We offer free update service for one year!
https://www.certqueen.com

**Exam** : **PAM-DEF-SEN**

**Title** : CyberArk Defender – PAM & Sentry – PAM

**Version** : DEMO

1.If a user is a member of more than one group that has authorizations on a safe, by default that user is granted_____.
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:** D
**Explanation:**
When a user is a member of more than one group that has authorizations on a safe, by default that user is granted the cumulative permissions of all groups to which that user belongs. This means that the user will have the highest level of access that any of the groups have on the safe. For example, if one group has View and Retrieve permissions, and another group has Add and Delete permissions, the user will have View, Retrieve, Add, and Delete permissions on the safe. This is the default behavior of the vault, unless the Exclusive option is enabled on the safe. The Exclusive option restricts the user's permissions to only those of the group added to the safe first.
Reference: [Defender PAM eLearning Course], Module 3: Safes and Permissions, Lesson 3.2: Safe Permissions, Slide 8: Cumulative Permissions
[Defender PAM Sample Items Study Guide], Question 1: Safe Permissions
[CyberArk Documentation Portal], CyberArk Privileged Access Security Implementation Guide, Chapter 3: Managing Safes, Section: Safe Properties, Subsection: Exclusive

2.It is possible to control the hours of the day during which a user may log into the vault.
A. TRUE
B. FALSE
**Answer:** A
**Explanation:**
It is possible to control the hours of the day during which a user may log into the vault by using the Time Restrictions feature. This feature allows administrators to define the days and times that users can access the vault. Users who try to log in outside the permitted hours will be denied access and receive a message informing them of the restriction. Time restrictions can be applied to individual users or groups of users.
Reference: [Defender PAM eLearning Course], Module 3: Safes and Permissions, Lesson 3.3: User Management,
Slide 7: Time Restrictions
[Defender PAM Sample Items Study Guide], Question 2: Time Restrictions
[CyberArk Documentation Portal], CyberArk Privileged Access Security Implementation Guide, Chapter 4: Managing Users and Groups, Section: Time Restrictions

3.VAULT authorizations may be granted to_____.
A. Vault Users
B. Vault Groups
C. LDAP Users
D. LDAP Groups
**Answer:** AC

**Explanation:**
Vault Authorizations
• Can be assigned only to users (not groups).
• Cannot be inherited via group membership.
• Defined only via the Private Ark Client. Safe Auth
• Assigned to users and/or groups.
• Can be inherited via group membership.
• Can be defined in the Private Ark Client or PVWA

4.What is the purpose of the Interval setting in a CPM policy?
A. To control how often the CPM looks for System Initiated CPM work.
B. To control how often the CPM looks for User Initiated CPM work.
C. To control how long the CPM rests between password changes.
D. To control the maximum amount of time the CPM will wait for a password change to complete.
**Answer:** A
**Explanation:**
The Interval setting in a CPM policy is used to control how often the CPM looks for System Initiated CPM work, such as password changes, verifications, and reconciliations. The Interval setting defines the frequency, in minutes, that the CPM will check the accounts that are associated with the policy and perform the required actions. For example, if the Interval is set to 60, the CPM will check the accounts every hour and change, verify, or reconcile the passwords according to the policy settings. The Interval setting does not affect User Initiated CPM work, such as manual password changes or retrievals, which are performed immediately upon request. The Interval setting also does not control how long the CPM rests between password changes or the maximum amount of time the CPM will wait for a password change to complete. These parameters are configured in the CPM.ini file, which is stored in the root folder of the <CPM username> Safe.
Reference: [Defender PAM eLearning Course], Module 5: Password Management, Lesson 5.1: CPM Policies, Slide
9: CPM Policy Settings
[Defender PAM Sample Items Study Guide], Question 4: CPM Policy Settings
[CyberArk Documentation Portal], CyberArk Privileged Access Security Implementation Guide, Chapter 5: Managing Passwords, Section: CPM Policy Settings, Subsection: Interval

5.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 Operations Staff 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 Operations Managers never need to be able to use the show, copy or connect buttons themselves.
Which safe permission do you need to grant Operations Staff? Check all that apply.
A. Use Accounts
B. Retrieve Accounts
C. Authorize Password Requests
D. Access Safe without Authorization

**Answer:** A, B

**Explanation:**

To use the show, copy, and connect buttons on the accounts in the safe UnixRoot, the Operations Staff need to have the Use Accounts permission, which allows them to request access to the accounts and perform actions on them. However, since dual control is enabled for some of the accounts, they also need to have the Retrieve Accounts permission, which allows them to view the password of the account after it is authorized by another user. The Authorize Password

Requests permission is not needed, as it is only required for the users who can approve the requests, not the ones who make them. The Access Safe without Authorization permission is not needed, as it would bypass the dual control mechanism and allow the Operations Staff to access the accounts without approval.

Reference: [Defender PAM Sample Items Study Guide], page 10, question 5

[CyberArk Privileged Access Security Implementation Guide], page 30, table 2-1 [CyberArk Privileged Access Security Administration Guide], page 43, section 3.2.2.1