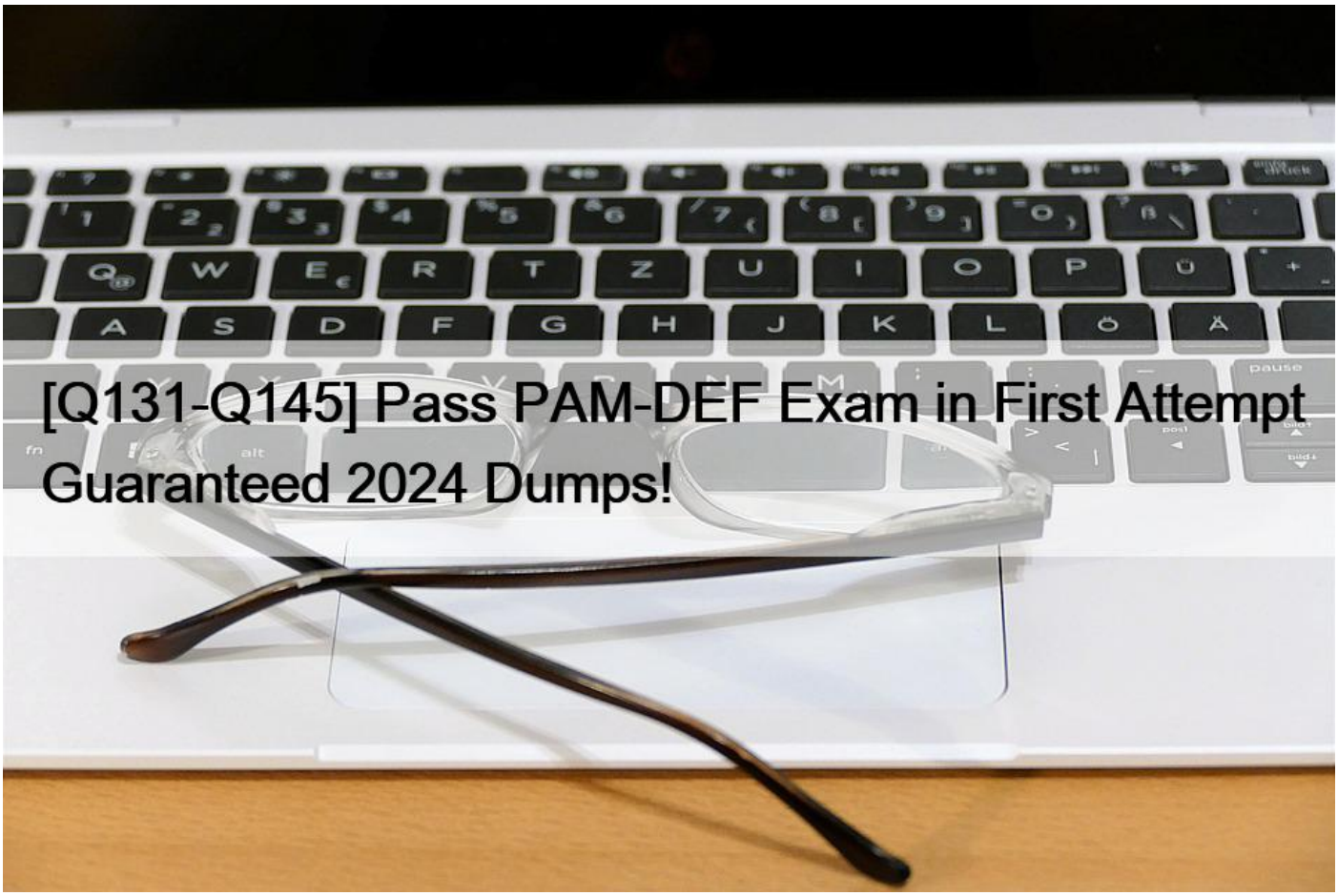
[Q131-Q145 Pass PAM-DEF Exam in First Attempt Guaranteed 2024 Dumps!



