



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

You are installing a CPM.

In addition to Add Safes, Add/Update Users, Reset Users' Passwords and Manage Server File Categories, which Vault authorization(s) does a CyberArk user need to install the CPM?

- A. Manage Directory Mapping
- B. Activate Users
- C. Backup All Safes, Restore All Safes
- D. Audit Users, Add Network Areas

Suggested Answer: B

Community vote distribution

B (100%)

ahmedsarfraz 2 months, 1 week ago

B is correct answer
upvoted 2 times

Cavdog 10 months, 3 weeks ago

Selected Answer: B

To install CPM, users must have the following Vault Authorisations: Add Safes, Add/Update Users, Reset Users' Passwords, Activate Users, Manage Server File Categories and be owners of the VaultInternal and Notification Engine safes.

upvoted 2 times

Fabri59 1 year, 2 months ago

Selected Answer: B

The answer is B.
upvoted 3 times

BigTo 1 year, 2 months ago

THIS EXAM HAS BEEN UPDATED. QUESTIONS ON THE ACTUAL EXAM HAVE CHANGED. PLEASE UPDATE YOUR QUESTIONS
upvoted 3 times

penuelaandy 1 year, 4 months ago

Selected Answer: B

B
upvoted 3 times

monkey_king 1 year, 4 months ago

Selected Answer: B

Activate users is the correct option
upvoted 2 times

flaw123456789 1 year, 5 months ago

Activate Users is the right answer
upvoted 2 times


In which configuration file do you add LoadBalancerClientAddressHeader when you enable x-forwarding on the PVWA loadbalancer?

- A. PVconfiguration.xml
- B. web.config
- C. apigw.ini
- D. CyberArkScheduledTasks.exe.config

Suggested Answer: B

Community vote distribution

B (100%)

 **penuelaandy** Highly Voted 1 year, 4 months ago

Selected Answer: B

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/PVWA-install-multiple-PVWA-env.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PVWA%7C___8#ConfigurethePVWAtoworkwiththeloadbalancer
upvoted 7 times

 **FastSloth** 1 year, 4 months ago


Please, try to work on all questions. most of your answers are correct according to docs. Thank you!

upvoted 3 times

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

B is correct answer


upvoted 1 times

 **Cavdog** 10 months, 3 weeks ago

Selected Answer: B


The LoadBalancerClientAddressHeader parameter should be updated in the web.config file on the PVWA to allow for the Vault to log incoming requests IP instead of that of the NLB.

<https://docs.cyberark.com/PAS/12.2/en/Content/PASREF/Password%20Vault%20Web%20Access%20Parameter%20File.htm#:~:text=LoadBalancerClient/>
upvoted 3 times

 **Fabri59** 1 year, 2 months ago

Selected Answer: B

The answer is B. https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/PVWA-install-multiple-PVWA-env.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PVWA%7C___8
upvoted 1 times

 **BigTo** 1 year, 2 months ago


THIS EXAM HAS BEEN UPDATED. QUESTIONS ON THE ACTUAL EXAM HAVE CHANGED. PLEASE UPDATE YOUR QUESTIONS

upvoted 4 times

 **Ketan_20** 1 year, 2 months ago

I scheduled on 14 May and wondering any help I get for questions

upvoted 1 times

 **Kaustav01** 10 months, 2 weeks ago

Please give us some feedback on the exam questions.

upvoted 1 times

 **TacoTeo** 1 year, 2 months ago

Did you pass?

upvoted 1 times

You are configuring SNMP remote monitoring for your organization's Vault servers.
In the PARAgent.ini, which parameter specifies the destination of the Vault SNMP traps?

- A. SNMHostIP
- B. SNMPTrapPort
- C. SNMPCommunity
- D. SNMPVersion

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ **Cavdog** 4 months, 2 weeks ago

Selected Answer: A

The SNMHostIP parameter in the PARAgent.ini file should be populated with the IP of the remote computer where SNMP traps will be sent.

<https://docs.cyberark.com/PAS/Latest/en/Content/PASREF/Remote%20Control%20Agent%20Parameter%20File.htm#:~:text=Remote%20Monitoring-,SNM%20Description>
upvoted 2 times

🗨️ **Fabri59** 8 months, 1 week ago

Selected Answer: A

The answer is A. https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PASREF/Remote%20Control%20Agent%20Parameter%20File.htm?tocpath=Administrator%7CReferences%7CConfiguration%20Files%7C___3
upvoted 1 times

🗨️ **BigTo** 8 months, 3 weeks ago

THIS EXAM HAS BEEN UPDATED. QUESTIONS ON THE ACTUAL EXAM HAVE CHANGED. PLEASE UPDATE YOUR QUESTIONS
upvoted 1 times

🗨️ **infoaravindr** 8 months, 2 weeks ago

I guess defender only update sentry same, Please confirm ?
upvoted 2 times

🗨️ **penuelaandy** 10 months, 3 weeks ago

Selected Answer: A

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASREF/Remote%20Control%20Agent%20Parameter%20File.htm>
upvoted 1 times

🗨️ **jacpicci** 10 months, 3 weeks ago

Selected Answer: A

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASREF/Remote%20Control%20Agent%20Parameter%20File.htm#_Ref363045992
upvoted 2 times

🗨️ **monkey_king** 11 months ago

Selected Answer: A

HostIP is the right option
upvoted 1 times

You want to improve performance on the CPM by restricting accounts for the CYBRWINDAD platform to only the WINDEMEA and WINDEMEA_Admin safes.

How do you set this in CyberArk?

- A. In the CYBRWINDAD platform, under Automatic Password Management/General, configure AllowedSafes and set to (WINDEMEA)|(WINDEMEA_ADMIN).
- B. In the settings for Configuration/CPM assigned to the WINDEMEA and WINDEMEAADMIN safes, configure AllowedSafes and set to (WINDEMEA)|(WINDEMEAADMIN).
- C. In the CYBRWINDAD platform, under UI&Workflows/Properties/Optional, configure AllowedSafes and set to (WINDEMEA)|(WINDEMEA_ADMIN).
- D. Modify cpm.ini on the relevant CPM/s and add the setting AllowedSafesCYBRWINDAD and set to (WINDEMEA)|(WINDEMEAADMIN).

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ **Cavdog** 4 months, 2 weeks ago

Selected Answer: A

The AllowedSafes parameter can be found in the Platform configuration under Automatic Password Management > General. The field is limited to 700 chars.

