Before the hardening process, your customer identified a PSM Universal Connector executable that will be required to run on the PSM. Which file should you update to allow this to run?

A. PSMConfigureAppLocker.xml

B. PSMHardening.xml

C. PSMAppConfig.xml

D. PSMConfigureHardening.xml

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

---

🗖 👤 **bumika** 5 months ago

Selected Answer: A

answer is A

upvoted 2 times

🗖 👤 **bumika** 5 months ago

The correct answer is A. AppLocker rules influence which executables can run on the PSM servers. You must modify PSMConfigureAppLocker.xml when you need to run Chrome instead of Internet Explorer or support Java to run the web-based SSH client on the PSM server.

upvoted 1 times

🗖 👤 **dru0pa** 1 year, 5 months ago

Selected Answer: A

answer is A

upvoted 2 times

🗖 👤 **dru0pa** 1 year, 5 months ago

answer is A

PSMConfigureAppLocker.xml is the file that is edited to make changes to the Microsoft AppLocker

upvoted 1 times

As Vault Admin, you have been asked to configure LDAP authentication for your organization's CyberArk users. Which permissions do you need to complete this task?

A. Audit Users and Add Network Areas

B. Audit Users and Manage Directory Mapping

C. Audit Users and Add/Update Users

D. Audit Users and Activate Users

**Correct Answer:** *B*

*Community vote distribution*

B (100%)

---

☐ 👤 **bumika** 5 months ago

Selected Answer: B

When you configure a new LDAP authentication scheme it is necessary to connect basic PAM roles to proper LDAP groups - it is directory mapping.

upvoted 2 times

☐ 👤 **dru0pa** 1 year, 5 months ago

Selected Answer: B

Answer is B

upvoted 3 times

☐ 👤 **dru0pa** 1 year, 5 months ago

Answer is B

upvoted 2 times

In the screenshot displayed, you just configured the usage in CyberArk and want to update its password.

What is the least intrusive way to accomplish this?

**Required Properties:**
Address:                webserver1.lab.local
File Path:               C:\inetpub\wwwroot\web.config
XML Element:             /configuration/appSettings/add[@key="PASSWORD"]
Connection Type:         Windows File Sharing                    ▼
**Optional Properties:**
☐ Port:
☑ XML Attribute:         value
☑ Password Regex:        (.*)
☐ Backup Password File:  [Select]                                ▼
☐ Usage Display Name:

☐ Disable automatic management for this account
    Reason:   No Reason

   Save        Cancel

A. Use the "change" button on the usage's details page

B. Use the "change" button on the parent account's details page

C. Use the "sync" button on the usage's details page.

D. Use the "reconcile" button on the parent account's details page.

**Correct Answer:** *D*

*Community vote distribution*

| D (50%) | A (33%) | B (17%) |
| --- | --- | --- |

---

👤 **Sathesh** 1 week, 5 days ago

Selected Answer: B

B would be the right option, when the parent account password is correct not necessary to go for reconcile. Either it's Change or reconcile action when the password of parent account is changed CPM tries to update all the configured dependencies.

upvoted 1 times

---

👤 **144d6dd** 8 months, 2 weeks ago

Selected Answer: D

D. Use the "reconcile" button on the parent account's details page.

upvoted 1 times

---

👤 **bumika** 11 months ago

Selected Answer: D

The correct answer is D. You can initiate actions on the parent account's page. "Change" is too intrusive because it modifies the password on the account. "Reconcile" provides the refresh on all occurrences.

upvoted 2 times

---

👤 **dru0pa** 1 year, 11 months ago

Selected Answer: A

answer is a

upvoted 2 times

DRAG DROP -

Arrange the steps to complete CPM Hardening for Out-of-Domain Deployment in the correct sequence.

**Actions**

Open Powershell as Administrator and run the script

Review the script log called HardeningScript log

Locate the CPM_Hardening.ps1 script in the installation media

Review the script log called CYBRHardeningsecedit.log

**Answer Area**

>

<

**Correct Answer:** *Locate the CPM_Hardnering.ps1 script in the installation media*

*Review the Script log call hardeningscript Log*

*Review the script log called CYBRHardneringsecedit.log*

*Open PowerShell as administrator and run the script*

---

👤 **M4rt1n0** 3 months, 3 weeks ago

For me, and according to CyberArk Documentation, the steps must be in this order:

1-Locate the CPM_Hardnering.ps1 script in the installation media

2-Open PowerShell as administrator and run the script

3-Review the Script log call hardeningscript Log

4-Review the script log called CYBRHardneringsecedit.log

upvoted 4 times

👤 **dru0pa** 11 months, 4 weeks ago

Locate the CPM_Hardnering.ps1 script in the installation media

Open PowerShell as administrator and run the script

Review the script log called CYBRHardneringsecedit.log

upvoted 2 times

Which certificate type do you need to configure the vault for LDAP over SSL?

A. the CA Certificate that signed the certificate used by the External Directory

B. a CA signed Certificate for the Vault server

C. a CA signed Certificate for the PVWA server

D. a self-signed Certificate for the Vault

**Correct Answer:** *A*

*Community vote distribution*

A (83%) | B (17%)

---

 **rayjohn28** 8 months ago

**Selected Answer: A**

A is the correct answer

upvoted 1 times

 **144d6dd** 8 months, 3 weeks ago

**Selected Answer: A**

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).

ADAC

upvoted 1 times

 **bumika** 11 months ago

**Selected Answer: A**

The Vault application must validate the LDAPS certificate, so it needs to accept the CA certificate as a trusted issuer.

upvoted 1 times

 **M4rt1n0** 1 year, 3 months ago

**Selected Answer: A**

the answer is A "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)." Source: CyberArk Documentation

upvoted 2 times

 **jconcha** 1 year, 7 months ago

the answer is A https://docs.cyberark.com/PAS/12.6/en/Content/PAS%20INST/Configuring-Transparent-User-Management.htm

upvoted 3 times

 **dru0pa** 1 year, 11 months ago

**Selected Answer: B**

Is correct as this is local between the AD and the Vault

upvoted 1 times

You are creating a new Rest API user that utilizes CyberArk Authentication.
What is a correct process to provision this user?

