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
CyberArk User Neil is trying to connect to the Target Linux server 192.168.1.164 using a domain user ACME\linuxuser01 on domain acme.corp using PSM for SSH server 192.168.65.145.
What is the correct syntax?

A. ssh neil@linuxuser01:acme.corp@192.168.1.164@192.168.65.145
B. ssh neil@linuxuser01#acme.corp@192.168.1.164@192.168.65.145
C. sshneil@linuxuser01@192.168.1.164@192.168.65.145
D. ssh neil@linuxuser01@acme.corp@192.168.1.164@192.168.65.145

Answer: B

Explanation:
In CyberArk Privilege Cloud, when connecting to a target server using the Privileged Session Manager (PSM) for SSH, the correct syntax for the SSH command includes the following format: ssh neil@linuxuser01#acme.corp@192.168.1.164@192.168.65.145. This syntax breaks down as follows:
? neil: The CyberArk username.
? linuxuser01#acme.corp: The domain user on the target Linux server, formatted as username#domain.
? 192.168.1.164: The IP address of the target Linux server.
? 192.168.65.145: The IP address of the PSM for SSH server.
This specific format ensures that the CyberArk Privileged Access Manager correctly interprets and routes the connection through the PSM for SSH to the intended target server.
References:
? CyberArk Privilege Cloud Introduction
? CyberArk Privileged Access Manager
? CyberArk Privilege Cloud - Manage Safe Members
? CyberArk Security Fundamentals

NEW QUESTION 4
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 5

Which browser is supported for PSM Web Connectors developed using the CyberArk Plugin Generator Utility (PGU)?

A. Internet Explorer
B. Google Chrome
C. Opera
D. Firefox

Answer: B

Explanation:
For PSM Web Connectors developed using the CyberArk Plugin Generator Utility (PGU), the supported browser is Google Chrome. This is because the PGU is designed to create plugins that are most compatible with Chrome's web technologies and security frameworks. Chrome is generally recommended by CyberArk for its up-to-date security features and extensive support for web applications. This is further supported by the CyberArk documentation on the Plugin Generator Utility, which specifies browser compatibility and the optimal environment for deploying web connectors.

NEW QUESTION 6
How can a platform be configured to work with load-balanced PSMs?

A. Remove all entries from configured PSM Servers except for the ID of the PSMs with load balancing.
B. Create a new PSM definition that targets the load balancer IP address and assign to the platform.
C. Include details of the PSMs with load balancing in the Basic_psm.ini file on each PSM server.
D. Use the Privilege Cloud Portal to update the Session Management settings for the platform in the Master Policy.

Answer: B

Explanation:
To configure a platform to work with load-balanced Privileged Session Managers (PSMs), you should:
? Create a new PSM definition that targets the load balancer IP address and assign
it to the platform (Option B). This approach involves configuring the platform settings to direct session traffic through a load balancer that distributes the load across multiple PSM servers. This is effective in environments where high availability and fault tolerance are priorities.
Reference: CyberArk??s setup guidelines for high-availability environments typically recommend configuring platforms to utilize load balancers to ensure continuous availability and optimal distribution of session management tasks.

