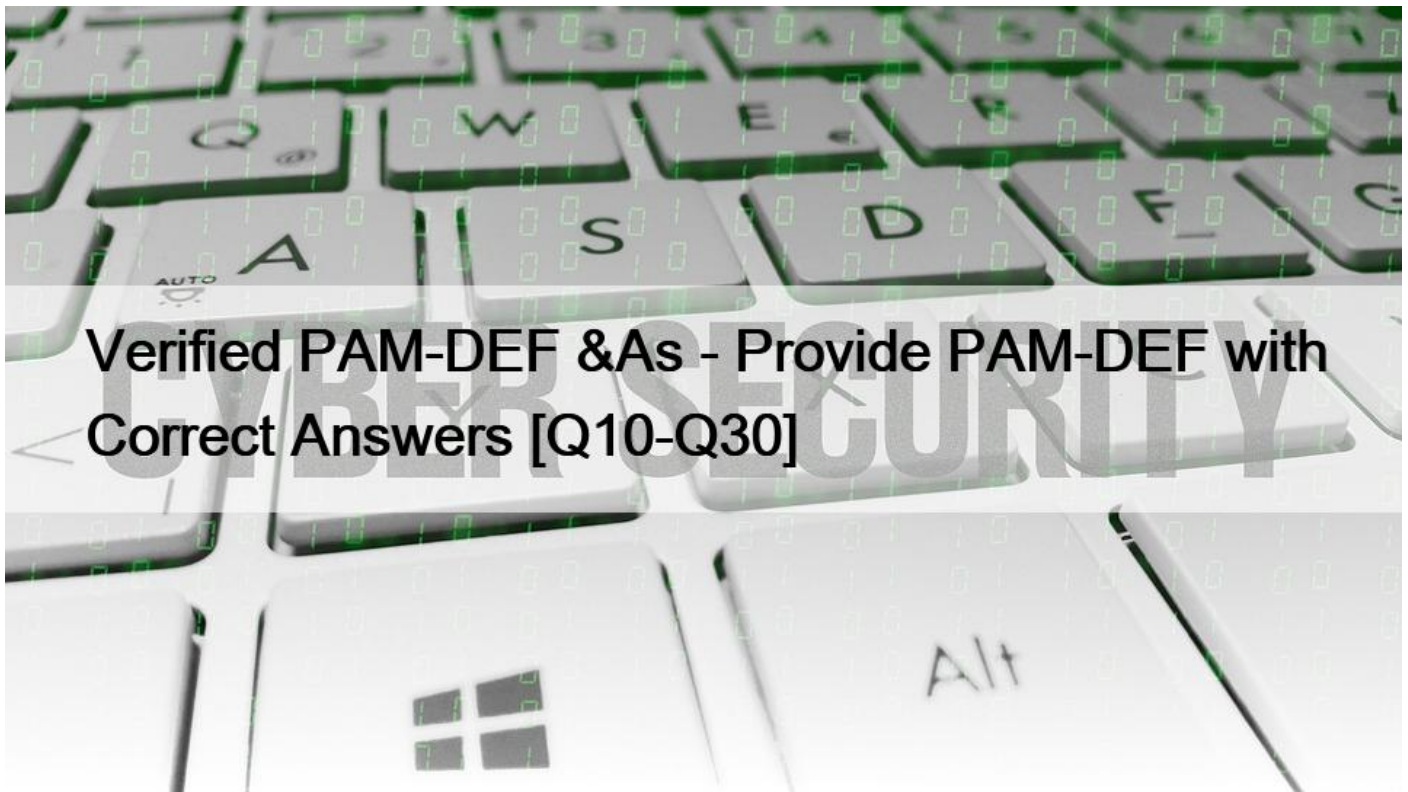


## Verified PAM-DEF &As - Provide PAM-DEF with Correct Answers [Q10-Q30]



Verified PAM-DEF Exam Dumps Q&As - Provide PAM-DEF with Correct Answers  
Pass Your PAM-DEF Dumps Free Latest CyberArk Practice Tests

**NO.10** What is the purpose of the password change process?

- \* To test that CyberArk is storing accurate credentials for accounts
- \* To change the password of an account according to organizationally defined password rules
- \* To allow CyberArk to manage unknown or lost credentials
- \* To generate a new complex password

**NO.11** You have been asked to turn off the time access restrictions for a safe.

Where is this setting found?

- \* PrivateArk
- \* RestAPI
- \* Password Vault Web Access (PVWA)
- \* Vault

**NO.12** What is the purpose of the HeadStartInterval setting in a platform?

- \* It determines how far in advance audit data is collected for reports
- \* It instructs the CPM to initiate the password change process X number of days before expiration.
- \* It instructs the AIM Provider to skip the cache during the defined time period
- \* It alerts users of upcoming password changes x number of days before expiration.

**NO.13** Which of the Following can be configured in the Master Pky? Choose all that apply.

- \* Dual Control
- \* One Time Passwords
- \* Exclusive Passwords
- \* Password Reconciliation
- \* Ticketing Integration
- \* Required Properties
- \* Custom Connection Components
- \* Password Aging Rules

**NO.14** To manage automated onboarding rules, a CyberArk user must be a member of which group?

- \* Vault Admins
- \* CPM User
- \* Auditors
- \* Administrators

**NO.15** Users are unable to launch Web Type Connection components from the PSM server. Your manager asked you to open the case with CyberArk Support.