A. Private Ark Client > Tools > Administrative Tools > Users and Groups > New > User

B. Private Ark Client > Tools-> Administrative Tools > Directory Mapping > Add

C. PVWA > User Provisioning > LDAP Integration > Add Mapping

D. PVWA > User Provisioning > Users and Groups > New > User

**Correct Answer:** *A*

*Community vote distribution*

A (86%) | 14%
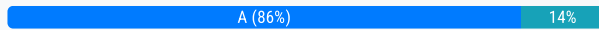
👤 **Sathesh** 2 weeks, 3 days ago

Selected Answer: D

For latest version A and D both works

upvoted 1 times

👤 **bumika** 5 months ago

Selected Answer: A

Local users (CyberArk auth) can be created using the PrivateArk client.

upvoted 1 times

👤 **M4rt1n0** 9 months, 3 weeks ago

Selected Answer: A

The user must be added in PrivateArk

upvoted 2 times

👤 **dru0pa** 1 year, 2 months ago

Selected Answer: A

The answer is A

upvoted 3 times

DRAG DROP -

For each listed prerequisite, identify if it is mandatory or not mandatory to run the PSM Health Check.

| PSM service installed on Windows 2008 R2, Windows 2012 R2, or Windows 2016 | Drag answer here |
| PSM service installed on Windows 2012 R2, Windows 2016, or Windows 2019 | Drag answer here |
| A valid SSL certificate is installed on the Web Server | Drag answer here |
| Web Server (IIS 8.5) role is installed | Drag answer here |

Mandatory

Not Mandatory

**Correct Answer:**

| PSM service installed on Windows 2008 R2, Windows 2012 R2, or Windows 2016 | Not Mandatory |
| PSM service installed on Windows 2012 R2, Windows 2016, or Windows 2019 | Mandatory |
| A valid SSL certificate is installed on the Web Server | Mandatory |
| Web Server (IIS 8.5) role is installed | Mandatory |

☐ 👤 **144d6dd** 8 months, 3 weeks ago

1-PSM service installed on Windows 2008 R2 (NOT Mandatory)

2-PSM service installed on Windows 2016, Windows 2019, or Windows 2022(Mandatory)

3-Web Server (IIS) role is installed(Mandatory)

4-The web server is defined with a site binding that is configured to HTTPs using a valid SSL certificate. (Mandatory)

Not mandatory

Mandatory

Mandatory

Mandatory

https://docs.cyberark.com/pam-self-hosted/Latest/en/Content/PSM/psm_healthcheck.htm

DR

  upvoted 1 times

  ☐ 👤 **M4rt1n0** 1 year, 3 months ago

Mandatory services:

PSM service installed on Windows 2016 or Windows 2019

Web Server (IIS 8.5) role is installed

A valid SSL certificate is installed on the Web Server

  upvoted 1 times

  ☐ 👤 **LiamNg** 1 year, 9 months ago

The provided answer is correct. (Not mandatory, mandatory, mandatory, mandatory)

Ref Prerequisites of PSM health check

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PSM/psm_healthcheck.htm

  upvoted 3 times

  ☐ 👤 **dru0pa** 1 year, 11 months ago

PSM server installing on Windows 2008 R2, Windows 2012 R2, or Windows 2016 - Not Mandatory - Windows 2008 R2 is not supported.

PSM server installing on Windows 2012 R2, Windows 2016, or Windows 2019 - Mandatory

A valid SSL certificate installed on the Webserver - Not Mandatory

WebServer (IIS 8.5) role is installed - Not Mandatory -Not installed

  upvoted 1 times

What is mandatory for a PVWA Installation?

     A. A DNS entry for the PVWA url must be created.

     B. A company-signed TLS certificate must be imported into the server.

     C. A Vault Administrative User must be used to register the PVWA.

     D. Data Execution Prevention must be disabled.

**Correct Answer:** *C*

*Community vote distribution*

C (100%)

---

👤 **bumika** 5 months ago

Selected Answer: C

During the installation process the PVWA installer must log in to the Vault using Administrator-level credentials

upvoted 1 times

👤 **M4rt1n0** 9 months, 3 weeks ago

Selected Answer: C

Administrator account is required during installation of PVWA

upvoted 1 times

👤 **dru0pa** 1 year, 5 months ago

Selected Answer: C

C is the answer

upvoted 2 times

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

- A. Master Policy

- B. Safe Templates

- C. PVWAConfig.xml

- D. Platform Configuration

**Correct Answer:** *A*

*Community vote distribution*

| A (75%) | D (25%) |
|---|---|

---

⊟ 👤 **144d6dd** 8 months, 3 weeks ago

A. Master Policy

DR

upvoted 1 times

⊟ 👤 **144d6dd** 8 months, 2 weeks ago

https://docs.cyberark.com/privilege-cloud-shared-services/latest/en/Content/Privilege%20Cloud/privCloud-master-policy-rules.htm

upvoted 1 times

⊟ 👤 **bumika** 11 months ago

**Selected Answer: A**

The answer is A: all passwords - Master policy

upvoted 1 times

⊟ 👤 **omardw** 1 year ago

the correct is A

upvoted 1 times

⊟ 👤 **M4rt1n0** 1 year, 3 months ago

**Selected Answer: A**

Master Policy overides Platform configuration, except exceptions

upvoted 1 times

⊟ 👤 **dru0pa** 1 year, 8 months ago

**Selected Answer: A**

The answer is A

upvoted 1 times

⊟ 👤 **LiamNg** 1 year, 9 months ago

**Selected Answer: A**

The answer is A

upvoted 1 times

⊟ 👤 **dru0pa** 1 year, 11 months ago

**Selected Answer: A**

The answer is A to change all password organization

upvoted 2 times

⊟ 👤 **monkey_king** 2 years ago

**Selected Answer: D**

Correct Answer should be A since it is mentioned for all the passwords

upvoted 2 times

⊟ 👤 **monkey_king** 2 years ago

Correct Answer should be A since it is mentioned for all the passwords

upvoted 3 times

When running a "Privileged Accounts inventory" Report through the Reports page in PVWA on a specific safe, which permission/s are required on that safe to show complete account inventory information?

