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
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
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 3
CyberArk User Neil is trying to connect to the Target Linux server 192.168.1.164 using a domain user ACME\linuxuser01 on domain acme.corp using PSM for SSH server 192.168.65.145.
What is the correct syntax?

A. ssh neil@linuxuser01:acme.corp@192.168.1.164@192.168.65.145
B. ssh neil@linuxuser01#acme.corp@192.168.1.164@192.168.65.145
C. sshneil@linuxuser01@192.168.1.164@192.168.65.145
D. ssh neil@linuxuser01@acme.corp@192.168.1.164@192.168.65.145

Answer: B

Explanation:
In CyberArk Privilege Cloud, when connecting to a target server using the Privileged Session Manager (PSM) for SSH, the correct syntax for the SSH command includes the following format: ssh neil@linuxuser01#acme.corp@192.168.1.164@192.168.65.145. This syntax breaks down as follows:
? neil: The CyberArk username.
? linuxuser01#acme.corp: The domain user on the target Linux server, formatted as username#domain.
? 192.168.1.164: The IP address of the target Linux server.
? 192.168.65.145: The IP address of the PSM for SSH server.
This specific format ensures that the CyberArk Privileged Access Manager correctly interprets and routes the connection through the PSM for SSH to the intended target server.
References:
? CyberArk Privilege Cloud Introduction
? CyberArk Privileged Access Manager
? CyberArk Privilege Cloud - Manage Safe Members
? CyberArk Security Fundamentals

NEW QUESTION 4
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 5
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 6
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 7
During CPM hardening, which locally created users are granted Logon as a Service rights in the local group policy? (Choose 2.)

A. PasswordManager
B. PluginManagerUser
C. ScannerUser
D. PasswordManagerUser
E. CPMServiceAccount

Answer: AD

Explanation:
During the Central Policy Manager (CPM) hardening process, the locally created users that are granted 'Logon as a Service' rights in the local group policy are typically PasswordManager and PasswordManagerUser. These accounts are crucial for the CPM??s operation as they handle password management tasks and require the ability to log on as a service to perform their functions effectively. This configuration is established to ensure that these service accounts can operate under service control manager without interruption, which is critical for automated password rotations and other security processes managed by the CPM. This detail is typically outlined in the CyberArk CPM installation and configuration guide.

NEW QUESTION 8
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 9
How can a platform be configured to work with load-balanced PSMs?

A. Remove all entries from configured PSM Servers except for the ID of the PSMs with load balancing.
B. Create a new PSM definition that targets the load balancer IP address and assign to the platform.
C. Include details of the PSMs with load balancing in the Basic_psm.ini file on each PSM server.
D. Use the Privilege Cloud Portal to update the Session Management settings for the platform in the Master Policy.

Answer: B

Explanation:

To configure a platform to work with load-balanced Privileged Session Managers (PSMs), you should:
? Create a new PSM definition that targets the load balancer IP address and assign
it to the platform (Option B). This approach involves configuring the platform settings to direct session traffic through a load balancer that distributes the load across multiple PSM servers. This is effective in environments where high availability and fault tolerance are priorities.
Reference: CyberArk??s setup guidelines for high-availability environments typically recommend configuring platforms to utilize load balancers to ensure continuous availability and optimal distribution of session management tasks.

