



- Expert Verified, Online, **Free**.



## **CERTIFICATION TEST**

- [CertificationTest.net](https://CertificationTest.net) - Cheap & Quality Resources With Best Support

What do you need on the Vault to support LDAP over SSL?

- A. CA Certificate(s) used to sign the External Directory certificate
- B. RECPRV.key
- C. a private key for the external directory
- D. self-signed Certificate(s) for the Vault

**Suggested Answer: A**

*Community vote distribution*

A (100%)

  **Jabelo** Highly Voted 1 year, 5 months ago

I think A is correct! From CyberArk Docs: "On the Vault machine, import the CA Certificate that signed the certificate used by the External Directory into the Windows certificate store to facilitate an SSL connection between the Vault and the External Directory (recommended)."



upvoted 5 times

  **asyouwish007** Most Recent 2 weeks, 4 days ago

**Selected Answer: A**

Did anyone see any of these questions on the actual exam?



upvoted 1 times

  **cf57f90** 8 months, 2 weeks ago

**Selected Answer: A**

A is correct

upvoted 1 times

  **Imdroc** 9 months, 3 weeks ago

**Selected Answer: A**

The Answer is: A

upvoted 1 times

  **Bob\_Irawan** 1 year, 6 months ago

**Selected Answer: A**

A is correct



upvoted 1 times

  **potatobee** 1 year, 8 months ago

**Selected Answer: A**

A is correct

upvoted 1 times

  **Datovid** 1 year, 9 months ago

A is correct

upvoted 1 times

  **Nivaisman** 1 year, 10 months ago

**Selected Answer: A**

In order to have an LDAPs integration with the Vault, You must have the Organizational Root-CA cert in the Trusted-Root folder.



upvoted 2 times

  **brossva** 2 years ago

**Selected Answer: A**

A is correct

upvoted 1 times

  **Takumi** 2 years, 3 months ago



**Selected Answer: A**

The answer is A, here it is mentioned:

Configure LDAP over SSL connections (recommended):



On the Vault machine, import the CA certificate that signed the certificate used by the external directory into the Windows certificate store to facilitate an SSL connection between the vault and the external directory (recommended).

upvoted 3 times

  **jafyyy** 2 years, 4 months ago

A is correct answer.

upvoted 1 times

  **MOO\_A** 2 years, 4 months ago

**Selected Answer: A**

Shouldn't the answer be A?

upvoted 1 times

You are troubleshooting a PVWA slow response.  
Which log files should you analyze first? (Choose two.)

- A. ITALog.log
- B. web.config
- C. CyberArk.WebApplication.log
- D. CyberArk.WebConsole.log

**Suggested Answer:** CD

Community vote distribution

CD (100%)

🗳️ 👤 **f0f4e87** 1 week, 6 days ago

**Selected Answer:** CD

<https://docs.cyberark.com/pam-self-hosted/14.4/en/content/pasimp/pvwa-logging.htm>  
upvoted 1 times

🗳️ 👤 **michael\_roszbach** 1 month, 2 weeks ago

**Selected Answer:** CD

these are the only logs that relate to the PVWA  
upvoted 1 times

🗳️ 👤 **2a13b08** 6 months, 2 weeks ago

**Selected Answer:** CD

CD are the only log files  
upvoted 1 times

🗳️ 👤 **Daxuz\_Security** 8 months, 1 week ago

I chose A. ITALog.log and C. CyberArk.WebApplication.log because the first one gives details about authentication and transactions, helping to spot delays in those processes. The second log shows how the web application is behaving and helps identify any bottlenecks or errors affecting response times. Both logs are key for figuring out performance issues in PVWA.  
upvoted 1 times

🗳️ 👤 **cf57f90** 8 months, 2 weeks ago

**Selected Answer:** CD

C and D are correct  
upvoted 1 times

🗳️ 👤 **Imdroc** 9 months, 3 weeks ago

**Selected Answer:** CD

The answer is: CD  
upvoted 1 times

🗳️ 👤 **Prasant\_Shanmugasekar** 1 year, 6 months ago

**Selected Answer:** CD

CD are the only log files related to PVWA  
upvoted 2 times

🗳️ 👤 **miky\_Cissp** 1 year, 8 months ago

CD  
PVWA log files:

PVWA.App.log

PVWA.Reports.log

PVWA.Console.log

PVWA.Casos.log

CyberArk.WebSession.General.log

CyberArk.WebServiceSession.log

CyberArk.WebServiceSession.<sessionId>.log

upvoted 2 times

What is the easiest way to duplicate an existing platform?

- A. From PrivateArk, copy/paste the appropriate Policy.ini file; then rename it.
- B. From the PVWA, navigate to the platforms page, select an existing platform that is similar to the new target account platform and then click Duplicate; name the new platform.
- C. From PrivateArk, copy/paste the appropriate settings in PVConfiguration.xml; then update the policyName variable.
- D. From the PVWA, navigate to the platforms page, select an existing platform that is similar to the new target account platform, manually update the platform settings and click "Save as" INSTEAD of save to duplicate and rename the platform.

**Suggested Answer: B**

Community vote distribution

B (100%)

🗳️ **f0f4e87** 1 week, 6 days ago

**Selected Answer: B**

<https://docs.cyberark.com/pam-self-hosted/14.4/en/content/pasimp/adding-new-platforms.htm#Duplicat>  
upvoted 1 times

🗳️ **mukeshdev** 5 months, 3 weeks ago

**Selected Answer: B**

The easiest and most efficient way to duplicate an existing platform is through the PVWA (Privileged Vault Web Access) interface. This allows you to:

Select an existing platform as a base.

Duplicate it with minimal manual effort.

Name the new platform appropriately.

Customize the settings for the new platform as needed.

This method avoids the risks of manual configuration errors and ensures a streamlined, user-friendly process.

upvoted 1 times

🗳️ **cf57f90** 8 months, 2 weeks ago

**Selected Answer: B**

B is correct

upvoted 1 times

🗳️ **Imdroc** 9 months, 3 weeks ago

**Selected Answer: B**

The Answer is: B

upvoted 1 times

🗳️ **[Removed]** 10 months, 1 week ago

Examtopics needs to do a better job of answering these questions. This is like the simplest question ever. How do we trust the more difficult ones?

upvoted 2 times

🗳️ **Bob\_Irawan** 1 year, 6 months ago

**Selected Answer: B**

B Is the most

upvoted 1 times

🗳️ **Prasant\_Shanmugasekar** 1 year, 6 months ago

**Selected Answer: B**

Option B

upvoted 1 times

🗳️ **rindra** 1 year, 10 months ago

B you can see if you login in the PVWA

upvoted 1 times

🗳️ **MIZTER** 1 year, 10 months ago

B is correct



upvoted 1 times

  **brossva** 2 years ago

**Selected Answer: B**

B is correct



upvoted 1 times

  **Examtim71** 2 years, 1 month ago

**Selected Answer: B**

answer B is correct

upvoted 1 times

  **MOO\_A** 2 years, 4 months ago

**Selected Answer: B**

Answer should be B

upvoted 1 times

DRAG DROP -

Match each key to its recommended storage location.

Recovery Private Key	Drag answer here	Store in a Physical Safe
Recovery Public Key	Drag answer here	Store in a Hardware Security Module
Server Key	Drag answer here	Store on the Vault Server Disk Drive
SSH Keys	Drag answer here	Store in the Vault.

**Suggested Answer:** *Recovery Private Key: Store in a Physical Safe*

*Recovery Public Key: Store on the Vault Server Disk Drive*

*Server Key: Store in a Hardware Security Module*

*SSH Keys: Store in the Vault.*

 **penuelaandy** Highly Voted 2 years, 4 months ago

Recovery Private Key: Store in a Physical Safe

Recovery Public Key: Store on the Vault Server Disk Drive

Server Key: Store in a Hardware Security Module

SSH Keys: Store in the Vault.

upvoted 12 times

 **e3fe132** Most Recent 7 months, 2 weeks ago

I believe it should be all but ssh keys stored in a physical safe, and the ssh keys should be stored on the vault.

upvoted 1 times

 **cf57f90** 8 months, 2 weeks ago


Recovery Private Key: Store in a Physical Safe

Recovery Public Key: Store on the Vault Server Disk Drive

Server Key: Store in a Hardware Security Module

SSH Keys: Store in the Vault.

upvoted 1 times

 **Bob\_Irawan** 1 year, 6 months ago

Recovery Private Key: Store in a Physical Safe (Master CD)

Recovery Public Key: Store on the Vault Server Disk Drive

Server Key: Store in a Hardware Security Module

SSH Keys: Store in the Vault.

upvoted 3 times

 **Prasant\_Shanmugasekar** 1 year, 6 months ago

Recovery Private Key: Store in a Physical Safe

Recovery Public Key: Store on the Vault Server Disk Drive

Server Key: Store in a Hardware Security Module

SSH Keys: Store in the Vault

upvoted 2 times



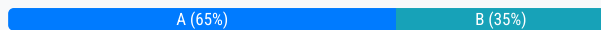
Due to corporate storage constraints, you have been asked to disable session monitoring and recording for 500 testing accounts used for your lab environment.

How do you accomplish this?

- A. Master Policy>select Session Management>add Exceptions to the platform(s)>disable Session Monitoring and Recording policies
- B. Administration>Platform Management>select the platform(s)>disable Session Monitoring and Recording
- C. Polices>Access Control (Safes)>select the safe(s)>disable Session Monitoring and Recording policies
- D. Administration>Configuration Options>Options>select Privilege Session Management>disable Session Monitoring and Recording policies

**Suggested Answer: A**

*Community vote distribution*



**michael\_roszbach** 1 month, 2 weeks ago

**Selected Answer: A**

Recording is set at the platform level by the master policy. The other answers either do not change the recording or change it for all accounts in the safe. A is correct

upvoted 1 times

**mukeshdev** 5 months, 3 weeks ago

**Selected Answer: A**

A is correct.

upvoted 1 times

**Imdroc** 9 months, 3 weeks ago

**Selected Answer: A**

Answer is A

upvoted 1 times

**Imdroc** 9 months, 3 weeks ago

A is the correct answer

upvoted 1 times

**JasonLee** 1 year ago

**Selected Answer: A**

Enable session recording in the Master Policy for all platforms or for specific platforms by use of exceptions.

From training.

upvoted 2 times

**JM\_Olympus** 1 year, 1 month ago

B:

Overview

Authorized users can monitor active sessions from their workstation and take part in controlling these sessions. Users can also suspend or terminate active sessions based on their group assignment.

By default, active session monitoring is enabled at system level for all authorized users, and can be disabled at platform level. Active session monitoring can also be disabled at system level, but when it is disabled, it cannot be enabled at platform level.

upvoted 2 times

**gical** 1 year, 4 months ago

Definitely A

We want to save disk space by not recording and not disable live monitoring.

upvoted 1 times

**Bob\_Irawan** 1 year, 6 months ago

**Selected Answer: A**

A is the correct answer

upvoted 2 times

🗨️ 👤 **Prasant\_Shanmugasekar** 1 year, 6 months ago

**Selected Answer: A**

Other than option A, the rest of the option doesn't make sense

upvoted 2 times

🗨️ 👤 **angie77** 1 year, 8 months ago

I think it is A. The step is missing "PSM" before step disabled session monitoring, also the word disable session monitoring seems not accurate cause we are adding excluded users & group. Using A we can add exception at platform level.

upvoted 1 times

🗨️ 👤 **miky\_Cissp** 1 year, 8 months ago

B

In the PVWA, click Administration , and then click Platform Management.

Click the platform type that you want to edit=>edit

In the left pane, expand UI & Workflows, right-click Privileged Session Management and select Add Exclude Recorded Users and Groups.

