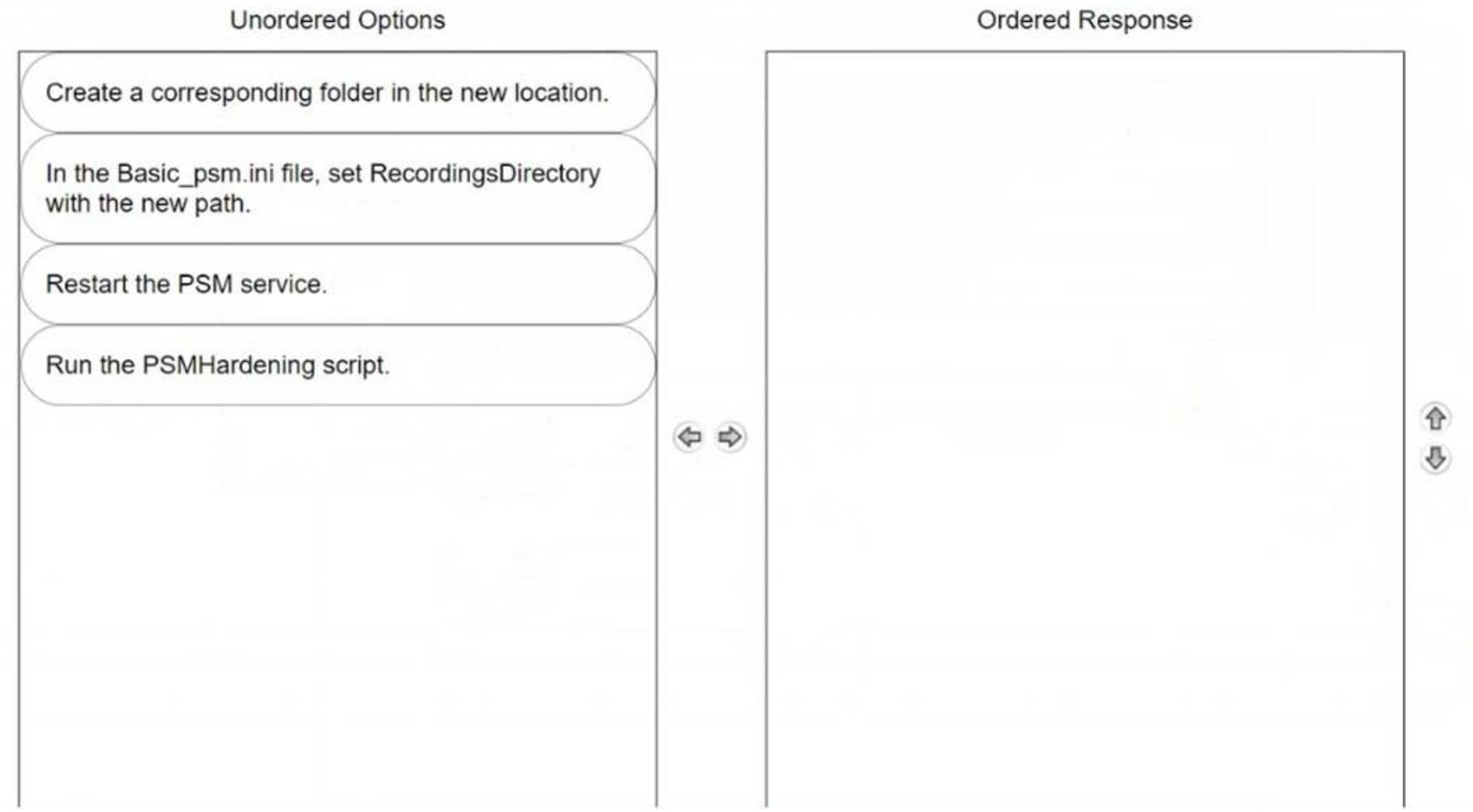
CyberArk

Exam Questions CPC-SEN

CyberArk Sentry - Privilege Cloud

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
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
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 5
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 6
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 7
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 8
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 9
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.