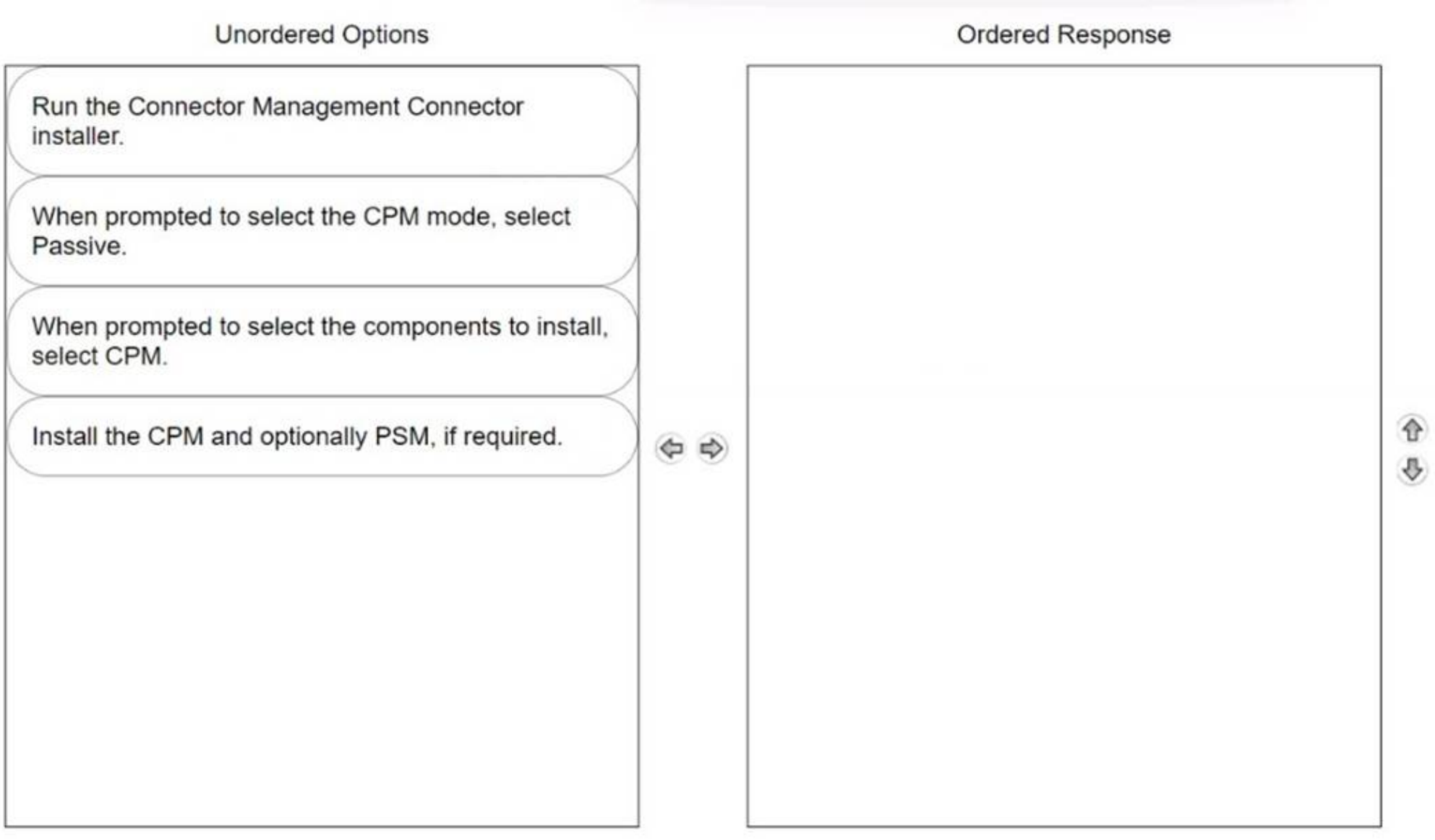
NEW QUESTION 7
When installing the first CPM within Privilege Cloud using the Connector Management Agent, what should you set the Installation Mode to in the CPM section?

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 8
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 9
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 10
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 10
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 12
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 15
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 17
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 20
'What is a default authentication profile to access CyberArk Identity?

A. Default New User Login Profile
B. Default New Device Login Profile
C. Default New Authenticator Profile
D. Default New Password Profile

Answer: B

Explanation:
The default authentication profile to access CyberArk Identity is typically the Default New Device Login Profile. This profile is used to manage the authentication settings and security measures for devices accessing CyberArk services for the first time. It includes configurations such as authentication methods, security checks, and compliance requirements, ensuring that new devices meet the organization??s security standards before gaining access.

NEW QUESTION 23
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 26
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 32
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 36
.....

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