



CyberArk

Exam Questions CPC-SEN

CyberArk Sentry - Privilege Cloud

NEW QUESTION 1

DRAG DROP

You want to change the default PSM recordings folder path on the Privilege Cloud Connector Arrange the steps to accomplish this in the correct sequence.

Unordered Options	Ordered Response
<div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; margin-bottom: 5px;">Create a corresponding folder in the new location.</div> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; margin-bottom: 5px;">In the Basic_psm.ini file, set RecordingsDirectory with the new path.</div> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; margin-bottom: 5px;">Restart the PSM service.</div> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px;">Run the PSMHardening script.</div>	<div style="border: 1px solid #ccc; height: 300px; width: 100%;"></div>
← →	↑ ↓

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To correctly change the default PSM recordings folder path on the Privilege Cloud Connector, the sequence of steps should be:

- ? Create a corresponding folder in the new location. Before making changes to configuration files, ensure the new directory for PSM recordings is created. This is where all session recordings will be stored moving forward.
- ? In the Basic_psm.ini file, set RecordingsDirectory with the new path. Update the Basic_psm.ini file to reflect the new path for the recordings. This step is crucial as it directs the PSM to start using the newly created directory for all future session recordings.
- ? Restart the PSM service. After updating the path in the configuration file, restart the PSM service to apply the changes. This ensures that all new sessions are recorded in the new specified location.
- ? Run the PSMHardening script. Once the service is restarted and the new settings are in place, run the PSMHardening script. This script ensures that all security measures are re-applied to the new recordings directory, maintaining the security integrity of the session recordings.

Following these steps in the given order will successfully change the recording directory for PSM sessions on the Privilege Cloud Connector, ensuring a smooth transition to the new storage location with all necessary security measures intact.

NEW QUESTION 2

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 3

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 4

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 5

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 6

What is the correct CyberArk user to use when installing the Privilege Cloud Connector software?

- A. installeruser@<suffix>
- B. Administrator
- C. <subdomain>_admin
- D. Installer

Answer: C

Explanation:

The correct CyberArk user to use when installing the Privilege Cloud Connector software is typically formatted as <subdomain>_admin. This username format indicates a privileged administrative account associated with the specific subdomain of the CyberArk Privilege Cloud installation. It ensures that the user has sufficient permissions to perform installation tasks across the environment, which are crucial for setting up and configuring the connectors correctly. Details about user roles and permissions can be found in the CyberArk Privilege Cloud installation and configuration guide.

NEW QUESTION 7

How should you configure PSM for SSH to support load balancing?

- A. by using a network load balancer
- B. in PVWA > Options > PSM for SSH Proxy > Servers
- C. in PVWA > Options > PSM for SSH Proxy > Servers > VIP
- D. by editing sshd.config on the all the PSM for SSH servers

Answer: A

Explanation:

To support load balancing for PSM for SSH, the configuration should be done by using a network load balancer. This method involves placing a network load balancer in front of multiple PSM for SSH servers to distribute incoming SSH traffic evenly among them. This setup enhances the availability and scalability of PSM for SSH by ensuring that no single server becomes a bottleneck, thereby improving performance and reliability during high usage scenarios.

NEW QUESTION 8

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 9

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 10

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 10

Which option correctly describes the authentication differences between CyberArk Privilege Cloud and CyberArk PAM Self-Hosted?

- A. CyberArk Privilege Cloud only provides a username and password authentication without third-party IdP integration; CyberArk PAM Self-Hosted uses traditional on-premises methods such as Windows and LDA
- B. but lacks modern protocols such as SAML or OIDC.
- C. CyberArk Privilege Cloud uses cloud-based methods, integrating with CyberArk Identity for MF
- D. and supports SAML and OIDC; CyberArk PAM Self-Hosted depends on on-premises methods such as RADIUS and LDAP, but can adopt SAML or OIDC with additional setups.
- E. CyberArk Privilege Cloud requires on-premises components for all authentication and does not support other cloud-based authentication protocols; CyberArk PAM Self-Hosted offers a wide array of methods, including support for SAM
- F. OID
- G. and other modern protocols, without needing on-premises components.
- H. Both use the same authentication methods.

