New CAU302 Test Materials & Valid CAU302 Test Engine [Q15-Q37
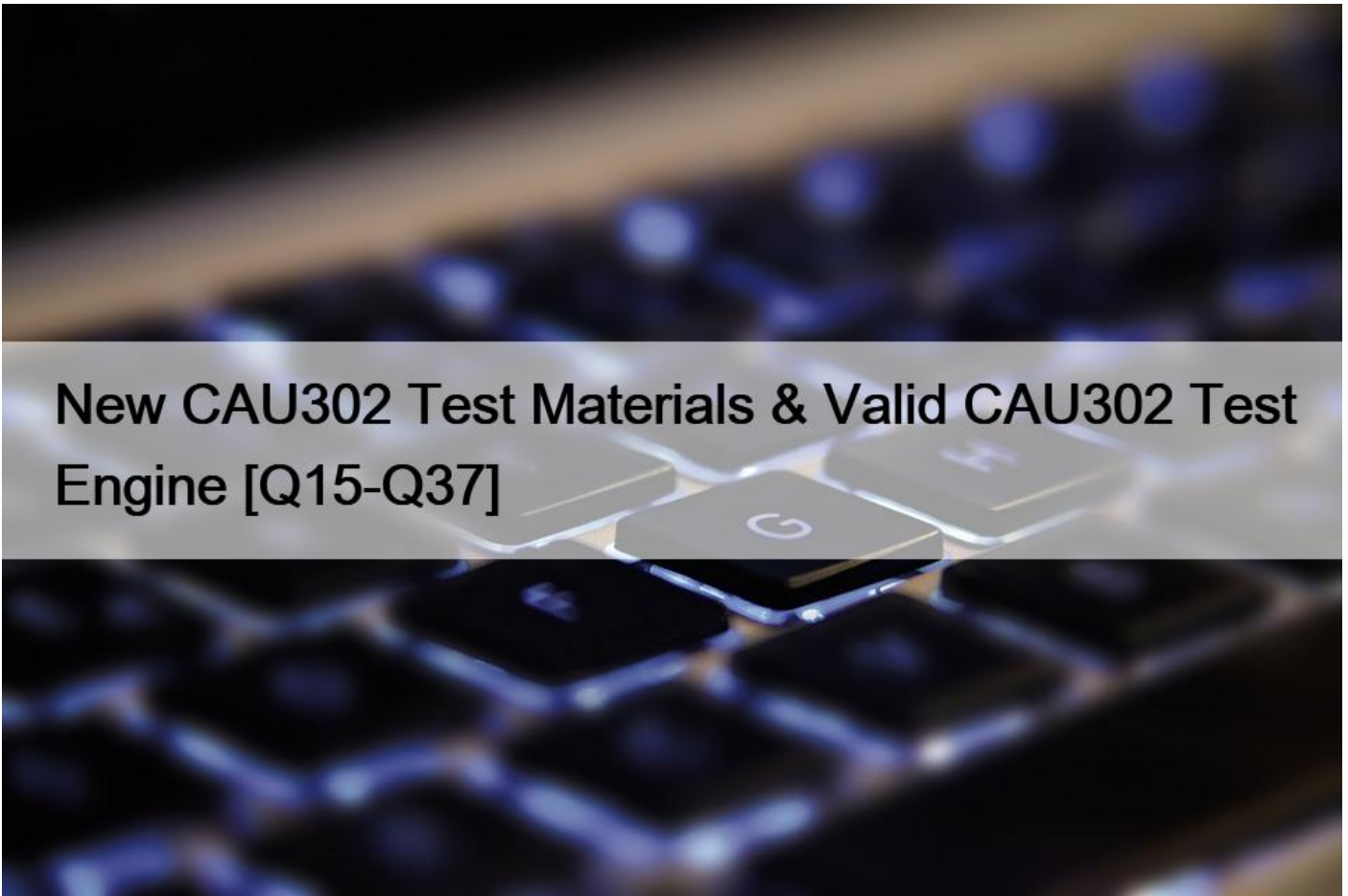

New CAU302 Test Materials & Valid CAU302 Test Engine
CAU302 Updated Exam Dumps [2022] Practice Valid Exam Dumps Question

QUESTION 15

Which user is automatically given all Safe authorizations on all Safes?
* Administrator
* Master
* Auditor
* Operator

QUESTION 16

PSM for Windows (previously known as “RDP Proxy”) supports connections to the following target systems:

_____ .

* Windows
* UNIX

* Oracle
* All of the above
Explanation/Reference:

QUESTION 17

In accordance with best practice, SSH access is denied for root accounts on UNIX/LINUX systems. 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.
Explanation

QUESTION 18

During the process of installing the Central Policy Manager (CPM), the Vault administrator will be asked to provide the credentials for an administrative user in the Vault. For which purpose are these credentials used?
* The credentials will be used later by the CPM to retrieve passwords from the Vault.
* The credentials are used by the installer to register the CPM in the CyberArk database.
* The credentials are used by the installer to authenticate to the Vault and create the Central Policy Manager (CPM) environment (Safes, users, etc.).
* The credentials will be used later by the CPM to update passwords in the Vault.

