Free Questions for CPC-SEN by dumpssheet

Shared by Stokes on 14-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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?

Options:

A- sshd.config

B- basic_psmpserver.conf

C- sshd_config

D- psmpparms

Answer:

C

Explanation:

Thesshd_configfile 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 theAllowGroupsparameter within thesshd_configfile to grant them the necessary permissions.

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.

Question 2

Question Type: **MultipleChoice**

What creating a new safe, what is the default number of password versions stored if using 'Save latest account versions' within version management settings?

Options:

A- 5

B- 10

C- 30

D- 90

Answer:

B

Explanation:

When creating a new safe and configuring the 'Save latest account versions' within version management settings, the default number of password versions stored is 10. This setting allows the safe to maintain up to 10 past versions of each password managed within it. This capability is essential for ensuring that previous password states can be accessed if needed, such as for audit purposes or rollback scenarios in the event of an update error or compromise.

Question 3

Question Type: MultipleChoice

When installing the PSM and CPM components on the same Privilege Cloud Connector, what should you consider when hardening?

Options:

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.

Question 4

Question Type: MultipleChoice

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

Options:

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.

Question 5

Question Type: MultipleChoice

According to best practice, when considering the location of PSM Connector servers in Privilege Cloud environments, where should the PSM be placed?

Options:

A- near the CPM servers

B- near the target devices

C- near the Vault (closer to the external internet connection)

D- near the Users

Answer:

B

Explanation:

According to best practice, when considering the location of PSM Connector servers in Privilege Cloud environments, the PSM should be placed near the target devices. This placement minimizes latency and maximizes performance by reducing the distance that data has to travel between the PSM servers and the devices they are managing. This is particularly important for maintaining high efficiency and response times during remote session management and operations, which are critical for the overall effectiveness of the Privilege Cloud environment.

Question 6

Question Type: MultipleChoice

'What is a default authentication profile to access CyberArk Identity?

Options:

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.

Question 7

Question Type: **MultipleChoice**

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?

Options:

A- RDP/389 HTTP/443

B- RDP/3389 HTTPS/443

C UDP/53 HTTPS/389

D- RDP/636 HTTPS/443

Answer:

B

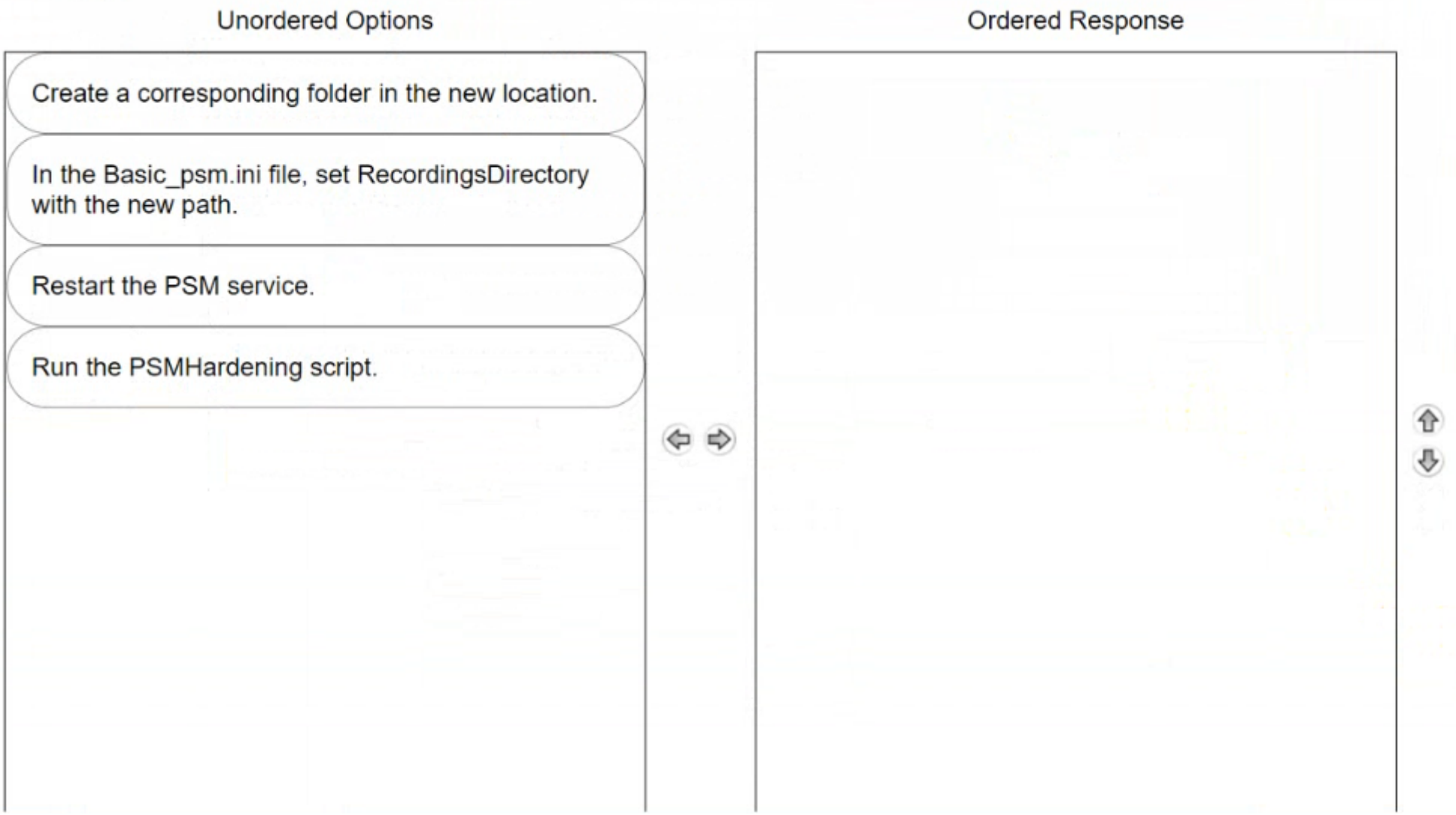
Explanation:

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.

Question 8

Question Type: **OrderList**

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
Create a corresponding folder in the new location.
In the Basic_psm.ini file, set RecordingsDirectory with the new path.
Restart the PSM service.
Run the PSMHardening script.

Answer:

Create a corresponding folder in the new location with the new path. Restar

Question 9

Question Type: MultipleChoice

Following the installation of the PSM for SSH server, which additional tasks should be performed? (Choose 2.)

Options:

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:

A, C

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.

Question 10

Question Type: MultipleChoice

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

Options:

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.

Question 11

Question Type: **OrderList**

Arrange the steps to failover to the passive CPM in the correct sequence.

Unordered Options

- Enable the CPM services on the passive CPM.
- Validate that the active CPM's services are stopped and set to manual.
- On the passive CPM, confirm details in the Vault.ini configuration file, reset the password to the CPM user, and recreate the credential file.
- Review logs to confirm the passive CPM services are running as expected.

Ordered Response

Answer: