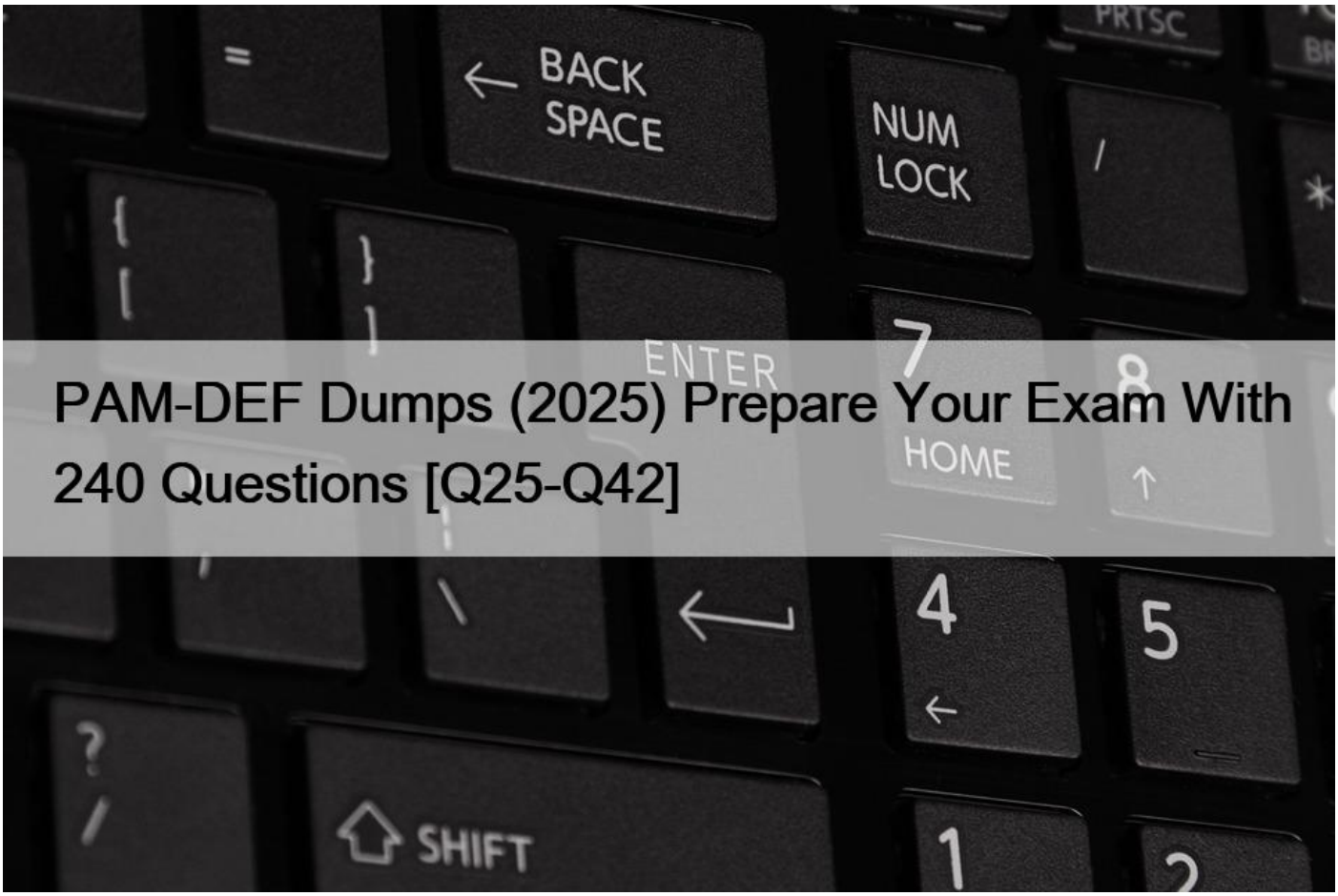
PAM-DEF Dumps (2025) Prepare Your Exam With 240 Questions [Q25-Q42



PAM-DEF Dumps (2025) Prepare Your Exam With 240 Questions New PAM-DEF Dumps - Real CyberArk Exam Questions NEW QUESTION 25

In the Private Ark client under the Tools menu > Administrative Tools > Users and Groups, which option do you use to update users’ Vault group memberships?
* Update > General tab
* Update > Authorizations tab
* Update > Member Of tab
* Update > Group tab

Explanation

In the PrivateArk client, to update users’ Vault group memberships, you use the Member Of tab. After logging in as an administrative user and navigating to the Users and Groups window, you select a user and click Update. In the Member Of tab, you can manage the user’s group memberships by adding or removing them from groups within the Vault1.

