CyberArk CPC-SEN Practice Questions

Shared by Mcmillan on 21-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

CyberArk User Neil is trying to connect to the Target Linux server 192.168.1.164 using a domain user ACME\linuxuser01 on domain acme.corp using PSM for SSH server

192.168.65.145.

What is the correct syntax?

Options:

A- ssh neil@linuxuser01:acme.corp@192.168.1.164@192.168.65.145
B- ssh neil@linuxuser01#acme.corp@192.168.1.164@192.168.65.145
C- sshneil@linuxuser01@192.168.1.164@192.168.65.145
D- ssh neil@linuxuser01@acme.corp@192.168.1.164@192.168.65.145

Answer:

B

Explanation:

In CyberArk Privilege Cloud, when connecting to a target server using the Privileged Session Manager (PSM) for SSH, the correct syntax for the SSH command includes the following format: ssh neil@linuxuser01#acme.corp@192.168.1.164@192.168.65.145. This syntax breaks down as follows:

neil: The CyberArk username.

linuxuser01#acme.corp: The domain user on the target Linux server, formatted as username#domain.

192.168.1.164: The IP address of the target Linux server.

192.168.65.145: The IP address of the PSM for SSH server.

This specific format ensures that the CyberArk Privileged Access Manager correctly interprets and routes the connection through the PSM for SSH to the intended target server.

CyberArk Privilege Cloud Introduction

CyberArk Privileged Access Manager

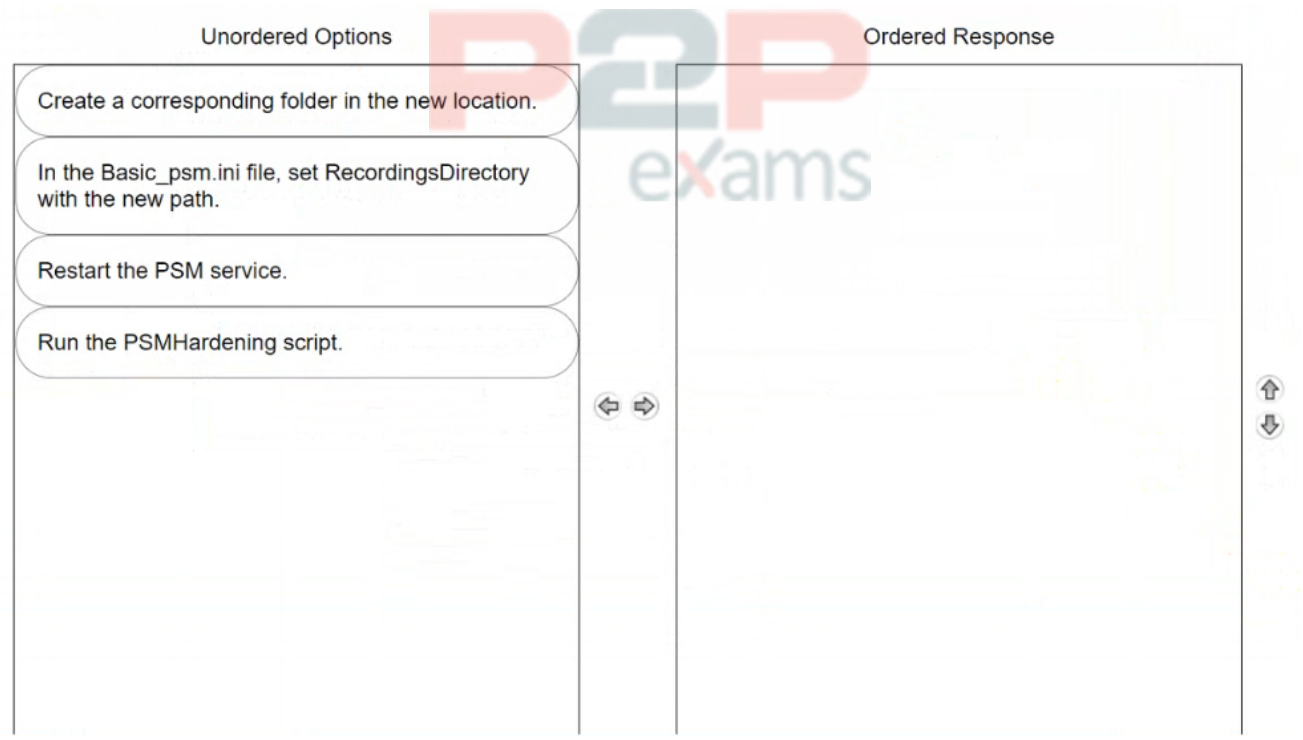
CyberArk Privilege Cloud - Manage Safe Members

CyberArk Security Fundamentals

Question 2

Question Type: OrderList

You want to change the default PSM recordings folder path on the Privilege Cloud Connector Arrange the steps to accomplish this in the correct sequence.