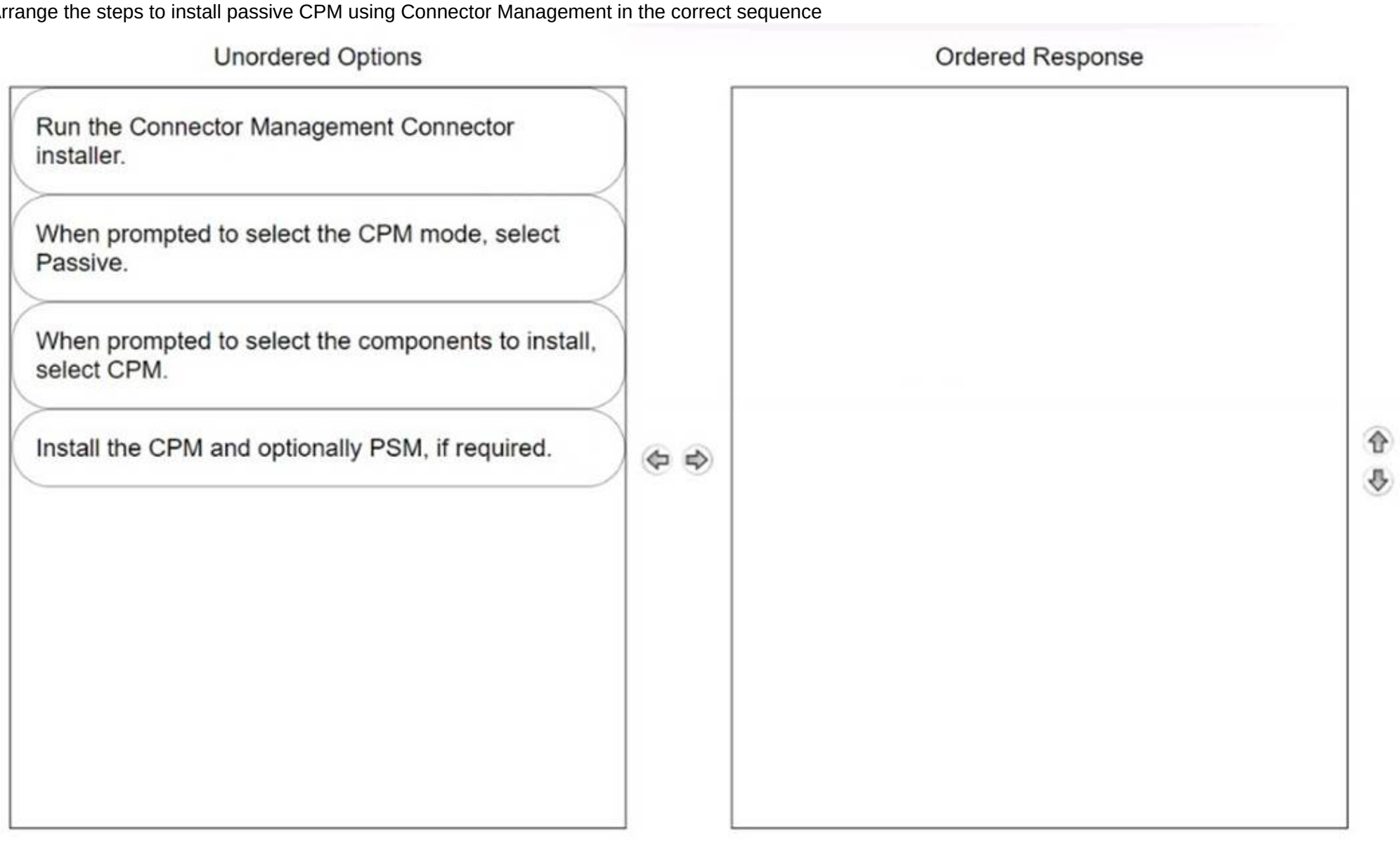
NEW QUESTION 10
When installing the first CPM within Privilege Cloud using the Connector Management Agent, what should you set the Installation Mode to in the CPM section?

A. Active
B. Passive
C. Default
D. Primary

Answer: A

Explanation:
When installing the first CyberArk Privilege Management (CPM) instance in the Privilege Cloud using the Connector Management Agent, the installation mode should be set to "Active". This configuration sets the CPM to be actively involved in password management and task processing without being in a standby or passive mode. Here are the step-by-step details:
? Download the Connector Management Agent: Obtain the installer from the CyberArk Marketplace or your installation kit.
? Run the Installer: Start the setup and select the CPM component to install.
? Choose Installation Mode: When prompted, select "Active" as the installation mode. This sets up the CPM as the primary node responsible for handling password management operations.
This setup ensures that the CPM is immediately active and capable of handling requests without waiting for manual intervention or failover.
Reference: CyberArk??s official documentation provides guidance on setting up the CPM, where it specifies the modes and their purposes.

NEW QUESTION 10
DRAG DROP
Arrange the steps to install passive CPM using Connector Management in the correct sequence



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 15
What creating a new safe, what is the default number of password versions stored if using 'Save latest account versions' within version management settings?

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.

NEW QUESTION 16
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.

