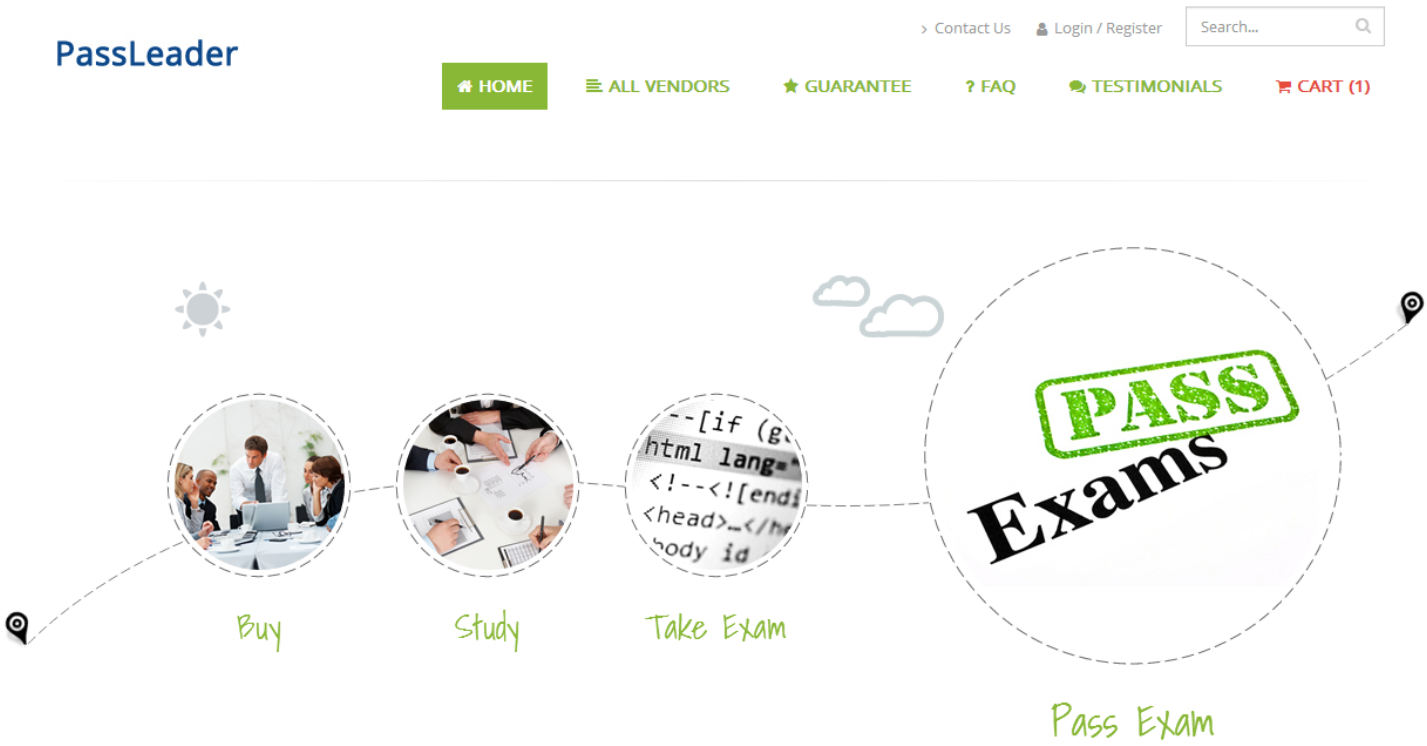
PassLeader



Try **PDF Demo** before you buy

We're not the only ones **happy** about PassLeader Practice Material ...

63159+ customers in 100+ countries use PassLeader Test Engine. Meet our customers.

