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
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 3
A support team has asked you to provide the previous password for an account that had its password recently changed by the CPM. In which tab within the account's overview page can you retrieve this information?

A. Activities
B. Details
C. Versions

Answer: D

Explanation:
To retrieve the previous password for an account that had its password changed by the CPM, you should look under the Versions tab within the account's overview page. This tab maintains a history of password changes, including previous passwords, along with other historical data points that allow for tracking changes over time. This feature is critical for auditing and rollback purposes in environments where knowing past credentials is necessary for troubleshooting or compliance.

NEW QUESTION 4
What is the recommended method to enable load balancing and failover of the CyberArk Identity Connector?

A. Setup IIS based Application Request Routing on two or more CyberArk Identity Connector servers.
B. Set up a network load balancer between two or more CyberArk Identity Connector servers.
C. Set up two or more CyberArk Identity Connector servers only.
D. Set up a Microsoft Failover Cluster on two or more CyberArk Identity Connector servers.

Answer: B

Explanation:
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.

NEW QUESTION 5
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 6
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 7
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?

A. PSMConfigureAppLocker.xml
B. PSMHardening.xml
C. PSMAppConfig.xml
D. PSMConfigureHardening xml

Answer: A

Explanation:
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. References 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.

NEW QUESTION 8
In the directory lookup order, which directory service is always looked up first for the CyberArk Privilege Cloud solution?

A. Active Directory
B. LDAP
C. Federated Directory
D. CyberArk Cloud Directory

Answer: D

Explanation:
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.
Reference: CyberArk's architectural documentation usually emphasizes the role of the CyberArk Cloud Directory in managing and authenticating user access in cloud-based deployments, highlighting its precedence in the directory lookup process.

NEW QUESTION 9
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 10
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 14
Your customer is using Privilege Cloud Shared Services. What is the correct CyberArk Vault address for this customer?

A. carkvault-<subdomain>.privilegecloud.cyberark.cloud
B. vault-<subdomain>.privilegecloud.cyberark.cloud
C. v-<subdomain>.privilegecloud.cyberark.cloud
D. carkvlt-<subdomain> privilegecloud.cyberark.cloud

Answer: B

Explanation:
For customers using CyberArk Privilege Cloud Shared Services, the correct format for the CyberArk Vault address is:
? vault-<subdomain>.privilegecloud.cyberark.cloud (Option B). This format is used to access the vault services provided by CyberArk in the cloud environment, where <subdomain> is the unique identifier assigned to the customer??s specific instance of the Privilege Cloud.
Reference: CyberArk??s Privilege Cloud documentation provides details on how to access various services, including the vault. The standard naming convention for accessing the vault services in the cloud typically follows this format.

NEW QUESTION 17
Your customer recently merged with a smaller organization. The customer's connector has no network connectivity to the smaller organization's infrastructure. You need to map LDAP users from both your customer and the smaller organization. How is this achieved?

A. Create the required users in one directory and configure the Identity Connector to read that directory, as there can only be one Identity Connector.
B. Create mappings for both directories from the original Identity Connector.
C. Deploy Identity Connectors in the newly acquired infrastructure and create user mappings.
D. Switch all users to SAML authentication as there can only be one Identity Connector.

Answer: C

Explanation:
To map LDAP users from both your customer and the smaller organization they have merged with, especially when there is no network connectivity between the two infrastructures, the best approach is to:
? Deploy Identity Connectors in the newly acquired infrastructure and create user mappings (Option C). This involves setting up additional Identity Connectors within the smaller organization??s network. These connectors will facilitate the integration of user directories from both organizations into the customer??s Privilege Cloud environment.
Reference: CyberArk documentation on Identity Connectors often outlines the capability of deploying multiple connectors to manage different user directories, especially useful in scenarios involving mergers or acquisitions where separate infrastructures need integration.

NEW QUESTION 22
Which authentication methods does PSM for SSH support? (Choose 2.)

A. OIDC
B. MFA Caching

C. SAML
D. RADIUS
E. Client Authentication Certificate

Answer: DE

Explanation:
PSM for SSH supports various authentication methods, specifically focusing on secure and verified access mechanisms. The supported methods include:
? RADIUS (D): Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting management for users who connect and use a network service. PSM for SSH utilizes RADIUS to authenticate SSH sessions, which adds an additional layer of security by centralizing authentication requests to a RADIUS server.
? Client Authentication Certificate (E): This method uses certificates for authentication, where a client presents a certificate that the server verifies against known trusted certificates. This type of authentication is highly secure as it ensures that both parties involved in the communication are precisely who they claim to be, making it suitable for environments that require stringent security measures.
These methods provide robust security options for SSH sessions managed through CyberArk's PSM, ensuring that only authorized users can access critical systems.

