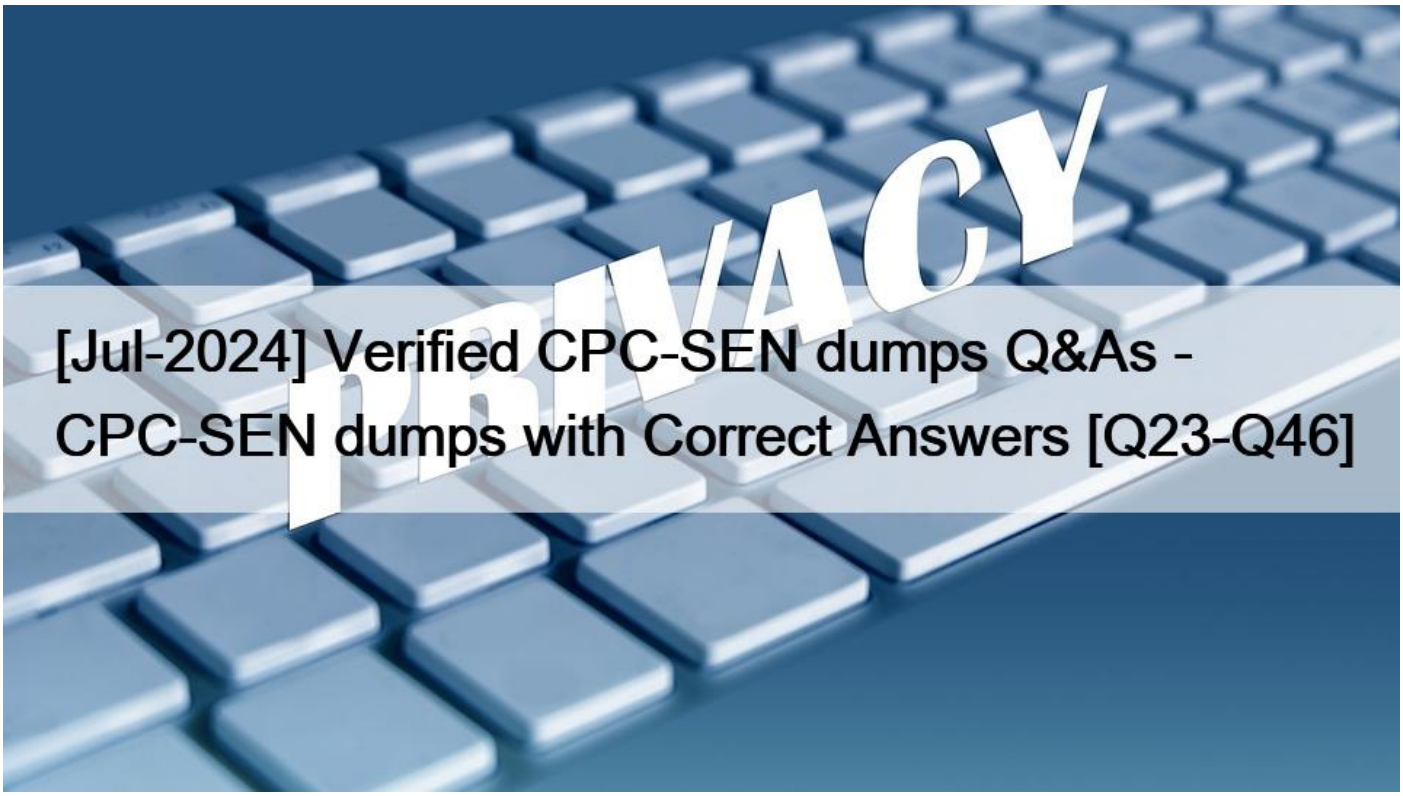
[Jul-2024 Verified CPC-SEN dumps Q&As - CPC-SEN dumps with Correct Answers [Q23-Q46



[Jul-2024] Verified CPC-SEN dumps Q&As - CPC-SEN dumps with Correct Answers
The Best CyberArk Sentry Study Guide for the CPC-SEN Exam

NO.23 In the directory lookup order, which directory service is always looked up first for the CyberArk Privilege Cloud solution?
* Active Directory
* LDAP
* Federated Directory
* CyberArk Cloud Directory

In the directory lookup order for the CyberArk Privilege Cloud solution, the “CyberArk Cloud Directory” is always looked up first. This directory service is a part of the CyberArk Privilege Cloud infrastructure and is specifically designed to handle identity and access management within the cloud environment efficiently. It prioritizes the CyberArk Cloud Directory for authentication and identity resolution before consulting any external directory services.

