Free Questions for CPC-SEN by braindumpscollection

Shared by Nunez on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

A- OIDC

B- MFA Caching

C- SAML

D- RADIUS

E- Client Authentication Certificate

Answer:

D, E

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.

Question 2

Question Type: MultipleChoice

What must be done before configuring directory mappings in the CyberArk Privilege Cloud Standard Portal for LDAP integration?

Options:

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.

Question 3

Question Type: **MultipleChoice**

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?

Options:

A- Overview

B- Activities

C- Details

D- 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.

Question 4

Question Type: MultipleChoice

What are dependencies to update or change the CPM credential? (Choose 2.)

Options:

A- APIKeyManager.exe

B- CreateCredFile.exe

C- CPM/nDomain_Hardening.ps1

D- CyberArk.TPC.exe

E- Data Execution Prevention

Answer:

B, D

Explanation:

To update or change the Central Policy Manager (CPM) credentials, dependencies include:

CreateCredFile.exe (B): This utility is used to create or modify the encrypted file that stores the CPM's credentials. It is essential for securely handling the credential updates.

CyberArk.TPC.exe (D): This executable is part of the CyberArk suite that manages trusted platform module operations, which can include tasks related to credential security and management, particularly when hardware security modules are involved.

Question 5

Question Type: **MultipleChoice**

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.)

Options:

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:

A, C

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.

Question 6

Question Type: MultipleChoice

A CyberArk Privileged Cloud Shared Services customer asks you how to find recent failed login events for all users. Where can you do this without generating reports?

Options:

A- Privileged Cloud Portal

B- Identity Administration Portal

C both Identity Administration and Identity User Portals

D- Identity User Portal

Answer:

A

Explanation:

To find recent failed login events for all users in CyberArk Privileged Cloud Shared Services without generating reports, you can use the Privileged Cloud Portal. This portal provides administrators with direct access to security and audit logs, including failed login attempts. It offers a real-time view and monitoring capabilities that allow for immediate visibility into authentication activities and potential security issues. This feature is crucial for maintaining the security and integrity of privileged accounts, enabling administrators to quickly respond to and investigate authentication failures.

Question 7

Question Type: MultipleChoice

What are the basic network requirements to deploy a CPM server?

Options:

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.

Question 8

Question Type: MultipleChoice

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

Options:

A- Privilege Cloud Portal

B- PrivateArk Client

C- REST API

D- PACLI

E- PTA

Answer:

A, C

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.