Pass PAM-DEF Exam in First Attempt Guaranteed 2024 Dumps!
PAM-DEF Dumps Full Questions - Exam Study Guide

NO.131 You need to enable the PSM for all platforms.

Where do you perform this task?
* Platform Management > (Platform) > UI & Workflows
* Master Policy > Session Management
* Master Policy > Privileged Access Workflows
* Administration > Options > Connection Components

Explanation

To enable PSM for specific platforms, you need to go to Platform Management, select the platform you want to configure, click Edit, expand UI & Workflows, and select Privileged Session Management. There you can customize the PSM settings for that platform, such as the PSM server ID, the connection components, the PSM connection method, and the PSM recording options. You can also disable dual control for PSM connections if needed. References: Configure PSM for Specific Platforms

NO.132 One can create exceptions to the Master Policy based on _____.

* Safes
* Platforms
* Policies
* Accounts

NO.133 Which dependent accounts does the CPM support out-of-the-box? (Choose three.)
* Solaris Configuration file
* Windows Services
* Windows Scheduled
* Windows DCOM Applications
* Windows Registry
* Key Tab file

NO.134 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.135 user has successfully conducted a short PSM session and logged off. However, the user cannot access the Monitoring tab to view the recordings.

What is the issue?
* The user must login as PSMAdminConnect
* The PSM service is not running
* The user is not a member of the PVWAMonitor group
* The user is not a member of the Auditors group

NO.136 When creating an onboarding rule, it will be executed upon .
* Both “All accounts in the pending accounts list” and “Any future accounts discovered by a discovery process”
* Any future accounts discovered by a discovery process
* All accounts in the pending accounts list

NO.137 Which parameters can be used to harden the Credential Files (CredFiles) while using CreateCredFile Utility?

(Choose three.)
* Operating System Username
* Host IP Address
* Client Hostname
* Operating System Type (Linux/Windows/HP-UX)
* Vault IP Address
* Time Frame

Explanation

When using the CreateCredFile Utility to harden Credential Files (CredFiles), it is important to include parameters that enhance security. The Host IP Address, Client Hostname, and Vault IP Address are parameters that can be used to specify the environment in which the CredFile is valid, thereby restricting its use to specific machines or networks1. This helps prevent unauthorized access to the CredFile and ensures that it is only used in the intended context.

References:

* CyberArk’s official documentation on the CreateCredFile utility provides insights into the security mechanisms used to protect credential files, including the use of environmental key materials such as application-based, machine-based, and component-based materials1.

* For a deeper understanding of how to secure Credential Files and the use of the CreateCredFile Utility, refer to the CyberArk Defender PAM course materials and study guide2.

NO.138 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
Explanation

When onboarding multiple accounts from the Pending Accounts list, all the selected accounts must be associated with the same platform. This is necessary because the platform setting determines how the accounts will be managed within CyberArk, including the policies and behaviors that apply to those accounts.

If an account contains dependencies, those dependencies are automatically onboarded with the account. This ensures that all accounts and their dependencies are managed consistently and according to the correct policies1.

References:

* CyberArk’s official documentation on Onboarding Accounts and SSH Keys1.

NO.139 In a default CyberArk installation, which group must a user be a member of to view the “reports” page in PVWA?
* PVWAMonitor
* ReportUsers
* PVWAReports
* Operators
Explanation

In a default CyberArk installation, to view the “reports” page in the PVWA (Privileged Web Access), a user must be a member of the PVWAMonitor group1. This group is specified in the ManageReportsGroup parameter in the Reports section of the Web Access Options in the System Configuration page. Being a member of this group grants the user the necessary permissions to generate and view reports within the PVWA.

References:

* CyberArk’s official documentation on Reports in PVWA outlines the requirement for users to belong to the PVWAMonitor group to access the reports page and generate reports1.