In the left pane, expand UI & Workflows, right-click Privileged Session Management and select Add Recorded Users and Groups.

upvoted 1 times

🗨️ 👤 **R90000000** 1 year, 8 months ago

A is correct

upvoted 1 times

🗨️ 👤 **Remy** 1 year, 9 months ago

**Selected Answer: A**

A

upvoted 1 times

🗨️ 👤 **d\_dragos95** 2 years ago

**Selected Answer: B**

B is correct. Check this link to see how you disable session monitoring and recording at platform lvl.

upvoted 2 times

🗨️ 👤 **brossva** 2 years ago

**Selected Answer: A**

A is correct

upvoted 1 times

🗨️ 👤 **Swaminathanm** 2 years ago

Selected Answer: A

Correct Answer: A

upvoted 1 times

🗨️ 👤 **brossva** 2 years, 1 month ago

A is correct

upvoted 2 times

A user requested access to view a password secured by dual-control and is unsure who to contact to expedite the approval process. The Vault Admin has been asked to look at the account and identify who can approve their request.  
What is the correct location to identify users or groups who can approve?

- A. PVWA > Administration > Platform Configuration > Edit Platform > UI & Workflow > Dual Control > Approvers
- B. PVWA > Policies > Access Control (Safes) > Select the safe > Safe Members > Workflow > Authorize Password Requests
- C. PVWA > Account List > Edit > Show Advanced Settings > Dual Control > Direct Managers
- D. PrivateArk > Admin Tools > Users and Groups > Auditors (Group Membership)

**Suggested Answer: B**

*Community vote distribution*

B (100%)

🗲️ 👤 **Iolinh** 7 months, 2 weeks ago

B is correct

upvoted 1 times

🗲️ 👤 **Imdroc** 9 months, 3 weeks ago

**Selected Answer: B**

The Answer is: B

upvoted 1 times

🗲️ 👤 **Jaheim** 1 year, 7 months ago

B is correct

upvoted 2 times

🗲️ 👤 **brossva** 2 years ago

B is correct

upvoted 1 times

🗲️ 👤 **Swaminathanm** 2 years ago

**Selected Answer: B**

Correct Answer: B

upvoted 1 times

🗲️ 👤 **Takumi** 2 years, 3 months ago

The question is somewhat confusing about dual control and knowing the location of the approvers, it still seems that the answer is B

upvoted 1 times

What must you specify when configuring a discovery scan for UNIX? (Choose two.)

- A. Vault Administrator
- B. CPM Scanner
- C. root password for each machine
- D. list of machines to scan
- E. safe for discovered accounts

**Suggested Answer:** BD

Community vote distribution

BD (100%)

penuelaandy **Highly Voted** 2 years, 4 months ago

**Selected Answer: BD**

BD

upvoted 6 times

Imdroc **Most Recent** 9 months, 2 weeks ago

**Selected Answer: BD**

Answer is BD

upvoted 1 times

Imdroc 9 months, 3 weeks ago

Correct Answer: BD

upvoted 1 times

JM\_Olympus 1 year, 1 month ago

BD

upvoted 1 times

ThomasKong 1 year, 2 months ago

C,D

without the root, how to login and grab the server info ?

If Windows you can do that.

upvoted 1 times

miky\_Cissp 1 year, 8 months ago

BD

B. CPM Scanner: This is essential as it determines which CPM will run the discovery.

D. list of machines to scan: The discovery process needs to know which machines to scan, so providing a list or defining a source is crucial.

upvoted 1 times

Swaminathanm 2 years ago

**Selected Answer: BD**

BD

upvoted 3 times

To change the safe where recordings are kept for a specific platform, which setting must you update in the platform configuration?

- A. SessionRecorderSafe
- B. SessionSafe
- C. RecordingsPath
- D. RecordingLocation

**Suggested Answer: A**

*Community vote distribution*

A (100%)

🗳️ 👤 **cf57f90** 8 months, 2 weeks ago

**Selected Answer: A**

A

upvoted 1 times

🗳️ 👤 **Imdroc** 9 months, 3 weeks ago

**Selected Answer: A**

The answer is: A

upvoted 1 times

🗳️ 👤 **Jakub4444** 1 year, 6 months ago

**Selected Answer: A**

A

upvoted 3 times

🗳️ 👤 **WHudson** 1 year, 9 months ago

**Selected Answer: A**

It is for sure A.

upvoted 2 times

🗳️ 👤 **Swaminathanm** 2 years ago

**Selected Answer: A**

SessionRecorderSafe

upvoted 2 times

🗳️ 👤 **ExamsAE** 2 years ago

**Selected Answer: A**

SessionRecorderSafe

upvoted 2 times

🗳️ 👤 **VIZZ\_27** 2 years, 1 month ago

**Selected Answer: A**

I believe answer is A.

upvoted 2 times

🗳️ 👤 **Takumi** 2 years, 3 months ago

**Selected Answer: A**

In SessionRecorderSafe , specify the name of the Safe to store recordings of activities for accounts associated with the platform. Enter the relevant information:

upvoted 2 times

🗳️ 👤 **penuelaandy** 2 years, 4 months ago

**Selected Answer: A**

A

upvoted 4 times

🗳️ 👤 **flaw123456789** 2 years, 4 months ago

SessionRecorderSafe is the correct answer  
upvoted 1 times

Which processes reduce the risk of credential theft? (Choose two.)



- A. require dual control password access approval
- B. require password change every X days
- C. enforce check-in/check-out exclusive access
- D. enforce one-time password access

**Suggested Answer:** BD

Community vote distribution

BD (63%)


CD (38%)

  **uswarrior** Highly Voted 1 year, 11 months ago

**Selected Answer:** BD

I think the answer should be B and D. In order to prevent credential theft, one needs to rotate passwords and make use of OTPs. Dual control is to prevent insider threat and exclusive access (check in and check out) is for user accountability.

upvoted 8 times

  **penuelaandy** Highly Voted 2 years, 4 months ago

**Selected Answer:** CD

Sample exam by cyberark says the process to reduce the risk is using one-time passwords. Using Dual-Control is to enforce collusion, IMO.


upvoted 7 times

  **michael\_roszbach** Most Recent 1 month, 2 weeks ago

**Selected Answer:** BD

Answers A and C are about Access control, not password security. Once the password is released (through dual control and access) the password is exposed. Preventing the theft is about rotation, either through programatic timed rotation or OTP

upvoted 1 times

  **cf57f90** 8 months, 2 weeks ago

**Selected Answer:** CD

The Answer is: CD

upvoted 2 times

  **Imdroc** 9 months, 3 weeks ago

**Selected Answer:** CD

The Answer is: CD

upvoted 1 times



  **JasonLee** 1 year ago

**Selected Answer:** CD

To achieve personal accountability, enable this rule and the Enforce check-in/check-out exclusive access rule together. The timeframe that an account will be available before it will be automatically changed is determined by the MinValidityPeriod platform setting or by the timeframe defined in the dual control request.

<https://docs.cyberark.com/privilege-cloud-standard/Latest/en/Content/Privilege%20Cloud/privCloud-master-policy-rules.htm>



upvoted 1 times

  **Jabelo** 1 year, 5 months ago

**Selected Answer:** BD

BD is correct

upvoted 3 times

  **acello** 1 year, 7 months ago

**Selected Answer:** BD

BD because if credential theft is suspected, one would rotate credentials. Only B and D present options for rotating credentials while A and C focus on non-repudiation specifically.

upvoted 4 times

🗨️ 👤 **ThomasKong** 1 year, 8 months ago

From my perspective, my answer is A & B

A - Dual Control - Let say Password A has been hacked, but B still holding by another approval person.

B - Change password x day - usually this is offer for those ID after usage or the ID keep on rotate min 1 day/1 hour after usage. Its will reduce the Password get stolen risk.

C & D - Enforce means, check in and one time password seem like the security not still strong yet. Although, the method seem strong, but just give an example. Is the hacker, require try few times to enter your system ?

check in check out and enforce to login one time, seem enough time to hacker go into your system. And this 2 method seem like same concept, is only allow a single person login into server. So, what is the prevent and control here ?

upvoted 1 times

🗨️ 👤 **miky\_Cissp** 1 year, 8 months ago

AC

A. Require dual control password access approval: This process ensures that users must receive approval from authorized users before they can access passwords, reducing the risk of unauthorized access.

C. Enforce check-in/check-out exclusive access: This process ensures that only one user can access a privileged credential at a given time, providing a clear audit trail and reducing the risk of credential theft.

upvoted 2 times

🗨️ 👤 **WHudson** 1 year, 9 months ago

**Selected Answer: BD**

BD - according to the sample CyberArk questions:

Exclusive access - Non-repudiation (individual accountability)

One Time Password - Reduced risk of credential theft

Dual Control - To force "collusion to commit"

upvoted 5 times

🗨️ 👤 **Remy** 1 year, 10 months ago

**Selected Answer: BD**

<https://docs.cyberark.com/PrivCloud/Latest/en/Content/Privilege%20Cloud/privCloud-master-policy-rules.htm>

upvoted 1 times

🗨️ 👤 **brossva** 2 years ago

**Selected Answer: CD**

CD is correcct

upvoted 1 times

🗨️ 👤 **umesh02** 2 years, 3 months ago

A,D

both impact stopping credential theft immediately

upvoted 1 times

🗨️ 👤 **umesh02** 2 years, 3 months ago

Its CD

upvoted 3 times

🗨️ 👤 **Ketan\_20** 2 years, 3 months ago

Answers: B,C

<https://cyberark-customers.force.com/s/article/Securing-Human-Interactive-PAM-Administrator-PowerShell-Scripts#:~:text=Shorter%20rotation%20intervals%20and%20the%20use%20of%20one-time,PAM%20administrator%20credentials%20because%20of%20their%20high-risk%20nature.>

Scripts#:~:text=Shorter%20rotation%20intervals%20and%20the%20use%20of%20one-time,PAM%20administrator%20credentials%20because%20of%20their%20high-risk%20nature.

upvoted 1 times



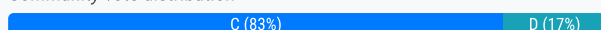
You are onboarding 5,000 UNIX root accounts for rotation by the CPM. You discover that the CPM is unable to log in directly with the root account and will need to use a secondary account.

How can this be configured to allow for password management using least privilege?

- A. Configure each CPM to use the correct logon account.
- B. Configure each CPM to use the correct reconcile account.
- C. Configure the UNIX platform to use the correct logon account.
- D. Configure the UNIX platform to use the correct reconcile account.

**Suggested Answer: C**

Community vote distribution



cf57f90 8 months, 2 weeks ago

Selected Answer: C

The Answer is: C  
upvoted 1 times

Imdroc 9 months, 3 weeks ago

Selected Answer: C

The Answer is: C  
upvoted 1 times

diogofreire 1 year, 1 month ago

Selected Answer: C

Deve ser inserido a conta de logon na conta/plataforma da conta root  
upvoted 2 times

ThomasKong 1 year, 2 months ago

it always a best practices from CyberArk Vendor or Principle.

When cannot direct login with Using Root or others high privilege ID Logon Account/ID will be the secondary login ID, then only others ID can login.  
upvoted 2 times

Azie80 1 year, 7 months ago

Selected Answer: D

The question mentioned password management. Its a tricked question..  
upvoted 3 times

miky\_Cissp 1 year, 8 months ago

C. Configure the UNIX platform to use the correct logon account is the correct answer. This is because the logon account is the secondary account that the CPM uses to first log into the UNIX system before switching to the root account for password management. The logon account provides the CPM with the necessary permissions to manage the root account's password without having direct root access.  
upvoted 3 times

brossva 2 years ago

Selected Answer: C

C is correct  
upvoted 2 times

Swaminathanm 2 years ago

Selected Answer: C

Configure the UNIX platform to use the correct logon account.  
upvoted 1 times

penuelaandy 2 years, 4 months ago



Selected Answer: C

The logon account can be defined on the target account level or on the platform level, making it available to all accounts associated with the platform.

Note: Logon accounts can also be defined for PSM and PSM for SSH connections. In this case, they can be retrieved from the account level only.

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Linked-PAS-Accounts.htm#Overview>

upvoted 3 times

  **jafyyy** 2 years, 4 months ago

C is the correct answer. must be logon account for UNIX.

upvoted 1 times

## DRAG DROP -

ADR Vault became active due to a failure of the primary Vault. Service on the primary Vault has now been restored. Arrange the steps to return the DR vault to its normal standby mode in the correct sequence.

## Unordered Options

Shut down the PrivateArk Server Service on the DR Vault.

In the PADR.ini file, set Failover Mode = No and remove the last two lines.