<https://docs.cyberark.com/PAS/Latest/en/Content/PASIMP/Limit-Platforms-to-Specific-Safes.htm>

upvoted 2 times

🗨️ **Fabri59** 8 months, 1 week ago

Selected Answer: A

The answer is A. https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PASIMP/Limit-Platforms-to-Specific-Safes.htm?tocpath=End%20user%7CPrivileged%20Accounts%7CClassic%20Interface%7CManage%20platforms%20classic%20interface%7C____7

upvoted 2 times

🗨️ **BigTo** 8 months, 3 weeks ago

THIS EXAM HAS BEEN UPDATED. QUESTIONS ON THE ACTUAL EXAM HAVE CHANGED. PLEASE UPDATE YOUR QUESTIONS

upvoted 1 times

🗨️ **penuelaandy** 10 months, 3 weeks ago

Selected Answer: A

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Limit-Platforms-to-Specific-Safes.htm#Limitaplatfromtoaspecificsafe>

upvoted 3 times

🗨️ **monkey_king** 11 months ago

Selected Answer: A

Allowed safes is found automatic password management under platform settings

upvoted 3 times


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

Suggested Answer: A

Community vote distribution

A (100%)

 **penuelaandy** Highly Voted 10 months, 3 weeks ago

Selected Answer: A


https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/Install_PSM_harden.htm#RunAppLockerrules
upvoted 5 times

 **Cavdog** Most Recent 4 months, 2 weeks ago

Selected Answer: A

PSMConfigureAppLocker.xml is the file that feeds into the PSMConfigureAppLocker.ps1 script which is run during the hardening process and should be configured to allow required applications to run on the PSM server post hardening.

https://docs.cyberark.com/PAS/Latest/en/Content/PAS%20INST/Configure_Applocker.htm
upvoted 4 times


 **Fabri59** 8 months, 1 week ago

Selected Answer: A

The answer is A. https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/Install_PSM_harden.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PSM%7CPSM%20troubleshooting%7C____3
upvoted 1 times

 **BigTo** 8 months, 3 weeks ago

THIS EXAM HAS BEEN UPDATED. QUESTIONS ON THE ACTUAL EXAM HAVE CHANGED. PLEASE UPDATE YOUR QUESTIONS
upvoted 1 times

 **jacpicci** 10 months, 3 weeks ago

Selected Answer: A

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.2/en/Content/PAS%20INST/Configure_Applocker.htm
upvoted 1 times

 **monkey_king** 11 months ago

Selected Answer: A

A is correct
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

Suggested Answer: A

Community vote distribution

A (83%)

D (17%)

🗨️ **Sanve87** 3 months, 3 weeks ago

Selected Answer: D

<https://community.cyberark.com/s/article/00004777>

upvoted 1 times

🗨️ **Cavdog** 1 year, 4 months ago

Selected Answer: A

In accordance with the following article an NLB should be used as it is not supported by CyberArk natively.

upvoted 1 times

🗨️ **penuelaandy** 1 year, 10 months ago

Selected Answer: A

Doesn't exists an option

upvoted 2 times

🗨️ **penuelaandy** 1 year, 10 months ago

a

upvoted 1 times

🗨️ **monkey_king** 1 year, 11 months ago

Selected Answer: A

There is no option to load balance PSM for SSH from cyberark you have to use general load balancer

upvoted 2 times

In which configuration file on the Vault can filters be configured to either include or exclude log messages that are sent through SNMP?

- A. PARAgent.ini
- B. DBParm.ini
- C. TSParm.ini
- D. CyberArkv2 MIB file

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **Cavdog** 4 months, 3 weeks ago

Selected Answer: A

The following parameters within the PARAgent.ini can be used to include/exclude log messages:

upvoted 3 times

🗳️ 👤 **Fabri59** 8 months, 1 week ago

Selected Answer: A

The answer is A.

upvoted 1 times

🗳️ 👤 **penuelaandy** 10 months, 3 weeks ago

Selected Answer: A

A

upvoted 4 times

A first PSM server has been installed.

What should you confirm before installing any additional PSM servers?

- A. The PSM ID of the first installed PSM server was changed and the additional PSM server can use the same PSM ID.
- B. The user performing the installation is a direct owner in the PSMUnmanagedSessionAccounts Safe, PSM safe and member of PVWAMonitor group.
- C. The user performing the installation is not a direct owner in the PSMUnmanagedSessionAccounts Safe.
- D. The path of the Recordings Folder must be different on all PSM installations.

Suggested Answer: C

Community vote distribution

C (100%)

🗨️ **bternyak** 3 months ago

C;

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

upvoted 1 times

🗨️ **Cavdog** 1 year, 4 months ago

Selected Answer: C

Of those stated, the only requirement is C.

upvoted 2 times

🗨️ **Fabri59** 1 year, 8 months ago

Selected Answer: C

The answer is C.

upvoted 2 times

🗨️ **penuelaandy** 1 year, 10 months ago

Selected Answer: C

C

upvoted 2 times

🗨️ **jacpicci** 1 year, 10 months ago

Selected Answer: C

C

upvoted 2 times

During the PSM installation process, Safes and a User are created.

In addition to Add Safes, Add/Update Users, Reset Users' Passwords, and Activate Users, which authorization(s) does the Vault user installing the PSM need to enable them to be successfully created?

- A. Manage Vault File Categories
- B. Manage Server File Categories
- C. Manage Directory Mapping, Manage Server File Categories
- D. Manage Directory Mapping, Manage Vault File Categories

Suggested Answer: A

Community vote distribution

A (75%)

B (25%)

🗳️ 👤 **ROUNAK1** Highly Voted 👍 7 months, 1 week ago

Selected Answer: A

<https://docs.cyberark.com/PAS/Latest/en/Content/PAS%20INST/Before-Installing-PSM.htm>

upvoted 5 times

🗳️ 👤 **DLEVY** Most Recent 🕒 2 months, 1 week ago

Selected Answer: A

<https://docs.cyberark.com/PAS/Latest/en/Content/PAS%20INST/Before-Installing-PSM.htm>

upvoted 4 times

🗳️ 👤 **Ghost96** 4 months, 2 weeks ago

In reference to question 1 of the this exam, B is the correct answer

upvoted 2 times

🗳️ 👤 **c8f8172** 4 months, 2 weeks ago

When inspecting vault authorisations under PrivateArk Client > Tools > Users > Users and Groups > *user* > authorizations, it is clear that there is only one vault file category authorisation; "Manage server file categories". The authorisation "manage vault file categories" does not exist. This may be due to an update which has not been reflected in the documentation. For this reason, the only possible solution is B.

upvoted 3 times

🗳️ 👤 **ROUNAK1** 7 months, 1 week ago

Selected Answer: B

B: <https://docs.cyberark.com/PAS/Latest/en/Content/PAS%20INST/Before-Installing-PSM.htm>

upvoted 2 times

🗳️ 👤 **conjuror** 9 months ago

Selected Answer: B

Gotta fix the ratio. Answer is B. Yes, the documentation says Manage Vault File Categories; No that is not a real authorization, it is a mistake.

Install CPM has the same vault authorizations, shown here: https://docs.cyberark.com/PAS/13.2/en/Content/PAS%20INST/CPM-install-requirements.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20CPM%7C___2#Vaultuserauthorizations

upvoted 2 times

🗳️ 👤 **conjuror** 7 months, 1 week ago

After taking the exam, I suspect this was the question I missed, so if I took it again I would pick A. If anyone gets 100% with this question, please confirm.

upvoted 1 times

🗳️ 👤 **Innuendo** 9 months ago

Selected Answer: B

It's B. Manage Server File Categories is a real and valid authorization

upvoted 1 times



🗳️ 👤 **Cavdog** 11 months ago

Selected Answer: A

Manage Directory Mapping is not a requirement and Manage Server File Categories is not a valid authorisation therefore answer is A.