NEW QUESTION 23
Which users are Privilege Cloud Standard built-in users? (Choose 2.)

A. NASCorp
B. saascorps
C. CyberArkAdmin
D. remoteAccessAppUser
E. PASReporterUser

Answer: CE

Explanation:
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.
Reference: CyberArk??s Privilege Cloud setup and administration guides usually list these users as part of the default configuration to facilitate initial setup and ongoing management of the platform.

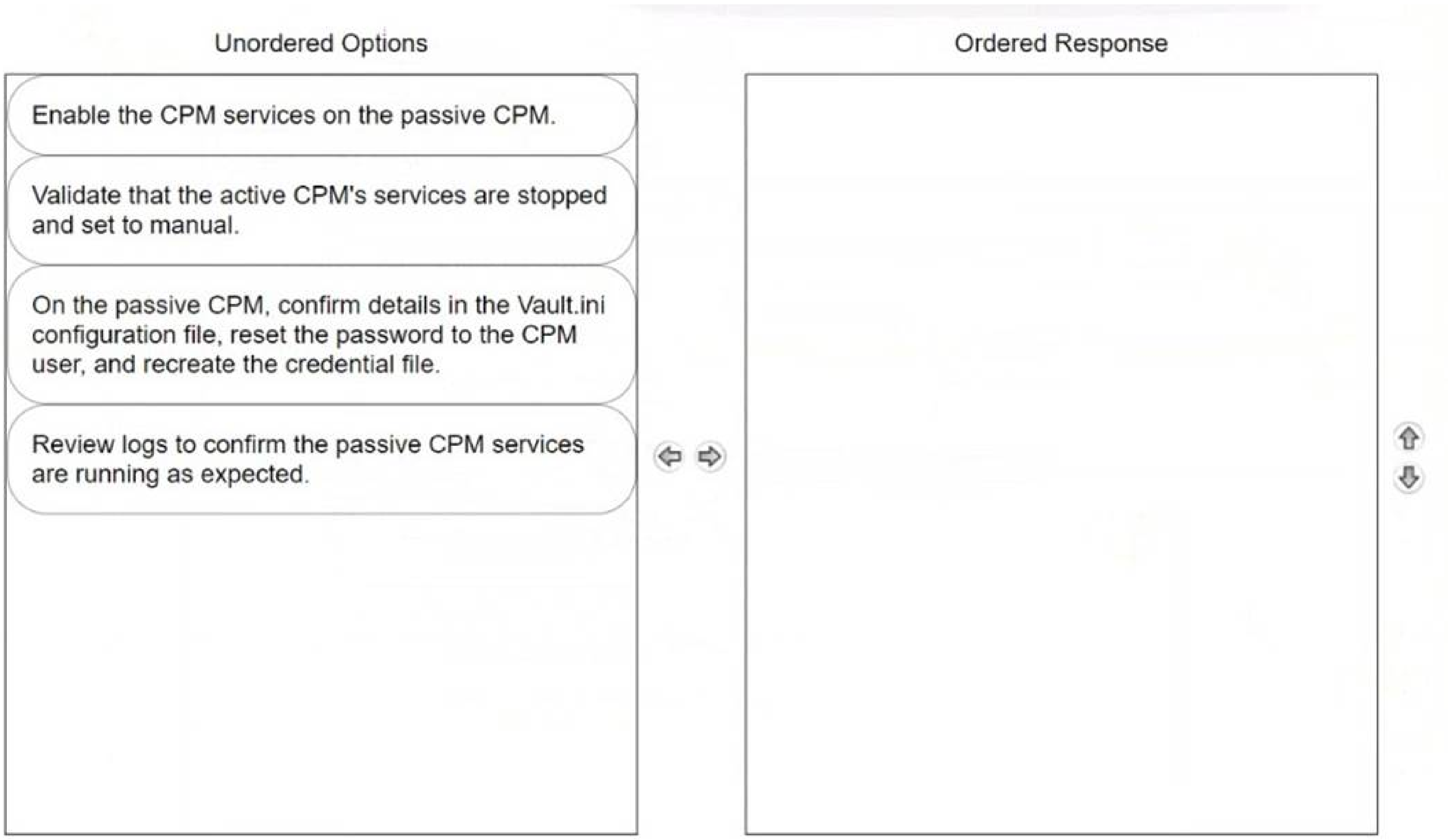
NEW QUESTION 25
On Privilege Cloud, what can you use to update users' Permissions on Safes? (Choose 2.)

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 27
DRAG DROP
Arrange the steps to failover to the passive CPM in the correct sequence.



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.

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 32
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons 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