# CyberArk PAM-DEF Practice Questions

**Shared by Keller on 21-08-2026**

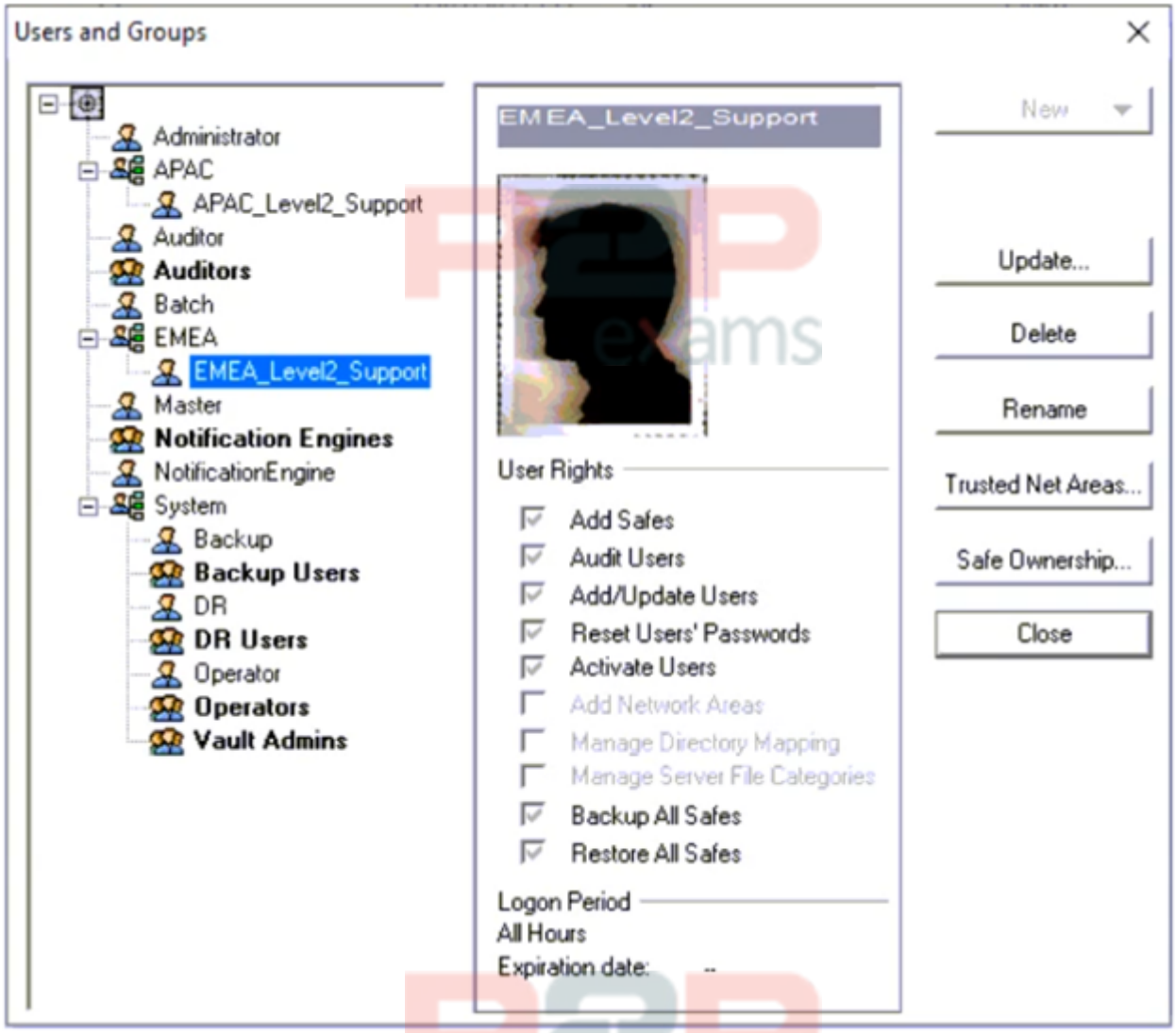
**For More Free Questions and Preparation Resources**

Check the Links on Last Page

## Question 1

Question Type: MultipleChoice

Refer to the exhibit.




Why is user "EMEALevel2Support" unable to change the password for user "Operator"?

## Options:

A- EMEALevel2Support's hierarchy level is not the same or higher than Operator.
B- EMEALevel2Support does not have the 'Manage Directory Mapping' role.
C- Operator can only be reset by the Master user.
D- EMEALevel2Support does not have rights to reset passwords for other users.