<https://docs.cyberark.com/PAS/12.6/en/Content/PAS%20INST/Optional-Installing-Multiple-PSM-Servers.htm#:~:text=After%20installing%20the%20first%20PSM%20server%2C%20before%20installing%20additional%20PSM%20servers%2C%20make%2C>

upvoted 1 times

  **Cavdog** 10 months, 2 weeks ago



The documentation is actually wrong for this one the answer is actually B. same as the installation requirements for all other components.

upvoted 2 times

  **DeanSizzle** 11 months, 1 week ago

The answer is A. The documentation needs to be corrected, there is no Vault Authorization called "Manage Vault File Categories"

upvoted 2 times


  **Fabri59** 1 year, 2 months ago

Selected Answer: A

The answer is A. [https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/Before-Installing-PSM.htm?](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/Before-Installing-PSM.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PSM%7C____2)

[tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PSM%7C____2](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/Before-Installing-PSM.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PSM%7C____2)

upvoted 1 times

  **penuelaandy** 1 year, 4 months ago

Selected Answer: A

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/Before-Installing-PSM.htm?](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/Before-Installing-PSM.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PSM%7C____2#Permissionstoinstall)

[tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PSM%7C____2#Permissionstoinstall](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/Before-Installing-PSM.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PSM%7C____2#Permissionstoinstall)

upvoted 4 times

Your customer wants to store the Safes Data on Vault Drive D instead of Drive C.
Which file should you edit?

- A. TSparm.ini
- B. Vault.ini
- C. DBparm.ini
- D. user.ini

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ **Cavdog** 4 months, 2 weeks ago

Selected Answer: A

The TSParm.ini file is used to specify the directories on the Vault (or other storage solution) in which to store safes (databases). Multiple directories can be listed by specifying the SafesDirectory again on a new line within the file.

<https://docs.cyberark.com/PAS/12.2/en/Content/PASREF/TSParm%20ini.htm>

upvoted 1 times

🗨️ **Fabri59** 8 months, 1 week ago

Selected Answer: A

The answer is A. https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASREF/TSParm%20ini.htm?tocpath=Administrator%7CReferences%7CConfiguration%20Files%7CCyberArk%20Vault%20Server%20Parameter%20Files%7C____2
upvoted 1 times

🗨️ **penuelaandy** 10 months, 3 weeks ago

Selected Answer: A

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASREF/TSParm%20ini.htm?tocpath=Administrator%7CReferences%7CConfiguration%20Files%7CCyberArk%20Vault%20Server%20Parameter%20Files%7C____2
upvoted 3 times

What must you do to prepare a Windows server for PVWA installation?

- A. In the InstallationAutomation folder, run the PVWA_Prerequisites.ps1 file as an administrator in Powershell.
- B. Install the PrivateArk client.
- C. Verify the user performing the installation is Domain Administrator and has logon access to the Vault server.
- D. Enable IPv6.

Suggested Answer: A

Community vote distribution

A (100%)

 **Cavdog** 4 months, 2 weeks ago

Selected Answer: A

The first step of the PVWA pre-installation tasks is to log on to the PVWA as an administrator, close all other applications and run the PVWA_Prerequisites.ps1 script.

<https://docs.cyberark.com/PAS/12.2/en/Content/PAS%20INST/PVWA-install-preinstall-tasks.htm>

upvoted 1 times

 **Fabri59** 8 months, 1 week ago

Selected Answer: A

The answer is A. https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/PVWA-install-preinstall-tasks.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PVWA%7C____3


upvoted 1 times

 **penuelaandy** 10 months, 3 weeks ago

Selected Answer: A

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/PVWA-install-preinstall-tasks.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PVWA%7C____3

upvoted 3 times

 **ewitkop** 10 months, 3 weeks ago

A. is correct.

upvoted 1 times

Which statement about REST API is correct? (Choose two.)

- A. When a user successfully authenticates to the Vault, an authentication token is returned.
- B. REST API Windows authentication method allows skipping the logon API by using the Windows default credentials with a Kerberos ticket.
- C. To allow High Availability, REST API can be configured to support Session Load Balancing by editing the PVConfiguration.xml and setting the AllowPVWASessionRedandancy=Yes.
- D. Each REST API call requires that a valid authentication token be provided.
- E. REST calls are directly sent to the currently active Vault using Port 1858.

Suggested Answer: AD

Community vote distribution

AD (100%)

 **Fabri59** Highly Voted 8 months, 1 week ago

Selected Answer: AD

The answer are A and D.

Statement B is incorrect because the REST API Windows authentication method does not allow skipping the logon API.

Statement C is incorrect because the REST API cannot be configured to support Session Load Balancing by editing the PVConfiguration.xml and setting the AllowPVWASessionRedandancy=Yes. This setting only applies to the PVWA session load balancing feature.

Statement E is incorrect because REST calls are not directly sent to the currently active Vault using Port 1858. REST calls are made to the CyberArk API Gateway, which then forwards the call to the appropriate Vault.

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

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

upvoted 7 times

 **Cavdog** Most Recent 4 months, 3 weeks ago

Selected Answer: AD

Answer is A. & D.

https://docs.cyberark.com/PAS/13.2/en/Content/SDK/CyberArk%20Authentication%20-%20Logon_v10.htm?tocpath=Developer%7CREST%20APIs%7CAuth

[https://docs.cyberark.com/PAS/13.2/en/Content/WebServices/Implementing%20Privileged%20Account%20Security%20Web%20Services%20.htm?](https://docs.cyberark.com/PAS/13.2/en/Content/WebServices/Implementing%20Privileged%20Account%20Security%20Web%20Services%20.htm?tocpath=Developer%7CREST%20APIs%7C___0#:~:text=For%20every%20REST%20API%20call%20except%20for%20Logon%2C%20the%20request%20must)

[tocpath=Developer%7CREST%20APIs%7C___0#:~:text=For%20every%20REST%20API%20call%20except%20for%20Logon%2C%20the%20request%20must](https://docs.cyberark.com/PAS/13.2/en/Content/WebServices/Implementing%20Privileged%20Account%20Security%20Web%20Services%20.htm?tocpath=Developer%7CREST%20APIs%7C___0#:~:text=For%20every%20REST%20API%20call%20except%20for%20Logon%2C%20the%20request%20must)

upvoted 1 times

 **penuelaandy** 10 months, 3 weeks ago

Selected Answer: AD

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/SDK/CyberArk%20Authentication%20-%20Logon_v10.htm?](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/SDK/CyberArk%20Authentication%20-%20Logon_v10.htm?TocPath=Developer%7CREST%20APIs%7CAuthentication%7CLogon%7C___1)

[TocPath=Developer%7CREST%20APIs%7CAuthentication%7CLogon%7C___1](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/SDK/CyberArk%20Authentication%20-%20Logon_v10.htm?TocPath=Developer%7CREST%20APIs%7CAuthentication%7CLogon%7C___1)

upvoted 1 times

HTML5 Gateway can be installed on which supported UNIX OS versions? (Choose two.)

- A. Red Hat Enterprise Linux 7.x
- B. CentOS 7.x
- C. Ubuntu 20.x
- D. AK 7.x
- E. Android 11.x

Suggested Answer: AB

Community vote distribution

AB (100%)

🗨️ **Cavdog** 4 months, 3 weeks ago

As of version 13 up, the ability to install via Container Manager means that the answers are A. B. and C.

https://docs.cyberark.com/PAS/Latest/en/Content/PAS%20INST/Install_PSM_HTML5_Docker.htm

https://docs.cyberark.com/PAS/Latest/en/Content/PAS%20INST/Install_PSM_HTML5_RPM.htm

upvoted 2 times

🗨️ **Fabri59** 8 months, 1 week ago

Selected Answer: AB

The answer are A and B. [https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/Install_PSM_HTML5_RPM.htm?](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/Install_PSM_HTML5_RPM.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PSM%7CAdvanced%20PSM%20Implementations%7CInstall%20PSM%20HTML5%20Gateway%7C____2)

tocpath=Installation%7CInstall%20PAM%20-%20Self-

Hosted%7CInstall%20PSM%7CAdvanced%20PSM%20Implementations%7CInstall%20PSM%20HTML5%20Gateway%7C____2

upvoted 2 times

🗨️ **penuelaandy** 10 months, 3 weeks ago

Selected Answer: AB

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/Install_PSM_HTML5_RPM.htm?](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/Install_PSM_HTML5_RPM.htm?TocPath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PSM%7CAdvanced%20PSM%20Implementations%7CInstall%20PSM%20HTML5%20Gateway%7C____3#Softwareprerequisites)

TocPath=Installation%7CInstall%20PAM%20-%20Self-

Hosted%7CInstall%20PSM%7CAdvanced%20PSM%20Implementations%7CInstall%20PSM%20HTML5%20Gateway%7C____3#Softwareprerequisites

But v13.0.1 and higher - Install PSM HTML5 Gateway using a container manager permits Ubuntu 20.X

upvoted 3 times

Which utility should be used to register the Vault in Amazon Web Services?

