PassQueen
a.k.a dumpsqueen.com

CyberArk CDE Recertification

CyberArk CAU305

Version Demo

Total Demo Questions: 8

Total Premium Questions: 86

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

When a DR Vault Server becomes an active vault, it will automatically revert back to DR mode once the Primary Vault comes back online.

A. True, this is the default behavior.

B. False, the Vault administrator must manually set the DR Vault to DR mode by setting "FailoverMode=no" in the padr.ini file.

C. True, if the AllowFailback setting is set to "yes" in the padr.ini file.

D. False, the Vault administrator must manually set the DR Vault to DR mode by setting "FailoverMode=no" in the dbparm.ini file.

ANSWER: B

Explanation:

False, the Vault administrator must manually set the DR Vault to DR mode by setting "FailoverMode=no" in the padr.ini file. A Disaster Recovery Vault that has failed over and become the active Vault does not automatically fail back merely because the original Primary Vault is online again. This design prevents an unplanned role change while recovery validation, replication status checks, and operational readiness activities are still being completed. The administrator controls the failback process and must explicitly return the Disaster Recovery Vault to its standby role.

The `FailoverMode` parameter is maintained in the DR configuration file, `padr.ini`. Setting `FailoverMode=no` instructs the DR Vault not to operate in failover mode, which is part of the controlled procedure for returning it to DR operation after the Primary Vault has been restored. Administrators should follow the documented failback procedure, including confirming that the Primary Vault is operational and synchronization is healthy, before changing roles. CyberArk documents DR configuration and failover behavior in its Disaster Recovery guidance and provides additional implementation details in the Implementing Disaster Recovery documentation.

QUESTION NO: 2

Which actions can the Central Policy Manager (CPM) perform for a managed account when the applicable platform is configured? (Choose three.)

A. Verify password

B. Change password

C. Reconcile password

D. Record privileged sessions

ANSWER: A B C

Explanation:

Verify password, **change password**, and **reconcile password** are CPM password-management operations. Verification checks whether the credential stored in the Vault matches the credential on the target system. A change operation updates the target credential according to policy and stores the new value in the Vault. Reconciliation is used when the Vault credential is unknown or out of synchronization and CPM must reset the managed account through a configured reconcile account.

CPM does not record privileged sessions. Session recording is performed by Privileged Session Manager (PSM). See the CyberArk Central Policy Manager documentation and password management documentation.

QUESTION NO: 3

Which of the following components can be used to create a tape backup of the Vault?

A. Disaster Recovery

B. Distributed Vaults

C. Replicate

D. High Availability

ANSWER: C

Explanation:

Replicate is the CyberArk Vault component and utility used to create a backup copy of Vault data, including a copy written to tape media where tape backup infrastructure is available. It performs a controlled replication of the Vault's data, producing a backup that can be retained independently of the production Vault and used as part of the organization's recovery strategy. This is distinct from the operational availability and recovery architecture: the relevant point for this question is that Replicate is specifically associated with creating Vault backup copies and supports tape as a backup target. Administrators should run and monitor backups according to their organization's retention, media-handling, and recovery-testing procedures, ensuring that backup media is protected with at least the same care as the Vault itself. CyberArk's product documentation provides the authoritative guidance for Vault administration, backup, and recovery operations; see the CyberArk PAM Self-Hosted documentation and the CyberArk documentation portal for the version-specific Vault backup procedures applicable to the deployment.

QUESTION NO: 4

Which is the purpose of the allowed Safes parameter in a Central Policy Manager (CPM) policy? (Choose two.)

A. To improve performance by reducing CPM workload

B. To prevent accidental use of a policy in the wrong Safe

C. To allow users to access only the passwords they should be able to access

D. To enforce Least Privilege in CyberArk

ANSWER: A B

Explanation:

The allowed Safes parameter defines the specific CyberArk Safes in which a CPM policy is permitted to manage accounts. Selecting *To improve performance by reducing CPM workload* is correct because the CPM can limit its account-processing scope to the Safes relevant to that policy. This reduces unnecessary account scanning and policy evaluation across Safes that are not intended to use the policy, helping the CPM operate more efficiently in environments with many accounts and policies.