VOREED GetCustom JET ORANGE iCompany Paradoxx iMessenger

http://www.passleader.top/

Latest Exam Guide & Learning Materials

Exam : **CPC-SEN**

Title : CyberArk Sentry - Privilege Cloud

Vendor : CyberArk

Version : DEMO

NO.1 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: B,E

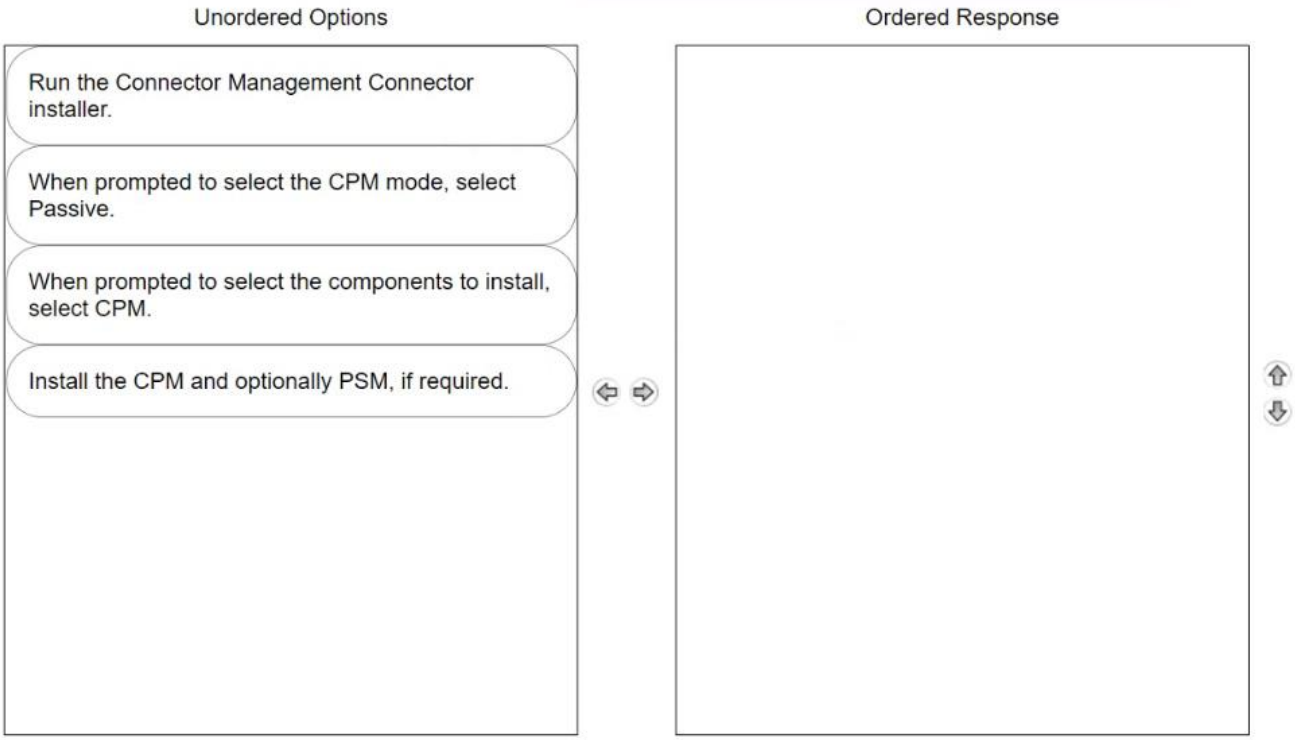
Explanation:

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.

NO.2 Arrange the steps to install passive CPM using Connector Management in the correct sequence



Answer:

Answer Area

Run the Connector Management Connector installer.
When prompted to select the components to install, select CPM.
When prompted to select the CPM mode, select Passive.
Install the CPM and optionally PSM, if required.

1 - Run the Connector Management Connector installer.
2 - When prompted to select the components to install, select CPM.
3 - When prompted to select the CPM mode, select Passive.
4 - Install the CPM and optionally PSM, if required.

NO.3 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.
Reference:
CyberArk documentation on PSM post-installation tasks1.
CyberArk documentation on disabling the screen saver for PSM local users

NO.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 RADIUS. SAML OpenID Connect (OIDC)

B. Windows. PKI. RADIUS. CyberArk, LDAP. SAML. OpenID Connect (OIDC)

C. Privilege Cloud Shared Services fully utilize CyberArk Identity and its MFA options.

D. 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.

NO.5 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.