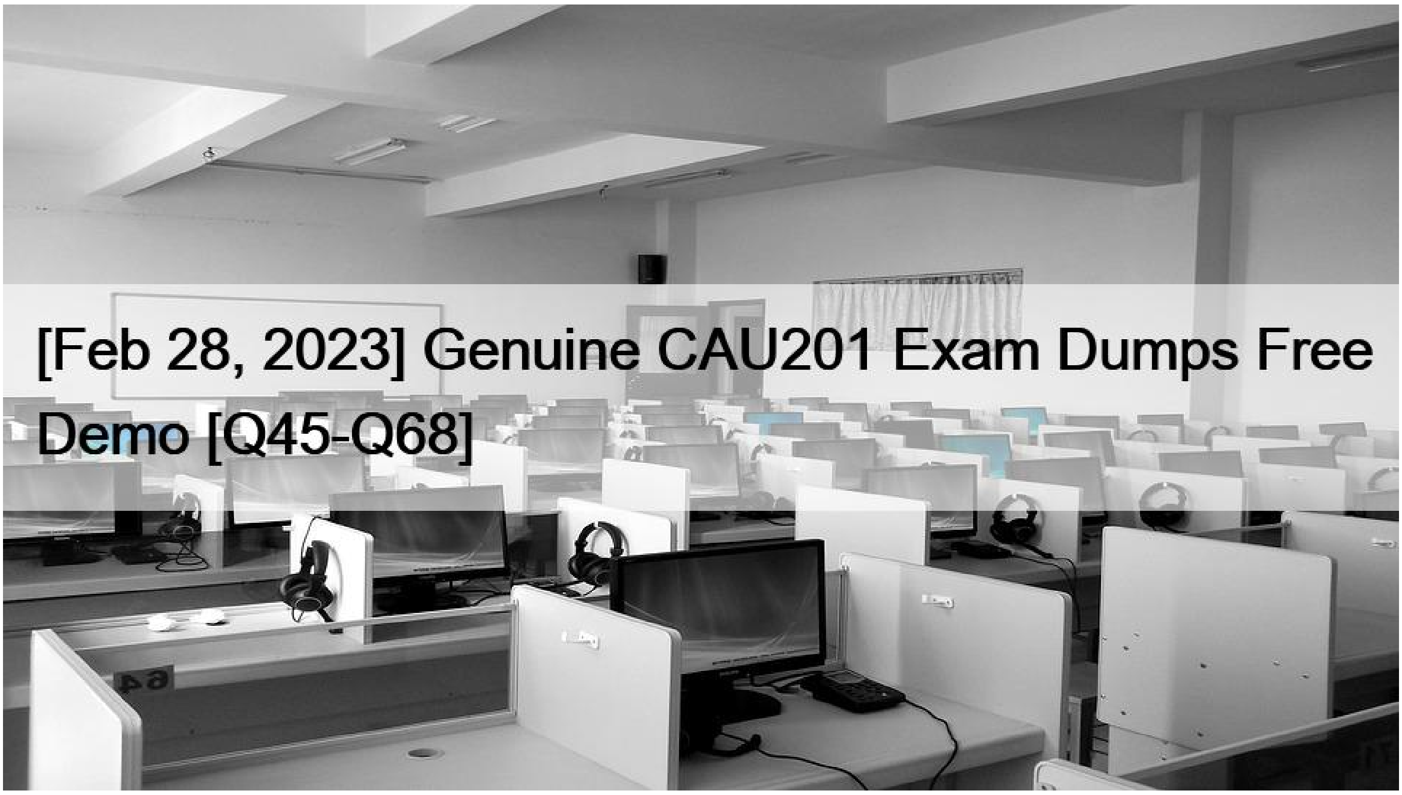
[Feb 28, 2023 Genuine CAU201 Exam Dumps Free Demo [Q45-Q68



[Feb 28, 2023 Genuine CAU201 Exam Dumps Free Demo Printable & Easy to Use CyberArk Defender CAU201 Dumps 100% Same Q&A In Your Real Exam NO.45 Which combination of Safe member permissions will allow end users to log in to a remote machine transparently but NOT show or copy the password?
- Use Accounts, Retrieve Accounts, List Accounts
- Use Accounts, List Accounts
- Use Accounts
- List Accounts, Retrieve Accounts

NO.46 dbparm.ini is the main configuration file for the Vault.
- True
- False

NO.47 Which one the following reports is NOT generated by using the PVWA?
- Accounts Inventory
- Application Inventory
- Sales List
- Convince Status