- A. CAVaultManager
- B. StorageManager
- C. CloudVaultManager
- D. CACert

Suggested Answer: A

Community vote distribution


A (100%)

 **penuelaandy** Highly Voted 10 months, 3 weeks ago

Selected Answer: A

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20Cloud/AWS-Manual-PrimaryVault.htm?TocPath=Installation%7CInstall%20PAM%2%A0in%20a%20cloud%20environment%7CInstall%20the%20Digital%20Vault%20on%20the%20cloud%7C____5#

upvoted 6 times


 **Cavdog** Most Recent 4 months, 2 weeks ago

Selected Answer: A

CAVaultManager is the utility used to configure the Vault to work in AWS as well as to secure the server.key in Amazon KMS.

<https://docs.cyberark.com/PAS/11.5/en/Content/PAS%20Cloud/AWS-Manual-PrimaryVault.htm#:~:text=Run%20the%20following%20CAVaultManager%20PostInstall%20command>

upvoted 3 times

 **Fabri59** 8 months, 1 week ago

Selected Answer: A

The answer is A. https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20Cloud/Azure-Manual-PrimaryVault.htm?tocpath=Installation%7CInstall%20Privileged%20Access%20Manager%20-%20Self-Hosted%2%A0in%20a%20cloud%20environment%7CInstall%20the%20Digital%20Vault%20on%20the%20cloud%7C____9

upvoted 3 times

 **monkey_king** 11 months ago

Selected Answer: A

CAVaultManager
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

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ **Cavdog** 4 months, 2 weeks ago

Selected Answer: A

The only acceptable values for the SyslogServerProtocol parameter in the dbparm.ini are TCP, UDP and TLS.
<https://docs.cyberark.com/PAS/Latest/en/Content/PASREF/DBParm.ini.htm#:~:text=SyslogServerProtocol>
upvoted 2 times

🗨️ **Fabri59** 8 months, 1 week ago

Selected Answer: A

The answer is A.

The SyslogServerProtocol parameter in the DBParm.INI file specifies the protocol that is used to send syslog audit data to the SIEM solution. The valid values for this parameter are:

UDP
TCP
TLS

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PASREF/DBParm.ini.htm?tocpath=Administrator%7CReferences%7CConfiguration%20Files%7CCyberArk%20Vault%20Server%20Parameter%20Files%7C____1
upvoted 2 times

🗨️ **penuelaandy** 10 months, 3 weeks ago

Selected Answer: A

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASREF/DBParm.ini.htm?tocpath=Administrator%7CReferences%7CConfiguration%20Files%7CCyberArk%20Vault%20Server%20Parameter%20Files%7C____1
upvoted 3 times


When creating a distributed Vault environment architecture, what is the maximum number of Vault servers that can be deployed?

- A. 5 - number of primary and satellite Vaults can be specified during installation
- B. 3 - all primary
- C. 6 - 1 primary and 5 satellite
- D. 10 - 2 primary and 8 satellite

Suggested Answer: C

Community vote distribution


C (100%)

 **Cavdog** 4 months, 3 weeks ago

Selected Answer: C

The answer is C. or 6 with 1 primary and 5 satellite.

<https://docs.cyberark.com/PAS/Latest/en/Content/PAS%20INST/Distributed-Vault-Limitations.htm#:~:text=You%20can%20deploy%20up%20to%20six%20Vault%20servers%2C%20one%20Primary%20Vault%20and%20five%20Satellite%20V>
upvoted 3 times

 **Fabri59** 8 months, 1 week ago

Selected Answer: C

The answer is C. <https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/Distributed-Vaults-Introduction.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CCyberArk%20Digital%20Vault%20installation%7CIntroduction%20to%20Digital%20Vault%20installation%7CDistributed%20Vaults%20environme>
upvoted 3 times

 **penuelaandy** 10 months, 3 weeks ago

Selected Answer: C

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/Distributed-Vaults-Introduction.htm?tocpath=Installation%7CInsta>
Hosted%7CCyberArk%20Digital%20Vault%20installation%7CIntroduction%20to%20Digital%20Vault%20installation%7CDistributed%20Vaults%20environme
upvoted 3 times

 **monkey_king** 11 months ago

Selected Answer: C

As per Cyberark docs 6 is correct
upvoted 3 times

DRAG DROP -

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

Answer Area

Unordered Options

Open Powershell as Administrator and run the script.

Review these script logs: HardeningScript.log and CYBRHardeningsecedit.log.

Locate the CPM_Hardening.ps1 script in the installation media.



Ordered Response



Suggested Answer:

Ordered Response

- 1) Locate the CPM_Hardening.ps1 script in the installation media.
- 2) Open Powershell as Administrator and run the script.
- 3) Review these script logs: HardeningScript.log and CYBRHardeningsecedit.log.

The correct sequence for completing CPM Hardening for Out-of-Domain Deployment is to first locate the CPM_Hardening.ps1 script in the installation media, then open Powershell as Administrator and run the script, followed by reviewing the HardeningScript.log and CYBRHardeningsecedit.log script logs. This ensures that all the necessary steps are taken in order to properly secure an out-of-domain deployment of CPM.

Cavdog 4 months, 3 weeks ago

The correct order is to locate the CPM_Hardening.ps1 script , run in powershell as administrator and then check the logs.

https://docs.cyberark.com/PAS/Latest/en/Content/PAS%20INST/CPM-hardening-runsript.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20CPM%7CCPM%20Hardening%7CHarden%20the%20CPM%20server%7C___0#:~:text=by%20the%20CPM-,Run%20the%20hardening%20If%20you%20have

<https://cyberark-customers.force.com/s/article/Where-do-I-find-the-logs>

upvoted 3 times

ildab 3 months, 3 weeks ago

C,A,B is the correct order

upvoted 1 times

To enable LDAP over SSL for a Vault when DNS lookups are blocked, which step must be completed?

- A. Add the FQDN & IP details for each LDAP host into the local hosts file of the Vault server.
- B. Configure an AllowNonStandardFWAddresses rule in DBParm.ini on the Vault to allow outbound TCP 53 to the organization's DNS servers.
- C. Ensure LDAP hosts added to the directory mapping configuration are defined using only IP addresses.
- D. Set the ReferralsDNSLookup parameter value to "No" in the directory configuration.

