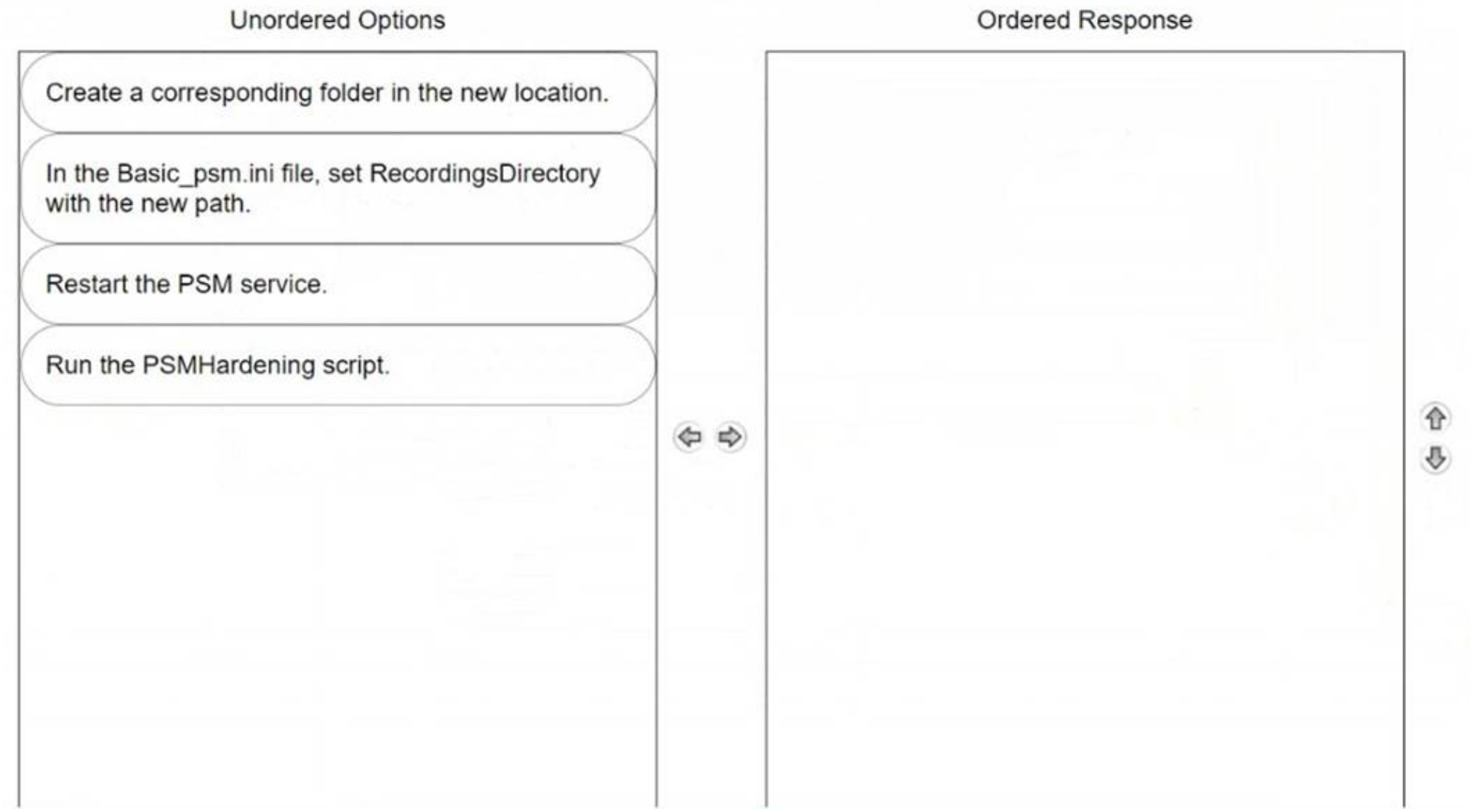
# CyberArk

## 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**
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**
Which statement best describes a PSM server's network requirements?

A. It must reach the target system using its native protocols.
B. It requires limited outbound connectivity to Ports 1858 and 443 only.

C. It requires direct access to the internet.
D. It requires broad inbound firewall rules and outbound traffic should be limited to Port 1858.