Start the PrivateArk Disaster Recovery Service.



## Ordered Response

**Suggested Answer:** 1. Shut down the PrivateArk Server Service on the DR Vault.  
 2. In the PADR.ini file, set Failover Mode = No and remove the last two lines.  
 3. Start the PrivateArk Disaster Recovery Service.

**Jakub4444** Highly Voted 1 year ago

The Exercise Guide from the lab part of PAM Administration course says that's the way to go:

1. Edit padr.ini and set FailoverMode to No, delete last 2 lines
2. Stop the PrivateArk Server service on DR
3. Start the CyberArk Vault Disaster Recovery service on DR

upvoted 13 times

**gical** 10 months, 3 weeks ago

<https://cyberark.my.site.com/s/article/Running-a-Disaster-Recovery-Exercise-for-CyberArk-PAM-A-Comprehensive-Guide#:~:text=In%20the%20padr.,the%20PADR%20Service%20is%20started.>

upvoted 2 times

**penuelaandy** Highly Voted 1 year, 10 months ago

1. Stop the Vault Server using the PrivateArk Server Administration Console (For HA Vault, use the Cluster Administrator) and confirm that the Cyberark Event Notification Engine service has been stopped via the services.msc console.
2. Set the "FailoverMode" variable in \Program Files (x86)\Privateark\padr\padr.ini to No.
3. Delete the following two entries in the padr.ini: NextBinaryLogNumberToStartAt, LastDataReplicationTimestamp
4. Start "CyberArk Disaster Recovery service"
5. Check \Program Files (x86)\Privateark\padr\padr.log to make sure replication is successful from Production Vault to DR Vault.

upvoted 6 times

**penuelaandy** 1 year, 10 months ago

<https://cyberark-customers.force.com/s/article/How-to-perform-a-manual-DR-Failover>

upvoted 4 times

**Swaminathanm** Most Recent 1 year, 6 months ago

1. Stop the Vault Server using the PrivateArk Server Administration Console (For HA Vault, use the Cluster Administrator) and confirm that the Cyberark Event Notification Engine service has been stopped via the services.msc console.
2. Set the "FailoverMode" variable in \Program Files (x86)\Privateark\padr\padr.ini to No.
3. Delete the following two entries in the padr.ini: NextBinaryLogNumberToStartAt, LastDataReplicationTimestamp
4. Start "CyberArk Disaster Recovery service"
5. Check \Program Files (x86)\Privateark\padr\padr.log to make sure replication is successful from Production Vault to DR Vault.

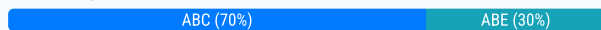
upvoted 3 times

Which methods can you use to add a user directly to the Vault Admin Group? (Choose three.)

- A. REST API
- B. PrivateArk Client
- C. PACLI
- D. PVWA
- E. Active Directory
- F. Sailpoint

**Suggested Answer:** ABC

Community vote distribution



**cyberbratz** Highly Voted 1 year, 7 months ago

ABC

Option E allows you to add a user to an LDAP security group that is added as a vault admin but the question asks that you "add a user directly into the vault admin group" so E is incorrect.

A and B are definitely correct. Using PACLI, it seems there is an option to use the command ADDGROUPMEMBER to add a user directly to the vault admin group. So definitely A, B, and C are correct.

upvoted 6 times

**Srudd** Most Recent 1 month ago

Selected Answer: ACE

I checked ChatGPT and it says ACE

upvoted 1 times

**cf57f90** 8 months, 2 weeks ago

Selected Answer: ABC

ABC

upvoted 1 times

**Imdroc** 9 months, 1 week ago

Selected Answer: ABC

Answer is ABC

upvoted 1 times

**2995142** 1 year, 2 months ago

ABD, we can use the User Provisioning feature through PVWA to add an user to a group

upvoted 2 times

**Bob\_Irawan** 1 year, 6 months ago

Selected Answer: ABC

ABC is the most correct answer in my opinion

upvoted 2 times

**celjouhari** 1 year, 6 months ago

Selected Answer: ABC

ABC

<https://docs.cyberark.com/PAS/Latest/en/Content/PACLI/User-Management-Functions.htm#UpdateGroup>

upvoted 3 times

**Prasant\_Shanmugasekar** 1 year, 6 months ago

Selected Answer: ABE

PACLI can't be used to directly add users to the Vault Admin group. You will have to first create the user and then add it using another command.

upvoted 3 times

**Imdroc** 9 months, 1 week ago

You can't use Active directory to add users to Vault Admin Group. Answer is ABC

upvoted 1 times

  **miky\_Cissp** 1 year, 8 months ago

[https://docs.cyberark.com/PAS/13.0/en/Content/WebServices/Add%20Account%20v10.htm?  
tocpath=Developer%7CREST%20APIs%7CAccounts%7C\\_\\_\\_\\_\\_5](https://docs.cyberark.com/PAS/13.0/en/Content/WebServices/Add%20Account%20v10.htm?tocpath=Developer%7CREST%20APIs%7CAccounts%7C_____5)



upvoted 1 times

  **miky\_Cissp** 1 year, 8 months ago

ABC

[https://docs.cyberark.com/PAS/13.0/en/Content/PACLI/User-Management-Functions.htm?  
tocpath=Developer%7CCommand%20Line%20Interface%20\(PACLI\)%7C\\_\\_\\_\\_\\_3](https://docs.cyberark.com/PAS/13.0/en/Content/PACLI/User-Management-Functions.htm?tocpath=Developer%7CCommand%20Line%20Interface%20(PACLI)%7C_____3)

upvoted 1 times

  **zoldik** 2 years, 3 months ago

Answer Correct ABE

upvoted 2 times

Which Automatic Remediation is configurable for a PTA detection of a "Suspected Credential Theft"?

- A. Add to Pending
- B. Rotate Credentials
- C. Reconcile Credentials
- D. Disable Account

**Suggested Answer: B**

*Community vote distribution*

B (100%)

🗳️ 👤 **cf57f90** 8 months, 2 weeks ago

**Selected Answer: B**

Answer is B

upvoted 1 times

🗳️ 👤 **Imdroc** 9 months, 3 weeks ago

**Selected Answer: B**

Answer is B

upvoted 1 times

🗳️ 👤 **Jakub4444** 1 year, 6 months ago

**Selected Answer: B**

[https://docs.cyberark.com/PAS/13.0/en/Content/PTA/Security-Configuration.htm?TocPath=End%20user%7CSecurity%20Events%7C\\_\\_\\_\\_3](https://docs.cyberark.com/PAS/13.0/en/Content/PTA/Security-Configuration.htm?TocPath=End%20user%7CSecurity%20Events%7C____3)

upvoted 4 times

🗳️ 👤 **KKKHHHh** 1 year, 10 months ago

correct is B

upvoted 1 times

🗳️ 👤 **penuelaandy** 2 years, 4 months ago

**Selected Answer: B**

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PTA/Viewing-Automatic-Containment-Responses.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Threat%20Analytics%7CTroubleshoot%20PTA%20Configuration%7CUse%20the%20diamond.log%20>

upvoted 3 times

Which item is an option for PSM recording customization?

- 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

**Suggested Answer:** C

Community vote distribution

C (91%)

9%

🗳️ 👤 **ExamsAE** Highly Voted 👍 2 years ago

**Selected Answer: C**

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Configuring-Recordings-and-Audits-in-PSM.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%7CConfiguration%7C\\_\\_\\_\\_\\_5#CustomizerecordingsinPSM](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Configuring-Recordings-and-Audits-in-PSM.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%7CConfiguration%7C_____5#CustomizerecordingsinPSM)  
upvoted 9 times

🗳️ 👤 **SayItAint** Most Recent 🕒 9 months, 1 week ago

I agree with the answer C  
but I don't know like the last word there (disabled)  
upvoted 1 times

🗳️ 👤 **Imdroc** 9 months, 2 weeks ago

**Selected Answer: C**

Answer is C  
upvoted 1 times

🗳️ 👤 **Imdroc** 9 months, 3 weeks ago

Correct Answer : C  
upvoted 1 times

🗳️ 👤 **miky\_Cissp** 1 year, 8 months ago

Universal keystrokes text recorder with windows events text recorder disabled: This is mentioned in the content. To enable universal keystrokes text recording, one must first disable Windows events text recording.  
upvoted 1 times

🗳️ 👤 **Shivani\_Goyal** 2 years, 1 month ago

Answer is C:  
Universal keystroke recording and Windows events recording cannot be configured for the same PSM-RDP connection. Windows events recording is enabled for PSM-RDP connections by default. To enable universal keystrokes recording, first disable Windows events recording. From below URL:  
[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Configuring-Recordings-and-Audits-in-PSM.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%7CConfiguration%7C\\_\\_\\_\\_\\_5#CustomizerecordingsinPSM](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Configuring-Recordings-and-Audits-in-PSM.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%7CConfiguration%7C_____5#CustomizerecordingsinPSM)  
upvoted 2 times

🗳️ 👤 **Kneebee** 2 years, 1 month ago

Concur with Taco Teo, the correct answer is C.  
upvoted 1 times

🗳️ 👤 **penuelaandy** 2 years, 4 months ago

**Selected Answer: B**

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Configuring-Recordings-and-Audits-in-PSM.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%7CConfiguration%7C\\_\\_\\_\\_\\_5#CustomizerecordingsinPSM](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Configuring-Recordings-and-Audits-in-PSM.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%7CConfiguration%7C_____5#CustomizerecordingsinPSM)  
upvoted 1 times

🗳️ 👤 **TacoTeo** 2 years, 2 months ago

That link literally says it is impossible to run Text Recorder and Keystrokes through the same connection. So B can not be the answer.... It's C  
upvoted 9 times

DRAG DROP -

Match the built-in Vault user with the correct definition.

This user appears on the highest level of the User hierarchy and has all the possible permissions. As such, it can create and manage other Users on any level on the Users' hierarchy.

Drag answer here

Administrator

This user appears at the top of the User hierarchy, enabling it to view all the Users and accounts in the Safes. The user can produce reports of Safe activities and User activities, which enables it to keep track of activity in the Safe and User requirements.

Drag answer here

Auditor

This user is an internal user that cannot be logged onto and carries out internal tasks, such as automatically clearing expired user and Safe history.

Drag answer here

Batch

This user has all available Safe member authorizations except Authorize password requests. This user has complete system control, manages a full recovery when necessary and cannot be removed from any Safe.

Drag answer here

Master


#### Suggested Answer:

**Administrator:** This user appears at the top of the User hierarchy, enabling it to view all the Users and accounts in the Safes. The user can produce reports of Safe activities and User activities, which enables it to keep track of activity in the Safe and User requirements.

**Auditor:** This user has all available Safe member authorizations except Authorize password requests. This user has complete system control, manages a full recovery when necessary and cannot be removed from any Safe.

**Batch:** This user appears on the highest level of the User hierarchy and has all the possible permissions. As such, it can create and manage other Users on any level on the Users' hierarchy.

**Master:** This user is an internal user that cannot be logged onto and carries out internal tasks, such as automatically clearing expired user and Safe history.

 **aydriman** Highly Voted 1 year, 6 months ago

Administrator ==> highest user

Auditor ==> Top level users

Batch==> internal user

Master ==> user used to manage full recovery if needed and can not be removed

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Predefined-Users-and-Groups.htm>

upvoted 11 times

 **Praveen33** Most Recent 10 months, 1 week ago

**Administrator** - This user appears on the highest level of the User hierarchy and has all possible permissions. As such, it can create and manage other Users on any level on the User hierarchy.

**Auditor** - This user appears at the top of the User hierarchy, enabling it to view all the Users in the Safe. The Auditor User can produce reports of Safe activities and User activities. This enables it to keep track of activity in the Safe and User requirements.



**Batch** - This user is an internal user that cannot be logged onto. This user carries out internal tasks, such as automatically clearing expired user and



Safe history.

Master - This user has all the available Safe member authorizations, except Authorize password requests, and therefore has complete control over the entire system. This user is used to manage a full recovery when necessary. It cannot be removed from any Safe.

upvoted 2 times

  **carloslapa** 1 year, 8 months ago

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Predefined-Users-and-Groups.htm>

upvoted 3 times

You want to create a new onboarding rule.