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ **Cavdog** 4 months, 2 weeks ago

Selected Answer: A

Enabling DNS (and associated firewall rules) on the Vault is strongly as it increases the attack surface of the system. Therefore hostname and IPs should

https://docs.cyberark.com/PAS/Latest/en/Content/PAS%20INST/Configuring-Transparent-User-Management.htm?tocpath=Administrator%7CUser%20Management%7CTransparent%20user%20management%20using%20LDAP%7C____1#:~:text=In%20the%20%25system

upvoted 2 times

🗨️ **Fabri59** 8 months, 1 week ago

Selected Answer: A

The answer is A. https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/Configuring-Transparent-User-Management.htm?tocpath=Administrator%7CUser%20Management%7CTransparent%20user%20management%20using%20LDAP%7C____1

upvoted 2 times

🗨️ **Riaan_M** 9 months, 3 weeks ago

A is correct.

If the PVWA or CPM cannot resolve the domain name, add DNS server configuration to the PVWA or CPM network interface configuration.

10.10.10.10 dc1.mydomain.com

As the Vault cannot be configured with a DNS server, add a row to the HOSTS file for every domain controller that specifies the IP address and corresponding domain name.

upvoted 2 times

🗨️ **penuelaandy** 10 months, 3 weeks ago

Selected Answer: A

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/Configuring-Transparent-User-Management.htm?tocpath=Administrator%7CUser%20Management%7CTransparent%20user%20management%20using%20LDAP%7C____1#ConfigureLDAPoverSSLconnecti

upvoted 2 times


In which file must the attribute 'SignAuthnRequest="true"' be added to the PartnerIdentityProvider element to support signed SAML requests?

- A. saml.config
- B. samlconfig.ini
- C. PVWAConfig.xml
- D. PVConfiguration.xml

Suggested Answer: A

Community vote distribution

A (100%)


 **Cavdog** 4 months, 3 weeks ago

Selected Answer: A

It must be added to the saml.config file on the PVWA

https://docs.cyberark.com/PAS/Latest/en/Content/PAS%20INST/SAML-Authentication.htm?tocpath=Administrator%7CUser%20Management%7CAuthentication%7CConfigure%20authentication%20methods%7C___5#:~:text=the%20certificate%3E%22%20/%3E%0A%3C/LocalCertificates%3E-,Add%20the%20%3A

upvoted 3 times

 **Fabri59** 8 months, 1 week ago

Selected Answer: A

The answer is A. https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/SAML-Authentication.htm?tocpath=Administrator%7CUser%20Management%7CAuthentication%20to%20Privileged%20Access%20Manager%20-%20Self-Hosted%7CConfigure%20authentication%20methods%7C___5


upvoted 3 times

 **penuelaandy** 10 months, 3 weeks ago

Selected Answer: A

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/SAML-Authentication.htm?tocpath=Administrator%7CUser%20Management%7CAuthentication%20to%20Privileged%20Access%20Manager%20-%20Self-Hosted%7CConfigure%20authentication%20methods%7C___5#ConfigureSAMLauthenticationinPAMSelfHosted

upvoted 3 times

 **ewitkop** 10 months, 3 weeks ago

A. is correct.

upvoted 3 times

A customer is moving from an on-premises to a public cloud deployment.

What is the best and most cost-effective option to secure the server key?


- A. Install the Vault in the cloud the same way you would in an on-premises environment. Place the server key in a password protected folder on the operating system.
- B. Install the Vault in the cloud the same way you would in an on-premises environment. Purchase a Hardware Security Module to secure the server key.
- C. Install the Vault using the native cloud images and secure the server key using native cloud Key Management Systems.
- D. Install the Vault using the native cloud images and secure the server key with a Hardware Security Module.

Suggested Answer: C

Community vote distribution

C (67%)

A (33%)


 **Cavdog** 4 months, 3 weeks ago

Selected Answer: C


The recommendation from Cyberark is to use KMS (as per the reference) however this would not be anywhere near as "cost-effective" as just storing the permissions as per a normal on-prem deployment but my understanding is that this is strongly discouraged. There are also several difference between tl "Install the Vault in the cloud the same way you would in an on-premises environment." isn't exactly true either. Therefore I'd say the answer is C.

[https://docs.cyberark.com/PAS/Latest/en/Content/PAS%20Cloud/ChangeServerKeys-](https://docs.cyberark.com/PAS/Latest/en/Content/PAS%20Cloud/ChangeServerKeys-cloud.htm#:~:text=To%20ensure%20the%20security%20of%20the%20keys%20in%20AWS%2C%20it%20is%20recommended%20to%20follow%20AWS%20be)

[cloud.htm#:~:text=To%20ensure%20the%20security%20of%20the%20keys%20in%20AWS%2C%20it%20is%20recommended%20to%20follow%20AWS%20be](https://docs.cyberark.com/PAS/Latest/en/Content/PAS%20Cloud/ChangeServerKeys-cloud.htm#:~:text=To%20ensure%20the%20security%20of%20the%20keys%20in%20AWS%2C%20it%20is%20recommended%20to%20follow%20AWS%20be)
upvoted 2 times

 **Cavdog** 4 months, 3 weeks ago

mods, just delete this haha
upvoted 1 times

 **Cavdog** 4 months, 3 weeks ago


Correction the paramter does exist I'm trippin ><

However there is no requirement for a passphrase and it will work without it.

upvoted 1 times

 **Cavdog** 4 months, 3 weeks ago


The answer is A.
upvoted 1 times

 **pamlover** 6 months, 3 weeks ago

Selected Answer: A

You would use CAVaultManager.exe ChangeAwsKeys to make new keys and store in the cloud.

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20Cloud/ChangeServerKeys-](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20Cloud/ChangeServerKeys-cloud.htm#ChangetheserverkeyonthePrimaryVault)
[cloud.htm#ChangetheserverkeyonthePrimaryVault](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20Cloud/ChangeServerKeys-cloud.htm#ChangetheserverkeyonthePrimaryVault)
upvoted 1 times

 **Fabri59** 8 months, 1 week ago

Selected Answer: C

The answer is C. <https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20Cloud/ChangeServerKeys-cloud.htm?>

[tocpath=Installation%7CInstall%20Privileged%20Access%20Manager%20-%20Self-](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20Cloud/ChangeServerKeys-cloud.htm?)

[Hosted%2%A0in%20a%20cloud%20environment%7CInstall%20the%20Digital%20Vault%20on%20the%20cloud%7C___14](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20Cloud/ChangeServerKeys-cloud.htm?)



upvoted 2 times

 **marcosneves** 10 months ago

Selected Answer: A

A is correct

upvoted 2 times

  **Riaan_M** 9 months, 2 weeks ago

Nope. This is NOT the cost-efficient choice.

upvoted 1 times

  **penuelaandy** 10 months, 3 weeks ago

Selected Answer: C

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20Cloud/ChangeServerKeys-cloud.htm?](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20Cloud/ChangeServerKeys-cloud.htm?TocPath=Installation%7CInstall%20PAM%C2%A0in%20a%20cloud%20environment%7CInstall%20the%20Digital%20Vault%20on%20the%20cloud%7C____14)

[TocPath=Installation%7CInstall%20PAM%C2%A0in%20a%20cloud%20environment%7CInstall%20the%20Digital%20Vault%20on%20the%20cloud%7C____14](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20Cloud/ChangeServerKeys-cloud.htm?TocPath=Installation%7CInstall%20PAM%C2%A0in%20a%20cloud%20environment%7CInstall%20the%20Digital%20Vault%20on%20the%20cloud%7C____14)

upvoted 2 times

Your customer upgraded recently to version 12.2 to allow the Linux team to use the new MFA caching feature. The PSM for SSH was installed with default configuration settings. After setting the Authentication to SSH key and enabling MFA Caching from the PVWA interface, the Linux Team cannot connect successfully using the new MFA caching feature.