Answer: B

Explanation:

The correct description of the authentication differences between CyberArk Privilege Cloud and CyberArk PAM Self-Hosted is that CyberArk Privilege Cloud uses cloud-based methods, integrating with CyberArk Identity for Multi-Factor Authentication (MFA), and supports SAML and OIDC, while CyberArk PAM Self-Hosted relies on on-premises methods such as RADIUS and LDAP, but can adopt SAML or OIDC with additional setups. CyberArk Privilege Cloud is designed to leverage modern cloud-based authentication protocols to enhance security and ease of use, particularly in distributed and diverse IT environments. In contrast, CyberArk PAM Self-Hosted offers flexibility to use traditional on-premises authentication methods but also supports modern protocols if configured to do so.

NEW QUESTION 14

You have been tasked with deploying a Privilege Cloud PSM for SSH connector. When the initial installation has successfully completed, you create and permission several maintenance users to be used for administering the connector.

Which configuration file must be updated to define these maintenance users?

- A. sshd.config
- B. basic_psmserver.conf
- C. sshd_config
- D. psmpparms

Answer: C

Explanation:

The sshd_config file is the correct configuration file that must be updated to define maintenance users for administering the Privilege Cloud PSM for SSH connector. This file contains configurations for the SSH daemon, including user permissions and group settings. When adding maintenance users, their user accounts are created on the PSM

server, and then they are added to the AllowGroups parameter within the sshd_config file to grant them the necessary permissions.

References:

? CyberArk documentation on the PSM for SSH environment1.

? CyberArk Sentry guide on how to add maintenance users for SSH PSM

? When deploying a Privilege Cloud PSM for SSH connector, the configuration file that must be updated to define maintenance users is "sshd_config". This file is used to configure options specific to the SSH daemon, which includes user permissions, authentication methods, and other security-related settings. To add and configure maintenance users for the PSM for SSH, you will need to modify this file to specify allowed users and their respective privileges.

Reference: The configuration of SSH-related components typically involves the "sshd_config" file, as outlined in SSH and PSM for SSH setup guides. This is a standard practice in systems that utilize SSH for secure communications and management.

NEW QUESTION 16

In the directory lookup order, which directory service is always looked up first for the CyberArk Privilege Cloud solution?

- A. Active Directory
- B. LDAP
- C. Federated Directory
- D. CyberArk Cloud Directory

Answer: D

Explanation:

In the directory lookup order for the CyberArk Privilege Cloud solution, the "CyberArk Cloud

Directory" is always looked up first. This directory service is a part of the CyberArk Privilege Cloud infrastructure and is specifically designed to handle identity and access management within the cloud environment efficiently. It prioritizes the CyberArk Cloud Directory for authentication and identity resolution before consulting any external directory services.

Reference: CyberArk's architectural documentation usually emphasizes the role of the CyberArk Cloud Directory in managing and authenticating user access in cloud-based deployments, highlighting its precedence in the directory lookup process.

NEW QUESTION 20

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 21

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 22

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 23

Your customer is using Privilege Cloud Shared Services. What is the correct CyberArk Vault address for this customer?

- A. carkvault-<subdomain>.privilegecloud.cyberark.cloud
- B. vault-<subdomain>.privilegecloud.cyberark.cloud
- C. v-<subdomain>.privilegecloud.cyberark.cloud
- D. carkvlt-<subdomain> privilegecloud.cyberark.cloud

Answer: B

Explanation:

For customers using CyberArk Privilege Cloud Shared Services, the correct format for the CyberArk Vault address is: vault-<subdomain>.privilegecloud.cyberark.cloud (Option B). This format is used to access the vault services provided by CyberArk in the cloud environment, where <subdomain> is the unique identifier assigned to the customer's specific instance of the Privilege Cloud. Reference: CyberArk's Privilege Cloud documentation provides details on how to access various services, including the vault. The standard naming convention for accessing the vault services in the cloud typically follows this format.

NEW QUESTION 27

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 28

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 30

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 35

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 36

What is the default username for the PSM for SSH maintenance user?

- A. proxymng
- B. psm_maintenance
- C. psmmaintenanceuser
- D. proxyusr

Answer: B

Explanation:

The default username for the Privileged Session Manager (PSM) for SSH maintenance user in CyberArk Privilege Cloud is psm_maintenance. This account is used for maintenance purposes and is integral for administrative tasks and configurations related to SSH sessions managed by the PSM. The username is predefined and standardized across deployments to maintain consistency and ensure security best practices are adhered to. The username is mentioned in the CyberArk official documentation regarding PSM configuration for SSH.

NEW QUESTION 39

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 40

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 43

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 48

.....

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](#)