



CyberArk

Exam Questions CPC-SEN

CyberArk Sentry - Privilege Cloud

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

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 PSMAAdminConnect 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 PSMAAdminConnect 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 2

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 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 plan to install Privilege Cloud Connectors on your AWS and Azure environments.

What is the maximum number of concurrent RDP/SSH sessions that each connector can handle for Large Implementations?

- A. 1-10
- B. 31-60
- C. 100
- D. 200

Answer: B

Explanation:

For large implementations of CyberArk Privilege Cloud Connectors in AWS and Azure environments, each connector can handle between 31-60 concurrent RDP/SSH sessions.

This capacity is specified in the CyberArk documentation concerning Privilege Cloud Connectors and their scalability options. It is designed to support a higher volume of concurrent sessions to meet the needs of larger enterprise environments, ensuring that multiple users can securely access resources without significant performance degradation.

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

You are implementing LDAPS Integration for a standard Privilege Cloud environment.
Which information must be provided to the CyberArk Privilege Cloud support team through a Service Request? (Choose 2.)

- A. LDAPS certificate chain for all domain controllers to be integrated
- B. LDAP bind username and password used to authenticate to the directory to be integrated
- C. Domain Base Context used to locate the users and groups in the Active Directory to be integrated
- D. Fully Qualified Domain Name and IP Address of the domain controllers to be integrated
- E. remote port set during secure tunnel configuration for each domain controller to be integrated

Answer: AD

Explanation:

When implementing LDAPS Integration for a standard Privilege Cloud environment, certain information is crucial and must be provided to the CyberArk Privilege Cloud support team through a Service Request. The necessary details include:

- ? LDAPS certificate chain for all domain controllers to be integrated (Option A): This information is critical to establishing a trusted secure connection between the Privilege Cloud and the domain controllers using LDAP over SSL (LDAPS).
 - ? Fully Qualified Domain Name and IP Address of the domain controllers to be integrated (Option D): This information is essential for accurately identifying and configuring the network connections to each domain controller that will be integrated with the Privilege Cloud.
- Reference: The process of setting up LDAPS integration typically requires detailed network and security information about the domain controllers to ensure secure and reliable connectivity. CyberArk support documentation and service request forms usually specify the need for these details.

NEW QUESTION 7

DRAG DROP
Arrange the steps to install passive CPM using Connector Management in the correct sequence

Unordered Options

Run the Connector Management Connector installer.

When prompted to select the CPM mode, select Passive.

When prompted to select the components to install, select CPM.

Install the CPM and optionally PSM, if required.

Ordered Response

- 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 8

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 9

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

- 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.

NEW QUESTION 10

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 DBPARAM.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: BE

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.

Reference: CyberArk's SIEM integration documentation and support articles often discuss these steps as part of setting up comprehensive security and monitoring configurations.

NEW QUESTION 10

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 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 14

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 19

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 22

.....

Relate Links

100% Pass Your CPC-SEN Exam with Examible Prep Materials

<https://www.examible.com/CPC-SEN-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.examible.com/>