What is the most probable cause?

- A. OpenSSH 7.8 or above is not installed.
- B. The MFACaching parameter in the psmpparms file is not set to True.
- C. A passphrase policy must be added.
- D. MFA caching is not supported when the PSM for SSH is deployed with default settings.

Suggested Answer: A

Community vote distribution

A (88%) 13%

 **penuelaandy** Highly Voted 10 months ago

Selected Answer: A

Sorry. Option A is correct.

Because the question say PSM for SSH is installed with default configuration, so starting from version 12.0, the default installation mode of PSM for SSH To use MFA caching in Integrated mode (InstallCyberArkSSHD=Integrated), OpenSSH 7.8 and above is required on the PSM for SSH machine.

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.2/en/Content/PASIMP/MFA-Caching.htm?searchString=&from=0&sortBy=_score&orderBy=desc0242ac120009&resultsPerPage=10&exactPhrase=&withOneOrMore=&withoutTheWords=&pageSize=10&language=en&state=1&suCaseCreate=false#:~:t
upvoted 8 times

 **penuelaandy** 10 months ago

B. The MFACaching parameter in the psmpparms file is not set to True. INVALID.

Because that parameter doesn't exist.

C. A passphrase policy must be added. INVALID

Because passphrase policy is needed if you enable passphrase to greater security. But you can use MFACaching without passphrase.

D. MFA caching is not supported when the PSM for SSH is deployed with default settings. INVALID.

Because the question say MFACaching was enabled.


upvoted 5 times

 **Cavdog** Most Recent 4 months, 3 weeks ago

Selected Answer: A

This one is also a bit tricky in the sense that the default settings have MFA Caching disabled which would make either B. or D. correct however it specifically states that it was enabled via the PVWA and there is no MFACaching parameter in psmpparms so that leaves the prerequisite for OpenSSH 7.8+ as the only reasonable cause.

<https://docs.cyberark.com/PAS/Latest/en/Content/PASIMP/MFA-Caching.htm#:~:text=OpenSSH%207.8%20and%20above%20is%20required%20on%20the%20PSM%20for%20SSH%20machine>
upvoted 3 times

 **Fabri59** 8 months, 1 week ago

Selected Answer: A

The answer is A. https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20Cloud/ChangeServerKeys-cloud.htm?tocpath=Installation%7CInstall%20Privileged%20Access%20Manager%20-%20Self-Hosted%2%A0in%20a%20cloud%20environment%7CInstall%20the%20Digital%20Vault%20on%20the%20cloud%7C___14

upvoted 3 times

 **penuelaandy** 10 months, 3 weeks ago

Selected Answer: C

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/MFA-Caching.htm#Addapassphrasepolicy>

upvoted 2 times

Which service must be set to Automatic (delayed start) after the Vault is installed and configured?

- A. Windows Time service
- B. PrivateArk Database
- C. Windows Update service
- D. PrivateArk Server

Suggested Answer: A

Community vote distribution

A (94%)

6%

 **jacpicci** Highly Voted 10 months, 2 weeks ago

Selected Answer: A


https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/following-vault-Installation.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CCyberArk%20Digital%20Vault%20installation%7CInstall%20a%20Primary-DR%20Environment%7C___7#ConfiguretimesynchronizationontheVaultServerusingNTP
upvoted 8 times

 **Cavdog** Most Recent 4 months, 3 weeks ago

Selected Answer: A

As per the vendor recommendations the answer is A.

[https://docs.cyberark.com/PAS/Latest/en/Content/PAS%20INST/following-vault-Installation.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CCyberArk%20Digital%20Vault%20installation%7CInstall%20a%20Primary-DR%20Environment%7C___7#:~:text=you%20must%20set%20the%20Windows%20Time%20service%20to%20Automatic%20\(Delayed%20start\)](https://docs.cyberark.com/PAS/Latest/en/Content/PAS%20INST/following-vault-Installation.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CCyberArk%20Digital%20Vault%20installation%7CInstall%20a%20Primary-DR%20Environment%7C___7#:~:text=you%20must%20set%20the%20Windows%20Time%20service%20to%20Automatic%20(Delayed%20start))
upvoted 2 times

 **Fabri59** 8 months, 1 week ago

Selected Answer: A

The answer is A. https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/following-vault-Installation.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CCyberArk%20Digital%20Vault%20installation%7CInstall%20a%20Primary-DR%20Environment%7C___7
upvoted 2 times

 **Att84** 10 months, 1 week ago

Selected Answer: A

"After configuring the NTP settings and registration keys (refer to the Microsoft documentation for details), you must set the Windows Time service to Automatic (Delayed start) and start it in order for the settings to take effect."
upvoted 4 times

 **penuelaandy** 10 months, 3 weeks ago

Selected Answer: D

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/Install-the-CyberArk-Vault-Normal-Installation.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CCyberArk%20Digital%20Vault%20installation%7CInstall%20a%20Primary-DR%20Environment%7C___3#InstalltheDigitalVaultapplication
upvoted 1 times

 **penuelaandy** 10 months ago

Sorry, A es correct

upvoted 5 times

You want to add an additional maintenance user on the PSM for SSH.
How can you accomplish this if InstallCyberarkSSHD is set to Yes or No?

- A. Create a local user and add it to the PSMMaintenance Group.
- B. Create a local user called proxymng<number>.
- C. Create a local user and add it to group configured for the parameter AllowGroups in the /etc/sshd_config file.
- D. Create a local user, called psmmng<number>.

Suggested Answer: B

Community vote distribution

B (80%)

C (20%)

🗨️ **JM_Olympus** 1 month, 4 weeks ago

C:

<https://docs.cyberark.com/pam-self-hosted/13.0/en/Content/PASIMP/Administrating-the-PSMP.htm#Createamaintenanceuser>
upvoted 2 times

🗨️ **Cavdog** 11 months ago

Selected Answer: B

The only logical answer could be B. as there is no such group as PSMMaintenance, the path in C. is missing a folder and is targeted towards InstallCyberarkSSHD config being set to "Integrated" and D. is not identified as a maintenance user.

<https://docs.cyberark.com/PAS/13.0/en/Content/PASIMP/Administrating-the-PSMP.htm#:~:text=SSH%C2%A0server%3A-,proxymng,-proxymng%3Cnumber%3E>
upvoted 4 times

🗨️ **Fabri59** 1 year, 2 months ago

Selected Answer: B

The answer is B. https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PASIMP/Administrating-the-PSMP.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%20for%20SSH%7C____3
upvoted 2 times

🗨️ **Riaan_M** 1 year, 3 months ago

The answer is C:

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Administrating-the-PSMP.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%20for%20SSH%7C____3

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Administrating-the-PSMP.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%20for%20SSH%7C____3
upvoted 2 times

🗨️ **marcosneves** 1 year, 3 months ago

Selected Answer: B

The sshd_config file path is not /etc/sshd_config.

The correct path is /etc/ssh/sshd_config.

That is, answer C is invalid.

The documentation is very clear, the proxymng user is recognized by default as a maintenance user, and to add additional maintenance users, just create proxymng<number>.

When the maintenance user name does not follow the default name, in that case we need to keep adding these names (user_adm01, user_adm02, etc) in the sshd_config file following the documentation parameters.