Answer:

Create a corresponding folder in the new location.In the Basic_psm.ini file, set RecordingsDirectory with the new path.Restart the PSM service.Run the PSMHardening script.

Question 3

Question Type: MultipleChoice

You are configuring firewall rules between the Privilege Cloud components and the Privilege Cloud. Which firewall rules should be set up to allow connections?

Options:

A- from the CyberArk Privilege Cloud to the Privilege Cloud components
B- from the Privilege Cloud components to the CyberArk Privilege Cloud
C- bi-directionally between the Privilege Cloud components and the CyberArk Privilege cloud
D- from the Privilege Cloud components to CyberArk.com

Answer:

C

Explanation:

When configuring firewall rules for CyberArk Privilege Cloud, it is essential to allow bi-directional communication between the Privilege Cloud components and the CyberArk Privilege Cloud. This ensures that all necessary communications for operations and management can occur securely in both directions.

CyberArk documentation on system requirements for outbound traffic network and port requirements1.

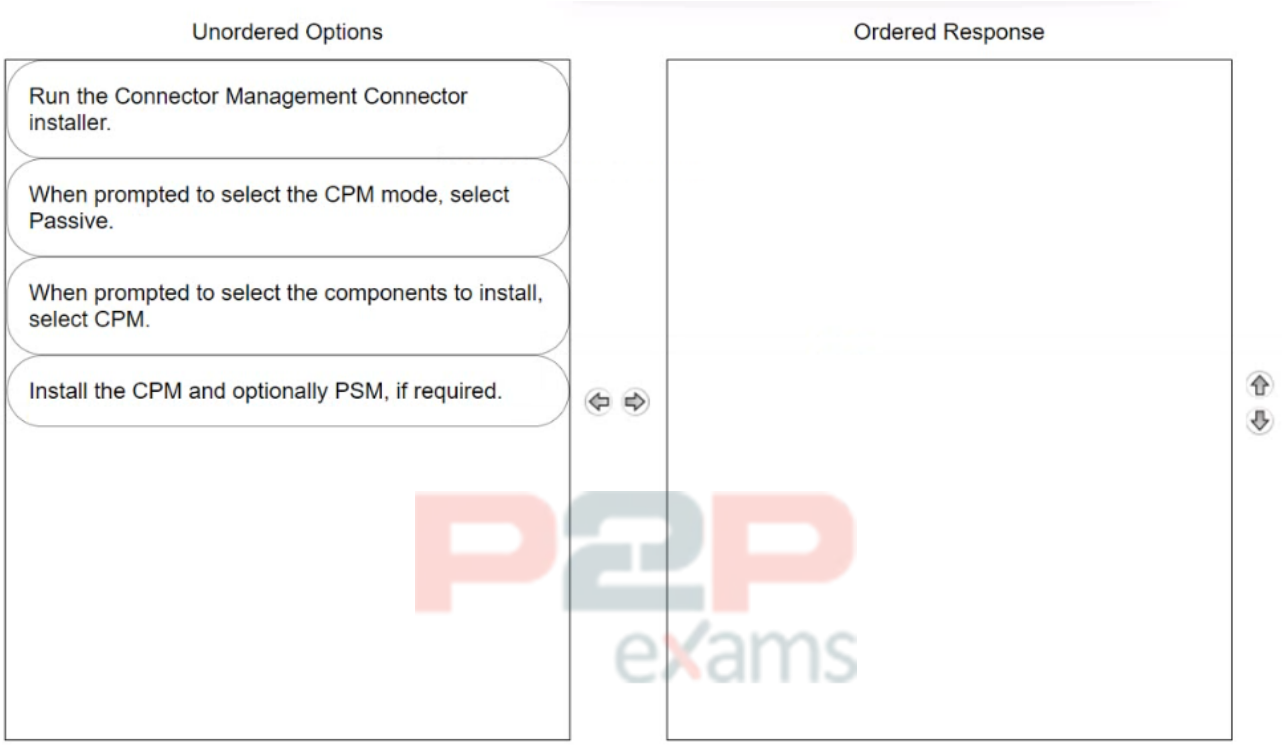
CyberArk documentation on setting up an IP allowlist, which enables Privilege Cloud customer-side components to communicate with the Privilege Cloud SaaS environment2.