References:

* CyberArk Docs – Manage users in PrivateArk client1

NEW QUESTION 26

What is the purpose of the CyberArk Event Notification Engine service?
* It sends email messages from the Central Policy Manager (CPM)
* It sends email messages from the Vault
* It processes audit report messages
* It makes Vault data available to components

NEW QUESTION 27

PSM for Windows (previously known as “RDP Proxy”) supports connections to the following target systems
* Windows
* UNIX
* Oracle
* All of the above

NEW QUESTION 28

When should vault keys be rotated?
* when it is copied to file systems outside the vault
* annually
* whenever a CyberArk user leaves the organization
* when migrating to a new data center

Explanation

Vault keys should be rotated when there is a significant event that could potentially compromise the security of the keys, such as when migrating to a new data center. This is because the keys may be exposed to new environments and systems, and rotating them ensures that any potential exposure does not result in a security breach. Additionally, periodic rotation of encryption keys is recommended to maintain the integrity of the encryption and to adhere to best practices for security1. References:

* CyberArk Docs: Credentials Rotation Policy2

* HashiCorp Developer: Key Rotation

NEW QUESTION 29

A recently-hired colleague onboarded five new Local Accounts that are used for five standalone Windows Servers. After attempting to connect to the servers from PVWA, the colleague noticed that the “Connect” button was greyed out for all five new accounts.

What can you do to help your colleague resolve this issue? (Choose two.)
* Verify that the address field is populated with an IP or FQDN of each server.
* Verify that the correct PSM connection component appears within account platform settings.
* Verify that the address field is blank and that the correct PSM connection component appears within account platform settings.
* Notify the Windows Team that created the new accounts that the CyberArk PAM solution is not designed to manage local accounts on Windows Servers.
* Verify that the “Disable automatic management for this account” setting for each account is not enabled.

NEW QUESTION 30

A newly created platform allows users to access a Linux endpoint. When users click to connect, nothing happens.

Which piece of the platform is missing?
* PSM-SSH Connection Component
* UnixPrompts.ini
* UnixProcess.ini
* PSM-RDP Connection Component

NEW QUESTION 31

You are creating a Dual Control workflow for a team’s safe.

Which safe permissions must you grant to the Approvers group?
* List accounts, Authorize account request
* Retrieve accounts, Access Safe without confirmation
* Retrieve accounts, Authorize account request
* List accounts, Unlock accounts

NEW QUESTION 32

Due to corporate storage constraints, you have been asked to disable session monitoring and recording for 500 testing accounts used for your lab environment.

How do you accomplish this?
* Master Policy>select Session Management>add Exceptions to the platform(s)>disable Session Monitoring and Recording policies
* Administration>Platform Management>select the platform(s)>disable Session Monitoring and Recording Most Voted
* Polices>Access Control (Safes)>select the safe(s)>disable Session Monitoring and Recording policies
* Administration>Configuration Options>Options>select Privilege Session Management>disable Session Monitoring and Recording policies

Explanation

To disable session monitoring and recording for a large number of accounts due to storage constraints, you would navigate to the Administration section of the CyberArk Privileged Access Security (PAS) solution, specifically to the Configuration Options. From there, you would select the Privilege Session Management (PSM) options and disable the Session Monitoring and Recording policies. This action would apply the changes to the specified accounts, thus disabling the session monitoring and recording features for them1.

References: The answer is based on general knowledge of CyberArk PAS and best practices for managing session policies within the system. For specific steps and detailed procedures, please refer to the official CyberArk Defender PAM course materials and documentation

NEW QUESTION 33

Which master policy settings ensure non-repudiation?
* Require password verification every X days and enforce one-time password access.
* Enforce check-in/check-out exclusive access and enforce one-time password access.
* Allow EPV transparent connections (‘Click to connect’) and enforce check-in/check-out exclusive access.
* Allow EPV transparent connections (‘Click to connect’) and enforce one-time password access.