So, the correct answer is B.

upvoted 2 times

🗨️ **penuelaandy** 1 year, 4 months ago

Selected Answer: C


[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Administrating-the-PSMP.htm?
tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%20for%20SSH%7C____3#Createamaintenanceuser](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Administrating-the-PSMP.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%20for%20SSH%7C____3#Createamaintenanceuser)
upvoted 3 times

 **Att84** 1 year, 4 months ago

C looks more like installcyberarkSSHD is set to integrated. Then you use the allowgroups parameter.
The question is about if set yes of no:

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Administrating-the-PSMP.htm?
tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%20for%20SSH%7C____3#](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Administrating-the-PSMP.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%20for%20SSH%7C____3#)

And pathname misses a folder: ssh ..(etc\ssh\sshd_config)
upvoted 1 times

 **Att84** 1 year, 4 months ago

Selected Answer: B

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Administrating-the-PSMP.htm?
tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%20for%20SSH%7C____3](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Administrating-the-PSMP.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%20for%20SSH%7C____3)
upvoted 4 times

Which SMTP address can be set on the Notification Settings page to re-invoke the ENE setup wizard after the initial Vault installation?

- A. 255.255.255.255
- B. 8.8.8.8
- C. 192.168.1.1
- D. 1.1.1.1

Suggested Answer: D

Community vote distribution


D (77%)

A (23%)

 **penuelaandy** Highly Voted 10 months, 3 weeks ago

Selected Answer: D

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Event-Notification-Engine.htm#EnabletheENE>
upvoted 7 times

 **Riaan_M** 9 months, 3 weeks ago

Correct.

upvoted 2 times

 **Cavdog** Most Recent 4 months, 3 weeks ago

Selected Answer: A

In order to re-invoke the ENE setup the SMTP address must be set to 1.1.1.1


[https://docs.cyberark.com/PAS/13.0/en/Content/PASIMP/Event-Notification-Engine.htm?](https://docs.cyberark.com/PAS/13.0/en/Content/PASIMP/Event-Notification-Engine.htm?tocpath=Administrator%7CComponents%7CEmail%20notifications%7C____0#:~:text=the%20ENE%20setup%20wizard%20will%20only%20be%20enabled%2)

[tocpath=Administrator%7CComponents%7CEmail%20notifications%7C____0#:~:text=the%20ENE%20setup%20wizard%20will%20only%20be%20enabled%2](https://docs.cyberark.com/PAS/13.0/en/Content/PASIMP/Event-Notification-Engine.htm?tocpath=Administrator%7CComponents%7CEmail%20notifications%7C____0#:~:text=the%20ENE%20setup%20wizard%20will%20only%20be%20enabled%2)
upvoted 1 times

 **Cavdog** 4 months, 2 weeks ago

Correction, the answer is D.


upvoted 3 times

 **dominicx** 5 months, 1 week ago

Selected Answer: D

1.1.1.1 for re config the ene config


upvoted 3 times

 **Fabri59** 8 months, 1 week ago

Selected Answer: A

The answer is A. <https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PASIMP/Event-Notification-Engine.htm>

upvoted 2 times

 **Fabri59** 8 months, 1 week ago

The answer is D 1.1.1.1. <https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PASIMP/Event-Notification-Engine.htm>

upvoted 2 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`

Suggested Answer: B

Community vote distribution

B (69%) C (25%) 6%

🗳️ 👤 **2995142** 2 months, 2 weeks ago

C is correct

linuxadmin01@root01@centos.acme.corp @10.0.1.16 -> From Lab
upvoted 2 times

🗳️ 👤 **2995142** 2 months, 1 week ago

well went through the document and there is mentioned about the # sign which an optional char, so the answer will be B here
upvoted 1 times

🗳️ 👤 **hyuraki** 8 months, 1 week ago

Selected Answer: D

Example find in CyberArk Lab training documentation:

carlos@logon01@target-lin.acme.corp@psm-ssh-gw.acme.corp
upvoted 1 times

🗳️ 👤 **hyuraki** 8 months ago

I selected wrong, the answer is C based in training documentation
upvoted 2 times

🗳️ 👤 **Cavdog** 11 months ago

Selected Answer: B

After revisiting this question can confirm that the answer is B. as optional parameters can be sperated from required parameters using '#' such as addin domain in the example provided. This is covered off in the reference below. However to use this syntax, the InstallCyberArkSSHD parameter must be set Integrated.

<https://docs.cyberark.com/PAS/Latest/en/Content/PASIMP/PSSO-PMSP.htm?>

tocpath=End%20user%7CConnect%20to%20Accounts%7CPrivileged%20Single%20Sign-

On%7C____3#:~:text=Required%20parameters%20are%20separated%20from%20optional%20parameters%20by%20E2%80%98%23%E2%80%99%20(hash
upvoted 4 times

🗳️ 👤 **rlam** 1 year ago

Selected Answer: B

Answer B is correct indeed from the doc sent. However it is really tricky as you never get to look at it that way in i&c training.
upvoted 3 times

🗳️ 👤 **Fabri59** 1 year, 2 months ago

The answer is B. <https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PASIMP/PSSO-PMSP.htm?>

tocpath=End%20user%7CConnect%20to%20Accounts%7CPrivileged%20Single%20Sign-On%7C____3

upvoted 3 times



🗳️ 👤 **laternak26** 1 year, 3 months ago

Selected Answer: B

With default config, the domain delimiter will be #



<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/PSSO-PMSP.htm#PSMforSSHCommand>

upvoted 4 times

  **Att84** 1 year, 3 months ago

You're right!

upvoted 1 times

  **Att84** 1 year, 4 months ago

Selected Answer: C

C is correct

upvoted 1 times

  **penuelaandy** 1 year, 4 months ago

Selected Answer: C

C is correct

upvoted 3 times

In addition to bit rate and estimated total duration of recordings per day, what is needed to determine the amount of storage required for PSM recordings?

- A. retention period
- B. number of PSMs
- C. number of users
- D. number of targets

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ **Cavdog** 4 months, 3 weeks ago

Selected Answer: A

As per CyberArk documentation the retention period is one of the most important considerations when calculating storage requirements. Therefore the answer would be A.

https://docs.cyberark.com/PAS/13.2/en/Content/PAS%20INST/Considerations-Before-Installing-PSM.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PSM%7C____1#:~:text=of%20your%20implementation.,Planning%20capacity,-Determine%20the%20amount

upvoted 2 times

🗨️ **Fabri59** 8 months, 1 week ago

Selected Answer: A

The answer is A. https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/Considerations-Before-Installing-PSM.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PSM%7C____1
upvoted 1 times

🗨️ **penuelaandy** 10 months, 3 weeks ago

Selected Answer: A

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/Considerations-Before-Installing-PSM.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PSM%7C____1#Planningcapacity
upvoted 3 times


Which components can connect to a satellite Vault in a distributed Vault architecture?

- A. CPM, EPM, PTA
- B. PVWA, PSM
- C. CPM, PVWA, PSM
- D. CPM, PSM

Suggested Answer: B

Community vote distribution


B (100%)

 **Cavdog** 4 months, 3 weeks ago

Selected Answer: B


Even with environments with multiple CPMs they should only ever be connected to the primary Vault therefore the answer is B.