Where do you accomplish this?

- A. In PVWA, click Reports > Unmanaged Accounts > Rules
- B. In PVWA, click Options > Platform Management > Onboarding Rules
- C. In PrivateArk, click Tools > Onboarding Rules
- D. In PVWA, click Accounts > Onboarding Rules

**Suggested Answer: D**

*Community vote distribution*

D (100%)

penuelaandy **Highly Voted** 2 years, 4 months ago

**Selected Answer: D**

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/automatic\\_onboarding\\_rules.htm#Createonboardingrules](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/automatic_onboarding_rules.htm#Createonboardingrules)  
upvoted 9 times

Imdroc **Most Recent** 9 months, 3 weeks ago

**Selected Answer: D**

The Answer is: D  
upvoted 1 times

Praveen33 1 year, 4 months ago

**Selected Answer: D**

To Create Onboarding Rule  
In the PVWA, click Accounts > Onboarding Rules  
upvoted 1 times

LawrenceA 1 year, 8 months ago

D is the correct answer  
upvoted 1 times

WHudson 1 year, 9 months ago

**Selected Answer: D**

D is correct answer  
upvoted 1 times

brossva 2 years ago

**Selected Answer: D**

D is correct  
upvoted 1 times

What does the Export Vault Data (EVD) utility do?

- A. exports data from the Vault to TXT or CSV files, or to MSSQL databases
- B. generates a backup file that can be used as a cold backup
- C. exports all passwords and imports them into another instance of CyberArk
- D. keeps two active vaults in sync

**Suggested Answer: A**

*Community vote distribution*

A (100%)

 **penuelaandy** Highly Voted 2 years, 4 months ago

**Selected Answer: A**

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20SysReq/System%20Requirements%20-%20EVD.htm>

upvoted 9 times

 **Imdroc** Most Recent 9 months, 3 weeks ago

**Selected Answer: A**

The Answer is: A

upvoted 1 times

 **KKKHHHh** 1 year, 10 months ago

Answer is A

upvoted 1 times

When are external vault users and groups synchronized by default?

- A. They are synchronized once every 24 hours between 1 AM and 5 AM.
- B. They are synchronized once every 24 hours between 7 PM and 12 AM.
- C. They are synchronized every 2 hours.
- D. They are not synchronized according to a specific schedule.

**Suggested Answer: A**

Community vote distribution

A (100%)



  **penuelaandy** Highly Voted 2 years, 4 months ago

**Selected Answer: A**

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/Synchronizing-External-Users-and-Groups-in-the-Vault-with-the-External-Directory.htm?](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/Synchronizing-External-Users-and-Groups-in-the-Vault-with-the-External-Directory.htm?tocpath=Administrator%7CUser%20Management%7CTransparent%20user%20management%20using%20LDAP%7C_____11#Synchronizationschedule)

[tocpath=Administrator%7CUser%20Management%7CTransparent%20user%20management%20using%20LDAP%7C\\_\\_\\_\\_\\_11#Synchronizationschedule](#)

upvoted 14 times

  **Imdroc** Most Recent 9 months, 2 weeks ago

**Selected Answer: A**

Answer is A

upvoted 1 times

  **Imdroc** 9 months, 3 weeks ago



Correct Answer: A

upvoted 1 times

  **KKKHHHh** 1 year, 10 months ago

answer is A

upvoted 1 times

  **jafyyy** 2 years, 4 months ago

A is correct answer

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.3/en/Content/PAS%20INST/Synchronizing-External-Users-and-Groups-in-the-Vault-with-the-External-Directory.htm>

upvoted 1 times

You created a new safe and need to ensure the user group cannot see the password, but can connect through the PSM.  
Which safe permissions must you grant to the group? (Choose two.)

- A. List Accounts
- B. Use Accounts
- C. Access Safe without Confirmation
- D. Retrieve Files
- E. Confirm Request

**Suggested Answer:** AB

Community vote distribution

AB (100%)

penuelaandy Highly Voted 2 years, 4 months ago

Selected Answer: AB

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Safes-add-a-safe-member-V12-6.htm?](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Safes-add-a-safe-member-V12-6.htm?TocPath=Administrator%7CPrivileged%20Accounts%7CAccess%20Control%7CSafes%20and%20Safe%20members%7CNew%20interface%7C_____3#Safemen)

TocPath=Administrator%7CPrivileged%20Accounts%7CAccess%20Control%7CSafes%20and%20Safe%20members%7CNew%20interface%7C\_\_\_\_\_3#Safemen  
upvoted 10 times

Imdroc Most Recent 9 months, 3 weeks ago

Selected Answer: AB

The Answer is: AB  
upvoted 1 times

voidgoel 11 months, 3 weeks ago

AB is correct  
upvoted 1 times

WHudson 1 year, 9 months ago

Selected Answer: AB

Needs List to see the account and Use to use it - can't have the Retrieve.  
upvoted 2 times

brossva 2 years ago

Selected Answer: AB

AB is correct  
upvoted 2 times

jafyyy 2 years, 4 months ago

AB are correct answer.  
retrieve permission for copy and show the pw.  
upvoted 3 times

MOO\_A 2 years, 4 months ago

Selected Answer: AB

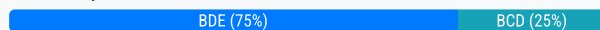
is AB?  
upvoted 3 times

During a High Availability node switch you notice an error and the Cluster Vault Manager Utility fails back to the original node. Which log files should you check to investigate the cause of the issue? (Choose three.)

- A. CyberArk Webconsole.log
- B. VaultDB.log
- C. PM\_Error.log
- D. ITALog.log
- E. ClusterVault.console.log
- F. logiccontainer.log

**Suggested Answer:** BDE

Community vote distribution



**miky\_Cissp** Highly Voted 1 year, 8 months ago

BDE

B. VaultDB.log: This log is included in the list and might contain information related to the Vault's database operations.

D. ITALog.log: This log is included in the list and might contain information related to various Vault operations.

E. ClusterVault.console.log: This log is included in the list and is likely directly related to the clustering mechanism of the Vault.

upvoted 7 times

**Imdroc** Most Recent 9 months, 2 weeks ago

Selected Answer: BDE

Answer is BDE

upvoted 1 times

**Imdroc** 9 months, 3 weeks ago

Correct Answer : BDE

upvoted 1 times

**voidgoel** 11 months, 3 weeks ago

BDE is correct

upvoted 2 times

**KKKHHHh** 1 year, 10 months ago

BDE is correct

upvoted 2 times

**uswarrior** 1 year, 11 months ago

Selected Answer: BDE

The answer should be BDE. The remaining logs are found on other components.

upvoted 2 times

**brossva** 2 years ago

BDE is correct

upvoted 2 times

**Examtim71** 2 years, 1 month ago

Selected Answer: BDE

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Collecting-Log-Files.htm>

upvoted 3 times

**TacoTeo** 2 years, 2 months ago

It's CDE

upvoted 1 times

**Takumi** 2 years, 3 months ago

Selected Answer: BCD

I think the answer is BCD

upvoted 2 times

Which parameters can be used to harden the Credential Files (CredFiles) while using CreateCredFile Utility? (Choose three.)

- A. OS Username
- B. Current machine IP
- C. Current machine hostname
- D. Operating System Type (Linux/Windows/HP-UX)
- E. Vault IP Address
- F. Time Frame

**Suggested Answer:** ABC

*Community vote distribution*

ABC (100%)

  **miche17777** Highly Voted 2 years, 3 months ago

ABC

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.2/en/Content/PASIMP/CreateCredFile-Utility.htm#\\_Ref364687382](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.2/en/Content/PASIMP/CreateCredFile-Utility.htm#_Ref364687382)



upvoted 8 times

  **Imdroc** Most Recent 9 months, 3 weeks ago

**Selected Answer: ABC**



The Answer is: ABC

upvoted 1 times

  **voidgoel** 11 months, 3 weeks ago

ABC is correct



upvoted 1 times

  **jafyyy** 2 years, 4 months ago

ABC

Reference: <https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.2/en/Content/PASIMP/CreateCredFile-Utility.htm>

upvoted 2 times

  **MOO\_A** 2 years, 4 months ago

**Selected Answer: ABC**

is ABC?

upvoted 4 times



Where can a user with the appropriate permissions generate a report? (Choose two.)

- A. PVWA > Reports
- B. PrivateArk Client
- C. Cluster Vault Manager
- D. PrivateArk Server Monitor
- E. PARClient

**Suggested Answer:** AB

Community vote distribution

AB (100%)

🗳️ 👤 **Imdroc** 9 months, 3 weeks ago

**Selected Answer:** AB

The Answer is: AB

upvoted 1 times

🗳️ 👤 **voidgoel** 11 months, 3 weeks ago

A and B is correct.

upvoted 1 times

🗳️ 👤 **gical** 1 year, 4 months ago

AB

A better link: <https://docs.cyberark.com/pam-self-hosted/14.0/en/Content/PASIMP/Auditing-sessions.htm>

upvoted 1 times

🗳️ 👤 **brossva** 2 years ago

AB is correct

upvoted 2 times

🗳️ 👤 **d\_dragos95** 2 years ago

**Selected Answer:** AB

AB is correct

upvoted 3 times

🗳️ 👤 **zoldik** 2 years, 3 months ago

A and B

upvoted 1 times

🗳️ 👤 **penuelaandy** 2 years, 4 months ago

**Selected Answer:** AB

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PrivCloud/Latest/en/Content/Privilege%20Cloud/privCloud-generate-reports.htm?](https://docs.cyberark.com/Product-Doc/OnlineHelp/PrivCloud/Latest/en/Content/Privilege%20Cloud/privCloud-generate-reports.htm?TocPath=Administrators%7CManage%20reports%7C_____2#Whocanviewandgeneratereports)

[TocPath=Administrators%7CManage%20reports%7C\\_\\_\\_\\_\\_2#Whocanviewandgeneratereports](https://docs.cyberark.com/Product-Doc/OnlineHelp/PrivCloud/Latest/en/Content/Privilege%20Cloud/privCloud-generate-reports.htm?TocPath=Administrators%7CManage%20reports%7C_____2#Whocanviewandgeneratereports)

upvoted 2 times

🗳️ 👤 **jafyyy** 2 years, 4 months ago

A and B?

upvoted 2 times

Users are unable to launch Web Type Connection components from the PSM server. Your manager asked you to open the case with CyberArk Support.

Which logs will be most useful for the CyberArk Support Team to debug the issue? (Choose three.)

- A. PSMConsole.log
- B. PSMDebug.log
- C. PSMTrace.log
- D. <Session\_ID>.Component.log
- E. PMconsole.log
- F. ITALog.log

**Suggested Answer:** ACD

Community vote distribution

ACD (100%)

  **d\_dragos95**  2 years ago

**Selected Answer:** ACD

ACD is correct.

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/10.10/en/Content/PASIMP/Administrating-the-Privileged-Session-Manager.htm>

upvoted 5 times

  **Imdroc**  9 months, 2 weeks ago

**Selected Answer:** ACD

Answer is ACD

upvoted 1 times

  **Imdroc** 9 months, 3 weeks ago

Correct Answer : ACD

upvoted 1 times

  **LostSoul4ever** 1 year, 8 months ago

**Selected Answer:** ACD

ACD, checked each log against documentation

upvoted 4 times

  **brossva** 2 years ago

ACD IS CORRECT

upvoted 1 times

  **ROUNAK1** 2 years, 2 months ago



BCF is the correct answer [https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.6/en/Content/PSMC/PSMC\\_Troubleshooting.htm](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.6/en/Content/PSMC/PSMC_Troubleshooting.htm)

upvoted 1 times

  **Halotototto** 2 years, 3 months ago



A, C and D are correct

upvoted 3 times

  **xxhulyanxx** 2 years, 3 months ago

BCF are the answers

upvoted 1 times

  **jafyyy** 2 years, 4 months ago

A, C and D are correct.

upvoted 2 times

You have been asked to identify the up or down status of Vault Services.  
Which CyberArk utility can you use to accomplish this task?