Explanation

Non-repudiation in the context of CyberArk Master Policy settings refers to the assurance that a user cannot deny the validity of their actions. The settings that ensure non-repudiation are those that enforce accountability and traceability of actions. Enforcing check-in/check-out exclusive access ensures that only one user can access an account at a time, and their actions can be traced back to themEnforcing one-time password access means that passwords are used only once and then changed, which prevents the reuse of credentials and ties actions to specific instances of access12.

References:

* CyberArk Docs: Master Policy Rules2

* CyberArk Docs: The Master Policy1

NEW QUESTION 34

Which change could CyberArk make to the REST API that could cause existing scripts to fail?
* adding optional parameters in the request
* adding additional REST methods
* removing parameters
* returning additional values in the response

NEW QUESTION 35

Time of day or day of week restrictions on when password verifications can occur configured in

_____.
* The Master Policy
* The Platform settings
* The Safe settings
* The Account Details

NEW QUESTION 36

You are concerned about the Windows Domain password changes occurring during business hours.

Which settings must be updated to ensure passwords are only rotated outside of business hours?
* In the platform policy –

Automatic Password Management > Password Change > ToHour & FromHour
* in the Master Policy

Account Change Window > ToHour & From Hour
* Administration Settings –

CPM Settings > ToHour & FromHour
* On each individual account –

Edit > Advanced > ToHour & FromHour

NEW QUESTION 37

When running a “Privileged Accounts Inventory” Report through the Reports page in PVWA on a specific safe, which permission/s are required on that safe to show complete account inventory information?
* List Accounts, View Safe Members
* Manage Safe Owners
* List Accounts, Access Safe without confirmation
* Manage Safe, View Audit

NEW QUESTION 38

A logon account can be specified in the platform settings.
* True
* False
Explanation

A logon account can be specified in the platform settings of CyberArk, a security software that manages privileged accounts and credentials. According to the CyberArk documentation1, “In the Account Details window, in the CPM pane, in the accounts section, you can associate either a logon account or a reconciliation account. If a default logon account has been configured for the platform that manages this account, that account is listed. You can associate another logon account or leave the default account as it is.”1 A logon account is an account that is used to log on to a target system and perform password management operations on other accounts. A reconciliation account is an account that is used to restore access to a target system when the logon account fails.

NEW QUESTION 39

Which statement is true about setting the reconcile account at the platform level?
* This is the only way to enable automatic reconciliation of account passwords.
* CPM performance will be improved when the reconcile account is set at the platform level.
* A rule can be used to specify the reconcile account dynamically or a specific reconcile account can be selected.
* This configuration prevents the association from becoming broken if the reconcile account is moved to a different safe.

NEW QUESTION 40

By default, members of which built-in groups will be able to view and configure Automatic Remediation and Session Analysis and Response in the PVWA?
* Vault Admins
* Security Admins
* Security Operators
* Auditors

NEW QUESTION 41

What is required to manage loosely connected devices?
* PSM for SSH
* EPM
* PSM
* PTA

NEW QUESTION 42

In PVWA, you are attempting to play a recording made of a session by user jsmith, but there is no option to “Fast Forward” within the video. It plays and only allows you to skip between commands instead. You are also unable to download the video.

What could be the cause?
* Recording is of a PSM for SSH session.
* The browser you are using is out of date and needs an update to be supported.
* You do not have the “View Audit” permission on the safe where the account is stored.
* You need to update the recorder settings in the platform to enable screen capture every 10000 ms or less.

CyberArk PAM-DEF (CyberArk Defender - PAM) Certification Exam is a certification program designed by CyberArk for professionals in the field of cybersecurity. CyberArk Defender - PAM certification is designed to validate the skills and knowledge of professionals who are responsible for securing privileged accounts and preventing cyber attacks on these accounts. The CyberArk PAM-DEF certification exam is designed to assess the proficiency of professionals in the use of CyberArk's privileged access management (PAM) solutions.

CyberArk Defender ? PAM Certification Exam is a rigorous exam that requires candidates to demonstrate their understanding of CyberArk's PAM solutions and their ability to apply that knowledge in real-world scenarios. PAM-DEF exam consists of 50 multiple-choice questions that must be answered in 90 minutes. Candidates must score at least 70% to pass the exam and earn the CyberArk Defender ? PAM Certification.

Get Ready with PAM-DEF Exam Dumps: https://www.dumpsmaterials.com/PAM-DEF-real-torrent.html]