

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

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?

- 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.

References:

? CyberArk Privilege Cloud Introduction

? CyberArk Privileged Access Manager

? CyberArk Privilege Cloud - Manage Safe Members

? CyberArk Security Fundamentals

NEW QUESTION 3

Which browser is supported for PSM Web Connectors developed using the CyberArk Plugin Generator Utility (PGU)?

- A. Internet Explorer
- B. Google Chrome
- C. Opera
- D. Firefox

Answer: B

Explanation:

For PSM Web Connectors developed using the CyberArk Plugin Generator Utility (PGU), the supported browser is Google Chrome. This is because the PGU is designed to create plugins that are most compatible with Chrome's web technologies and security frameworks. Chrome is generally recommended by CyberArk for its up-to-date security features and extensive support for web applications. This is further supported by the CyberArk documentation on the Plugin Generator Utility, which specifies browser compatibility and the optimal environment for deploying web connectors.

NEW QUESTION 4

Which statement is correct regarding the LDAP integration with CyberArk Privilege Cloud Standard?

- A. You must track the expiration date of the directory server certificate and contact CyberArk Support to renew it.
- B. LDAPS integration with Privilege Cloud requires StartTLS for secure and encrypted communication.
- C. For certificate trust to your directory server, only the Issuing CA certificate is required.
- D. The top-level domain entry of the directory must be unique in the chosen Privilege Cloud region.

Answer: C

Explanation:

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.

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 implementing LDAPS Integration for a standard Privilege Cloud environment.
Which information must be provided to the CyberArk Privilege Cloud support team through a Service Request? (Choose 2.)

- A. LDAPS certificate chain for all domain controllers to be integrated
- B. LDAP bind username and password used to authenticate to the directory to be integrated
- C. Domain Base Context used to locate the users and groups in the Active Directory to be integrated
- D. Fully Qualified Domain Name and IP Address of the domain controllers to be integrated
- E. remote port set during secure tunnel configuration for each domain controller to be integrated

Answer: AD

Explanation:

When implementing LDAPS Integration for a standard Privilege Cloud environment, certain information is crucial and must be provided to the CyberArk Privilege Cloud support team through a Service Request. The necessary details include:

- ? LDAPS certificate chain for all domain controllers to be integrated (Option A): This information is critical to establishing a trusted secure connection between the Privilege Cloud and the domain controllers using LDAP over SSL (LDAPS).
- ? Fully Qualified Domain Name and IP Address of the domain controllers to be integrated (Option D): This information is essential for accurately identifying and configuring the network connections to each domain controller that will be integrated with the Privilege Cloud.

Reference: The process of setting up LDAPS integration typically requires detailed network and security information about the domain controllers to ensure secure and reliable connectivity. CyberArk support documentation and service request forms usually specify the need for these details.

NEW QUESTION 7

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 8

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 9

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 10

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 10

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 environment1.

? 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 12

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 13

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

- 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.

NEW QUESTION 15

What must be done to configure the syslog server IP address(es) for SIEM integration? (Choose 2.)

- A. Submit a service request to CyberArk Support.
- B. Update the syslog server IP address through the Privilege Cloud Portal.
- C. Update the DBPARAM.ini file with the correct syslog server IP address.

- D. Update the vault.ini file with the correct syslog server IP address.
- E. Configure the Secure Tunnel for SIEM integration.

Answer: BE

Explanation:

To configure the syslog server IP addresses for SIEM integration in a CyberArk Privilege Cloud environment, the following steps are generally required:

? Update the syslog server IP address through the Privilege Cloud Portal (Option B):

This is typically done via the administrative interface where system logging configurations can be managed. It allows for straightforward integration of external logging tools by specifying the destination syslog server IP.

? Configure the Secure Tunnel for SIEM integration (Option E): Establishing a secure tunnel is often necessary for secure and reliable data transmission between the CyberArk Privilege Cloud and the external syslog server, particularly when integrating SIEM systems that require encrypted and secure data pathways.

Reference: CyberArk's SIEM integration documentation and support articles often discuss these steps as part of setting up comprehensive security and monitoring configurations.

NEW QUESTION 16

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 19

According to best practice, when considering the location of PSM Connector servers in Privilege Cloud environments, where should the PSM be placed?

- A. near the CPM servers
- B. near the target devices
- C. near the Vault (closer to the external internet connection)
- D. near the Users

Answer: B

Explanation:

According to best practice, when considering the location of PSM Connector servers in Privilege Cloud environments, the PSM should be placed near the target devices. This placement minimizes latency and maximizes performance by reducing the distance that data has to travel between the PSM servers and the devices they are managing. This is particularly important for maintaining high efficiency and response times during remote session management and operations, which are critical for the overall effectiveness of the Privilege Cloud environment.

NEW QUESTION 20

DRAG DROP

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

Unordered Options

Enable the CPM services on the passive CPM.

Validate that the active CPM's services are stopped and set to manual.

On the passive CPM, confirm details in the Vault.ini configuration file, reset the password to the CPM user, and recreate the credential file.

Review logs to confirm the passive CPM services are running as expected.

Ordered Response

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To properly arrange the steps for failing over to a passive Central Policy Manager (CPM) in CyberArk, the sequence should be as follows:

? Validate that the active CPM's services are stopped and set to manual.Before enabling the passive CPM, ensure that the services on the active CPM are stopped. This prevents any conflicts or data corruption by making sure that only one CPM is active at a time. Setting the services to manual ensures they do not restart automatically, which is crucial during a failover scenario.

? On the passive CPM, confirm details in the Vault.ini configuration file, reset the password to the CPM user, and recreate the credential file.This step involves making sure the passive CPM has the correct configuration to seamlessly take over operations. Adjustments in the Vault.ini file may be necessary to ensure it is pointing to the correct Vault and network settings. Resetting the password and recreating the credential file are critical to secure the login and authentication process for the newly active CPM.

? Enable the CPM services on the passive CPM.Once the passive CPM is correctly configured and ready, enable its services to begin handling the tasks and responsibilities of the primary CPM. This action effectively switches the role from passive to active, enabling the passive CPM to function as the new operational manager.

? Review logs to confirm the passive CPM services are running as expected.Finally, review the system and application logs to confirm that the now-active CPM is operating correctly and that all services have started without errors. This step is vital for verifying that the failover process was successful and that the system is stable.

Following this ordered sequence ensures a smooth transition of roles from the active CPM to the passive CPM, minimizing downtime and potential disruptions in the privileged access management operations.

NEW QUESTION 23

.....

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](#)