Exam Questions CPC-SEN

CyberArk Sentry - Privilege Cloud

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

NEW QUESTION 1
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 2
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 3
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?

A. 1-10
B. 31-60
C. 100
D. 200

Answer: B

Explanation:
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.

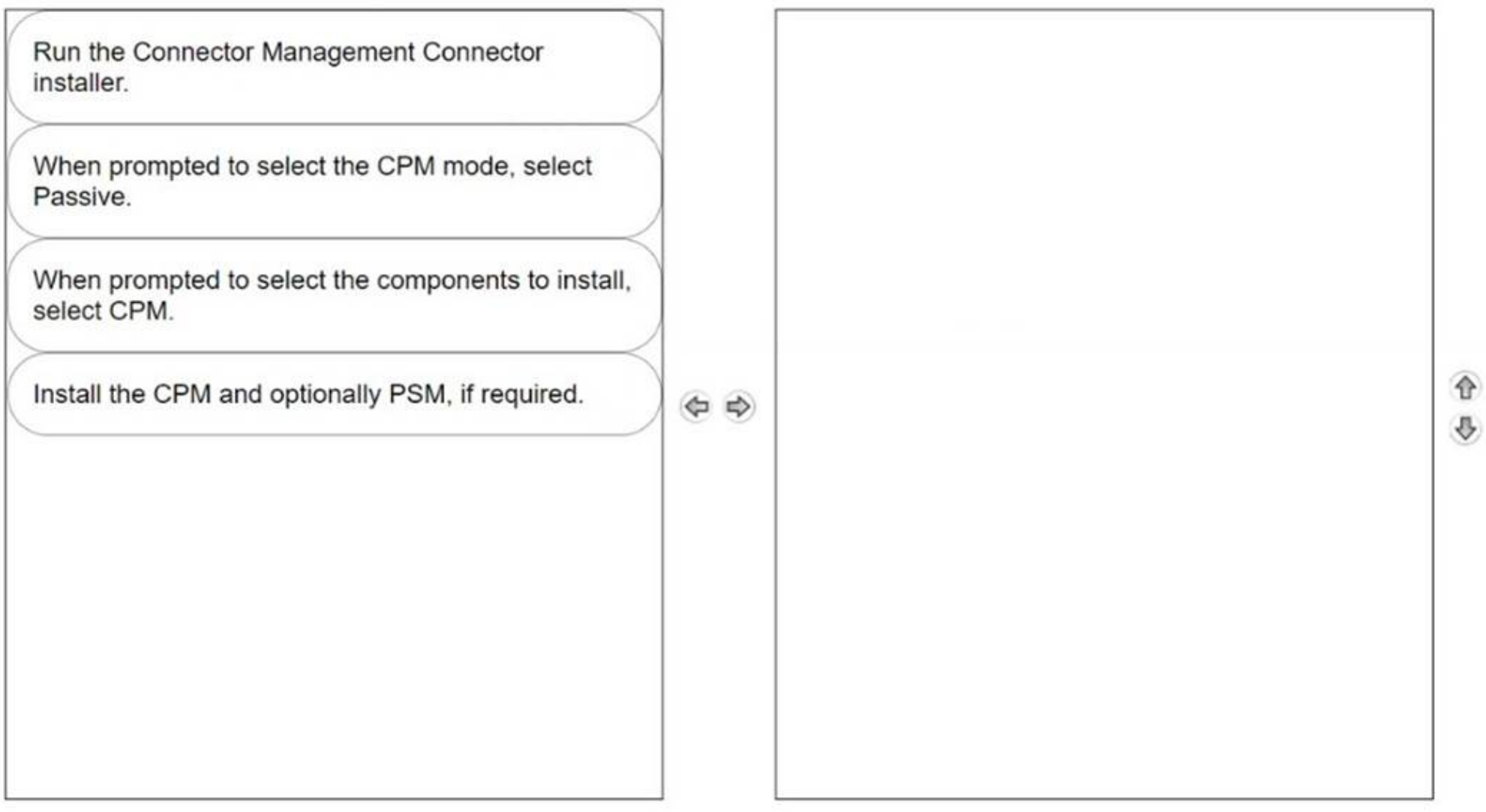
NEW QUESTION 4
When installing the first CPM within Privilege Cloud using the Connector Management Agent, what should you set the Installation Mode to in the CPM section?

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 5
DRAG DROP
Arrange the steps to install passive CPM using Connector Management in the correct sequence



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 6
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 7
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 8
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.)

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

Answer: AC

Explanation:
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.

NEW QUESTION 9
What is a supported certificate format for retrieving the LDAPS certificate when not using the Cyberark provided LDAPS certificate tool?

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.

NEW QUESTION 10
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.