## Answer:

D

## Explanation:

The image description indicates that ''EMEALevel2Support'' has the following rights: Add/Update Users, Manage Server File Categories, Manage Directory Mapping, Backup All Files, Restore All Files. Since there is no mention of the right to reset passwords for other users, this suggests that ''EMEALevel2Support'' lacks the necessary permission to change the password for ''Operator''.

# Question 2

Question Type: MultipleChoice

Which statement is correct concerning accounts that are discovered, but cannot be added to the Vault by an automated onboarding rule?

## Options:

A- They are added to the Pending Accounts list and can be reviewed and manually uploaded.
B- They cannot be onboarded to the Password Vault.
C- They must be uploaded using third party tools.
D- They are not part of the Discovery Process.

## Answer:

A

## Explanation:

When accounts are discovered by CyberArk but do not match any automated onboarding rule, they are added to thePending Accounts list. This allows administrators to review these accounts and decide whether to onboard them manually into the Vault.The Pending Accounts list serves as a holding area for accounts that require further review or do not meet the criteria set by existing onboarding rules1.

CyberArk's official documentation on Onboarding Rules, which explains the process of managing accounts that are discovered but not automatically onboarded1.

## Question 3

Question Type: MultipleChoice

You have been asked to turn off the time access restrictions for a safe.

Where is this setting found?

### Options:

A- PrivateArk
B- RestAPI
C- Password Vault Web Access (PVWA)
D- Vault

### Answer:

A

### Explanation:

The time access restrictions for a safe are configured in the PrivateArk Administrative Client, which is a graphical user interface that allows users to manage safes and their properties. The time access restrictions are set in theTime Access Restrictionstab of the Safe properties window. This tab enables users to specify the days and hours when the safe can be accessed. If the time access restrictions are turned off, the safe can be accessed at any time.Reference:PrivateArk Safe management,Advanced Safe Management

## Question 4

Question Type: MultipleChoice

Which type of automatic remediation can be performed by the PTA in case of a suspected credential theft security event?

### Options:

A- Password change
B- Password reconciliation
C- Session suspension

D- Session termination

## Answer:

A

## Explanation:

The PTA can perform automatic password change as a type of remediation in case of a suspected credential theft security event.According to the CyberArk documentation1, 'Rotate credentials - for OverPass the Hash attack and Suspected credentials theft events.'1This means that the PTA can initiate a password change request to the CPM for the affected account, which will generate a new random password and update it on the target system and the Vault. This way, the PTA can prevent the attacker from using the stolen credentials to access the target system or launch further attacks.Reference:

Configure PTA Remediations - CyberArk, section ''Remediation Initiation''

# Question 5

Question Type: MultipleChoice

SAFE Authorizations may be granted to_____.

Choose all that apply.

## Options:

A- Vault Users
B- Vault Group
C- LDAP Users
D- LDAP Groups

## Answer:

A, B, C, D

## Explanation:

SAFE Authorizations may be granted to Vault Users, Vault Groups, LDAP Users, and LDAP Groups. These are the four types of users that can be defined in the Vault and assigned

permissions to access Safes and manage passwords. Vault Users and Vault Groups are created and managed within the Vault, while LDAP Users and LDAP Groups are imported from an external directory service such as Active Directory.Reference:

Defender PAM Course, Module 4: Managing Safes, Lesson 4.2: Safe Authorizations, slide 4

Defender PAM Sample Items Study Guide, Question 39, page 15

CyberArk Privileged Access Security Documentation, Vault Administration Guide, Chapter 4: Managing Safes, Section: Safe Authorizations, page 4-12

## Question 6

Question Type: MultipleChoice

In a default CyberArk installation, which group must a user be a member of to view the ''reports'' page in PVWA?

### Options:

A- PVWAMonitor
B- ReportUsers
C- PVWAReports
D- Operators

### Answer:

A

### Explanation:

In a default CyberArk installation, to view the ''reports'' page in the PVWA (Privileged Web Access), a user must be a member of thePVWAMonitorgroup1. This group is specified in theManageReportsGroupparameter in the Reports section of the Web Access Options in the System Configuration page. Being a member of this group grants the user the necessary permissions to generate and view reports within the PVWA.

CyberArk's official documentation on Reports in PVWA outlines the requirement for users to belong to the PVWAMonitor group to access the reports page and generate reports1.

## Question 7

Question Type: MultipleChoice

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.....

### Options:

A- Log in to the system as root, then change root's password
B- Log in to the system as the logon account, then change roofs password
C- Log in to the system as the logon account, run the su command to log in as root, and then change root's password.
D- None of these

### Answer:

C

### Explanation:

When attempting to change the root account's password, the CPM will log in to the system as the logon account, run the su command to log in as root, and then change root's password. This is because the logon account is used to initiate sessions to machines that do not permit direct logon, such as Unix systems that restrict root access. When a logon account is associated with a privileged account, it will be used to log onto the remote machine and then elevate itself to the role of the privileged user. As different types of machines might have different logon prompts or elevation commands, the CPM can use the AutoLogonSequenceWithLogonAccount parameter to define the logon process and the elevation to the privileged account. This parameter contains regular expression prompts and responses that define the logon process and subsequent activities.The regular expressions can include dynamic values that the CPM reads from the account properties, user parameters, or client-specific parameters1. For example, the following is a possible AutoLogonSequenceWithLogonAccount parameter for a Unix platform:

```
AutoLogonSequenceWithLogonAccount=
login: {LogonUsername}
Password: {LogonPassword}
{LogonUsername}@.*\$ su -
Password: {LogonPassword}
root@.*# {ChangeCommand}
root@.*# exit
{LogonUsername}@.*\$ exit
```

This parameter instructs the CPM to log in to the system as the logon account, enter the logon

password, run the su - command to switch to the root user, enter the logon password again, run the change command to change the root password, exit the root session, and exit the logon session1.

The other options are not correct, as follows:

A . Log in to the system as root, then change root's password. This option is not possible, because the root account cannot be used for direct logon.The logon account is associated with the root account to enable the CPM to access the system and change the password1.

B . Log in to the system as the logon account, then change root's password. This option is not effective, because the logon account does not have the permission to change the root's password.The logon account needs to elevate itself to the root user by using the su command before changing the password1.

D . None of these. This option is not valid, because there is a correct answer among the choices.

1:Logon Accounts for SSH and Telnet Connections

## Question 8

Question Type: MultipleChoice

A Reconcile Account can be specified in the Master Policy.

### Options:

A- TRUE
B- FALSE

### Answer:

B

### Explanation:

A Reconcile Account is not specified in the Master Policy, but in the Platform settings. The Master Policy defines the general password management settings for all the accounts in the Vault, such as the frequency of password rotation and verification. The Platform settings define the specific password management settings for each type of target system, such as the password complexity and the Reconcile Account.Reference:

Defender PAM course, Module 2: Password Management, Lesson 2: Master Policy and

Platforms, slide 8

Defender PAM course, Module 2: Password Management, Lesson 3: Reconcile and Logon Accounts, slide 2

Defender PAM Sample Items Study Guide, Question 37

CyberArk Privileged Access Security Documentation, Password Management - Master Policy

CyberArk Privileged Access Security Documentation, Password Management - Platforms

## Question 9

Question Type: MultipleChoice

When a DR Vault Server becomes an active vault, it will automatically revert back to DR mode once the Primary Vault comes back online.

### Options:

A- True; this is the default behavior
B- False, the Vault administrator must manually set the DR Vault to DR mode by setting ''FailoverMode=no'' in the padr.ini file
C- True, if the AllowFailback setting is set to ''yes'' in the padr.ini file
D- False, the Vault administrator must manually set the DR Vault to DR mode by setting ''FailoverMode=no'' in the dbparm.ini file

### Answer:

B

### Explanation:

According to the web search results, when a DR Vault Server becomes an active vault, it will not automatically revert back to DR mode once the Primary Vault comes back online.The Vault administrator must manually set the DR Vault to DR mode by setting ''FailoverMode=no'' in the padr.ini file1.This file is located in the /opt/CARKaim/conf directory on the DR Vault machine2.The Vault administrator must also stop the replication process on the DR Vault and restart the PrivateArk Server service1.This procedure is known as a DR failback, which restores the original roles of the Primary Vault and the DR Vault after a failover1.The AllowFailback setting in the padr.ini file does not affect the DR failback process, as it only determines whether the DR Vault can be used as a backup for another DR Vault in a cascading DR scenario3. The dbparm.ini file is not relevant for the DR failback process, as it contains the database

parameters for the Vault server.Reference:

Initiate a DR failback to the Production Vault - CyberArk

Install the Disaster Recovery application - CyberArk

Cascading DR - CyberArk

[dbparm.ini file - CyberArk]