A. List Accounts, View Safe Members

B. Manage Safe Owners

C. List Accounts, Access Safe without confirmation

D. Manage Safe, View Audit

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

---

☐ 👤 **144d6dd** 8 months, 2 weeks ago

**Selected Answer: A**

A. List Accounts, View Safe Members

https://docs.cyberark.com/pam-self-hosted/Latest/en/Content/PASIMP/ReportsInPVWA.htm

DR

upvoted 1 times

☐ 👤 **bumika** 11 months ago

**Selected Answer: A**

View safe members permission is needed to access other user's activities

upvoted 1 times

☐ 👤 **LiamNg** 1 year, 9 months ago

**Selected Answer: A**

Answer is A

upvoted 2 times

☐ 👤 **dru0pa** 1 year, 11 months ago

**Selected Answer: A**

List accounts and View Safe members in the Safes that will be included in the report.

upvoted 2 times

☐ 👤 **monkey_king** 2 years ago

**Selected Answer: A**

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/ReportsInPVWA.htm#

upvoted 1 times

In a rule using "Privileged Session Analysis and Response" in PTA, which session options are available to configure as responses to activities?

A. Suspend, Terminate, None

B. Suspend, Terminate, Lock Account

C. Pause, Terminate, None

D. Suspend, Terminate

**Correct Answer:** *A*

*Community vote distribution*

A (80%) | D (20%)

👤 **144d6dd** 8 months, 2 weeks ago

A. Suspend, Terminate, None

https://docs.cyberark.com/pam-self-hosted/Latest/en/Content/PTA/Security-Configuration.htm

DR

upvoted 1 times

👤 **bumika** 11 months ago

Selected Answer: A

Session response: "Determine the Session response, either None, Suspend, or Terminate, to the suspicious session activity."

upvoted 1 times

👤 **M4rt1n0** 1 year, 3 months ago

Selected Answer: A

3 options: Suspend, terminate, none

upvoted 1 times

👤 **LiamNg** 1 year, 9 months ago

Selected Answer: A

The answer should be A.

There are 3 options: suspend, terminate, none

upvoted 2 times

👤 **dru0pa** 1 year, 11 months ago

Selected Answer: D

n the Privileged Session Analysis and Response section, add a new rule or edit an existing rule to automatically suspend or terminate a session when the Suspicious activities detected in a privileged session event occurs

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PTA/Security-Configuration.htm

upvoted 1 times

👤 **LiamNg** 1 year, 9 months ago

The answer should be A.

Under "Add and Edit Rules", first captures show 3 options: suspend, terminate, none

upvoted 2 times

In addition to disabling Windows services or features not needed for PVWA operations, which tasks does PVWA_Hardening.ps1 perform when run?

A. performs IIS hardening; imports the CyberArk INF configuration

B. performs IIS hardening; configures all group policy settings

C. performs IIS hardening; renames the local Administrator Account

D. configures Windows Firewall; removes all installation files

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

---

 **144d6dd** 8 months, 2 weeks ago

A. performs IIS hardening; imports the CyberArk INF configuration

DR

upvoted 1 times

 **bumika** 11 months ago

Selected Answer: A

I think the user who typed the "official" correct answers is a lottery player. CyberArk provides INF files to harden PAM components.

upvoted 1 times

 **M4rt1n0** 1 year, 3 months ago

Selected Answer: A

Imports the INF configuration

upvoted 1 times

 **dru0pa** 1 year, 11 months ago

Selected Answer: A

Imports the INF configuration and hardens IIS

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/PVWA-hardening-task-descriptions.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PVWA%7CPVWA%20Hardening%7CHarden%20the%20PVWA%20server%7C_____1

upvoted 3 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 | | Safe |
| Add/Update Users | Drag answer here | | |
| Add Safes | Drag answer here | | |

**Correct Answer:**

| Add Accounts | Vault |
|---|---|
| Initiate CPM account management operations | Safe |
| Add/Update Users | Safe |
| Add Safes | Safe |

---

☐ 👤 **144d6dd** 8 months, 2 weeks ago

Add Accounts --> Safe
Initiate CPM account management operations -> Safe
Add/Update Users -> Vault
Add Safes -> Vault

DR
  upvoted 1 times

☐ 👤 **bumika** 11 months ago

Safe, Safe, Vault, Vault
  upvoted 1 times

☐ 👤 **LiamNg** 1 year, 9 months ago

Add Accounts: Safe
Initiate CPM account management operations: Safe
Add/Update Users: Vault
Add Safes: Vault

List of safe permissions:
https://docs.cyberark.com/Product-Doc/OnlineHelp/PrivCloud/Latest/en/Content/Privilege%20Cloud/privCloud-manage-safe-members.htm#EditSafememberpermissions

List of Vault authorizations:
https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Managing-Users.htm?Highlight=Authorizations%20tab
  upvoted 4 times

A customer has two data centers and requires a single PVWA url.

Which deployment provides the fastest time to reach the PVWA and the most redundancy?

A. Deploy two PVWAs behind a global traffic manager.

B. Deploy one PVWA only.

C. Deploy two PVWAs in an active/standby mode.

D. Deploy two PVWAs using DNS round robin.

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

---

 **bumika** 5 months ago

Selected Answer: A

Load Balancer solutions are the best methods to handle this type of problem

upvoted 1 times

 **M4rt1n0** 9 months, 3 weeks ago

Selected Answer: A

The traffic manager routes the traffic to the closest PVWA

upvoted 1 times

 **dru0pa** 1 year, 5 months ago

Selected Answer: A

as the load balancer can test which PVWA is up

upvoted 3 times

What is the recommended method to determine if a PVWA is unavailable and must be removed from the load balancing pool?

A. Monitor port 443 on the PVWA server.

B. Monitor port 1858 on the PVWA server.

C. Ping the PVWA server

D. Monitor port 3389 on the PVWA server.

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

**144d6dd** 8 months, 4 weeks ago

A. Monitor port 443 on the PVWA server.

upvoted 1 times

**bumika** 11 months ago

**Selected Answer: A**

Ping is not good because it only checks whether the server is alive. TCP/443 is the default port of HTTPS, so the load balancer can check whether the web server can accept HTTPS requests on TCP level.

upvoted 1 times

**dru0pa** 1 year, 11 months ago

**Selected Answer: A**

Monitor port 443 on the PVWA server. as 443 is https

upvoted 4 times

CyberArk User Neil is trying to connect to the Target Linux server 192.168.1.164 using a domain account ACME/linuxuser01 on domain acme.corp using PSM for SSH server 192.168.65.145.

