

CyberArk

Exam Questions CPC-SEN

CyberArk Sentry - Privilege Cloud



NEW QUESTION 1

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 enforcing manual 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 2

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 3

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

- A. APIKeyManager.exe
- B. CreateCredFile.exe
- C. CPM/nDomain_Hardening.ps1
- D. CyberArk.TPC.exe
- E. Data Execution Prevention

Answer: BD

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.

NEW QUESTION 4

You are creating a PSM Load Balanced Virtual Server Configuration.

What are the default service ports / protocols used for RDS and the PSM Health Check service?

- A. RDP/389 HTTP/443
- B. RDP/3389 HTTPS/443
- C. UDP/53 HTTPS/389
- D. RDP/636 HTTPS/443

Answer: B

Explanation:

In a PSM Load Balanced Virtual Server Configuration, the default service ports/protocols used are RDP/3389 and HTTPS/443. RDP (Remote Desktop Protocol) typically uses port 3389 for remote desktop services, which is essential for PSM functionalities involving remote sessions. HTTPS, which utilizes port 443, is used for the PSM Health Check service to ensure secure and encrypted communication during the monitoring and health verification processes of the PSM services.

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

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?

- 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.

NEW QUESTION 7

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 8

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 9

'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 10

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 10

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions 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

100% Actual & Verified — Instant Download, Please Click
[Order The CPC-SEN Practice Test Here](#)