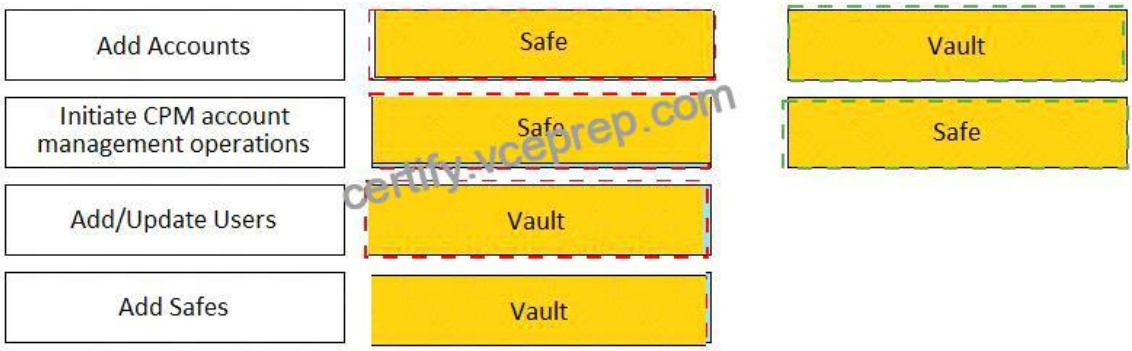
NO.140 Which statement is correct concerning accounts that are discovered, but cannot be added to the Vault by an automated onboarding rule?

* They are added to the Pending Accounts list and can be reviewed and manually uploaded.
* They cannot be onboarded to the Password Vault.
* They must be uploaded using third party tools.
* They are not part of the Discovery Process.

NO.141 Which permissions are needed for the Active Directory user required by the Windows Discovery process?

* Domain Admin
* LDAP Admin
* Read/Write
* Read

NO.142 Match each permission to where it can be found.



NO.143 To use PSM connections while in the PVWA, what are the minimum safe permissions a user or group will need?
* List Accounts, Use Accounts
* List Accounts, Use Accounts, Retrieve Accounts
* Use Accounts
* List Accounts, Use Accounts, Retrieve Accounts, Access Safe without confirmation

Explanation

To use PSM connections within the PVWA, a user or group needs to have permissions that allow them to list and use accounts, as well as retrieve account details. These permissions ensure that the user can view the accounts within a safe, initiate sessions using those accounts, and retrieve the necessary credentials for authentication during the session initiation process1.

References:

* CyberArk’s official documentation on Safe Settings and permissions required for each safe in CyberArk’s Enterprise Password Vault (EPV) components provides detailed information on the default safe configuration and permissions1.

* For more information on best practices for safe and safe member design, including the minimum permissions required for PSM connections, refer to CyberArk’s best practices articles and study guides

NO.144 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.145 How do you create a cold storage backup?
* On the DR Vault, install PAReplicate according to the Installation guide, configure the logon ini file, and define the Schedule tasks for full and incremental backups.
* Install the Vault Backup utility on a different machine from the Enterprise Password Vault server and trigger the full backup.
* Configure the backup options in the PVWA.
* On the DR Vault, configure the cold storage backup path in TSParm.ini file.

Explanation

To create a cold storage backup, you would install the PAReplicate utility on the DR Vault as per the installation guide. This utility is part of the CyberArk Vault’s backup solution and is used to export the encrypted contents of your Safes securely to a computer outside the Vault environment. After installation, you would configure the logon ini file with the necessary credentials and define the scheduled tasks for both full and incremental backups. This ensures that the Safes are regularly backed up and that the data is available for recovery if needed1.

References:

* CyberArk’s official documentation on using the CyberArk Backup Process, which includes details on the PAReplicate utility and how to configure it for cold storage backups1.

* Additional information on installing the Vault Backup Utility and configuring backup options, which

* provides context for the correct answer

CyberArk PAM-DEF Exam is essential for professionals who aspire to enhance their knowledge and experience in implementing and managing CyberArk PAM solutions. PAM-DEF examination serves as a standard measure of professional accomplishment and attests to a candidate's professional knowledge of CyberArk PAS solutions. Holding this certification demonstrates an individual's commitment to the field of cybersecurity and their mastery of privileged access security.

CyberArk Defender Free Certification Exam Material from VCEPrep with 240 Questions:
https://www.vceprep.com/PAM-DEF-latest-vce-prep.html]