

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

What is the recommended method to enable load balancing and failover of the CyberArk Identity Connector?

- A. Setup IIS based Application Request Routing on two or more CyberArk Identity Connector servers.
- B. Set up a network load balancer between two or more CyberArk Identity Connector servers.
- C. Set up two or more CyberArk Identity Connector servers only.
- D. Set up a Microsoft Failover Cluster on two or more CyberArk Identity Connector servers.

Answer: B

Explanation:

The recommended method to enable load balancing and failover of the CyberArk Identity Connector is to set up a network load balancer between two or more CyberArk Identity Connector servers. This setup allows for the distribution of requests across multiple servers, enhancing the availability and reliability of the service. Network load balancers efficiently manage traffic to ensure that no single connector server becomes a bottleneck, thereby improving overall performance and fault tolerance.

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

Which statement is correct regarding the LDAP integration with CyberArk Privilege Cloud Standard?

- A. You must track the expiration date of the directory server certificate and contact CyberArk Support to renew it.
- B. LDAPS integration with Privilege Cloud requires StartTLS for secure and encrypted communication.
- C. For certificate trust to your directory server, only the Issuing CA certificate is required.
- D. The top-level domain entry of the directory must be unique in the chosen Privilege Cloud region.

Answer: C

Explanation:

For LDAP integration with CyberArk Privilege Cloud Standard, the correct statement is that only the Issuing CA certificate is required for certificate trust to your directory server. This setup simplifies the process of establishing a trusted connection between CyberArk and the LDAP server by necessitating only the certification of the issuing Certificate Authority (CA), rather than needing multiple certificates from different levels of the trust chain. This approach ensures that the SSL/TLS communication between CyberArk and the LDAP server is secured based on the trust of the issuing CA's certificate.

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

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 7

Which tool configures the user object that will be used during the installation of the PSM for SSH component?

A. CreateUserPass

B. CreateCredFile

C. ConfigureCredFile

D. ConfigureUserPass

Answer: B

Explanation:

The tool used to configure the user object for the installation of the PSM for SSH component is CreateCredFile. This tool is responsible for creating a credentials file that stores the necessary user details required during the installation process, ensuring secure and correct authentication.

References:

? CyberArk Privilege Cloud Introduction

NEW QUESTION 8

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 9

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.)

Test Connection



Cannot contact the LDAP server. Possible causes of this error include: The transport connection to the LDAP server is not secured with SSL, the server running the connector does not trust the LDAP server's SSL certificate or the LDAP server is not reachable on the specified port (636 if not specified).

Close

- 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 10

'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 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 14

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 forest.
- 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 17

.....

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](#)