What is the correct syntax?

A. ssh neil@linuxuser01:acme.corp@192.168.1.164@192.168.65.145

B. ssh neil@linuxuser01#acme.corp@192.168.1.164@192.168.65.145

C. ssh neil@linuxuser01@192.168.1.164@192.168.65.145

D. ssh neil@linuxuser01@acme.corp@192.168.1.164@192.168.65.145

**Correct Answer:** *C*

*Community vote distribution*

| B (67%) | C (33%) |
|---------|---------|

---

👤 **bumika** 5 months ago

Selected Answer: B

Domain users will authenticate on the target server so that it needs to use a special character separating the user name from the domain name. Besides default settings @ is the global separator and # is used on this purpose.

upvoted 1 times

---

👤 **M4rt1n0** 9 months, 3 weeks ago

Selected Answer: B

B is the solution, if it was a local account, no need to specify nothing after Account (TargetUser), since it is a Domain account, domain name must be specified after # : Account#Domain

upvoted 1 times

---

👤 **sent3x** 10 months, 2 weeks ago

The answer is B. Neil wants to log in as ACME/linuxuser01, so he needs to specify the domain as well.

upvoted 1 times

---

👤 **dru0pa** 1 year, 5 months ago

Selected Answer: C

ssh VaultUser@TargetUser@TragetAddress@PSMPAddress

upvoted 1 times

Which permissions are needed for the Active Directory user required by the Windows Discovery process?

- A. Domain Admin
- B. LDAP Admin
- C. Read/Write
- D. Read

**Correct Answer:** *D*

*Community vote distribution*

D (75%) | A (25%)

---

 **144d6dd** 8 months, 2 weeks ago

**Selected Answer: D**

On Windows machines
In Active Directory On the target machines
Read permissions in the OU to scan and all sub-OUs
Domain Administrator an equivalent domain user with the following permissions:

Read permissions on the Active Directory
Local administrative rights for Windows on the target machine
Permissions to logon remotely to the target machine

upvoted 1 times

---

 **bumika** 11 months ago

**Selected Answer: A**

I do not think that D is the good answer. Windows discovery means access to the Active Directory and access to the Windows machines. Access to AD requires only a read permission but access to all Windows domain machines requires a Domain Admin (or equivalent) permission

upvoted 1 times

---

 **omardw** 1 year ago

JUST READ

upvoted 1 times

---

 **SergRodr** 1 year, 3 months ago

D

https://docs.cyberark.com/PrivCloud-SS/Latest/en/Content/Privilege%20Cloud/PrivCloud-account-discovery-permissions.htm

upvoted 1 times

---

 **LiamNg** 1 year, 9 months ago

**Selected Answer: D**

D should be correct.

upvoted 1 times

---

 **dru0pa** 1 year, 11 months ago

**Selected Answer: D**

D is the answer

upvoted 1 times

---

 **dru0pa** 2 years ago

D is the answer
Read permissions on the Active Directory
https://docs.cyberark.com/Product-Doc/OnlineHelp/PrivCloud-SS/Latest/en/Content/Privilege%20Cloud/privCloud-accounts-discovery.htm#Permissi

upvoted 2 times

---

 **LiamNg** 1 year, 9 months ago

D should be correct.

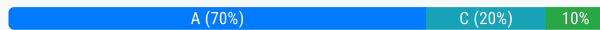"The user must have read permissions in the OU and all sub-OUs to scan."

To use PSM connections while in the PVWA, what are the minimum safe permissions a user or group will need?

A. List Accounts, Use Accounts

B. List Accounts, Use Accounts, Retrieve Accounts

C. Use Accounts

D. List Accounts, Use Accounts, Retrieve Accounts, Access Safe without confirmation

**Correct Answer:** *A*

*Community vote distribution*

A (70%) | C (20%) | 10%

---

**144d6dd** 8 months, 2 weeks ago

**Selected Answer: A**

A. List Accounts, Use Accounts

https://docs.cyberark.com/pam-self-hosted/13.0/en/Content/PASIMP/PSSO-PMSP.htm

DR

upvoted 1 times

---

**43aa45a** 10 months, 3 weeks ago

**Selected Answer: A**

I think this is a difficult question, but related to the "most likely use case scenario" - what I mean. In general, users will need List and Use permissions. And as for the secure connection https://docs.cyberark.com/privilege-cloud-shared-services/Latest/en/Content/PASIMP/Connecting-with-Secure-Connect.htm - this is only for Windows/Unix ad hoc connections, where List permissions are not necessary. So it will be the least permissions in this context, but not for all purposes. Assuming that the question is a general question, so it will be A. Because it was not specified for what purposes users need to connect and whether there is dual control or not. So a general question = a general answer.

upvoted 1 times

---

**bumika** 11 months ago

**Selected Answer: A**

You are in the PVWA - based on the question - so you need the List Account permission to choose the proper account. Use account is a must to use PSM.

upvoted 1 times

---

**NigilP** 1 year, 6 months ago

**Selected Answer: D**

C WITH SECURE CONNECT /RDP FILE

upvoted 1 times

---

**dru0pa** 1 year, 8 months ago

**Selected Answer: A**

Answer is A.

upvoted 1 times

---

**LiamNg** 1 year, 9 months ago

**Selected Answer: A**

Answer is A.

You require the Use accounts and List accounts permissions in the Safe to connect transparently to remote machines.

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/PSSO-PMSP.htm

upvoted 3 times

---

**dru0pa** 1 year, 11 months ago

**Selected Answer: C**

Use account

upvoted 1 times

---

**dru0pa** 1 year, 8 months ago

Answer is A.

upvoted 1 times

☐ 👤 **monkey_king** 2 years ago

Selected Answer: C

For using PSM connections only use accounts permission is sufficient.

upvoted 1 times

☐ 👤 **monkey_king** 2 years ago

Selected Answer: C

For using PSM connections only use accounts permission is sufficient.

upvoted 1 times

Which PTA sensors are required to detect suspected credential theft?