To prevent accidental use of a policy in the wrong Safe is also correct. By explicitly listing the Safes where the policy may be applied, administrators create a guardrail that ensures the policy is used only in approved locations. This is particularly useful when different Safes contain different account types, platforms, password-management requirements, or operational ownership. The setting therefore supports controlled policy assignment and reduces the chance that an account is managed under an unintended CPM policy. CyberArk documents Allowed Safes as a CPM policy property used to restrict the Safes in which the policy can be used. See the CyberArk CPM policy properties documentation and the CyberArk Central Policy Manager documentation.

QUESTION NO: 5

Which utilities could a Vault administrator use to change debugging levels on the Vault without having to restart the Vault? (Choose two.)

A. PAR Agent

B. PrivateArk Server Central Administration

C. Edit DBParm.ini in a text editor

D. Setup.exe

ANSWER: A B

Explanation:

PAR Agent and **PrivateArk Server Central Administration** are the Vault administration utilities that support changing Vault trace/debug settings dynamically, allowing an administrator to increase or decrease diagnostic logging while the Vault service remains online. This is particularly useful when troubleshooting an active issue: the administrator can enable the required tracing, reproduce or observe the behavior, collect the resulting logs, and then return the logging level to its normal setting without introducing a service interruption.

PAR Agent provides an administrative mechanism for communicating operational changes to the running Vault, including debug-level adjustments. PrivateArk Server Central Administration exposes Vault server administration settings through its management interface and can apply supported debugging-level changes to the active Vault process. Dynamic adjustment avoids the operational impact and temporary unavailability associated with restarting a production Vault, while still enabling CyberArk Support or the administrator to obtain the diagnostic detail required for investigation. CyberArk documents Vault server administration and troubleshooting procedures in its Vault Server documentation and provides product documentation entry points at CyberArk Docs.

QUESTION NO: 6

When creating an onboarding rule, it will be executed upon.

A. all accounts in the pending accounts list

B. any future accounts discovered by a discovery process

C. all accounts in the pending accounts list and any future accounts discovered by a discovery process

ANSWER: B

Explanation:

Any future accounts discovered by a discovery process is correct because an onboarding rule is evaluated when a discovery process identifies accounts and places eligible accounts into the Pending Accounts list. The rule supplies the criteria and onboarding properties that CyberArk should apply automatically, such as the target Safe, platform, and account properties. This makes onboarding repeatable for subsequently discovered accounts that match the rule, without requiring an administrator to configure each new account individually.

In practice, the discovery configuration gathers account information from the relevant target environment, and the onboarding rule acts on newly discovered account records as they are processed. Administrators can therefore define a consistent policy before recurring discovery runs occur, ensuring that accounts matching the defined conditions are automatically onboarded according to the organization's standards. CyberArk documents onboarding rules as part of the process for automatically onboarding accounts discovered by the Accounts Discovery capability. See the CyberArk documentation on onboarding rules and the CyberArk documentation on discovering accounts.

QUESTION NO: 7 - (SIMULATION)

In version 10.7 the correct order of installation for components changed.

Make the necessary corrections to the list below to show the new installation order.

ANSWER: Check the explanation for the answer

Explanation:

Place the components in this installation order:

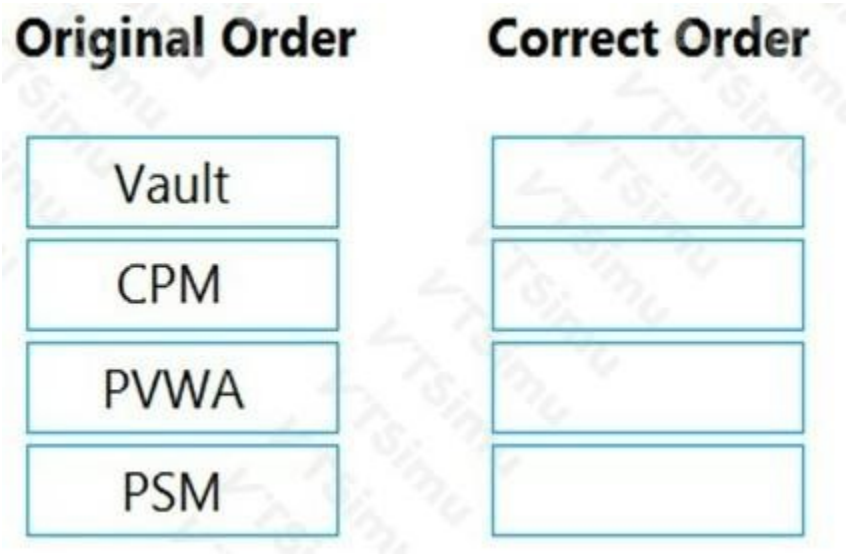
1. **Digital Vault** (install the Disaster Recovery Vault next, if one is deployed)
2. **Password Vault Web Access (PVWA)**
3. **Central Policy Manager (CPM)**
4. **Privileged Session Manager (PSM)**
5. **PSM for SSH**, if it is being deployed
6. **Credential Provider / Application Password Provider**, followed by **Central Credential Provider**, if these AAM components are being deployed