- A. PrivateArk Central Administration Console
- B. PAS Reporter
- C. PrivateArk Remote Control Agent
- D. Syslog

**Suggested Answer: C**

Community vote distribution

C (85%)

A (15%)


 **penuelaandy** Highly Voted 2 years, 4 months ago

**Selected Answer: C**

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Remote-Administration-for-the-Vault-DR-Vault.htm?](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Remote-Administration-for-the-Vault-DR-Vault.htm?tocpath=Administrator%7CComponents%7CDigital%20Vault%7COperate%20the%20CyberArk%20Vault%7CMonitor%20the%20Vault%7C_____1#ConfiguretheR)

[tocpath=Administrator%7CComponents%7CDigital%20Vault%7COperate%20the%20CyberArk%20Vault%7CMonitor%20the%20Vault%7C\\_\\_\\_\\_\\_1#ConfiguretheR](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Remote-Administration-for-the-Vault-DR-Vault.htm?tocpath=Administrator%7CComponents%7CDigital%20Vault%7COperate%20the%20CyberArk%20Vault%7CMonitor%20the%20Vault%7C_____1#ConfiguretheR)

upvoted 10 times

 **Imdroc** Most Recent 9 months, 3 weeks ago

**Selected Answer: C**

The Answer is: C

upvoted 1 times

 **JM\_Olympus** 1 year, 1 month ago

C

<https://docs.cyberark.com/pam-self-hosted/13.0/en/Content/PASIMP/Remote-Administration-for-the-Vault-DR-Vault.htm?Highlight=vault%20status>

Status Vault Show activity status of a Vault on the remote machine.

upvoted 1 times

 **ThomasKong** 1 year, 2 months ago

A, The answer will be A.

C shouldn't be the answer. As it mostly is monitoring the user and access issues.

PrivateArk Central Administrator console, it the live monitoring tools within Vault services either in AD or user unable to login or shut down or Firewall blocked and more. The question literally vault services, if not the vault PrivateArk Central Administrator then where else?

Unless there have a option in PVWA health status from the answer.

upvoted 2 times

 **Prasant\_Shanmugasekar** 1 year, 6 months ago

**Selected Answer: A**

The other components mentioned are used for various other purpose

upvoted 2 times

 **Jakub4444** 1 year, 5 months ago

Definitely not. It's 'C' as per the PAM Administration lab Exercise Guide.

upvoted 4 times

 **jafyyy** 2 years, 4 months ago

c is correct.

upvoted 3 times

A new colleague created a directory mapping between the Active Directory groups and the Vault.  
Where can the newly Configured directory mapping be tested?

- A. Connect to the Active Directory and ensure the organizational unit exists.
- B. Connect to Sailpoint (or similar tool) to ensure the organizational unit is correctly named; log in to the PVWA with "Administrator" and confirm authentication succeeds.
- C. Search for members that exist only in the mapping group to grant them safe permissions through the PVWA.
- D. Connect to the PrivateArk Client with the Administrator Account to see if there is a user in the Vault Admin Group.

**Suggested Answer: C**

Community vote distribution

C (67%)

D (33%)

🗳️ 👤 **uswarrior** Highly Voted 1 year, 11 months ago

The answer should be C. D is out of question since there is no vault admin group in picture.  
upvoted 11 times

🗳️ 👤 **Jabelo** Highly Voted 1 year, 4 months ago

**Selected Answer: C**

I agree with uswarrior. The answer is C. The vault admin group is not mentioned in the question.  
upvoted 5 times

🗳️ 👤 **Imdroc** Most Recent 9 months, 2 weeks ago

**Selected Answer: C**

Answer is C  
upvoted 1 times

🗳️ 👤 **Imdroc** 9 months, 3 weeks ago

Correct Answer : C  
upvoted 1 times

🗳️ 👤 **Imdroc** 9 months, 3 weeks ago

Correct Answer : C  
upvoted 1 times

🗳️ 👤 **abiurrunc** 1 year, 1 month ago

To test the newly configured directory mapping between Active Directory groups and the Vault in CyberArk, we have to follow these steps:  
1 -Log in to PVWA (Privileged Web Access):  
1.1 Log in to the PVWA using an account with "Administrator" privileges.  
Question ask where, and the first that we have to to is connect to PVWA.  
Answers is C  
upvoted 2 times

🗳️ 👤 **miky\_Cissp** 1 year, 8 months ago

C  
I vote for C  
upvoted 5 times

🗳️ 👤 **brossva** 2 years ago

D is correct  
upvoted 1 times

🗳️ 👤 **penuelaandy** 2 years, 4 months ago

**Selected Answer: D**

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Managing-Groups.htm?tocpath=Administrator%7CUser%20Management%7C\\_\\_\\_\\_\\_5#Managegroupmembers](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Managing-Groups.htm?tocpath=Administrator%7CUser%20Management%7C_____5#Managegroupmembers)  
upvoted 3 times

  **Manno099** 2 years, 4 months ago

D IS CORRECT

upvoted 2 times

A user needs to view recorded sessions through the PVWA.

Without giving auditor access, which safes does a user need access to view PSM recordings? (Choose two.)

- A. Recordings safe
- B. Safe the account is in
- C. System safe
- D. PVWAConfiguration safe
- E. VaultInternal safe

**Suggested Answer:** AB

Community vote distribution

AB (100%)

  **penuelaandy** Highly Voted  2 years, 4 months ago

Selected Answer: AB

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/NewUI/NewUI-Monitor-sessions.htm#Permissions>

upvoted 6 times

  **Imdroc** Most Recent  9 months, 3 weeks ago

Selected Answer: AB

The answer is: AB

upvoted 1 times

  **CyberDishu** 1 year, 10 months ago

AD is the correct answer as safe members don't have Session Recording view

upvoted 1 times

  **Jakub4444** 1 year, 5 months ago

Incorrect. It's AB indeed

upvoted 2 times

Which file must be edited on the Vault to configure it to send data to PTA?

- A. dbparm.ini
- B. PARAgent.ini
- C. my.ini
- D. padr.ini

**Suggested Answer: A**

*Community vote distribution*

A (100%)

 **penuelaandy** Highly Voted 2 years, 4 months ago

**Selected Answer: A**

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PTA/Configuring-Vault-Forward-syslog-Messages.htm>

upvoted 6 times

 **Imdroc** Most Recent 9 months, 3 weeks ago

**Selected Answer: A**

The Answer is: A


upvoted 1 times

 **brossva** 2 years ago

**Selected Answer: A**


A is correct

upvoted 2 times

 **zoldik** 2 years, 3 months ago

Answer is A

upvoted 1 times

 **jafyyy** 2 years, 4 months ago

A is correct.

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.3/en/Content/PTA/Configuring-Vault-Forward-syslog-Messages.htm>

upvoted 3 times

You want to build a connector that connects to a website through the Web applications for PSM framework.  
Which default connector do you duplicate and modify?

- A. PSM-ChromeSample
- B. PSM-WebForm
- C. PSM-WebApp
- D. PSM-WebAppSample

**Suggested Answer: D**

Community vote distribution

D (100%)

penuelaandy **Highly Voted** 1 year, 10 months ago

**Selected Answer: D**

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/psm\\_WebApplication.htm#Configuration](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/psm_WebApplication.htm#Configuration)  
upvoted 7 times

JM\_Olympus **Most Recent** 7 months, 1 week ago

D:

[https://docs.cyberark.com/pam-self-hosted/13.0/en/Content/PASIMP/psm\\_WebApplication.htm?Highlight=webappsample](https://docs.cyberark.com/pam-self-hosted/13.0/en/Content/PASIMP/psm_WebApplication.htm?Highlight=webappsample)

Right-click PSM-WebAppSample, and select Copy.

Right-click PSM-WebAppSample, and select Copy.

Right-click PSM-WebAppSample, and select Copy.  
upvoted 2 times

miky\_Cissp 1 year, 2 months ago

D. PSM-WebAppSample.

To build a connector that connects to a website through the Web applications for PSM framework, you would duplicate and modify the default connector named PSM-WebAppSample.  
upvoted 1 times

brossva 1 year, 6 months ago

D is correct

upvoted 1 times

Singa\_22 1 year, 9 months ago

D is the answer

upvoted 2 times

zoldik 1 year, 9 months ago

The answer is D, Need to duplicate PSM-WebAppSample  
upvoted 1 times




DRAG DROP -


A new HTML5 Gateway has been deployed in your organization.

From the PVWA, arrange the steps to configure a PSM host to use the HTML5 Gateway in the correct sequence.

The diagram illustrates the process of ordering options. On the left, a box labeled "Unordered Options" contains five items in rounded rectangles: "Administration>Options", "Privileged Session Management", "Configured PSM Servers and select existing PSM host", "Connection Details", and "Add PSM gateway". On the right, a large empty box is labeled "Ordered Response". A double-headed arrow connects the two boxes. On the right side of the "Ordered Response" box, there are two vertical arrows: an upward arrow and a downward arrow, indicating the ability to reorder the response.

**Suggested Answer:** Privileged Session Management -> Configured PSM Servers and select existing PSM host -> Connection Details -> Add PSM gateway -> Administration>Options.

 **jafyyy** Highly Voted 1 year, 10 months ago  
the existing unordered side is the correct ordered.  
upvoted 10 times

 **rdk89** 6 months, 1 week ago

. Repeat steps 3-4 for each PSM server you want to set to use the PSM Gateway.

Log into the PVWA with an administrative user.

Go to Options > Privileged Session Management > Configured PSM Servers

Select the PSM server entry that you want to set to use the PSM Gateway.

Right click Connection Details and select Add PSM Gateway and enter the following:

Parameter

Value

ID

The ID of the PSM Gateway that you created in Add PSM HTML5 Gateway server.

Enable

Yes

upvoted 2 times

  **amlal** Highly Voted  1 year, 1 month ago  
the unordered options is correct ordered:

## Configure the PSM server to use the HTML5 gateway

Multiple PSM Servers can work with the same gateway or with different gateways. Repeat steps 3-4 for each PSM server you want to set to use the PSM Gateway.

Log into the PVWA with an administrative user.

Go to Options > Privileged Session Management > Configured PSM Servers

Select the PSM server entry that you want to set to use the PSM Gateway.

Right click Connection Details and select Add PSM Gateway and enter the following:

[https://docs.cyberark.com/PAS/13.0/en/Content/PASIMP/PSM\\_HTML5.htm](https://docs.cyberark.com/PAS/13.0/en/Content/PASIMP/PSM_HTML5.htm)

upvoted 9 times

  **copluk** Most Recent 2 months, 1 week ago

ADMINISTRATION ► Configuration Options ► Options

Privileged Session Management ► Configured PSM Servers ► PSMServer ► Connection Details ► PSM Gateway

Set the Enable parameter to Yes and click the Apply button

1) Administration>Options


2) Privileged Session Management

3) COnfigured PSM Servers and select existing PSM Host

4) Connection Details

5) Add PSM gateway

upvoted 2 times

  **abiurrunc** 7 months, 1 week ago

To configure a PSM host to use the HTML5 Gateway in the correct sequence, follow these steps:

Log in to the PVWA (Privileged Web Access) with an administrative user.

Navigate to Administration > Options.

Go to Privileged Session Management > Configured PSM Servers and select the existing PSM host you want to configure.

Right-click on Connection Details and select Add PSM Gateway.

Specify the necessary details for the HTML5 Gateway configuration.

Finally, save the changes and ensure that the PSM host is now using the HTML5 Gateway for secure access.

Remember that configuring the HTML5 Gateway allows you to enhance the security and accessibility of your PSM sessions.

So, the unordered options is correct ordered.

upvoted 3 times

  **12a0526** 9 months, 3 weeks ago

answer is wrong. Administration Option is the first.

upvoted 1 times

  **miky\_Cissp** 1 year, 2 months ago

Log in to the PVWA with an administrative user.

Go to Administration > Options

Right click Privileged Session Management and select Add Configured PSM Gateway Servers.

Right click Configured PSM Gateway Servers and select Add PSM Gateway Server.

Select the newly added gateway server and enter a unique ID for the PSM HTML5 gateway.