Which logs will help the CyberArk Support Team debug the issue? (Choose three.)

- \* PSMConsole.log
- \* PSMDebug.log
- \* PSMTrace.log
- \* <Session\_ID>.Component.log
- \* PMconsole.log
- \* ITAlog.log

**NO.16** When a DR Vault Server becomes an active vault, it will automatically revert back to DR mode once the Primary Vault comes back online.

- \* True; this is the default behavior
- \* False, the Vault administrator must manually set the DR Vault to DR mode by setting `FailoverMode=no` in the `padr.ini` file
- \* True, if the `AllowFailback` setting is set to `yes` in the `padr.ini` file
- \* False, the Vault administrator must manually set the DR Vault to DR mode by setting `FailoverMode=no` in the `dbparm.ini` file

**NO.17** You have been asked to secure a set of shared accounts in CyberArk whose passwords will need to be used by end users. The account owner wants to be able to track who was using an account at any given moment.

Which security configuration should you recommend?

- \* Configure one-time passwords for the appropriate platform in Master Policy.
- \* Configure shared account mode on the appropriate safe.
- \* Configure both one-time passwords and exclusive access for the appropriate platform in Master Policy.
- \* Configure object level access control on the appropriate safe.

**NO.18** What is the purpose of the Immediate Interval setting in a CPM policy?

- \* To control how often the CPM looks for System Initiated CPM work.
- \* To control how often the CPM looks for User Initiated CPM work.
- \* To control how often the CPM rests between password changes.

- \* To Control the maximum amount of time the CPM will wait for a password change to complete.

Explanation

When the Master Policy enforces check-in/check-out exclusive access, passwords are changed when the user clicks the Release button and releases the account. This is based on the ImmediateInterval parameter in the applied platform. If the user forgets to release the account, it is automatically released and changed by the CPM after a predetermined number of minutes, defined in the MinValidityPeriod parameter specified in the platform

**NO.19** When onboarding multiple accounts from the Pending Accounts list, which associated setting must be the same across the selected accounts?

- \* Platform
- \* Connection Component
- \* CPM
- \* Vault

**NO.20** What is the primary purpose of Dual Control?

- \* Reduced risk of credential theft
- \* More frequent password changes
- \* Non-repudiation (individual accountability)
- \* To force a collusion to commit; fraud ensuring no single actor may use a password without authorization.

**NO.21** In accordance with best practice, SSH access is denied for root accounts on UNIX/LINUX system. What is the BEST way to allow CPM to manage root accounts.

- \* Create a privileged account on the target server. Allow this account the ability to SSH directly from the CPM machine. Configure this account as the Reconcile account of the target server's root account.
- \* Create a non-privileged account on the target server. Allow this account the ability to SSH directly from the CPM machine. Configure this account as the Logon account of the target server's root account.
- \* Configure the Unix system to allow SSH logins.
- \* Configure the CPM to allow SSH logins.

**NO.22** When managing SSH keys, the CPM stores the Public Key

- \* In the Vault
- \* On the target server
- \* A & B
- \* Nowhere because the public key can always be generated from the private key.

**NO.23** What is the purpose of the Immediate Interval setting in a CPM policy?

- \* To control how often the CPM looks for System Initiated CPM work.
- \* To control how often the CPM looks for User Initiated CPM work.
- \* To control how often the CPM rests between password changes.
- \* To Control the maximum amount of time the CPM will wait for a password change to complete.

**NO.24** A Simple Mail Transfer Protocol (SMTP) integration is critical for monitoring Vault activity and facilitating workflow processes, such as Dual Control.

- \* True
- \* False

**NO.25** Which CyberArk utility allows you to create lists of Master Policy Settings, owners and safes for output to text files or MSSQL databases?

- \* Export Vault Data

- \* Export Vault Information
- \* PrivateArk Client
- \* Privileged Threat Analytics

**NO.26** Which Master Policy Setting must be active in order to have an account checked-out by one user for a pre-determined amount of time?

- \* Require dual control password access Approval
- \* Enforce check-in/check-out exclusive access
- \* Enforce one-time password access
- \* Enforce check-in/check-out exclusive access & Enforce one-time password access

**NO.27** An auditor initiates a live monitoring session to PSM server to view an ongoing live session. When the auditor's machine makes an RDP connection the PSM server, which user will be used?

- \* PSMAdminConnect
- \* Shadowuser
- \* PSMConnect
- \* Credentials stored in the Vault for the target machine

**NO.28** Users can be resulted to using certain CyberArk interfaces (e.g.PVWA or PACLD).

- \* TRUE
- \* FALS

**NO.29** A Logon Account can be specified in the Master Policy.

- \* TRUE
- \* FALSE

**NO.30** What is the purpose of a linked account?

- \* To ensure that a particular collection of accounts all have the same password.
- \* To ensure a particular set of accounts all change at the same time.
- \* To connect the CPNI to a target system.
- \* To allow more than one account to work together as part of a password management process.

**Get Top-Rated CyberArk PAM-DEF Exam Dumps Now:**

[https://www.test4engine.com/PAM-DEF\\_exam-latest-braindumps.html](https://www.test4engine.com/PAM-DEF_exam-latest-braindumps.html)