#### NEW QUESTION 10

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 10

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 14

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 17

On the CPM, you want to verify if DEP is disabled for the required executables According to best practices, which executables should be listed? (Choose 2.)

- A. Telnet.exe
- B. Plink.exe
- C. putty.exe
- D. mstsc.exe

**Answer:** BC

## Explanation:

On the Central Policy Manager (CPM), it is crucial to verify that Data Execution Prevention (DEP) is disabled for specific executables required for proper operation according to best practices. The relevant executables include:

? Plink.exe (Option B): This executable is commonly used for SSH communications and may require DEP to be disabled to function correctly under certain configurations.

? putty.exe (Option C): Similar to Plink.exe, Putty is another essential tool for SSH communications and might also require DEP to be disabled to prevent any execution issues.

Reference: CyberArk's best practices for system configuration often highlight the need to adjust DEP settings for certain executables to ensure they run without interruption, particularly when these tools are crucial for secure communications and operations management.

## NEW QUESTION 21

You are deploying a CyberArk Identity Connector to integrate Privilege Cloud Shared Services with an Active Directory environment. Which requirement must be met?

- A. The Identity Connector Server must be joined to the Active Directory.
- B. The Server must be a member of the root domain of the Active Directory forest.
- C. The Identity Connector must be installed on a Domain Controller.
- D. The Identity Connector must be installed using Domain Administrator credentials.

**Answer:** A

## Explanation:

When deploying a CyberArk Identity Connector to integrate Privilege Cloud Shared Services with an Active Directory environment, the server hosting the Identity Connector must meet specific requirements to ensure proper integration and functionality. The necessary condition is:

? The Identity Connector Server must be joined to the Active Directory (Option A).

This requirement ensures that the server can communicate effectively with the Active Directory services and manage identity data securely and efficiently. Being part of the Active Directory domain facilitates authentication and authorization processes required for the connector to function correctly.  
Reference: CyberArk installation and configuration guides typically emphasize the importance of having the Identity Connector server joined to the domain to allow seamless interaction with Active Directory services.

## NEW QUESTION 22

.....



## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### 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

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The CPC-SEN Practice Test Here](#)**