Expand the newly created gateway server. Enter the following details on the Connection Details page:

upvoted 3 times

  **penuelaandy** 1 year, 10 months ago

Administration > Options

Privileged Session Managment

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/PSM\\_HTML5.htm](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/PSM_HTML5.htm)

Configured PSM Servers

Select the PSM server entry that you want to set to use the PSM Gateway.

Right click Connection Details and select Add PSM Gateway

upvoted 1 times

  **penuelaandy** 1 year, 10 months ago

Administration > Options

Privileged Session Managament



Configured PSM Servers

Select the PSM server entry that you want to set to use the PSM Gateway.

Right click Connection Details and select Add PSM Gateway

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/PSM\\_HTML5.htm](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/PSM_HTML5.htm)

upvoted 6 times

  **jafyyy** 1 year, 10 months ago

[https://docs.cyberark.com/Product-Doc/OnlineHelp/Alero/Latest/en/Content/Installation/PSM\\_HTML5.htm#Add](https://docs.cyberark.com/Product-Doc/OnlineHelp/Alero/Latest/en/Content/Installation/PSM_HTML5.htm#Add)

upvoted 3 times

When an account is unable to change its own password, how can you ensure that password reset with the reconcile account is performed each time instead of a change?

- A. Set the parameter RAllowManualReconciliation to Yes.
- B. Set the parameter ChangePasswordInResetMade to Yes.
- C. Set the parameter IgnoreReconcileOnMissingAccount to No.
- D. Set the UnlockUserOnReconcile to Yes.

**Suggested Answer: B**

Community vote distribution

B (79%)



A (21%)

  **bugmenotplease** Highly Voted 1 year, 8 months ago

The Answer is B

<https://cyberark-customers.force.com/s/article/What-is-ChangePasswordInResetMode-in-Platform-Settings-Additional-Policies>

upvoted 9 times

  **Examtim71** Highly Voted 1 year, 7 months ago

**Selected Answer: B**

section: Reset passwords using the reconciliation account

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Configuring-Accounts-for-Automatic-Management.htm#Reconcil>

upvoted 7 times

  **abiurrunc** Most Recent 7 months, 1 week ago

To ensure that password reset with the reconcile account is performed each time instead of a change when an account is unable to change its own password in CyberArk, you should:

- A. Set the parameter RAllowManualReconciliation to Yes.

By enabling this parameter, you allow manual reconciliation to take place when a password is detected as unsynchronized. This ensures that the passwords are resynchronized automatically without any manual intervention. The reconciliation account password specified for this purpose will be used to reset the unsynchronized password

upvoted 2 times

  **acello** 1 year, 1 month ago

**Selected Answer: A**

Answer is A because it's the only way to reconcile the accounts, the other options don't provide that feature

upvoted 3 times

  **Jakub4444** 12 months ago

B is correct

upvoted 4 times

  **Jabelo** 11 months ago

B is correct


upvoted 3 times

  **miky\_Cissp** 1 year, 2 months ago

- B. Set the parameter ChangePasswordInResetMade to Yes.

This parameter ensures that when a password reset is performed with the reconcile account, it will be done each time instead of a change when the account is unable to change its own password

upvoted 4 times

  **brossva** 1 year, 6 months ago

**Selected Answer: B**



B is correct

upvoted 4 times

  **brossva** 1 year, 6 months ago

A should be correct

upvoted 1 times

  **Takumi** 1 year, 8 months ago

**Selected Answer: A**

The answer is A

RCAllowManualReconciliation: Whether or not passwords will be reconciled when a user initiates the procedure manually through the PVWA interface.

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASREF/Automatic%20Password%20Management%20-%20Password%20Reconciliationpath=Administrator%7CReferences%7CConfigure%20the%20system%20through%20PVWA%7CPlatform%20properties%7CAutomatic%20Password%20Ma>

upvoted 1 times

  **penuelaandy** 1 year, 9 months ago

**Selected Answer: B**

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Configuring-Accounts-for-Automatic-Management.htm#Reconcilepasswords>

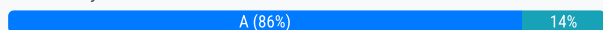
upvoted 4 times

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

- A. PVWAMonitor
- B. ReportUsers
- C. PVWAreports
- D. Operators

**Suggested Answer: A**

Community vote distribution



**Remy** Highly Voted 1 year, 3 months ago

**Selected Answer: A**

PVWAMonitor : The group that users who are authorized to generate reports must belong to.

PVWAreports : The name of the default Safe where generated reports will be saved.

<https://docs.cyberark.com/PAS/13.2/en/Content/PASREF/Report%20Generation.htm>

upvoted 7 times

**JM\_Olympus** Most Recent 7 months, 1 week ago

A:

<https://docs.cyberark.com/pam-self-hosted/13.2/en/Content/PASIMP/ReportsInPVWA.htm?Highlight=pvwamonitor>

By default, this is the PVWAMonitor group.

upvoted 2 times

**abiurrunc** 7 months, 1 week ago

**Selected Answer: A**

Answer is A

In a default CyberArk installation, to view the "reports" page in PVWA (Privileged Web Access), a user must be a member of the PVWAMonitor group1.

This group is specifically configured to allow users access to the reports section.

Remember that the PVWAMonitor group provides the necessary permissions for viewing and managing reports within the CyberArk environment.

upvoted 1 times

**miky\_Cissp** 1 year, 2 months ago

A

ManageReportsGroup

Description The group that users who are authorized to generate reports must belong to. This parameter is required. Acceptable Values

Acceptable Values Group name

Default Value PVWAMonitor

upvoted 1 times

**uswarrior** 1 year, 5 months ago

PVWA monitor is the right answer. Tested it.

upvoted 2 times

**brossva** 1 year, 6 months ago

A is correct

upvoted 1 times

**loucard** 1 year, 8 months ago

**Selected Answer: A**


ManageReportsGroup must be PVWAMonitor. Option A is the default safe name.

upvoted 4 times

**loucard** 1 year, 8 months ago

Option C is the default safe name

upvoted 1 times

  **penuelaandy** 1 year, 9 months ago

**Selected Answer: C**

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASREF/Report%20Generation.htm>

upvoted 2 times

  **penuelaandy** 1 year, 9 months ago

Option A

upvoted 2 times

Your organization requires all passwords be rotated every 90 days.  
Where can you set this requirement?

- A. Master Policy
- B. Safe Templates
- C. PVWAConfig.xml
- D. Platform Configuration

**Suggested Answer: A**

*Community vote distribution*

A (100%)

 **penuelaandy** Highly Voted 2 years, 3 months ago

**Selected Answer: A**

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Working-with-Master-Policy-Rules.htm#PasswordManagement>  
upvoted 8 times

 **Imdroc** Most Recent 9 months, 3 weeks ago

**Selected Answer: A**

The Answer is: A  
upvoted 1 times



According to CyberArk, which issues most commonly cause installed components to display as disconnected in the System Health Dashboard? (Choose two.)

- A. network instabilities/outages
- B. vault license expiry
- C. credential de-sync
- D. browser compatibility issues
- E. installed location file corruption

**Suggested Answer: AC**

Community vote distribution

AC (100%)


 **penuelaandy** Highly Voted 2 years, 3 months ago

**Selected Answer: AC**

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/SystemHealth.htm?](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/SystemHealth.htm?tocpath=Administrator%7C_____5#Restorecomponentconnectivity)

[tocpath=Administrator%7C\\_\\_\\_\\_\\_5#Restorecomponentconnectivity](#)


upvoted 9 times

 **Imdroc** Most Recent 9 months, 3 weeks ago

**Selected Answer: AC**

Answer is: AC

upvoted 1 times

 **abiurrunc** 1 year, 1 month ago

In a default CyberArk installation, the most common issues that cause installed components to display as disconnected in the System Health Dashboard are:

A - Network Instabilities/Outages: If there are network connectivity issues between the components (such as PVWA, PSM, or PTA) and the Vault, it can result in disconnection status.

C - Credential De-Sync: When the credentials used for communication between components become unsynchronized or invalid, the components may appear disconnected.

upvoted 1 times

 **brossva** 2 years ago

AC is correct

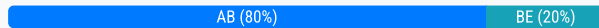
upvoted 3 times

Where can reconcile and/or logon accounts be linked to an account? (Choose two.)

- A. account settings
- B. platform settings
- C. master policy
- D. safe settings
- E. service account settings

**Suggested Answer: AB**

Community vote distribution



**Takumi** Highly Voted 2 years, 2 months ago

**Selected Answer: AB**

The answer is AB.

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.4/en/Content/PASIMP/Linked-PAS-Accounts.htm>

upvoted 11 times

**loucard** 2 years, 2 months ago

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Linked-PAS-Accounts.htm#\\_Ref152677694](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Linked-PAS-Accounts.htm#_Ref152677694)

upvoted 2 times

**Imdroc** Most Recent 9 months, 3 weeks ago

**Selected Answer: AB**

Answer is: AB

upvoted 1 times

**miky\_Cissp** 1 year, 8 months ago

AB

Logon account: This is an account that contains the password required to log on to a remote machine in order to perform a task using the regular account. A common use case for using a logon account is managing root accounts on a Unix system. The logon account can be defined on the target account level or on the platform level, making it available to all accounts associated with the platform.

Reconcile account: This account contains the password used in reconciliation processes. The reconcile account can also be defined on the target account level or on the platform level, making it available to all accounts associated with the platform.

upvoted 4 times

**brossva** 2 years ago

AB is correct

upvoted 1 times

**brossva** 2 years ago

AB is correct

upvoted 1 times

**penuelaandy** 2 years, 3 months ago

**Selected Answer: BE**

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Linked-Accounts.htm>

upvoted 3 times

You are running a "Privileged Accounts Inventory" Report through the Reports page in PVWA on a specific safe. To show complete account inventory information, which permission/s are needed on that safe?

- A. List Accounts, View Safe Members
- B. Manage Safe Owners
- C. List Accounts, Access Safe without confirmation
- D. Manage Safe, View Audit

**Suggested Answer: A**

*Community vote distribution*

A (100%)

penuelaandy **Highly Voted** 2 years, 3 months ago

**Selected Answer: A**

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/ReportsInPVWA.htm>  
upvoted 5 times

Imdroc **Most Recent** 9 months, 2 weeks ago

**Selected Answer: A**

Answer is A  
upvoted 1 times

Imdroc 9 months, 3 weeks ago

Answer is: A  
upvoted 1 times

dominicx 1 year, 11 months ago

**Selected Answer: A**

A List account and View Safe members  
upvoted 4 times

brossva 2 years ago

A is correct  
upvoted 2 times

Which dependent accounts does the CPM support out-of-the-box? (Choose three.)

- A. Solaris Configuration file
- B. Windows Services
- C. Windows Scheduled Tasks
- D. Windows DCOM Applications
- E. Windows Registry
- F. Key Tab file

**Suggested Answer:** BCE

Community vote distribution

BCE (100%)

  **penuelaandy** Highly Voted 2 years, 3 months ago

**Selected Answer:** BCE

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/Landing%20Pages/LPServicePlugins.htm>



upvoted 13 times

  **Imdroc** Most Recent 9 months, 2 weeks ago

**Selected Answer:** BCE

Answer is: BCE

upvoted 1 times

  **Imdroc** 9 months, 3 weeks ago

Answer is: BCE

upvoted 1 times

  **brossva** 2 years ago

BCE is correct

upvoted 3 times

A password compliance audit found:

- 1) One-time password access of 20 domain accounts that are members of Domain Admins group in Active Directory are not being enforced.
- 2) All the sessions of connecting to domain controllers are not being recorded by CyberArk PSM.

What should you do to address these findings?

- A. Edit the Master Policy and add two policy exceptions: enable "Enforce one-time password access", enable "Record and save session activity".
- B. Edit safe properties and add two policy exceptions: enable "Enforce one-time password access", enable "Record and save session activity".
- C. Edit CPM Settings and add two policy exceptions: enable "Enforce one-time password access", enable "Record and save session activity".
- D. Contact the Windows Administrators and request them to add two policy exceptions at Active Directory Level: enable "Enforce one-time password access", enable "Record and save session activity".