A. Logs, Vault Logs

B. Logs, Network Sensor, Vault Logs

C. Logs, PSM Logs, CPM Logs

D. Logs, Network Sensor, EPM

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

---

☐ 👤 **144d6dd** 8 months, 2 weeks ago

Selected Answer: A

A. Logs, Vault Logs

https://docs.cyberark.com/pam-self-hosted/10.10/en/Content/PTA/What-Does-PTA-Detect.htm

DR

upvoted 1 times

☐ 👤 **bumika** 11 months ago

Selected Answer: A

Reference below

upvoted 1 times

☐ 👤 **dru0pa** 1 year, 8 months ago

Selected Answer: A

A is the answer

upvoted 2 times

☐ 👤 **LiamNg** 1 year, 9 months ago

Selected Answer: A

Answer is A

Required Sensor:

Logs

Vault

AWS (optional)

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/10.10/en/Content/PTA/What-Does-PTA-Detect.htm

upvoted 4 times

☐ 👤 **dru0pa** 2 years ago

B is the answer

upvoted 1 times

☐ 👤 **kirankk0905** 1 year, 7 months ago

please stop spamming wrong answers, the answer is evident in the link provided

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/10.10/en/Content/PTA/What-Does-PTA-Detect.htm

upvoted 4 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 help the CyberArk Support Team 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

**Correct Answer:** *ACD*

*Community vote distribution*

ACD (83%) | ABD (17%)

---

⊟ 👤 **144d6dd** 8 months, 2 weeks ago

**Selected Answer: ABD**

A. PSMConsole.log

B. PSMDebug.log

D. <Session_ID>.Component.log

DR

upvoted 1 times

⊟ 👤 **144d6dd** 8 months, 1 week ago

ACD: these are PSM log files

upvoted 1 times

⊟ 👤 **bumika** 11 months ago

**Selected Answer: ACD**

ACD: these are PSM log files

upvoted 1 times

⊟ 👤 **NigilP** 1 year, 6 months ago

**Selected Answer: ACD**

Answer is ACD

upvoted 1 times

⊟ 👤 **LiamNg** 1 year, 9 months ago

**Selected Answer: ACD**

Answer is ACD

upvoted 1 times

⊟ 👤 **dru0pa** 1 year, 11 months ago

**Selected Answer: ACD**

B no file

E wrong server

F worng server

upvoted 2 times

Which component must be installed on the Vault if Distributed Vaults is used with PSM?

    A. RabbitMQ

    B. Disaster Recovery

    C. Remote Control Client

    D. Distributed Vault Server

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

---

 **144d6dd** 8 months, 2 weeks ago

Selected Answer: A

A. RabbitMQ

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.5/en/Content/PAS%20INST/Distributed-Vault-Limitations.htm

DR
upvoted 1 times

 **LiamNg** 1 year, 9 months ago

Selected Answer: A

answer is A

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.5/en/Content/PAS%20INST/Distributed-Vault-Limitations.htm
upvoted 2 times

You are configuring the Vault to send syslog audit data to your organization's SIEM solution.

What is a valid value for the SyslogServerProtocol parameter in DBPARM.INI file?

A. TLS

B. SSH

C. SMTP

D. SNMP

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

☐ 👤 **144d6dd** 8 months, 2 weeks ago

Selected Answer: A

A. TLS

https://docs.cyberark.com/pam-self-hosted/Latest/en/Content/PASREF/DBParm.ini.htm

DR
  upvoted 1 times

☐ 👤 **dru0pa** 1 year, 11 months ago

Selected Answer: A

Acceptable Values TCP/UDP/TLS
  upvoted 2 times

Which usage can be added as a service account platform?

    A. Kerberos Tokens

    B. IIS Application Pools

    C. PowerShell Libraries

    D. Loosely Connected Devices

**Correct Answer:** *B*

*Community vote distribution*

B (100%)

---

👤 **144d6dd** 8 months, 2 weeks ago

**Selected Answer: B**

B. IIS Application Pools

https://docs.cyberark.com/pam-self-hosted/Latest/en/Content/PASIMP/WindowsIISApplicationPools.htm

DR

upvoted 1 times

👤 **dru0pa** 1 year, 11 months ago

**Selected Answer: B**

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/10.10/en/Content/PASIMP/Managing-Service-Accounts.htm

upvoted 2 times

To enable the Automatic response "Add to Pending" within PTA when unmanaged credentials are found; what are the minimum permissions required by PTAUser for the PasswordManager_pending safe?

    A. List Accounts, View Safe members, Add accounts (includes update properties), Update Account content, Update Account properties

    B. List Accounts, Add accounts (includes update properties), Delete Accounts, Manage Safe

    C. Add accounts (includes update properties), Update Account content, Update Account properties, View Audit

    D. View Accounts, Update Account content, Update Account properties, Access Safe without confirmation, Manage Safe, View Audit

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

---

☐ 👤 **144d6dd** 8 months, 2 weeks ago

<span style="background:#f5c518">Selected Answer: A</span>

List Accounts, View Safe members, Add accounts (includes update properties), Update Account content, Update Account properties

DR

upvoted 1 times

☐ 👤 **144d6dd** 8 months, 3 weeks ago

List Accounts, View Safe members, Add accounts (includes update properties), Update Account content, Update Account properties

DR

upvoted 1 times

☐ 👤 **dru0pa** 1 year, 11 months ago

<span style="background:#f5c518">Selected Answer: A</span>

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.1/en/Content/PTA/Configuring-PVWA-for-PTA-Integration-with-EPV.htm

upvoted 3 times

You are logging into CyberArk as the Master user to recover an orphaned safe.

Which items are required to log in as Master?

A. Master CD, Master Password, console access to the Vault server, Private Ark Client

B. Operator CD, Master Password, console access to the PVWA server, PVWA access

C. Operator CD, Master Password, console access to the Vault server, Recover.exe

D. Master CD, Master Password, console access to the PVWA server, Recover.exe

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

---

👤 **144d6dd** 8 months, 2 weeks ago

Selected Answer: A

A. Master CD, Master Password, console access to the Vault server, Private Ark Client
The Master user can only log in with the Master CD, which contains the Private Recovery Key.