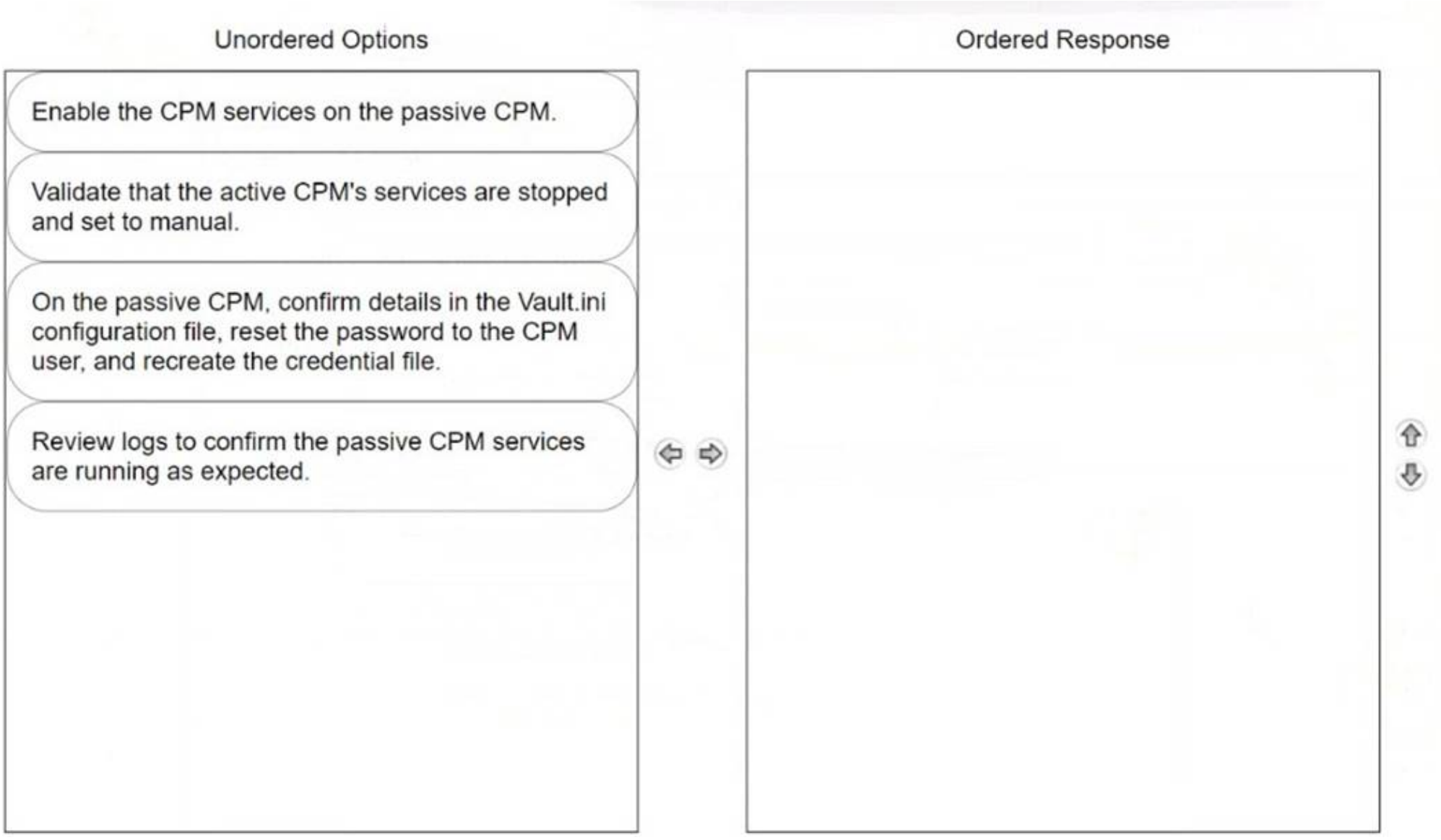
NEW QUESTION 19
'What is a default authentication profile to access CyberArk Identity?

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 20
DRAG DROP
Arrange the steps to failover to the passive CPM in the correct sequence.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
To properly arrange the steps for failing over to a passive Central Policy Manager (CPM) in CyberArk, the sequence should be as follows:
? Validate that the active CPM's services are stopped and set to manual.Before
enabling the passive CPM, ensure that the services on the active CPM are stopped. This prevents any conflicts or data corruption by making sure that only one CPM is active at a time. Setting the services to manual ensures they do not restart automatically, which is crucial during a failover scenario.
? On the passive CPM, confirm details in the Vault.ini configuration file, reset the
password to the CPM user, and recreate the credential file.This step involves making sure the passive CPM has the correct configuration to seamlessly take over operations. Adjustments in the Vault.ini file may be necessary to ensure it is pointing to the correct Vault and network settings. Resetting the password and recreating the credential file are critical to secure the login and authentication process for the newly active CPM.
? Enable the CPM services on the passive CPM.Once the passive CPM is correctly configured and ready, enable its services to begin handling the tasks and responsibilities of the primary CPM. This action effectively switches the role from passive to active, enabling the passive CPM to function as the new operational manager.
? Review logs to confirm the passive CPM services are running as expected.Finally, review the system and application logs to confirm that the now-active CPM is operating correctly and that all services have started without errors. This step is vital for verifying that the failover process was successful and that the system is stable.
Following this ordered sequence ensures a smooth transition of roles from the active CPM to the passive CPM, minimizing downtime and potential disruptions in the privileged access management operations.

NEW QUESTION 24
.....

Relate Links

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

https://www.exambible.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.exambible.com/