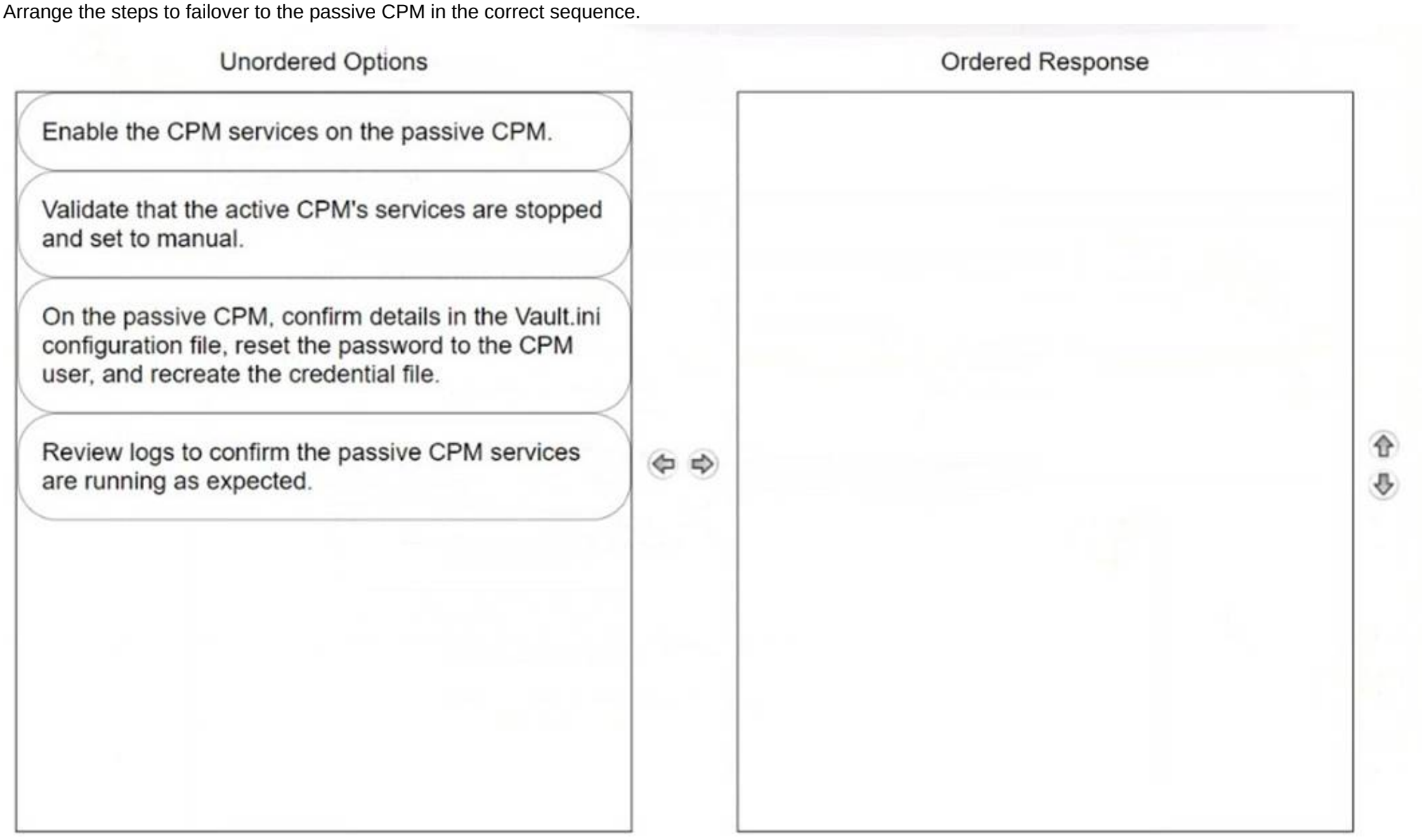
NEW QUESTION 10
On Privilege Cloud, what can you use to update users' Permissions on Safes? (Choose 2.)

A. Privilege Cloud Portal
B. PrivateArk Client
C. REST API
D. PACLI
E. PTA

Answer: AC

Explanation:
On CyberArk Privilege Cloud, updating users' permissions on safes can be done through the Privilege Cloud Portal and the REST API. The Privilege Cloud Portal provides a user- friendly graphical interface where administrators can manage user permissions directly within the portal's safe management settings. Additionally, the REST API offers a programmable way to automate permission updates across safes, which is especially useful for bulk changes or integrating with other management tools. Both methods provide effective means to manage and customize access controls in a CyberArk environment, allowing for detailed permission settings per user on specific safes.

NEW QUESTION 12
DRAG DROP
Arrange the steps to failover to the passive CPM in the correct sequence.



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 16
.....

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