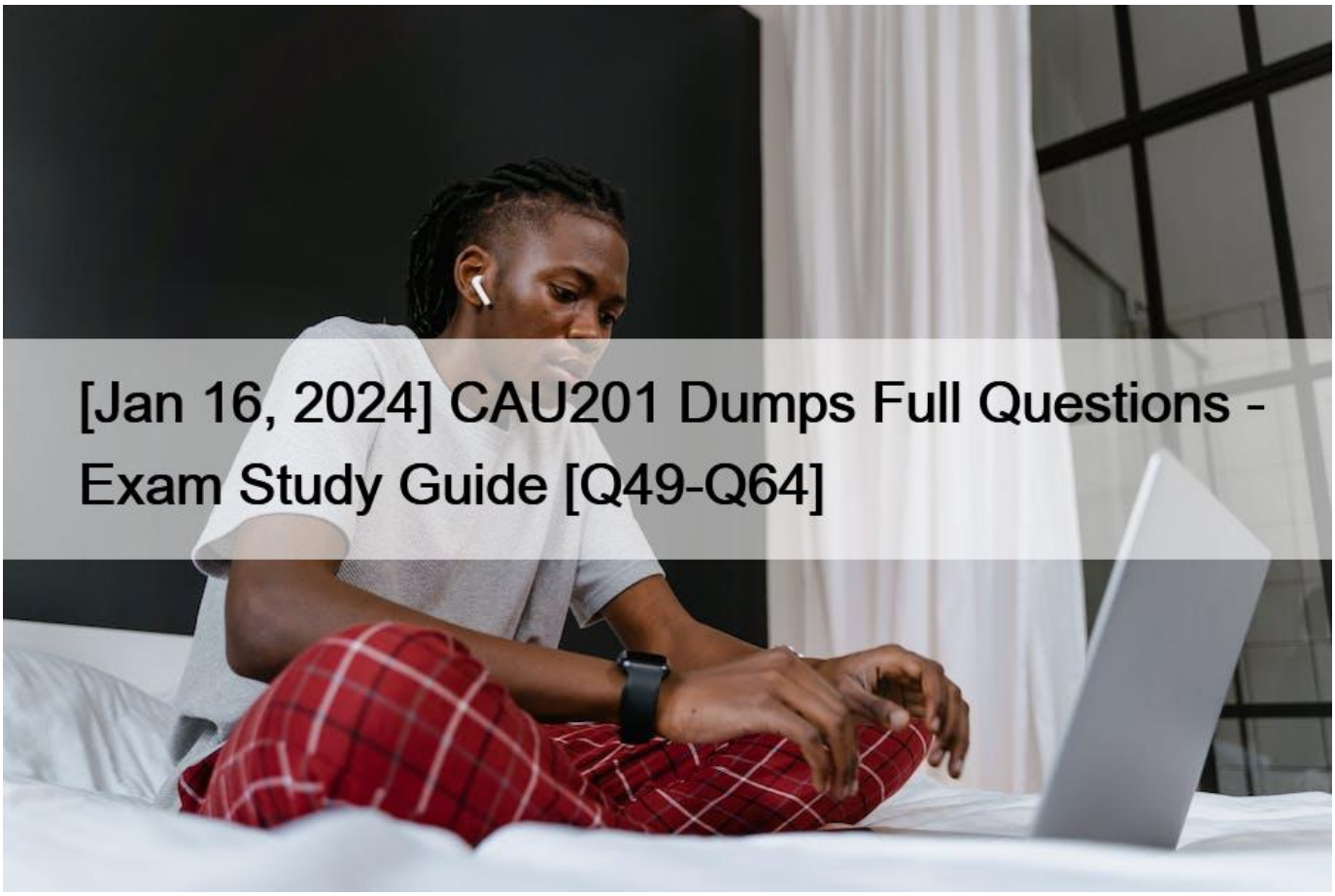
[Jan 16, 2024 CAU201 Dumps Full Questions - Exam Study Guide [Q49-Q64



[Jan 16, 2024] CAU201 Dumps Full Questions - Exam Study Guide
CyberArk Defender Free Certification Exam Material from Test4Engine with 179 Questions

Q49. The password upload utility must run from the CPM server
* TRUE
* FALSE
Explanation/Reference: https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Password-

