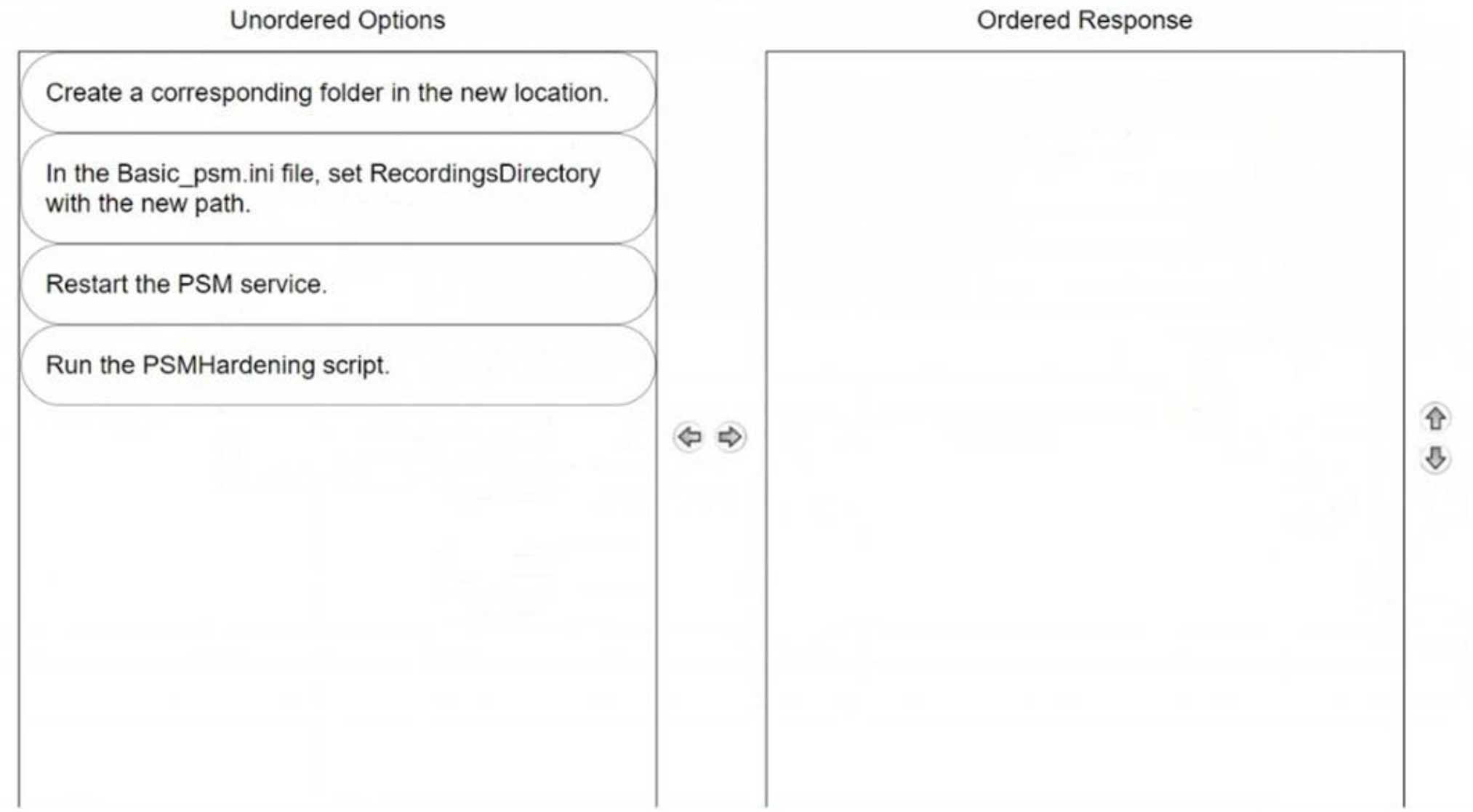
Exam Questions CPC-SEN

CyberArk Sentry - Privilege Cloud

https://www.2passeasy.com/dumps/CPC-SEN/

NEW QUESTION 1
DRAG DROP
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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
To correctly change the default PSM recordings folder path on the Privilege Cloud Connector, the sequence of steps should be:
? Create a corresponding folder in the new location.Before making changes to configuration files, ensure the new directory for PSM recordings is created. This is where all session recordings will be stored moving forward.
? In the Basic_psm.ini file, set RecordingsDirectory with the new path.Update the Basic_psm.ini file to reflect the new path for the recordings. This step is crucial as it directs the PSM to start using the newly created directory for all future session recordings.
? Restart the PSM service.After updating the path in the configuration file, restart the PSM service to apply the changes. This ensures that all new sessions are recorded in the new specified location.
? Run the PSMHardening script.Once the service is restarted and the new settings are in place, run the PSMHardening script. This script ensures that all security measures are re-applied to the new recordings directory, maintaining the security integrity of the session recordings.
Following these steps in the given order will successfully change the recording directory for PSM sessions on the Privilege Cloud Connector, ensuring a smooth transition to the new storage location with all necessary security measures intact.