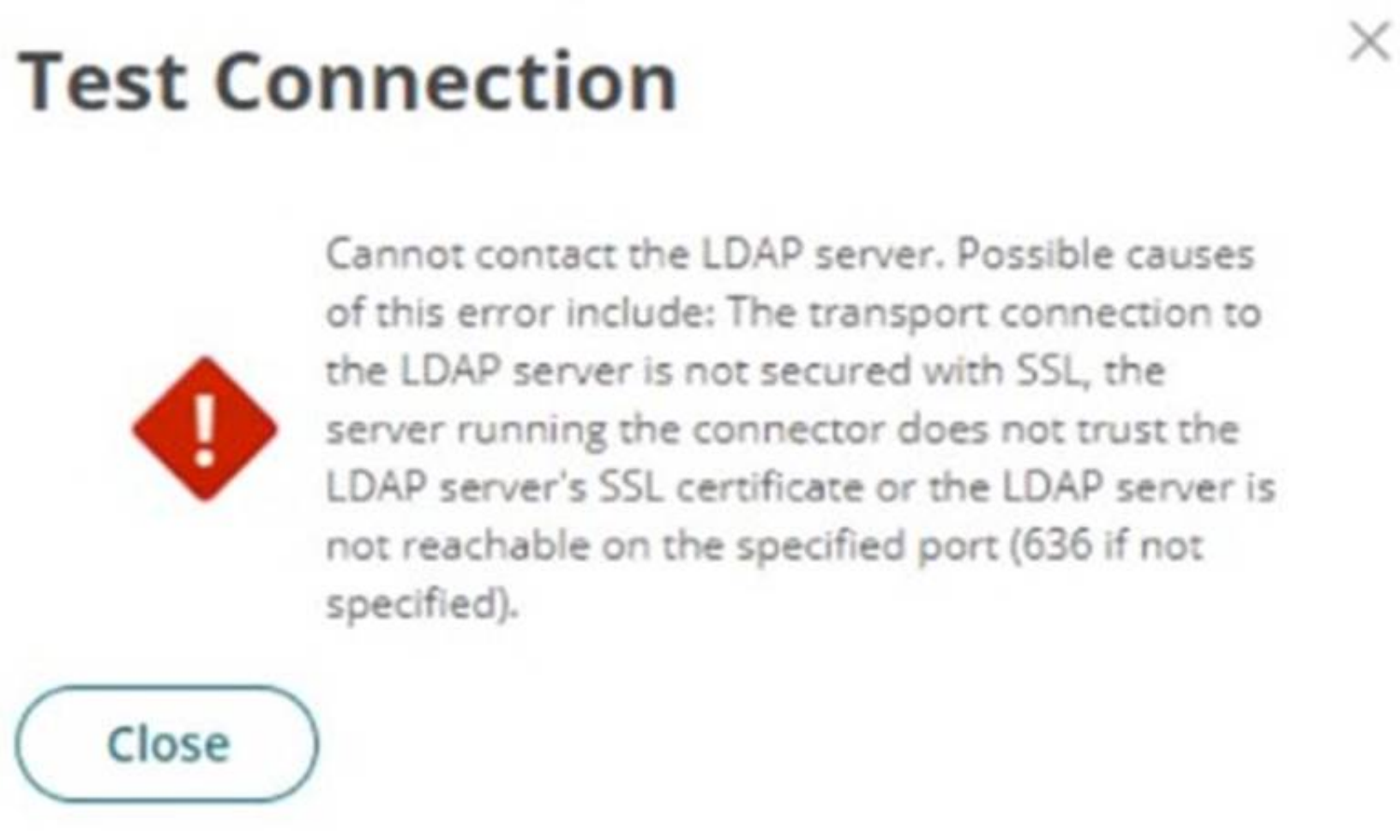
NEW QUESTION 10
What is a requirement when installing the PSM on multiple Privileged Cloud Connector servers?

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 10
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 12
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 16
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 18
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
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 25
To disable the PSM default Support for Browser Sessions, which option should be set to 'No* before running Hardening?

A. SupportWebApplications
B. SupportBrowsers
C. SupportWebBrowsers
D. SupportHTML5Content

Answer: B

Explanation:
To disable the PSM default support for browser sessions, the option SupportBrowsers should be set to 'No' before running the hardening process. This configuration change is made within the PSM??s configuration files, typically found in the PSM's administrative interface or directly within specific XML configuration files like PSMHardening.xml. Setting this option to 'No' prevents the PSM from processing session requests that involve web browsers, thereby enhancing security by limiting the session types the PSM will support. This setting is particularly important in environments where web browsing sessions are deemed unnecessary or too risky.

NEW QUESTION 28
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 29
.....

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