**Suggested Answer: A**

*Community vote distribution*

A (100%)

🗳️ 👤 **f0f4e87** 3 days, 16 hours ago

**Selected Answer: A**

These are all set under the Master Policy.

upvoted 1 times

🗳️ 👤 **Mattia8** 9 months, 2 weeks ago

**Selected Answer: A**

Absolutely A

upvoted 2 times

🗳️ 👤 **Imdroc** 9 months, 3 weeks ago

**Selected Answer: A**

Answer is: A

upvoted 2 times

🗳️ 👤 **brossva** 2 years ago

A is correct

upvoted 4 times

🗳️ 👤 **penuelaandy** 2 years, 3 months ago

**Selected Answer: A**

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Working-with-Master-Policy-Rules.htm?](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Working-with-Master-Policy-Rules.htm?tocpath=Administrator%7CPrivileged%20Accounts%7CSecurity%20Policy%7C_____2#MasterPolicyrules)

[tocpath=Administrator%7CPrivileged%20Accounts%7CSecurity%20Policy%7C\\_\\_\\_\\_\\_2#MasterPolicyrules](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Working-with-Master-Policy-Rules.htm?tocpath=Administrator%7CPrivileged%20Accounts%7CSecurity%20Policy%7C_____2#MasterPolicyrules)

upvoted 3 times

If PTA is integrated with a supported SIEM solution, which detection becomes available?


- A. unmanaged privileged account
- B. privileged access to the Vault during irregular days
- C. riskySPN
- D. exposed credentials

**Suggested Answer: A**

Community vote distribution

A (92%)


8%

 **penuelaandy** Highly Voted 2 years, 3 months ago

**Selected Answer: A**


<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PTA/What-Does-PTA-Detect.htm>

upvoted 7 times

 **TacoTeo** 2 years, 2 months ago

I believe it is exposed credentials, Unmanaged Privileged accounts is supported through the Vault.

upvoted 2 times

 **loucard** 2 years, 2 months ago

Unmanged privileged accounts is supported for both ( Vault and logs)

upvoted 1 times

 **Imdroc** Most Recent 9 months, 1 week ago

**Selected Answer: D**

Sorry, answer is D


upvoted 1 times

 **Prasant\_Shanmugasekar** 1 year, 6 months ago

**Selected Answer: A**

SIEM is required for Unmanaged privileged account and Suspected Credential Theft

upvoted 2 times

 **Remy** 1 year, 9 months ago

**Selected Answer: A**

Unmanaged privileged account : SIEM / Unix / AWS / Azure + Vault

Exposed credentials : Network Sensor or PTA Windows Agent

[https://docs.cyberark.com/PAS/13.0/en/Content/PTA/What-Does-PTA-Detect.htm?](https://docs.cyberark.com/PAS/13.0/en/Content/PTA/What-Does-PTA-Detect.htm?searchString=&from=0&sortBy=_score&orderBy=desc&pageNo=1&aggregations=%5B%5D&uid=0d99d231-d8b2-11ea-8f5c-0242ac120009&resultsPerPage=10&exactPhrase=&withOneOrMore=&withoutTheWords=&pageSize=10&language=en&state=1&suCaseCreate=false)

[searchString=&from=0&sortBy=\\_score&orderBy=desc&pageNo=1&aggregations=%5B%5D&uid=0d99d231-d8b2-11ea-8f5c-](https://docs.cyberark.com/PAS/13.0/en/Content/PTA/What-Does-PTA-Detect.htm?searchString=&from=0&sortBy=_score&orderBy=desc&pageNo=1&aggregations=%5B%5D&uid=0d99d231-d8b2-11ea-8f5c-0242ac120009&resultsPerPage=10&exactPhrase=&withOneOrMore=&withoutTheWords=&pageSize=10&language=en&state=1&suCaseCreate=false)

[0242ac120009&resultsPerPage=10&exactPhrase=&withOneOrMore=&withoutTheWords=&pageSize=10&language=en&state=1&suCaseCreate=false](https://docs.cyberark.com/PAS/13.0/en/Content/PTA/What-Does-PTA-Detect.htm?searchString=&from=0&sortBy=_score&orderBy=desc&pageNo=1&aggregations=%5B%5D&uid=0d99d231-d8b2-11ea-8f5c-0242ac120009&resultsPerPage=10&exactPhrase=&withOneOrMore=&withoutTheWords=&pageSize=10&language=en&state=1&suCaseCreate=false)

upvoted 3 times

 **umesh02** 2 years, 3 months ago

A

riskySPN is in case of AD

upvoted 1 times

Which change could CyberArk make to the REST API that could cause existing scripts to fail?

- A. adding optional parameters in the request
- B. adding additional REST methods
- C. removing parameters
- D. returning additional values in the response

**Suggested Answer:** C

*Community vote distribution*

C (100%)

 **penuelaandy** Highly Voted 2 years, 3 months ago

**Selected Answer:** C

[https://docs.cyberark.com/Product-](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/WebServices/Implementing%20Privileged%20Account%20Security%20Web%20Services%20.htm)

[Doc/OnlineHelp/PAS/13.0/en/Content/WebServices/Implementing%20Privileged%20Account%20Security%20Web%20Services%20.htm](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/WebServices/Implementing%20Privileged%20Account%20Security%20Web%20Services%20.htm)

upvoted 10 times

 **Imdroc** Most Recent 9 months, 2 weeks ago

**Selected Answer:** C

Answer is: C

upvoted 1 times

 **Imdroc** 9 months, 3 weeks ago

Answer is: C

upvoted 1 times

You created a new platform by duplicating the out-of-box Linux through the SSH platform.  
Without any change, which Text Recorder Type(s) will the new platform support? (Choose two.)

- A. SSH Text Recorder
- B. Universal Keystrokes Text Recorder
- C. Events Text Recorder
- D. SQL Text Recorder
- E. Telnet Commands Text Recorder

**Suggested Answer:** AB

*Community vote distribution*

AB (100%)

 **penuelaandy** Highly Voted 2 years, 3 months ago

**Selected Answer:** AB

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Configuring-Recordings-and-Audits-in-PSM.htm#CustomizerecordingsinPSM>

upvoted 9 times

 **Imdroc** Most Recent 9 months, 3 weeks ago

**Selected Answer:** AB

Answer is: AB

upvoted 1 times




You are creating a Dual Control workflow for a team's safe.  
Which safe permissions must you grant to the Approvers group?

- A. List accounts, Authorize account request
- B. Retrieve accounts, Access Safe without confirmation
- C. Retrieve accounts, Authorize account request
- D. List accounts, Unlock accounts

**Suggested Answer: A**

*Community vote distribution*

A (100%)

  **penuelaandy** Highly Voted 2 years, 3 months ago

**Selected Answer: A**

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/NewUI/NewUI-Review-requests.htm#Createanauthorizeduser>

Approvers no need to see the passwords

upvoted 9 times

  **Imdroc** Most Recent 9 months, 3 weeks ago

**Selected Answer: A**

Answer is: A

upvoted 1 times

  **2995142** 1 year, 2 months ago

A is correct answer

upvoted 1 times

  **Lolbando** 1 year, 5 months ago

**Selected Answer: A**

A is correcto.

upvoted 2 times

  **uswarrior** 1 year, 11 months ago

Correct answer is A.

upvoted 1 times

  **brossva** 2 years ago

A is correct

upvoted 2 times

In addition to add accounts and update account contents, which additional permission on the safe is required to add a single account?

- A. Upload Accounts Properties
- B. Rename Accounts
- C. Update Account Properties
- D. Manage Safe

**Suggested Answer:** C

Community vote distribution

C (100%)

🗳️ 👤 **Imdroc** 9 months, 3 weeks ago

**Selected Answer:** C

Answer is C

upvoted 1 times

🗳️ 👤 **hyuraki** 1 year, 8 months ago

**Selected Answer:** C

[https://docs.cyberark.com/PAS/Latest/en/Content/PASIMP/Adding-Accounts.htm?](https://docs.cyberark.com/PAS/Latest/en/Content/PASIMP/Adding-Accounts.htm?tocpath=End%20user%7CPrivileged%20accounts%7CClassic%20Interface%7CAccount%20Management%7C_____1)

[tocpath=End%20user%7CPrivileged%20accounts%7CClassic%20Interface%7CAccount%20Management%7C\\_\\_\\_\\_\\_1](https://docs.cyberark.com/PAS/Latest/en/Content/PASIMP/Adding-Accounts.htm?tocpath=End%20user%7CPrivileged%20accounts%7CClassic%20Interface%7CAccount%20Management%7C_____1)

Click Add Account; the Add Account page appears.

This button will only be displayed if you have Add accounts, Update password value, or Update password properties authorization in at least one Safe.

upvoted 4 times

🗳️ 👤 **Takumi** 2 years, 2 months ago

**Selected Answer:** C

the answer is C. <https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Editing-Account-Properties.htm>

upvoted 1 times

🗳️ 👤 **penuelaandy** 2 years, 3 months ago

**Selected Answer:** C

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/NewUI/NewUI-Add-accounts-in-PVWA.htm>

upvoted 2 times

You want to give a newly-created group rights to review security events under the Security pane. You also want to be able to update the status of these events.



Where must you update the group to allow this?

- A. in the PTAAuthorizationGroups parameter, found in Administration > Options > PTA
- B. in the PTAAuthorizationGroups parameter, found in Administration > Options > General
- C. in the SecurityEventsAuthorizationGroups parameter, found in Administration > Security > Options
- D. in the SecurityEventsFeedAuthorizationGroups parameter, found in Administration > Options > General

**Suggested Answer: D**

*Community vote distribution*

D (100%)

  **penuelaandy** Highly Voted 2 years, 3 months ago

**Selected Answer: D**

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PTA/Security-Events.htm?](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PTA/Security-Events.htm?TocPath=End%20User%7CSecurity%20Events%7C_____2#Permissions)

[TocPath=End%20User%7CSecurity%20Events%7C\\_\\_\\_\\_\\_2#Permissions](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PTA/Security-Events.htm?TocPath=End%20User%7CSecurity%20Events%7C_____2#Permissions)

upvoted 8 times

  **Imdroc** Most Recent 9 months, 2 weeks ago

**Selected Answer: D**


Answer is: D

upvoted 1 times

  **Imdroc** 9 months, 3 weeks ago

Answer is: D

upvoted 1 times

  **JM\_Olympus** 1 year, 1 month ago

Answer is D.

<https://docs.cyberark.com/pam-self-hosted/Latest/en/Content/PTA/Security-Events.htm?Highlight=securityeventsfeedauthorizationGroups#>

upvoted 1 times

  **brossva** 2 years ago

D is correct

upvoted 3 times

What is required to manage loosely connected devices?

- A. PSM for SSH
- B. EPM
- C. PSM
- D. PTA

**Suggested Answer:** B

Community vote distribution

B (100%)

 **penuelaandy** Highly Voted 1 year, 3 months ago

**Selected Answer:** B

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/LooselyConnectedDevices.htm>

upvoted 8 times

 **miky\_Cissp** Most Recent 8 months, 1 week ago

B

PAM - Self-Hosted uses CyberArk Endpoint Privilege Manager (EPM) to rotate credentials of accounts on Windows and macOS devices that are not always connected to the enterprise network. These devices are called loosely connected devices.

upvoted 3 times


Your organization has a requirement to allow only one user to "check out passwords" and connect through the PSM securely. What needs to be configured in the Master policy to ensure this will happen?

- A. Enforce check-in/check-out exclusive access = active; Require privileged session monitoring and isolation = active
- B. Enforce check-in/check-out exclusive access = inactive; Require privileged session monitoring and isolation = inactive
- C. Enforce check-in/check-out exclusive access = inactive; Record and save session activity = active
- D. Enforce check-in/check-out exclusive access = active; Record and save session activity = inactive

**Suggested Answer: A**

*Community vote distribution*

A (100%)

 **penuelaandy** Highly Voted 2 years, 3 months ago

**Selected Answer: A**

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Accounts-Check-out-and-Check-in.htm#\\_Ref180481442](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Accounts-Check-out-and-Check-in.htm#_Ref180481442)  
upvoted 5 times

 **Imdroc** Most Recent 9 months, 3 weeks ago

**Selected Answer: A**

Answer is: A

upvoted 1 times

When should vault keys be rotated?