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.0/en/Content/PASIMP/Predefined-Users-and-Groups.htm?
TocPath=Administration%7CUser%20Management%7C_____7


DR
upvoted 1 times

---

👤 **kai_jhuang** 1 year, 9 months ago

Selected Answer: A

Answer is A
upvoted 1 times

---

👤 **LiamNg** 1 year, 9 months ago

Selected Answer: A

Answer is A
The Master user can only log in with the Master CD, which contains the Private Recovery Key.Master User enables the predefined Users immediately after installation and the initial network areas which enable other Users to begin working with the PrivateArk Client.
https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.0/en/Content/PASIMP/Predefined-Users-and-Groups.htm?
TocPath=Administration%7CUser%20Management%7C_____7
upvoted 2 times

DRAG DROP -

Match each component to its respective Log File location.

| PTA System | | C:\Program Files (x86)\PrivateArk\Server\PADR |
| PSM for SSH (PSMP) | Drag answer here | /opt/tomcat/logs |
| Disaster Recovery | Drag answer here | /var/opt/CARKpsmp/logs/ |

**Correct Answer:**

| PTA System | /opt/tomcat/logs |
| PSM for SSH (PSMP) | /var/opt/CARKpsmp/logs/ |
| Disaster Recovery | C:\Program Files (x86)\PrivateArk\Server\PADR |

---

☐ 👤 **dru0pa** 5 months, 3 weeks ago

correct

upvoted 2 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

**Correct Answer:** *A*

*Community vote distribution*

| A (75%) | C (25%) |
|---------|---------|

**144d6dd** 8 months, 2 weeks ago

Selected Answer: A

A. List accounts, Authorize account request

DR

upvoted 1 times

**sent3x** 1 year, 4 months ago

The answer is A

upvoted 2 times

**NigilP** 1 year, 6 months ago

Selected Answer: A

aOORIVER DO NOT NEED TO USE THE PASSWORD ONLY APPROVE WHICH CAN BE DONE IN pvwa

upvoted 2 times

**dru0pa** 1 year, 11 months ago

Selected Answer: C

The system is now configured for dual control, and users who wish to retrieve accounts are required to request access confirmation from at least one authorized user. By default, requests are retained in the Safe for 30 days.

Select the authorizations that the Safe member/group will have in the Safe. Specifically, select Authorize password requests; the Confirmation Level options appear.

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/PVWA-Dual-Control.htm

upvoted 1 times

DRAG DROP -

Arrange the steps to install the Password Vault Web Access (PVWA) in the correct sequence.

Unordered Options | Ordered Response

**Unordered Options:**

- Run the PVWAInstallation.sp1 script in PowerShell as Administrator.
- Run the PVWA_Prerequisites.ps1 script in Powershell as Administrator.
- Run the PVWARegisterComponent.ps1 script with the Vault password.

**Correct Answer:**

Unordered Options:
- Run the PVWAInstallation.sp1 script in PowerShell as Administrator.
- Run the PVWA_Prerequisites.ps1 script in Powershell as Administrator.
- Run the PVWARegisterComponent.ps1 script with the Vault password.

Ordered Response:
- Run the PVWA_Prerequisites.ps1 script in Powershell as Administrator.
- Run the PVWAInstallation.sp1 script in PowerShell as Administrator.
- Run the PVWARegisterComponent.ps1 script with the Vault password.

&#9723; &#128100; **anotidaishe** 7 months ago
CORRECT
upvoted 1 times

&#9723; &#128100; **LiamNg** 1 year, 3 months ago
correct
upvoted 1 times

&#9723; &#128100; **dru0pa** 1 year, 5 months ago
correct
upvoted 3 times

A company requires challenge/response multi-factor authentication for PSMP sessions.
Which server must you integrate with the CyberArk Vault?

    A. LDAP

    B. PKI

    C. SAML

    D. RADIUS

**Correct Answer:** *D*

---

 👤 **144d6dd** 8 months, 3 weeks ago

D. RADIUS

DR
  upvoted 1 times

A customer asked you to help scope the company's PSM deployment.
What should be included in the scoping conversation?

- A. Recordings file path
- B. Recordings codec
- C. Recordings retention period
- D. Recordings file type

**Correct Answer:** *C*

---

👤 **144d6dd** 8 months, 3 weeks ago

C. Recordings retention period

https://docs.cyberark.com/pam-self-hosted/13.2/en/Content/PAS%20INST/Considerations-Before-Installing-PSM.htm#:~:text=of%20your%20implementation.-,Recordings%20Retention%20Period,-The%20length%20of

DR

upvoted 1 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. Vault Replicator

B. PAS Reporter

C. Remote Control Agent

D. Syslog

**Correct Answer:** *C*

Currently there are no comments in this discussion, be the first to comment!

DRAG DROP -

Match each key to its recommended storage location.

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

**Correct Answer:**

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

☐ 👤 **anotidaishe** `Highly Voted 👍` 7 months ago

SSH KEYS- VAULT

SERVER KEY- HSM

PRIVATE KEY (MASTER CD -PHYSICAL SAFE

PUBLIC KEY- VAULT SERVER DISK DRIVE

upvoted 6 times

What is a valid combination of primary and secondary layers of authentication to a company's two-factor authentication policy?

A. RSA SecurID Authentication (in PVWA) and LDAP Authentication

B. CyberArk Authentication and RADIUS Authentication

C. Oracle SSO (in PVWA) and SAML Authentication

D. LDAP Authentication and RADIUS Authentication

**Correct Answer:** *D*

*Community vote distribution*

A (67%) | D (33%)

---

 **duracell** 1 week, 3 days ago

Selected Answer: D

D is acutally correct. LDAP being WindowsAuth as primary, and RADIUS as secondary

upvoted 1 times

---

 **omardw** 6 months, 2 weeks ago

https://docs.cyberark.com/pam-self-hosted/Latest/en/Content/PAS%20INST/Authenticating-to-the-Privileged-Account-Security-Solution.htm?tocpath=Administrator%7CUser%20Management%7CAuthenticate%20to%20Privileged%20Access%20Manager%20-%20Self-Hosted%7C_____0

upvoted 1 times

---

 **anotidaishe** 7 months, 1 week ago

Selected Answer: A

FINAL ANSWER IS A.B IS INCORRECT

upvoted 2 times

---

 **anotidaishe** 7 months, 1 week ago

THE ANSWER IS B

upvoted 1 times

DRAG DROP -

Match each PTA alert category with the PTA sensors that collect the data for it.

| unmanaged privileged account | Drag answer here | | Vault |
|---|---|---|---|
| anomalous access to multiple machines | Drag answer here | | Logs, Vault, AWS (optional), Azure (optional) |
| suspicious activities detected in a privileged session | Drag answer here | | Logs, Vault, AD (optional), AWS (optional), Azure(Optional) |
| suspected credentials theft | Drag answer here | | Network Sensor, PTA Windows Agent |

**Correct Answer:**

| unmanaged privileged account | Logs, Vault, AD (optional), AWS (optional), Azure(Optional) |
|---|---|
| anomalous access to multiple machines | Network Sensor, PTA Windows Agent |
| suspicious activities detected in a privileged session | Vault |
| suspected credentials theft | Logs, Vault, AWS (optional), Azure (optional) |

👤 **omardw** 6 months, 2 weeks ago

https://docs.cyberark.com/pam-self-hosted/12.6/en/Content/PTA/What-Does-PTA-Detect.htm

upvoted 1 times

👤 **anotidaishe** 7 months ago

CORRECT

upvoted 2 times

You are beginning the post-install process after the PSM installation is completed

What must you do?

    A. Disable screen saver for the PSM local users

    B. Create a new group called PSMShadowUsers.

    C. Reset the PSMAdminConnect user password

    D. Enable load balancing on the PSM server.

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

---

  👤 **dru0pa** 7 months, 2 weeks ago

Selected Answer: A

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/PostInstall_mand.htm

  upvoted 3 times

A customer's environment has three data centers consisting of 5,000 servers in Germany, 10,000 servers Canada, 1,500 servers in Singapore. You want to manage target servers and avoid complex firewall rules.

How many CPMs should you deploy?

A. 1

B. 3 total, 1 per data center

C. 15

D. 6 total, 2 per data center

**Correct Answer:** *D*

☐ 👤 **rayjohn28** 8 months ago

B is correct while D is wrong and excessive. CPM does not have hot active redundancy due to split brain scenario which we do not want that to happen. Thus 2 CPM per site is not recommended considering max of 10k on one site, 1 cpm will suffice.

upvoted 1 times

☐ 👤 **Moneybag** 1 year ago

B is the answer, your answer is wrong

upvoted 1 times

How should you configure PSM for SSH to support load balancing?

A. by using a network load balancer

B. in PVWA > Options > PSM for SSH Proxy > Servers

C. in PVWA > Options > PSM for SSH Proxy > Servers > VIP

D. by editing sshd.config on the all the PSM for SSH servers

**Correct Answer:** *C*

*Community vote distribution*

A (100%)

---

👤 **omardw** 6 months, 2 weeks ago

A IS CORRECT

upvoted 1 times

---

👤 **dru0pa** 1 year, 1 month ago

Selected Answer: A

https://cyberark-customers.force.com/s/article/00004777#:~:text=Load%20balancing%20for%20PSMP%20can,an%20individual%20PSMP%20server%20address.

upvoted 1 times

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

A. They are added to the Pending Accounts list and can be reviewed and manually uploaded.

B. They cannot be onboarded to the Password Vault.

C. They must be uploaded using third party tools.

D. They are not part of the Discovery Process.

**Correct Answer:** *A*

☐ 👤 **omardw** 6 months, 2 weeks ago

A is correct

https://docs.cyberark.com/Product-Doc/OnlineHelp/PrivCloud/Latest/en/Content/Privilege%20Cloud/privCloud-accounts-discovery.htm

upvoted 1 times

Which of the following properties are mandatory when adding accounts from a file? (Choose three.)

A. Safe Name

B. Platform ID

C. All required properties specified in the Platform

D. Username

E. Address

F. Hostname

**Correct Answer:** *BDF*

*Community vote distribution*

ABC (100%)

---

☐ 👤 **rayjohn28** 8 months ago

Selected Answer: ABC

ABC is the correct answer

upvoted 2 times

☐ 👤 **Moneybag** 1 year ago

A,B,C is the correct answers

upvoted 1 times

☐ 👤 **sublimity96** 1 year, 4 months ago

A, B, C

upvoted 4 times

To manage automated onboarding rules, a CyberArk user must be a member of which group?

A. Vault Admins

B. CPM User

C. Auditors

D. Administrators

**Correct Answer:** *A*

⊟ 👤 **Moneybag** 6 months, 2 weeks ago
Yes, A is correct

upvoted 1 times

Which CyberArk group does a user need to be part of to view recordings or live monitor sessions?

A. Auditors

B. Vault Admin

C. DR Users

D. Operators

**Correct Answer:** *B*

*Community vote distribution*

A (100%)

□ 👤 **rayjohn28** 8 months ago

Selected Answer: A

A is the correct answer, vault admin does not have the right to view PSM recordings

upvoted 2 times

□ 👤 **GUDDIA** 11 months, 3 weeks ago

A is a correct answer

upvoted 1 times

□ 👤 **Moneybag** 1 year ago

A is the answer, B is wrong. Vault Admin user doesn't have the right to view PSM recorded videos because Vault Admin doesn't have access to the recording file path. Only Auditors does.

upvoted 1 times

After installing the first PSM server and before installing additional PSM servers, you must ensure the user performing the installation is not a direct owner of which safe?

    A. PSMUnmanagedSessionAccounts Safe

    B. PSMRecordingsSessionAccounts Safe

    C. PSMUnmanagedApplicationAccounts Safe

    D. PSMSessionBackupAccounts Safe

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

---

 👤 **144d6dd** 8 months, 2 weeks ago

**Selected Answer: A**

After installing the first PSM server, before installing additional PSM servers, make sure the user who will perform installation is not a direct owner in the PSMUnmanagedSessionAccounts Safe.

upvoted 1 times

 👤 **Moneybag** 1 year ago

Yes, A is correct

upvoted 1 times

 👤 **dru0pa** 1 year, 7 months ago

**Selected Answer: A**

A is the answer

upvoted 1 times

You are creating a shared safe for the help desk.
What must be considered regarding the naming convention?

    A. Ensure your naming convention is no longer than 20 characters.

    B. Combine environments, owners and platforms to minimize the total number of safes created.

    C. Safe owners should determine the safe name to enable them to easily remember it.

    D. The use of these characters V:*<>".| is not allowed.

**Correct Answer:** *D*

*Community vote distribution*

D (100%)

---

☐ 👤 **144d6dd** 8 months, 2 weeks ago

Selected Answer: D

Name of a Safe to create.