**Answer:** A

**Explanation:**
For a Privilege Session Manager (PSM) server, the network requirements primarily focus on its ability to interact with target systems securely and efficiently. The most accurate statement regarding these requirements is:
? It must reach the target system using its native protocols (Option A). This is essential for the PSM to manage sessions effectively, as it needs to communicate using the protocols that the target systems are configured to accept, such as SSH for Linux servers or RDP for Windows servers.
Reference: CyberArk??s PSM documentation typically outlines the need for PSM servers to have network paths configured to communicate directly with target systems using the relevant protocols to ensure secure and controlled session management.

**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.

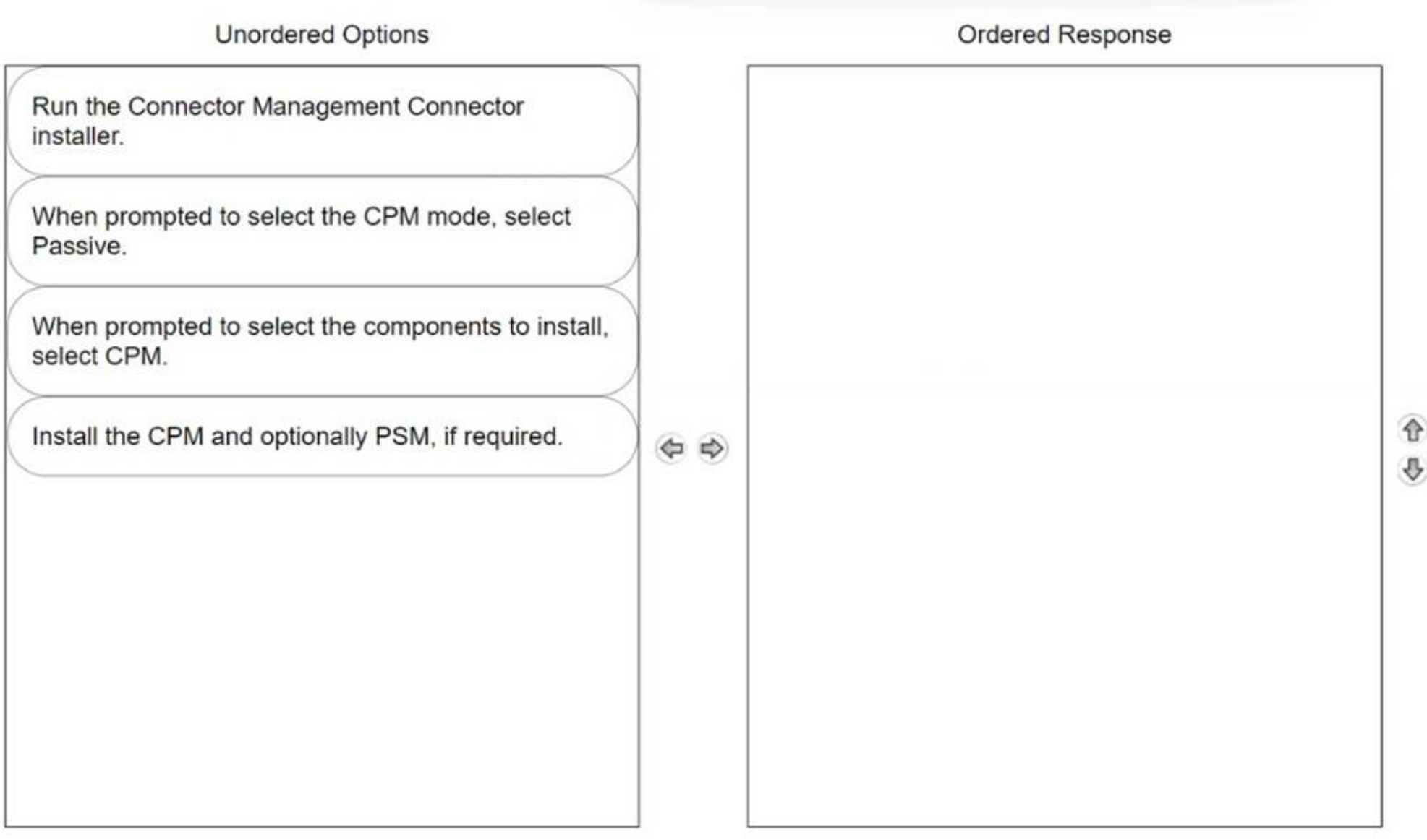
**NEW QUESTION 5**
You are configuring firewall rules between the Privilege Cloud components and the Privilege Cloud. Which firewall rules should be set up to allow connections?

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 6**
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 7**
After correctly configuring reconciliation parameters in the Prod-AIX-Root-Accounts Platform, this error message appears in the CPM log: CACPM410E Ending password policy Prod-AIX-Root-Accounts since the reconciliation task is active but the AllowedSafes parameter was not updated What caused this situation?

A. The reconciliation account defined in the Platform is in a locked state and is not accessible.
B. The CPM is currently configured to use to an unsigned engine.
C. The AllowedSafes parameter does not include the safe containing the reconciliation account defined in the Platform.
D. A second CPM is incorrectly configured to manage the reconciliation account's safe which is causing a deadlock situation between the two CPMs.

**Answer:** C

**Explanation:**
The error message "CACPM410E Ending password policy Prod-AIX-Root-Accounts since the reconciliation task is active but the AllowedSafes parameter was not updated" suggests an issue with configuration parameters. The likely cause is:
? The AllowedSafes parameter does not include the safe containing the
reconciliation account defined in the Platform (Option C). This parameter must accurately reflect all safes where the reconciliation account operates to ensure proper management and access by the Central Policy Manager (CPM). If the safe containing the reconciliation account is not listed, the CPM cannot perform its tasks, leading to this error.
Reference: CyberArk??s error codes and troubleshooting guides detail how specific configuration mismatches, like an incomplete AllowedSafes parameter, can disrupt normal operations, especially in reconciliation processes.

**NEW QUESTION 8**
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 9**
You have been tasked with deploying a Privilege Cloud PSM for SSH connector When the initial installation has successfully completed, you create and permission several maintenance users to be used for administering the connector.
Which configuration file must be updated to define these maintenance users?

A. sshd.config
B. basic_psmpserver.conf
C. sshd_config
D. psmpparms

**Answer:** C

**Explanation:**
The sshd_config file is the correct configuration file that must be updated to define maintenance users for administering the Privilege Cloud PSM for SSH connector. This file contains configurations for the SSH daemon, including user permissions and group settings. When adding maintenance users, their user accounts are created on the PSM
server, and then they are added to the AllowGroups parameter within the sshd_config file to grant them the necessary permissions.
References:
? CyberArk documentation on the PSM for SSH environment1.
? CyberArk Sentry guide on how to add maintenance users for SSH PSM
? When deploying a Privilege Cloud PSM for SSH connector, the configuration file that must be updated to define maintenance users is "sshd_config". This file is used to configure options specific to the SSH daemon, which includes user permissions, authentication methods, and other security-related settings. To add and configure maintenance users for the PSM for SSH, you will need to modify this file to specify allowed users and their respective privileges.
Reference: The configuration of SSH-related components typically involves the "sshd_config" file, as outlined in SSH and PSM for SSH setup guides. This is a standard practice in systems that utilize SSH for secure communications and management.