NEW QUESTION 2
Which statement is correct about using the AllowedSafes platform parameter?

A. It allows users to access accounts in specific safes.
B. It prevents the CPM from scanning all safes, restricting it to scan only safes that match the AllowedSafes configuration.
C. It allows the CPM to access PSM safes to monitor platform configuration and connection component changes.
D. It prevents the CPM from processing pending items in the Discovery safes enforcingmanual intervention to complete the onboarding process.

Answer: B

Explanation:
The correct statement about using the AllowedSafes platform parameter is that it prevents the Central Policy Manager (CPM) from scanning all safes, restricting it to scan only safes that match the AllowedSafes configuration. This parameter is crucial in large-scale deployments where efficiency and resource management are key. By specifying which safes the CPM should manage, unnecessary scanning of irrelevant safes is avoided, thus optimizing the CPM's performance and reducing the load on the CyberArk environment. This configuration can be found in the platform management section of the CyberArk documentation.

NEW QUESTION 3
What are dependencies to update or change the CPM credential? (Choose 2.)

A. APIKeyManager.exe
B. CreateCredFile.exe
C. CPM/nDomain_Hardening.ps1
D. CyberArk.TPC.exe

E. Data Execution Prevention

Answer: BD

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.

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

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.
References:
? 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

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
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 9
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 10
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 DBPARM.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 10
What is a requirement when installing the PSM on multiple Privileged Cloud Connector servers?

A. Each PSM must have the same path to the same recordings directory.
B. All PSMs in the environment must be configured to use load balancing.
C. Additional Privilege Cloud Connector servers cannot have CPM installed.
D. In-domain servers cannot be used when deploying multiple PSM servers.

Answer: A

Explanation:
When installing the Privileged Session Manager (PSM) on multiple servers, it is required that each PSM installation has the same path to the same recordings directory. This is necessary to ensure that session recordings are stored consistently across different PSM instances, which is important for high availability and

load balancing implementations, as well as for maintaining a unified audit trail.
References:
? CyberArk documentation on installing multiple PSM servers

NEW QUESTION 12
Following the installation of the PSM for SSH server, which additional tasks should be performed? (Choose 2.)

A. Delete the user.cred file used during installation.
B. Delete the vault.ini you used during installation.
C. Delete the psmpparms file you used during installation.
D. Package all installation log files for upload to CyberArk.

Answer: AC

Explanation:
Following the installation of the PSM for SSH server, certain security and cleanup tasks are crucial to secure the environment and eliminate potential vulnerabilities:
? Delete the user.cred file used during installation (A): The user.cred file contains sensitive credential information used during the installation process. Deleting this file post-installation ensures that this sensitive data is not left accessible on the system, mitigating the risk of unauthorized access.
? Delete the psmpparms file you used during installation (C): Similar to the user.cred file, the psmpparms file often contains parameters that might include sensitive configuration details. Removing this file after the installation process is completed helps in securing the server by removing potential leakage points of sensitive information.
These actions are part of best practices to secure the installation environment and reduce the risk of sensitive information exposure.

NEW QUESTION 13
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 16
What are the basic network requirements to deploy a CPM server?

A. Port 1858 to the Privilege Cloud Vault service backend and Port 443 to the Privilege Cloud Portal
B. Port 1858 only
C. any ports to the Privilege Cloud Vault service backend
D. Port UDP/1858 to the Privilege Cloud Vault service backend and all required ports to the targets and Port 3389 to the PSM

Answer: A

Explanation:
The basic network requirements to deploy a CyberArk Privilege Management Central Policy Manager (CPM) server include Port 1858 to the Privilege Cloud Vault service backend and Port 443 to the Privilege Cloud Portal. Port 1858 is necessary for communication with the CyberArk Vault, facilitating essential interactions like password retrieval and updates. Port 443 is required for secure web traffic to and from the Privilege Cloud Portal, ensuring that all management tasks performed through the web interface are secure and encrypted. These ports must be properly configured to allow for the efficient and secure operation of the CPM within the Privilege Cloud infrastructure.

NEW QUESTION 19
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CPC-SEN Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CPC-SEN Product From:

https://www.2passeasy.com/dumps/CPC-SEN/

Money Back Guarantee

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