NO.48 When a DR Vault Server becomes an active vault, it will automatically fail back to the original state once the Primary Vault comes back online.
- True; this is the default behavior
- False; this is not possible

* True, if the AllowFailback setting is set to &#8220;yes&#8221; in the padr.ini file
* True, if the AllowFailback setting is set to &#8220;yes&#8221; in the dbparm.ini file

NO.49 You have associated a logon account to one your UNIX cool accounts in the vault. When attempting to [b]change [/b] the root account&#8217;s password the CPM will&#8230;..
* Log in to the system as root, then change root&#8217;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&#8217;s password.
* None of these

NO.50 What is the primary purpose of Dual Control?
* Reduced risk of credential theft
* More frequent password changes
* Non-repudiation (individual accountability)
* To force a &#8216;collusion to commit&#8217; fraud ensuring no single actor may use a password without authorization.
Explanation/Reference: https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Dual- Control.htm

NO.51 Which is the primary purpose of exclusive accounts?
* Reduced risk of credential theft
* More frequent password changes
* Non-repudiation (individual accountability)
* To force a &#8216;collusion to commit&#8217; fraud ensuring no single actor may use a password without authorization

NO.52 The Password upload utility can be used to create safes.
* TRUE
* FALS

NO.53 If a user is a member of more than one group that has authorizations on a safe, by default that user is granted________.
* the vault will not allow this situation to occur.
* only those permissions that exist on the group added to the safe first.
* only those permissions that exist in all groups to which the user belongs.
* the cumulative permissions of all groups to which that user belongs.

NO.54 You are onboarding 5,000 UNIX root accounts for rotation by the CPM. You discover that the CPM is unable to log in directly with the root account and will need to use a secondary account.

How should this be configured to allow for password management using least privilege?
* Configure each CPM to use the correct logon account.
* Configure each CPM to use the correct reconcile account.
* Configure the UNIX platform to use the correct logon account.
* Configure the UNIX platform to use the correct reconcile account.

NO.55 For an account attached to a platform that requires Dual Control based on a Master Policy exception, how would you configure a group of users to access a password without approval.
* Create an exception to the Master Policy to exclude the group from the workflow process.
* Edit the master policy rule and modify the advanced &#8216;Access safe without approval&#8217; rule to include the group.
* On the safe in which the account is stored grant the group the &#8216;Access safe without audit&#8217; authorization.
* On the safe in which the account is stored grant the group the &#8216;Access safe without confirmation&#8217; authorization.
Explanation/Reference:

Reference: https://www.reddit.com/r/CyberARk/comments/6270zr/dual_control_on_specific_accounts/

NO.56 All of your Unix root passwords are stored in the safe UnixRoot. Dual control is enabled for some of the accounts in that safe. The members of the AD group UnixAdmins need to be able to use the show, copy, and connect buttons on those passwords at any time without confirmation. The members of the AD group OperationsStaff need to be able to use the show, copy and connect buttons on those passwords on an emergency basis, but only with the approval of a member of OperationsManagers. The members of OperationsManagers never need to be able to use the show, copy or connect buttons themselves.

Which safe permissions do you need to grant to OperationsStaff? Check all that apply.
* Use Accounts
* Retrieve Accounts
* List Accounts
* Authorize Password Requests
* Access Safe without Authorization
Explanation/Reference:

NO.57 When on-boarding account using Accounts Feed, Which of the following is true?
* You must specify an existing Safe where are account will be stored whenitis on boarded to the Vault
* You can specify the name of a new sale that will be created where the account will be stored when it is on-boarded to the Vault.
* You can specify the name of a new Platform that will be created and associated with the account
* Any account that is on boarded can beautomaticallyreconciled regardless ofthe platformit isassociated with.

NO.58 The Password upload utility can be used to create safes.
* TRUE
* FALSE
Explanation/Reference:

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Password-Upload- Utility.htm

NO.59 An auditor needs to login to the PSM in order to live monitor an active session. Which user ID is used to establish the RDP connection to the PSM server?
* PSMConnect
* PSMMaster
* PSMGwUser
* PSMAdminConnect

NO.60 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

NO.61 When on-boarding account using Accounts Feed, which of the following is true?
* You must specify an existing Safe where the account will be stored when it is on-boarded to the Vault.
* You can specify the name of a new safe that will be created where the account will be stored when it is on- boarded to the Vault.
* You can specify the name of a new Platform that will be created and associated with the account.
* Any account that is on-boarded can be automatically reconciled regardless of the platform it is associated with.
Explanation/Reference: https://www.cyberark.com/resource/automating-privileged-account-onboarding/

NO.62 Which one of the following reports is NOT generated by using the PVWA?
* Account Inventory
* Application Inventory

* Safes List
* Compliance Status

Explanation/Reference: https://techinsight.com.vn/language/en/privileged-account-security-solution-part-2/

NO.63 Secure Connect provides the following. Choose all that apply.