NO.24 How should you configure PSM for SSH to support load balancing?
* by using a network load balancer
* 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

To support load balancing for PSM for SSH, the configuration should be done by using a network load balancer. This method involves placing a network load balancer in front of multiple PSM for SSH servers to distribute incoming SSH traffic evenly among them. This setup enhances the availability and scalability of PSM for SSH by ensuring that no single server becomes a bottleneck,

thereby improving performance and reliability during high usage scenarios.

NO.25 After a scripted installation has successfully installed the PSM, which post-installation task is performed?
* The screen saver for the PSM local users is disabled.
* A new group called PSMShadowUsers is created.
* The PSMAdminConnect user password is reset.
* Remote desktop services are installed.

After the successful scripted installation of the Privileged Session Manager (PSM), one of the post-installation tasks is to disable the screen saver for the PSM local users. This is done to ensure that the PSMConnect and PSMAdminConnect users, which are created during the installation process, do not have a screen saver activated that could interfere with the operation of the PSM.

Reference:

CyberArk documentation on PSM post-installation tasks1.

CyberArk documentation on disabling the screen saver for PSM local users

NO.26 Which option correctly describes the authentication differences between CyberArk Privilege Cloud and CyberArk PAM Self-Hosted?
* 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.
* 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.
* 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.
* Both use the same authentication methods.

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.

NO.27 What are dependencies to update or change the CPM credential? (Choose 2.)
* APIKeyManager.exe
* CreateCredFile.exe
* CPM/nDomain_Hardening.ps1
* CyberArk.TPC.exe
* Data Execution Prevention

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.

NO.28 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?
* RDP/389 HTTP/443
* RDP/3389 HTTPS/443

C UDP/53 HTTPS/389
* RDP/636 HTTPS/443
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.

NO.29 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?
* PSMConfigureAppLocker.xml
* PSMHardening.xml
* PSMAppConfig.xml
* PSMConfigureHardening xml
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. Reference 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.

NO.30 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.)

* TCP Port 636 could be blocked by a network firewall, preventing communication between the CyberArk Identity Connector and the LDAP Server.
* All required CA Certificates have been installed on the CyberArk Identity Connector but the LDAP Bind credentials provided are incorrect.
* Verify Server Certificate’ is activated but the provided hostname is not listed as a Subject Alternative Name (SAN) in the

LDAP server’s certificate.
* TCP Port 636 could be blocked by a network firewall, preventing communication between the Secure Tunnel and the LDAP Server.
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.

NO.31 Which users are Privilege Cloud Standard built-in users? (Choose 2.)
* NASCorp
* saascorps
* CyberArkAdmin
* remoteAccessAppUser
* PASReporterUser
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.

NO.32 What is the recommended method to enable load balancing and failover of the CyberArk Identity Connector?
* Setup IIS based Application Request Routing on two or more CyberArk Identity Connector servers.
* Set up a network load balancer between two or more CyberArk Identity Connector servers.
* Set up two or more CyberArk Identity Connector servers only.
* Set up a Microsoft Failover Cluster on two or more CyberArk Identity Connector servers.
The recommended method to enable load balancing and failover of the CyberArk Identity Connector is to set up a network load balancer between two or more CyberArk Identity Connector servers. This setup allows for the distribution of requests across multiple servers, enhancing the availability and reliability of the service. Network load balancers efficiently manage traffic to ensure that no single connector server becomes a bottleneck, thereby improving overall performance and fault tolerance.

NO.33 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?
* 1-10
* 31-60
* 100
* 200
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.

