Free Questions for PAM-CDE-RECERT

Shared by Mcbride on 16-04-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which user(s) can access all passwords in the Vault?

Options:

A- Administrator
B- Any member of Vault administrators
C- Any member of auditors
D- Master

Answer:

D

Question 2

Question Type: MultipleChoice

Which option best PTA detections require the deployment of a Network Sensor or installing the PTA Agent on the domain controller?

Options:

A- Suspected credential theft
B- Over-Pass-The-Hash
C- Golden Ticket
D- Unmanaged privileged access

Answer:

C

Question 3

Question Type: MultipleChoice

To enable the Automatic response ''Add to Pending'' within PTA when unmanaged credentials are

found, what are the minimum permissions required by PTAUser for the PasswordManager_pending safe?

Options:

A- List Accounts, View Safe members, Add accounts (includes update properties), Update Account content, Update Account properties
B- List Accounts, Add accounts (includes update properties), Delete Accounts, Manage Safe
C- Add accounts (includes update properties), Update Account content, Update Account properties, View Audit
D- View Accounts, Update Account content, Update Account properties, Access Safe without confirmation, Manage Safe, View Audit

Answer:

A

Question 4

Question Type: MultipleChoice

For Digital Vault Cluster in a high availability configuration, how does the cluster determine if a node is down?

Options:

A- The heartbeat s no longer detected on the private network.
B- The shared storage array is offline.
C- An alert is generated in the Windows Event log.
D- The Digital Vault Cluster does not detect a node failure.

Answer:

A

Question 5

Question Type: MultipleChoice

In a rule using ''Privileged Session Analysis and Response'' in PTA, which session options are

available to configure as responses to activities?

Options:

A- Suspend, Terminate, None
B- Suspend, Terminate, Lock Account
C- Pause, Terminate, None
D- Suspend, Terminate

Answer:

D

Question 6

Question Type: MultipleChoice

Based on the DEFAULT Web Options settings, which group grants access to the REPORTS page?

Options:

A- PVWAUsers
B- Vault Admins
C- Auditors
D- PVWAMonitor

Answer:

D

Question 7

Question Type: MultipleChoice

If a user is a member of more than one group that has authorizations on a safe, by default that user is granted_____.

Options:

A- the vault will not allow this situation to occur.
B- only those permissions that exist on the group added to the safe first.
C- only those permissions that exist in all groups to which the user belongs.
D- the cumulative permissions of all groups to which that user belongs.

Answer:

B

Question 8

Question Type: MultipleChoice

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.

Options:

A- TRUE
B- FALSE

Answer:

B

Question 9

Question Type: MultipleChoice

Which item is an option for PSM recording customization?

Options:

A- Windows events text recorder with automatic play-back
B- Windows events text recorder and universal keystrokes recording simultaneously
C- Universal keystrokes text recorder with windows events text recorder disabled
D- Custom audio recording for windows events

Answer:

B

Question 10

Question Type: MultipleChoice

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?

Options:

A- PSMConnect
B- PSMMaster
C- PSMGwUser
D- PSMAdminConnect

Answer:

D

Question 11

Question Type: MultipleChoice

What is a prerequisite step betore CyberArk can be configured to support RADIUS authentication?

Options:

A- Log on to the PrivateArk Client display the User properties to the user to configure, run the Authentication method dropdown list and select Radius authentication.
B- In the RADIUS server define the CyberArk Vault as a RADIUS client/agent
C- In the Vault installation folder, run CAVaultManager as administrator with the SecureSecretFiles command
D- Navigate to /Server/Conf and open DBParm mi and set the RadiusServerslnfo parameter

Answer:

B