* PSM connections to target devices that are not managed by CyberArk.
* Session Recording
* Real-time live session monitoring.
* PSM connections from a terminal without the need to login to the PVWA

NO.64 Which of the following PTA detections are included in the Core PAS offering?

* Suspected Credential Theft
* Over-Pass-The Hash
* Golden Ticket
* Unmanaged Privileged Access

Explanation/Reference: https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PTA/What-Does-PTA-

Detect.htm

NO.65 In your organization the &#8220;click to connect&#8221; button is not active by default.

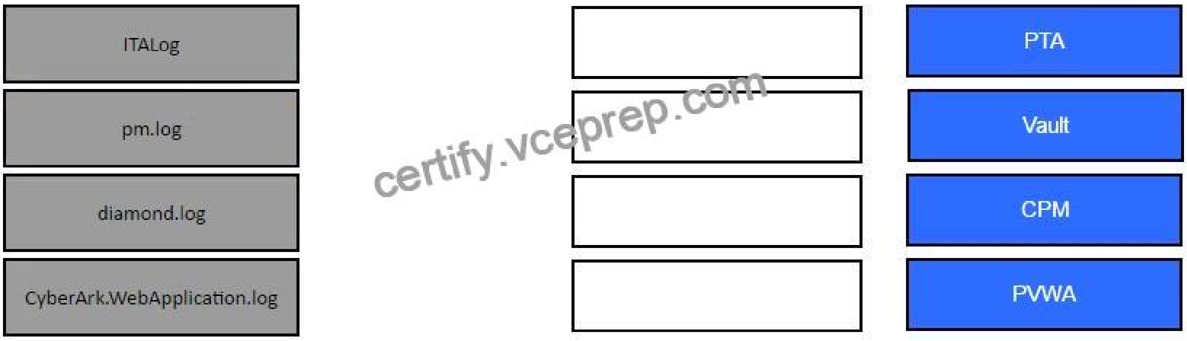
How can this feature be activated?

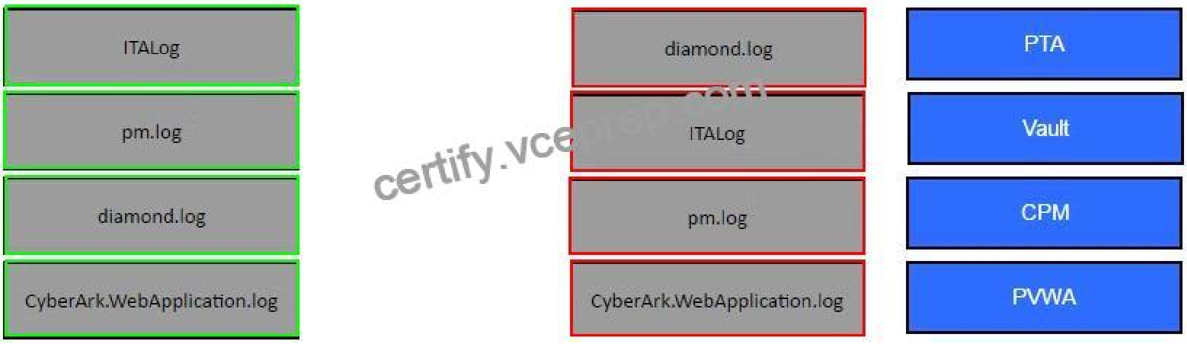
* Policies > Master Policy > Allow EPV transparent connections > Inactive
* Policies > Master Policy > Session Management > Require privileged session monitoring and isolation > Add Exception
* Policies > Master Policy > Allow EPV transparent connections > Active
* Policies > Master Policy > Password Management

NO.66 Which report provides a list of account stored in the vault.

* Privileged Accounts Inventory
* Privileged Accounts Compliance Status
* Entitlement Report
* Active Log

NO.67 Match the log file name with the CyberArk Component that generates the log.





NO.68 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

Explanation/Reference: https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PTA/Security-Configuration.htm

CAU201 Practice Test Give You First Time Success with 100% Money Back Guarantee!: https://www.vceprep.com/CAU201-latest-vce-prep.html]