Upload-Utility.htm

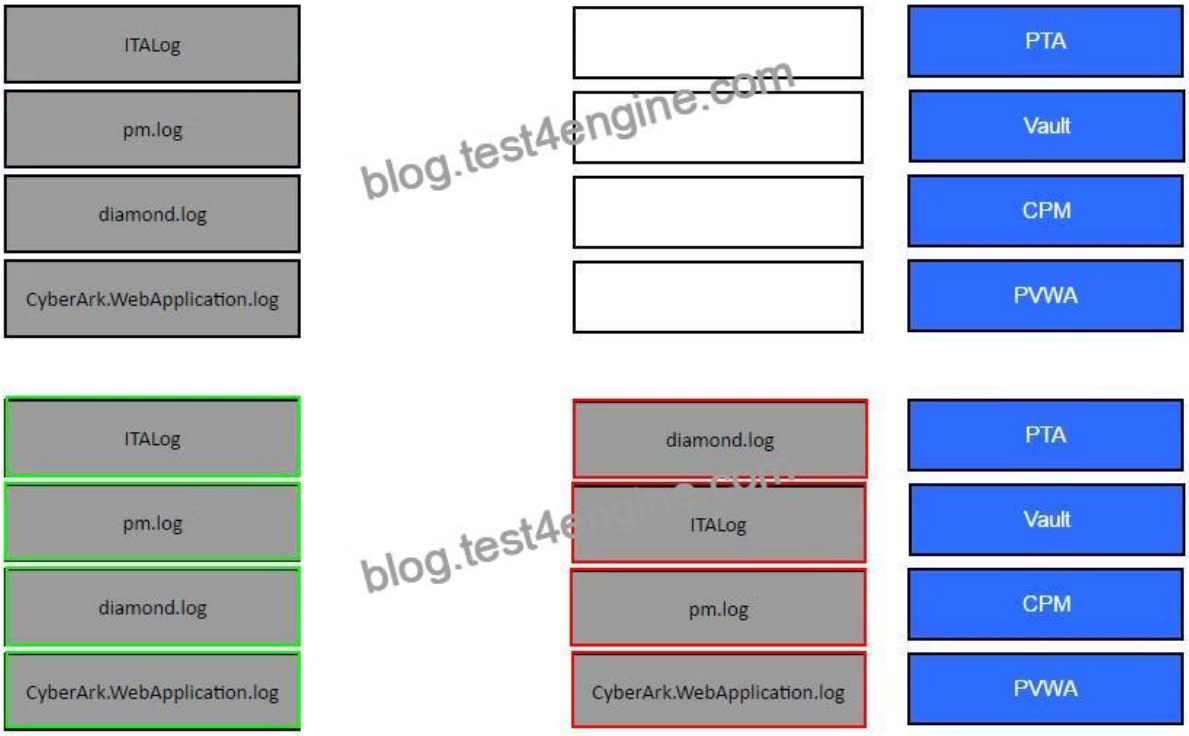
Q50. According to the DEFAULT Web Options settings, which group grants access to the REPORTS page?
* PVWAUsers
* Vault Admins
* Auditors
* PVWAMonitor

Q51. Can the ‘Connect’ button be used to initiate an SSH connection, as root, to a Unix system when SSH access for root is denied?

* Yes, when using the connect button, CyberArk uses the PMTerminal.exe process which bypasses the root SSH restriction.
* Yes, only if a logon account is associated with the root account and the user connects through the PSM- SSH connection component.
* Yes, if a logon account is associated with the root account.
* No, it is not possible.

Explanation/Reference: https://www.reddit.com/r/CyberARk/comments/7zx8w5/ssh_connection/

Q52. Match the log file name with the CyberArk Component that generates the log.



Q53. The primary purpose of exclusive accounts is to ensure non-repudiation (individual accountability).

* TRUE
* FALSE

Q54. You have associated a logon account to one your UNIX cool accounts in the vault. When attempting to

[b]change [/b] the root account’s password the CPM will….

* Log in to the system as root, then change root’s password
* Log in to the system as the logon account, then change roofs password
* Log in to the system as the logon account, run the su command to log in as root, and then change root’s password.
* None of these

Q55. Assuming a safe has been configured to be accessible during certain hours of the day, a Vault Admin may still access that safe outside of those hours.

* TRUE
* FALSE

Explanation/Reference: https://www.freshers360.com/wp-content/uploads/2019/05/Privileged-Account-Security-Implementation-Guide.pdf

Q56. As long as you are a member of the Vault Admins group, you can grant any permission on any safe that you have access to.
* TRUE
* FALS

Q57. Your organization has a requirement to allow users to “check out passwords” and connect to targets with the same account through the PSM.

What needs to be configured in the Master policy to ensure this will happen?
* Enforce check-in/check-out exclusive access = active; Require privileged session monitoring and isolation = active
* Enforce check-in/check-out exclusive access = inactive; Require privileged session monitoring and isolation = inactive
* Enforce check-in/check-out exclusive access = inactive; Record and save session activity = active
* Enforce check-in/check-out exclusive access = active; Record and save session activity = inactive

Q58. What is the name of the Platform parameters that controls how long a password will stay valid when One Time Passwords are enabled via the Master Policy?
* Min Validity Period
* Interval
* Immediate Interval
* Timeout

Min Validity Period -The number of minutes to wait from the last retrieval of the password until it is replaced. This gives the user a minimum period to be able to use the password before it is replaced. Use -1 to ignore this property. This parameter is also used to release exclusive accounts automatically Interval -” The number of minutes that the Central Policy Manager waits between running periodic searches for the platform. Note: It is recommended to leave the default value of 1440. If a change/verify policy has been configured, the Central Policy Manager will automatically align the periodic searches with the start of the defined timeframes.”

Q59. It is possible to restrict the time of day, or day of week that a reconcile process can occur.
* TRUE
* FALSE

Q60. A user is receiving the error message “ITATS006E Station is suspended for User jsmith” when attempting to sign into the Password Vault Web Access (PVWA). Which utility would a Vault administrator use to correct this problem?
* createcredfile.exe
* cavaultmanager.exe
* PrivateArk
* PVWA

Q61. PSM for Windows (previously known as “RDP Proxy”) supports connections to the following target systems
* Windows
* UNIX
* Oracle
* All of the above

Q62. 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

Q63. tsparm.ini is the main configuration file for the Vault.
* True
* False

Q64. A Simple Mail Transfer Protocol (SMTP) integration is critical for monitoring Vault activity and facilitating workflow processes, such as Dual Control.
* True
* False

Dumps Brief Outline Of The CAU201 Exam: https://www.test4engine.com/CAU201_exam-latest-braindumps.html]