- A. when it is copied to file systems outside the vault
- B. annually
- C. whenever a CyberArk user leaves the organization
- D. when migrating to a new data center

**Suggested Answer: A**

*Community vote distribution*

A (100%)

  **TacoTeo** Highly Voted 1 year, 8 months ago

The answer is A.

<https://cyberark-customers.force.com/s/article/What-risks-and-considerations-should-be-made-for-Vault-key-management>

What does the organization consider a compromise of encryption keys?

- Unknown chain of custody
- Keys copied to filesystems outside of the vault including network shares
- Copies being made without knowledge

upvoted 10 times

  **2995142** Most Recent 8 months ago

Answer is A

upvoted 2 times

  **Prasant\_Shanmugasekar** 1 year ago

Selected Answer: A

Option A

upvoted 2 times

  **ExamsAE** 1 year, 6 months ago

Selected Answer: A

<https://cyberark-customers.force.com/s/article/What-risks-and-considerations-should-be-made-for-Vault-key-management>

upvoted 4 times

Where can PTA be configured to send alerts? (Choose two.)

- A. SIEM
- B. Email
- C. Google Analytics
- D. EVD
- E. PAReplicate

**Suggested Answer:** AB

Community vote distribution

AB (100%)

 **penuelaandy** Highly Voted 2 years, 3 months ago

**Selected Answer:** AB

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PTA/Outbound-Sending-PTA-syslog-Records.htm?](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PTA/Outbound-Sending-PTA-syslog-Records.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Threat%20Analytics%7CConfigure%20Privileged%20Threat%20Analytics%7CSend%20PTA%20Data%3B)

[tocpath=Administrator%7CComponents%7CPrivileged%20Threat%20Analytics%7CConfigure%20Privileged%20Threat%20Analytics%7CSend%20PTA%20Data%3B">tocpath=Administrator%7CComponents%7CPrivileged%20Threat%20Analytics%7CConfigure%20Privileged%20Threat%20Analytics%7CSend%20PTA%20Data%3B](#)  
upvoted 5 times

 **Imdroc** Most Recent 9 months, 3 weeks ago

**Selected Answer:** AB

Answer is: AB

upvoted 1 times


In your organization the "click to connect" button is not active by default.  
How can this feature be activated?

- A. Policies > Master Policy > Allow EPV transparent connections > Inactive
- B. Policies > Master Policy > Session Management > Require privileged session monitoring and isolation > Add Exception
- C. Policies > Master Policy > Allow EPV transparent connections > Active
- D. Policies > Master Policy > Password Management

**Suggested Answer: C**


Community vote distribution

C (100%)

 **penuelaandy** Highly Voted 2 years, 3 months ago

**Selected Answer: C**

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Working-with-Master-Policy-Rules.htm#PrivilegedAccessWorkflows>  
upvoted 6 times

 **Imdroc** Most Recent 9 months, 3 weeks ago

**Selected Answer: C**

Answer is: C  
upvoted 1 times

 **miky\_Cissp** 1 year, 8 months ago

C  
Allow EPV transparent connections ("Click to connect"): Users can connect to remote devices without needing to know or specify the required password. This prevents the password from being exposed to the user and maintains productivity as the user does not have to open a login session and then copy and paste the password credentials into it. In addition, advanced settings define whether or not users are permitted to view passwords. This enforces strong authentication for accessing managed devices and restricts user access to passwords according to granular access control. By default, this rule is active  
upvoted 2 times



What are the mandatory fields when onboarding from Pending Accounts? (Choose two.)

- A. Address
- B. Safe
- C. Account Description
- D. Platform
- E. CPM

**Suggested Answer:** *BD*

*Community vote distribution*

BD (100%)

🗳️ 👤 **Imdroc** 9 months, 3 weeks ago

**Selected Answer:** BD

Answer is: BD

upvoted 1 times

🗳️ 👤 **KHKH2021** 1 year, 10 months ago

BD is correct

upvoted 3 times

🗳️ 👤 **uswarrior** 1 year, 11 months ago

B and D.

upvoted 2 times

🗳️ 👤 **brossva** 2 years ago

BD is correct

upvoted 2 times

🗳️ 👤 **penuelaandy** 2 years, 3 months ago

**Selected Answer:** BD

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/automatic\\_onboarding\\_rules.htm#Rule](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/automatic_onboarding_rules.htm#Rule)

upvoted 4 times

DRAG DROP -

Match each permission to where it can be found.


Add Accounts	Drag answer here	Vault
Initiate CPM account management operations	Drag answer here	
Add/Update Users	Drag answer here	
Add Safes	Drag answer here	
		Safe

**Suggested Answer:** Add Accounts - Vault -

Initiate CPM account management operations - Vault

Add/Update Users - Safe -

Add Safes - Safe

 **sebschter** Highly Voted 1 year, 9 months ago

It is

Add Accounts --> Safe

Initiate CPM account management operations -> Safe

Add/Update Users -> Vault

Add Safes -> Vault

upvoted 25 times

 **2995142** Most Recent 8 months, 1 week ago


Add Accounts --> Safe

Initiate CPM account management operations -> Safe

Add/Update Users -> Vault

Add Safes -> Vault

upvoted 1 times

 **Jabelo** 10 months, 3 weeks ago

Add Accounts --> Safe


Initiate CPM Password management operations => Safe

Add/Update Users => Vault

Add Safes => Vault

<https://cyberark.my.site.com/s/article/Safe-Authorizations-and-what-they-mean>

upvoted 3 times

 **miky\_Cissp** 1 year, 2 months ago

Add Accounts and Initiate CPM account management operations are permissions found at the Safe level.

Add/Update Users and Add Safes are permissions found at the Vault level.

upvoted 4 times

 **uswarrior** 1 year, 5 months ago



Add Accounts --> Safe

Initiate CPM account management operations -> Safe

Add/Update Users -> Vault

Add Safes -> Vault

upvoted 2 times

  **Takumi** 1 year, 8 months ago

My answer:


Add Accounts -> Vault

Initiate CPM account management operations -> Vault

Add/Update Users -> Safe

Add Safes -> Vault

upvoted 1 times

  **penuelaandy** 1 year, 9 months ago

Correct

upvoted 1 times

Which accounts can be selected for use in the Windows discovery process? (Choose two.)

- A. an account stored in the Vault
- B. an account specified by the user
- C. the Vault Administrator
- D. any user with Auditor membership
- E. the PasswordManager user

**Suggested Answer:** AB

Community vote distribution

AB (100%)

 **miky\_Cissp**  1 year, 8 months ago

AB

Select the user who will perform the scan. Either select an account from the Vault or manually specify a user and password:

Select from Vault – Select a Vault account to run the scan. This is recommended for recurrent scans.

Click Click to select an account from the Vault; a list of Vault accounts appears. These are all domain accounts in the specified domain  
upvoted 6 times

 **penuelaandy**  2 years, 3 months ago

**Selected Answer:** AB

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Managing-Discovery-Processes.htm#Creatediscoveryprocesses>  
upvoted 6 times

 **Imdroc**  9 months, 3 weeks ago

**Selected Answer:** AB

Answer is: AB

upvoted 1 times

You are concerned about the Windows Domain password changes occurring during business hours.  
Which settings must be updated to ensure passwords are only rotated outside of business hours?

- A. In the platform policy -  
Automatic Password Management > Password Change > ToHour & FromHour
- B. in the Master Policy  
Account Change Window > ToHour & From Hour
- C. Administration Settings -  
CPM Settings > ToHour & FromHour
- D. On each individual account -  
Edit > Advanced > ToHour & FromHour

**Suggested Answer: A**

*Community vote distribution*

A (100%)

  **penuelaandy** Highly Voted 2 years, 3 months ago


**Selected Answer: A**

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASREF/Automatic%20Password%20Management%20-%20Password%20Change.tocpath=Administrator%7CReferences%7CConfigure%20the%20system%20through%20PVWA%7CPlatform%20properties%7CAutomatic%20Password%20Ma>  
upvoted 7 times

  **Imdroc** Most Recent 9 months, 3 weeks ago

**Selected Answer: A**

Answer is: A  
upvoted 1 times

  **KHKH2021** 1 year, 10 months ago

A is correct  
upvoted 2 times

The Privileged Access Management solution provides an out-of-the-box target platform to manage SSH keys, called UNIX Via SSH Keys. How are these keys managed?

- A. CyberArk stores Private keys in the Vault and updates Public keys on target systems.
- B. CyberArk stores Public keys in the Vault and updates Private keys on target systems.
- C. CyberArk does not store Public or Private keys and instead uses a reconcile account to create keys on demand.
- D. CyberArk stores both Private and Public keys and can update target systems with either key.

**Suggested Answer: A**

Community vote distribution

A (100%)

🗳️ 👤 **Imdroc** 9 months, 3 weeks ago

**Selected Answer: A**

Answer is: A

upvoted 1 times

🗳️ 👤 **2995142** 1 year, 2 months ago

A, this has been clearly mentioned in PAM Admin training

upvoted 1 times

🗳️ 👤 **Jakub4444** 1 year, 5 months ago

**Selected Answer: A**

[https://docs.cyberark.com/PAS/Latest/en/Content/SSHKM/Protecting%20Securing.htm?](https://docs.cyberark.com/PAS/Latest/en/Content/SSHKM/Protecting%20Securing.htm?tocpath=Administrator%7CComponents%7CSSH%C2%A0Key%20Manager%7C____3)

[tocpath=Administrator%7CComponents%7CSSH%C2%A0Key%20Manager%7C\\_\\_\\_\\_3](https://docs.cyberark.com/PAS/Latest/en/Content/SSHKM/Protecting%20Securing.htm?tocpath=Administrator%7CComponents%7CSSH%C2%A0Key%20Manager%7C____3)

upvoted 1 times

🗳️ 👤 **hyuraki** 1 year, 8 months ago

**Selected Answer: A**

SSH Key Manager can automatically reconcile the SSH Key pair and resynchronize the private SSH Key stored in the Vault with all public SSH Keys on the target servers

upvoted 1 times

🗳️ 👤 **penuelaandy** 2 years, 3 months ago

**Selected Answer: A**

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/SSHKM/Managing%20SSH%20Keys.htm?](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/SSHKM/Managing%20SSH%20Keys.htm?TocPath=Administrator%7CComponents%7CSSH%C2%A0Key%20Manager%7C____5)

[TocPath=Administrator%7CComponents%7CSSH%C2%A0Key%20Manager%7C\\_\\_\\_\\_5](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/SSHKM/Managing%20SSH%20Keys.htm?TocPath=Administrator%7CComponents%7CSSH%C2%A0Key%20Manager%7C____5)

upvoted 4 times

The Active Directory User configured for Windows Discovery needs which permission(s) or membership?

- A. Member of Domain Admin Group
- B. Member of LDAP Admin Group
- C. Read and Write Permissions
- D. Read Only Permissions

**Suggested Answer:** D

Community vote distribution

D (100%)

 **penuelaandy** Highly Voted 2 years, 3 months ago

**Selected Answer: D**

This user requires read permissions in the OU and all sub-OU's to scan.


<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Managing-Discovery-Processes.htm#Creatediscoveryprocesses>  
upvoted 7 times

 **Imdroc** Most Recent 9 months, 3 weeks ago

**Selected Answer: D**

Answer is: D

upvoted 1 times

 **umesh02** 2 years, 3 months ago

D is the correct answer

upvoted 1 times

Which command generates a full backup of the Vault?

- A. PAReplicate.exe Vault.ini /LogonFromFile user.ini /FullBackup
- B. PAPreBackup.exe C:\PrivateArk\Server\Conf\Vault.ini Backup/Asdf1234 /full
- C. PARestore.exe PADR ini /LogonFromFile vault.ini /FullBackup
- D. CAVaultManager.exe RecoverBackupFiles /BackupPoolName BkpSvr1

**Suggested Answer: A**

*Community vote distribution*

A (100%)

 **penuelaandy** Highly Voted 2 years, 3 months ago

**Selected Answer: A**

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/Installing-the-Vault-Backup-Utility.htm#PAReplicate>  
upvoted 5 times

 **Imdroc** Most Recent 9 months, 3 weeks ago

**Selected Answer: A**

Answer is: A

upvoted 1 times