NO.34 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?
* Privileged Cloud Portal
* Identity Administration Portal

C both Identity Administration and Identity User Portals
* Identity User Portal
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.

NO.35 Which tool configures the user object that will be used during the installation of the PSM for SSH component?
* CreateUserPass
* CreateCredFile
* ConfigureCredFile
* ConfigureUserPass
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.

Reference:

CyberArk Privilege Cloud Introduction

NO.36 In large-scale environments, it is important to enable the CPM to focus its search operations on specific Safes instead of scanning all Safes it sees in the Vault. How is this accomplished?
* MaxConcurrentConnection parameter on each platform policy
* Administration > Options > CPM Scanner.
* AllowedSafes Parameter on each platform policy
* Administration Options > CPM Settings
In large-scale environments, to enable the Central Policy Manager (CPM) to focus its search operations on specific Safes instead of scanning all Safes it sees in the Vault, the AllowedSafes parameter on each platform policy is used. This parameter can be configured within the platform settings in the CyberArk administration interface. By specifying safes in the AllowedSafes parameter, the CPM will only manage credentials within those designated safes, thereby optimizing performance and managing resources more efficiently by not scanning unnecessary safes. This setting is crucial for large environments where the CPM needs to be as efficient as possible due to the volume of managed accounts.

NO.37 What is a supported certificate format for retrieving the LDAPS certificate when not using the Cyberark provided LDAPS certificate tool?
* .der
* .p7b
* p7c
* p12
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.

NO.38 CyberArk User Neil is trying to connect to the Target Linux server 192.168.1.164 using a domain user ACMElinuxuser01 on domain acme.corp using PSM for SSH server

192.168.65.145.

What is the correct syntax?
* ssh neil@linuxuser01:acme.corp@192.168.1.164@192.168.65.145
* ssh neil@linuxuser01#acme.corp@192.168.1.164@192.168.65.145
* sshneil@linuxuser01@192.168.1.164@192.168.65.145
* ssh neil@linuxuser01@acme.corp@192.168.1.164@192.168.65.145

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.

Reference:

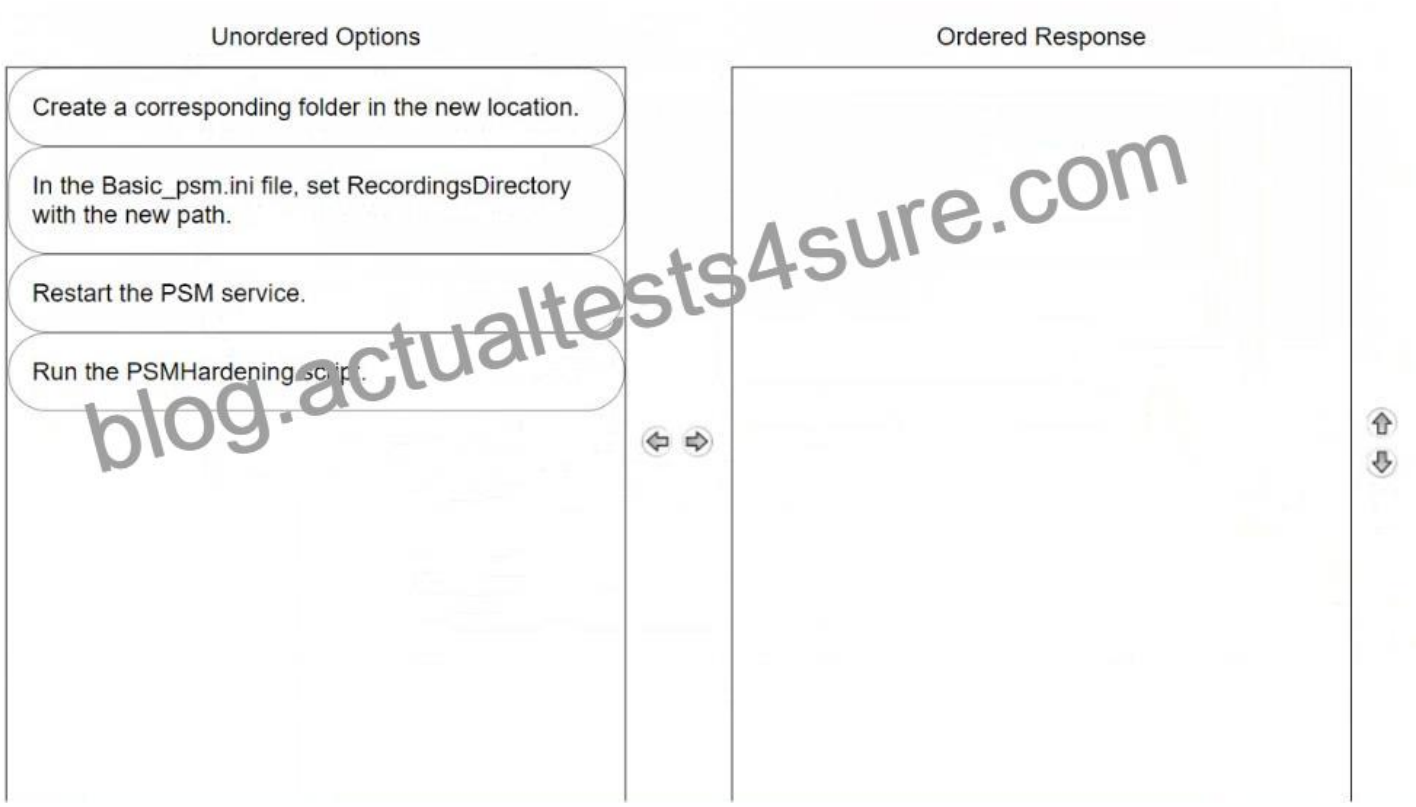
CyberArk Privilege Cloud Introduction

CyberArk Privileged Access Manager

CyberArk Privilege Cloud – Manage Safe Members

CyberArk Security Fundamentals

NO.39 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 Area

- 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.

1 – Create a corresponding folder in the new location.

2 – In the Basic_psm.ini file, set RecordingsDirectory with the new path.

3 – Restart the PSM service.

4 – Run the PSMHardening script.

NO.40 What must be done before configuring directory mappings in the CyberArk Privilege Cloud Standard Portal for LDAP integration?

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

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.

NO.41 Which statement is correct regarding the LDAP integration with CyberArk Privilege Cloud Standard?
* You must track the expiration date of the directory server certificate and contact CyberArk Support to renew it.
* LDAPS integration with Privilege Cloud requires StartTLS for secure and encrypted communication.
* For certificate trust to your directory server, only the Issuing CA certificate is required.
* The top-level domain entry of the directory must be unique in the chosen Privilege Cloud region.

For LDAP integration with CyberArk Privilege Cloud Standard, the correct statement is that only the Issuing CA certificate is required for certificate trust to your directory server. This setup simplifies the process of establishing a trusted connection between CyberArk and the LDAP server by necessitating only the certification of the issuing Certificate Authority (CA), rather than needing multiple certificates from different levels of the trust chain. This approach ensures that the SSL/TLS communication between CyberArk and the LDAP server is secured based on the trust of the issuing CA’s certificate.

NO.42 You are deploying a CyberArk Identity Connector to integrate Privilege Cloud Shared Services with an Active Directory environment. Which requirement must be met?
* The Identity Connector Server must be joined to the Active Directory.
* 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.
* The Identity Connector must be installed using Domain Administrator credentials.

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.

NO.43 How can a platform be configured to work with load-balanced PSMs?
* Remove all entries from configured PSM Servers except for the ID of the PSMs with load balancing.
* Create a new PSM definition that targets the load balancer IP address and assign to the platform.
* Include details of the PSMs with load balancing in the Basic_psm.ini file on each PSM server.
* Use the Privilege Cloud Portal to update the Session Management settings for the platform in the Master Policy.

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.

CPC-SEN certification guide Q&A from Training Expert Actualtests4sure:

https://www.actualtests4sure.com/CPC-SEN-test-questions.html]