

CyberArk

Exam Questions CPC-SEN

CyberArk Sentry - Privilege Cloud



NEW QUESTION 1

After a scripted installation has successfully installed the PSM, which post-installation task is performed?

- A. The screen saver for the PSM local users is disabled.
- B. A new group called PSMSHadowUsers is created.
- C. The PSMAdminConnect user password is reset.
- D. Remote desktop services are installed.

Answer: A

Explanation:

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.

References:

? CyberArk documentation on PSM post-installation tasks1.

? CyberArk documentation on disabling the screen saver for PSM local users

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

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

How should you configure PSM for SSH to support load balancing?

- A. by using a network load balancer
- B. in PVWA > Options > PSM for SSH Proxy > Servers
- C. in PVWA > Options > PSM for SSH Proxy > Servers > VIP
- D. by editing sshd.config on the all the PSM for SSH servers

Answer: A

Explanation:

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.

NEW QUESTION 5

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 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

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

- A. LDAR RADIU
- B. SAML OpenID Connect (OIDC)
- C. Window
- D. PK
- E. RADIU
- 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 8

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?

- A. Administration Options > CPM Settings
- B. AllowedSafes Parameter on each platform policy
- C. MaxConcurrentConnection parameter on each platform policy
- D. Administration > Options > CPM Scanner.

Answer: B

Explanation:

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.

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

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 10

.....

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](#)