Thus, for the core PAS components, the required v10.7 order is: `Vault → PVWA → CPM → PSM`. The Vault must be available first; PVWA is then used to manage and configure the remaining components.

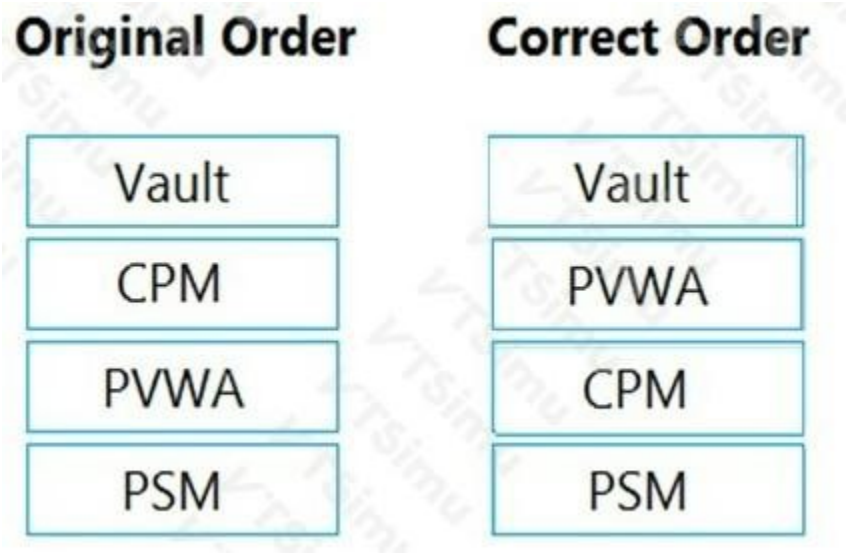
QUESTION NO: 8 - (DRAG DROP)

In version 10.7 the correct order of installation for components changed.

Make the necessary corrections to the list below to show the new installation order.



ANSWER:



Explanation:

The correct installation sequence is **Vault → PVWA → CPM → PSM**. The Vault is installed first because it is the secure, central repository and service foundation for the Privileged Access Security environment. It stores privileged account credentials, Safes, platform definitions, policies, encryption material, and the configuration data needed by the remaining components. The other components must be able to establish trusted communication with this Vault before they can be configured and used.

PVWA is installed next because it provides the web-based management interface through which administrators configure the environment, manage users and Safes, onboard accounts, and access the operational workflows of the solution. Installing it after the Vault makes the central administration interface available for the subsequent component setup.

CPM follows PVWA. CPM connects to the Vault to retrieve accounts and platform settings, perform password verification and reconciliation, and securely update managed credentials. With the Vault operational and the web administration layer available, CPM can be registered and configured in the intended management workflow.

PSM is installed last. PSM brokers, isolates, monitors, and records privileged sessions, while obtaining the required account and policy information from the established PAS environment. This dependency flow is why version 10.7 uses the displayed order rather than placing CPM ahead of PVWA. CyberArk's implementation documentation describes the Vault as the foundational component and provides deployment guidance for the PAS components: CyberArk PAS implementation documentation. Additional architecture context is available in the CyberArk Privileged Access Security Solution Architecture documentation.