CyberArk documentation on connecting to organization firewalls

Question 4

Question Type: OrderList

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



Answer:

Run the Connector Management Connector installer.When prompted to select the components to install, select CPM.When prompted to select the CPM mode, select Passive.Install the CPM and optionally PSM, if required.

Question 5

Question Type: MultipleChoice

What must be done before configuring directory mappings in the CyberArk Privilege Cloud Standard Portal for LDAP integration?

Options:

A- Retrieve the LDAPS certificate and deliver it to CyberArk.
B- Create a new domain in the Privilege Cloud Portal.
C- Make sure HTTPS (443/tcp) is reachable over the Secure Tunnel.
D- Ensure the user connecting to the domain has administrative privileges.

Answer:

C

Explanation:

Before configuring directory mappings in the CyberArk Privilege Cloud Standard Portal for LDAP integration, it is crucial to make sure HTTPS (443/tcp) is reachable over the Secure Tunnel. This setup ensures that the secure communication channel between the CyberArk Privilege Cloud and the LDAP server is operational. Secure Tunnel facilitates the encrypted and safe transmission of data, including LDAP queries and responses, essential for successful integration and ongoing operations.

Question 6

Question Type: MultipleChoice

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

Options:

A- LDAR RADIUS. SAML OpenID Connect (OIDC)
B- Windows. PKI. RADIUS. CyberArk, LDAP. SAML. OpenID Connect (OIDC)
C- Privilege Cloud Shared Services fully utilize CyberArk Identity and its MFA options.
D- 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.

Question 7

Question Type: MultipleChoice

What is a supported certificate format for retrieving the LDAPS certificate when not using the Cyberark provided LDAPS certificate tool?

Options:

A- .der
B- .p7b
C- p7c
D- p12

Answer:

A

Explanation:

For retrieving the LDAPS certificate when not using the CyberArk provided LDAPS certificate tool, the supported certificate format is .der. The DER (Distinguished Encoding Rules) format is a binary form of a certificate rather than the ASCII PEM format. This format is widely supported across various systems for securing LDAP connections by providing a mechanism for LDAP servers to authenticate themselves to users. This information can be verified by checking LDAP configuration guides and CyberArk's secure implementation documentation which outline supported certificate formats for LDAP integrations.

Question 8

Question Type: MultipleChoice

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

Options:

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 LDAP. but lacks modern protocols such as SAML or OIDC.
B- CyberArk Privilege Cloud uses cloud-based methods, integrating with CyberArk Identity for MFA. 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.
C- 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 SAML. OIDC. and other modern protocols, without needing on-premises components.
D- 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.

Question 9

Question Type: MultipleChoice

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

Options:

A- proxymng
B- psmp_maintenance
C- psmpmaintenanceuser
D- proxyusr

Answer:

B

Explanation:

The default username for the Privileged Session Manager (PSM) for SSH maintenance user in CyberArk Privilege Cloud is psmp_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.

Question 10

Question Type: MultipleChoice

What are dependencies to update or change the CPM credential? (Choose 2.)

Options:

A- APIKeyManager.exe
B- CreateCredFile.exe
C- CPM/nDomain_Hardening.ps1
D- CyberArk.TPC.exe
E- Data Execution Prevention

Answer:

B, D

Explanation:

To update or change the Central Policy Manager (CPM) credentials, dependencies include:

CreateCredFile.exe (B): This utility is used to create or modify the encrypted file that stores the CPM's credentials. It is essential for securely handling the credential updates.

CyberArk.TPC.exe (D): This executable is part of the CyberArk suite that manages trusted platform module operations, which can include tasks related to credential security and management, particularly when hardware security modules are involved.

Question 11

Question Type: MultipleChoice

What creating a new safe, What is the default number of password versions stored if using 'Save latest account versions' within version management settings?

Options:

A- 5
B- 10
C- 30
D- 90

Answer:

B

Explanation:

When creating a new safe and configuring the 'Save latest account versions' within version management settings, the default number of password versions stored is 10. This setting allows the safe to maintain up to 10 past versions of each password managed within it. This capability is essential for ensuring that previous password states can be accessed if needed, such as for audit purposes or rollback scenarios in the event of an update error or compromise.