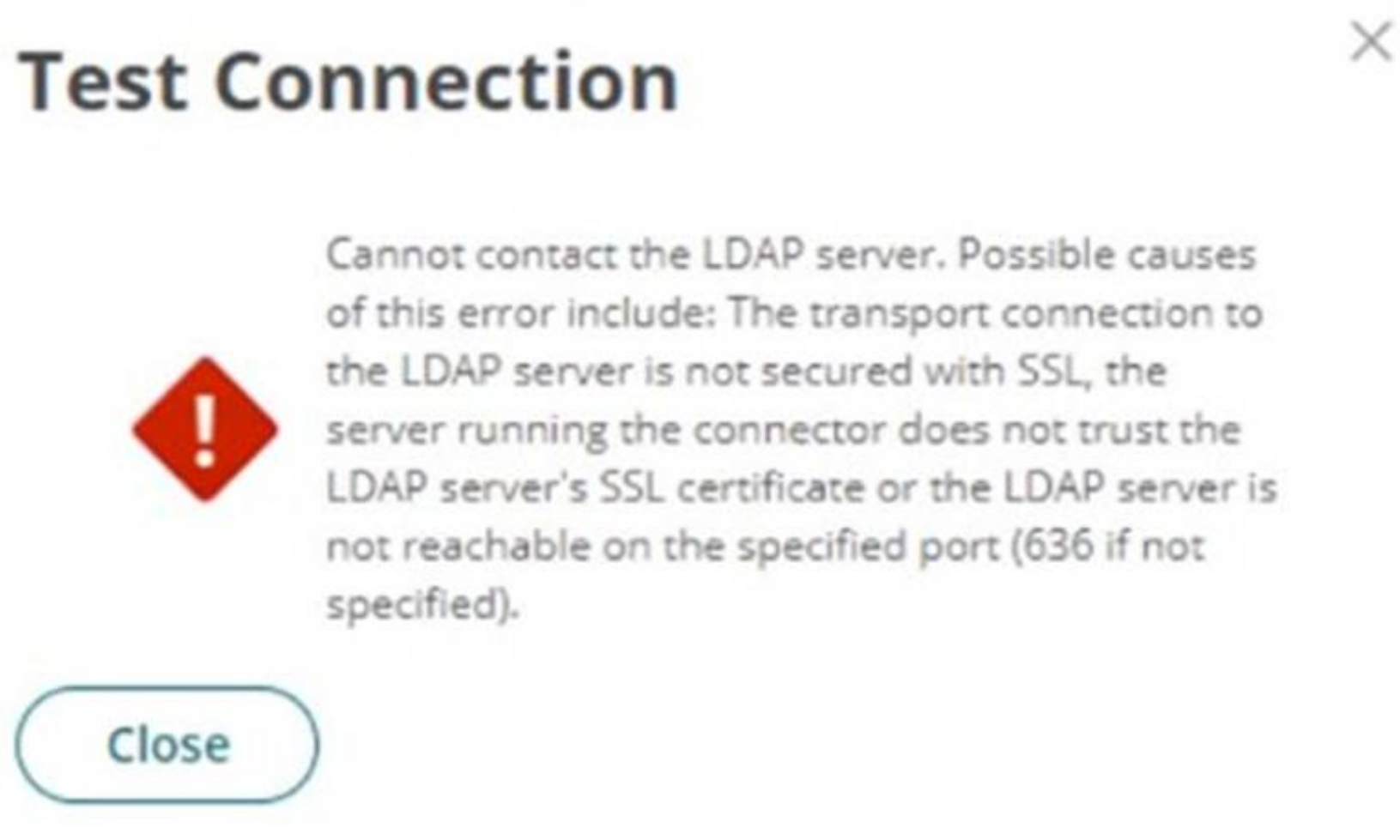
**NEW QUESTION 10**
Your customer is using Privilege Cloud Shared Services. What is the correct CyberArk Vault address for this customer?

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 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 14**
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 18**
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 20**
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 22**
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**
On the CPM, you want to verify if DEP is disabled for the required executables According to best practices, which executables should be listed? (Choose 2.)

A. Telnet.exe
B. Plink.exe
C. putty.exe
D. mstsc.exe

**Answer:** BC

**Explanation:**
On the Central Policy Manager (CPM), it is crucial to verify that Data Execution Prevention (DEP) is disabled for specific executables required for proper operation according to best practices. The relevant executables include:
? Plink.exe (Option B): This executable is commonly used for SSH communications and may require DEP to be disabled to function correctly under certain configurations.
? putty.exe (Option C): Similar to Plink.exe, Putty is another essential tool for SSH communications and might also require DEP to be disabled to prevent any execution issues.
Reference: CyberArk??s best practices for system configuration often highlight the need to adjust DEP settings for certain executables to ensure they run without interruption, particularly when these tools are crucial for secure communications and operations management.

**NEW QUESTION 30**
You are deploying a CyberArk Identity Connector to integrate Privilege Cloud Shared Services with an Active Directory environment. Which requirement must be met?

A. The Identity Connector Server must be joined to the Active Directory.
B. The Server must be a member of the root domain of the Active Directory fores
C. The Identity Connector must be installed on a Domain Controller.
D. The Identity Connector must be installed using Domain Administrator credentials.

**Answer:** A

**Explanation:**
When deploying a CyberArk Identity Connector to integrate Privilege Cloud Shared Services with an Active Directory environment, the server hosting the Identity Connector must meet specific requirements to ensure proper integration and functionality. The necessary condition is:
? The Identity Connector Server must be joined to the Active Directory (Option A).
This requirement ensures that the server can communicate effectively with the Active Directory services and manage identity data securely and efficiently. Being part of the Active Directory domain facilitates authentication and authorization processes required for the connector to function correctly.
Reference: CyberArk installation and configuration guides typically emphasize the importance of having the Identity Connector server joined to the domain to allow seamless interaction with Active Directory services.

**NEW QUESTION 35**

.....

# 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