QUESTION 19

What is the purpose of a password group?
* 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 CPM to a target system
* To allow more than one account to work together as part of a password management process

QUESTION 20

Ad-Hoc Access (formerly Secure Connect) provides the following features. (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

QUESTION 21

When a group is granted the ‘Authorize Account Requests’ permission on a safe Dual Control requests must be approved by:
* Any one person from that group
* Every person from that group
* The number of persons specified by the Master Policy
* That access cannot be granted to groups

QUESTION 22

A Reconcile Account can be specified in the Master Policy.
* TRUE
* FALSE

QUESTION 23

The Password upload utility can be used to create safes.
* TRUE
* FALSE

QUESTION 24

What is the maximum number of levels of authorizations you can set up in Dual Control?
* 1
* 2
* 3
* 4

QUESTION 25

If a transparent user belongs two different directory mappings, how does the system determine which user template to use?
* The system will use the template for the mapping listed first.
* The system will use the template for the mapping listed last.
* The system will grant all of the vault authorizations from the two templates.
* The system will grant only the vault authorizations that are listed in both templates.

QUESTION 26

Multiple PVWA servers are always all active.
* TRUE
* FALSE

QUESTION 27

In Accounts Discovery, you can configure a Windows discovery to scan_____.
* as many OUs as you wish
* up to three OUs.
* only one OU.
* a number of OUs determined by the OUstoScan setting under the Accounts Feed section in the Administration tab

QUESTION 28

An SNMP integration allows you to forward audit records from the vault to the SIEM.
* TRUE
* FALSE

QUESTION 29

The Vault needs to send Simple Network Management Protocol (SNMP) traps to an SNMP solution. In which configuration file do you set the IP address of the SNMP solution?

* PARAgent.ini
* dbparm.ini
* ENEConf.ini
* my.ini

Explanation

QUESTION 30

When managing SSH keys. CPM automatically pushes the Public Key to the target system.

* TRUE
* FALSE

QUESTION 31

Which keys are required to be present in order to start the PrivateArk Server Service?

* Server Key
* Recovery Public Key
* Recovery Private Key
* Safe Key

QUESTION 32

SAFE Authorizations may be granted to_____.

Select all that apply.

* Vault Users
* Vault Groups
* LDAP Users
* LDAP Groups

QUESTION 33

Which file does the Vault administrator need to edit in order to configure the integration of the Vault with the radius server?

* radius.ini
* PARagent.ini
* ENEConf.ini
* dbparm.ini

QUESTION 34

A Vault Administrator wants to change the PSM Server ID to comply with a naming standard What is the processfor changing the PSM Server ID?

* First, logon to the PrivateArk Client as Administrator and open the PVWAConfig safe. Retrieve and edit the PVConfiguration.xml file. Search for the PSMServer Name and update the ID of the server you want to rename Save the file and copy back to the PVWAConfig safe. Restart the “CyberArk Privileged Session Manager” service on the PSM server.
* Login to the PVWA. then change the PSMServer ID in Administration. System Configuration. Options, Privileged Session Management. Configured PSM Servers Run an IISRESET on all PVWA servers.

* First, login to the PVWA. browse to Administration. System Configuration. Options. Pnvileged Session Management. Configured PSM Servers and select the PSM Server you need to change from the list of servers In the properties pane, set the value of the ID property to the new Server ID. click Apply and OK. Next, edit the basic_psm.ini file located on the PSM server in the PSM root directory and update the PSMServerlD parameter with the new Server ID. save the file and restart the “CyberArk Privileged Session Manager” service on the PSM server
* Options A and B above is the correct procedure

QUESTION 35

PTA can automatically suspend sessions in case of suspicious activities detected in a privileged session, only if the session is made via the CyberArk PSM.
* True
* False, the PTA can suspend sessions whether the session is made via the PSM or not

QUESTION 36

What is the primary purpose of One Time Passwords?
* 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

QUESTION 37

CyberArk Logical Container
* CPMlog
* CPM_error.log
* pm.log
* pm.errors.log

CAU302 Sample with Accurate & Updated Questions: https://www.validbraindumps.com/CAU302-exam-prep.html]