Specify up to 28 characters.
The following characters aren't allowed: \/:*<>".|
Do not start a Safe name with a space.
  upvoted 1 times

☐ 👤 **Moneybag** 1 year ago

Yes, D is correct
  upvoted 1 times

What is the configuration file used by the CPM scanner when scanning UNIX/Linux devices?

A. UnixPrompts.ini

B. plink.exe

C. dbparm.ini

D. PVConfig.xml

**Correct Answer:** *D*

*Community vote distribution*

A (100%)

 rayjohn28 8 months ago

**Selected Answer: A**

A is the correct answer

upvoted 1 times

 144d6dd 8 months, 3 weeks ago

The correct answer is A

When scanning Unix/Linux devices, the CPM scanner uses various parameters in theUnixPrompts.ini

DR.

upvoted 1 times

 Moneybag 1 year ago

The correct answer is A

upvoted 1 times

 dee1969 1 year, 4 months ago

Answer is A

https://docs.cyberark.com/PAS/11.5/en/Content/PASIMP/PVWA-Accounts-Feed.htm

upvoted 1 times

You are setting up a Linux host to act as an HTML 5 gateway for PSM sessions.

Which servers need to be trusted by the Linux host to secure communications through the gateway?

A. PSM and PVWA

B. PSM and CPM

C. PVWA and Vault

D. Vault and PSM

**Correct Answer:** *B*

*Community vote distribution*

A (100%)

☐ 👤 **144d6dd** 8 months, 1 week ago

Selected Answer: A

A. PSM and PVWA

DR

upvoted 1 times

☐ 👤 **Moneybag** 1 year ago

The Answer is A

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 should 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

**Correct Answer:** *C*

*Community vote distribution*

| C (75%) | D (25%) |
| --- | --- |

---
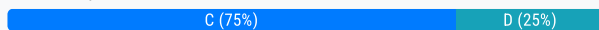
👤 **rayjohn28** 8 months ago

**Selected Answer: C**

C is the correct answer since you only need a logon account and do this via at the platform level

upvoted 1 times

---

👤 **144d6dd** 8 months, 1 week ago

**Selected Answer: C**

C. Configure the UNIX platform to use the correct logon account.

https://docs.cyberark.com/pam-self-hosted/13.0/en/Content/PASIMP/Linked-PAS-Accounts.htm#Overview

DR

upvoted 1 times

---

👤 **144d6dd** 8 months, 1 week ago

C. Configure the UNIX platform to use the correct logon account.

upvoted 1 times

---

👤 **d5ea0d0** 8 months, 3 weeks ago

**Selected Answer: D**

The clue is for password management. So option will be reconcile account

upvoted 1 times

---

👤 **Moneybag** 1 year ago

C is the answer, login account is what is needed not a reconcile account.

upvoted 1 times

---

👤 **dru0pa** 1 year, 7 months ago

**Selected Answer: C**

This is not to reconcile the account it to change the root password

upvoted 1 times

DRAG DROP -

Match the connection component to the corresponding OS/Function.

| PSM-SSH | Drag answer here | | Windows |
| PSM-RDP | Drag answer here | | UNIX File Transfer |
| PSM-WinSCP | Drag answer here | | UNIX |
| PSM-SQLPlus | Drag answer here | | Database |
| PSM-OS390 | Drag answer here | | Mainframe |

**Correct Answer:**

| PSM-SSH | UNIX |
| PSM-RDP | Windows |
| PSM-WinSCP | UNIX File Transfer |
| PSM-SQLPlus | Database |
| PSM-OS390 | Mainframe |

⊟ 👤 **omardw** 6 months, 2 weeks ago

Correct

upvoted 1 times

Which option in the Private Ark client is used to update users' Vault group memberships?

A. Update > General tab

B. Update > Authorizations tab

C. Update > Member Of tab

D. Update > Group tab

**Correct Answer:** *C*

☐ 👤 **omardw** 6 months, 2 weeks ago

c is correct

https://docs.cyberark.com/pam-self-hosted/11.3/en/Content/PASIMP/Managing-Users.htm

upvoted 1 times

If the AccountUploader Utility is used to create accounts with SSH keys, which parameter do you use to set the full or relative path of the SSH private key file that will be attached to the account?

A. KeyPath

B. KeyFile

C. ObjectName

D. Address

**Correct Answer:** *B*

*Community vote distribution*

B (100%)

👤 **dee1969** 4 months, 3 weeks ago

Selected Answer: B

https://docs.cyberark.com/PAS/11.5/en/Content/PASIMP/Adding-Accounts-with-SSH-Keys-using-the-AccountUploader-Utility-Appendix.htm

upvoted 1 times

There is a requirement for a password to change between 01:00 and 03:00 on Saturdays and Sundays; however, this does not work consistently.

Which platform setting may be the cause?

A. The Interval setting for the platform is incorrect and must be less than 120.

B. The ImmediateInterval setting for the platform is incorrect and must be greater than or equal to 1.

C. The DaysToRun setting for the platform is incorrect and must be set to Sat,Sun.

D. The HeadStartInterval setting for the platform is incorrect and must be set to 0.

**Correct Answer:** *C*

*Community vote distribution*

D (100%)

---

👤 **144d6dd** 8 months, 1 week ago

Selected Answer: D

D. The HeadStartInterval setting for the platform is incorrect and must be set to 0.

DR

upvoted 1 times

👤 **43aa45a** 10 months, 3 weeks ago

Selected Answer: D

Different value than 0 for HeadStartInterval will cause : "not work consistently change between 01:00 and 03:00 on Saturdays and Sundays".
F.e when set to 1 then password will not be changed on Sundays as it was speed up 1 day.

When it comes to Interval setting .
https://cyberark.my.site.com/s/article/00002885
"CPM 9.10 and up, when FromHour to ToHour is used, the interval will be used only within the FromHour to ToHour. Outside those hours, the interval will be ignored."
So it looks like the interval is different than defualt or current and the only will change the password within the FromHour to ToHour.

As well in article:
https://cyberark.my.site.com/s/article/00004112
"Since CPM version 9.10 and higher, this rule is not needed anymore and must not be used."

upvoted 1 times

👤 **Moneybag** 1 year ago

Yes, D is correct

upvoted 1 times

👤 **Manjula1492** 1 year, 2 months ago

Correct Answer is D

upvoted 2 times