<https://docs.cyberark.com/PAS/13.2/en/Content/PAS%20INST/Distributed-Vaults-Introduction.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CCyberArk%20Digital%20Vault%20installation%7CIntroduction%20to%20Digital%20Vault%20installation%7CDistributed%20Vaults%20environme>
upvoted 2 times

 **Fabri59** 8 months, 1 week ago

Selected Answer: B

The answer is B. <https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/Distributed-Vaults-Introduction.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CCyberArk%20Digital%20Vault%20installation%7CIntroduction%20to%20Digital%20Vault%20installation%7CDistributed%20Vaults%20environme>
upvoted 1 times

 **Att84** 10 months, 1 week ago

Selected Answer: B

Satelite is read-only and to avoid an split brain situation only the primary vault is connected to CPM's
upvoted 3 times

 **penuelaandy** 10 months, 3 weeks ago

Selected Answer: B

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/Distributed-Vaults-Introduction.htm?tocpath=Installation%7CInsta>
Hosted%7CCyberArk%20Digital%20Vault%20installation%7CIntroduction%20to%20Digital%20Vault%20installation%7CDistributed%20Vaults%20environme
upvoted 3 times

You are installing PSM for SSH with AD-Bridge and CyberArkSSHD mode set to integrated for your customer. Which additional packages do you need to install to meet the customer's needs? (Choose two.)

- A. CARKpsmp-infra
- B. libssh
- C. OpenSSH 7.8 or higher
- D. CARKpsmp-ADBridge
- E. CARKpsmp-SSHD

Suggested Answer: AB

Community vote distribution

AB (100%)

 **penuelaandy** Highly Voted 10 months, 3 weeks ago

Selected Answer: AB

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/Installing-the-PSMP.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PSM%20for%20SSH%7C____2#Installation
upvoted 6 times

 **Cavdog** Most Recent 4 months, 3 weeks ago

Selected Answer: AB

When installing PSM for SSH libssh is required regardless of which mode CyberArkSSHD is set to:


[https://docs.cyberark.com/PAS/13.2/en/Content/PAS%20INST/Installing-the-PSMP.htm#:~:text=InstallCyberArkSSHD%3DNo-,InstallCyberArkSSHD%20%3D%20Integrated,-\(this%20is%20the](https://docs.cyberark.com/PAS/13.2/en/Content/PAS%20INST/Installing-the-PSMP.htm#:~:text=InstallCyberArkSSHD%3DNo-,InstallCyberArkSSHD%20%3D%20Integrated,-(this%20is%20the)

However if CyberArkSSHD is set to integrated you must also install CARKpsmp-infra:

[https://docs.cyberark.com/PAS/13.2/en/Content/PAS%20INST/Installing-the-PSMP.htm#:~:text=InstallCyberArkSSHD%3DNo-,InstallCyberArkSSHD%20%3D%20Integrated,-\(this%20is%20the](https://docs.cyberark.com/PAS/13.2/en/Content/PAS%20INST/Installing-the-PSMP.htm#:~:text=InstallCyberArkSSHD%3DNo-,InstallCyberArkSSHD%20%3D%20Integrated,-(this%20is%20the)

Therefore the answers are A. & B.

upvoted 2 times

 **Fabri59** 8 months, 1 week ago

Selected Answer: AB

The answer are A and B. https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/Installing-the-PSMP.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PSM%20for%20SSH%7C____2
upvoted 2 times

Which component should be installed on the Vault if Distributed Vaults are used with PSM?

- A. RabbitMQ
- B. Disaster Recovery
- C. Remote Control Client
- D. Distributed Vault Server

Suggested Answer: A

Community vote distribution

A (100%)

 **penuelaandy** Highly Voted 10 months, 3 weeks ago

Selected Answer: A


https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/Following-Distributed-Vaults-Installation%20-%20Components.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CCyberArk%20Digital%20Vault%20installation%7CInstall%20a%20Distributed%20Vault%20Environment%7C____8#PSM
upvoted 6 times

 **Cavdog** Most Recent 4 months, 3 weeks ago

Selected Answer: A

As per step one under the Installations step in the reference (and as shown in the screenshot) RabbitMQ is required for distributed vault environment.

https://docs.cyberark.com/PAS/13.2/en/Content/PAS%20INST/Installing-the-CyberArk-Master-Vault.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CCyberArk%20Digital%20Vault%20installation%7CInstall%20a%20Distributed%20Vault%20Environment%7C____3#:~:text=Select%20installation%20install%20the
upvoted 2 times

 **Fabri59** 8 months, 1 week ago

Selected Answer: A

The answer is A. https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/Following-Distributed-Vaults-Installation%20-%20Components.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CCyberArk%20Digital%20Vault%20installation%7CInstall%20a%20Distributed%20Vault%20Environment%7C____8
upvoted 2 times

What is the default username for the PSM for SSH maintenance user when InstallCyberarkSSHD is set to yes?

- A. proxymng
- B. psmm_maintenance
- C. psmmaintenanceuser
- D. psmmnguser

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ **Cavdog** 4 months, 2 weeks ago

Selected Answer: A

By default PSM for SSH identifies proxymng as a maintenance user when they connect.

[https://docs.cyberark.com/PAS/13.2/en/Content/PASIMP/Administrating-the-PSMP.htm?](https://docs.cyberark.com/PAS/13.2/en/Content/PASIMP/Administrating-the-PSMP.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%20for%20SSH%7C____3#:~:text=SSH%C2%A0server%3A-,proxymng,-proxymng%3Cnumber%3E)

[tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%20for%20SSH%7C____3#:~:text=SSH%C2%A0server%3A-,proxymng,-proxymng%3Cnumber%3E](https://docs.cyberark.com/PAS/13.2/en/Content/PASIMP/Administrating-the-PSMP.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%20for%20SSH%7C____3#:~:text=SSH%C2%A0server%3A-,proxymng,-proxymng%3Cnumber%3E)

upvoted 3 times

🗨️ **Fabri59** 8 months, 1 week ago

Selected Answer: A

The answer is A. [https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PASIMP/Administrating-the-PSMP.htm?](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PASIMP/Administrating-the-PSMP.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%20for%20SSH%7C____3)

[tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%20for%20SSH%7C____3](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PASIMP/Administrating-the-PSMP.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%20for%20SSH%7C____3)

upvoted 3 times

🗨️ **penuelaandy** 10 months ago

Selected Answer: A

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Administrating-the-PSMP.htm?](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Administrating-the-PSMP.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%20for%20SSH%7C____3#Createamaintenanceuser)

[tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%20for%20SSH%7C____3#Createamaintenanceuser](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Administrating-the-PSMP.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%20for%20SSH%7C____3#Createamaintenanceuser)

upvoted 4 times

🗨️ **WadeLee** 10 months, 2 weeks ago

Correct answer is A

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Administrating-the-PSMP.htm?](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Administrating-the-PSMP.htm?Highlight=Maintenance%20user%20psmp)

[Highlight=Maintenance%20user%20psmp](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Administrating-the-PSMP.htm?Highlight=Maintenance%20user%20psmp)

upvoted 3 times

🗨️ **umesh02** 10 months, 2 weeks ago

proxymng is the default user

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Administrating-the-PSMP.htm?](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Administrating-the-PSMP.htm?Highlight=Maintenance%20user%20psmp)

[Highlight=Maintenance%20user%20psmp](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Administrating-the-PSMP.htm?Highlight=Maintenance%20user%20psmp)

upvoted 3 times

Which parameter must be identical for both the Identity Provider (IdP) and the PVWA?

- A. IdP "EntityID" and "PartnerIdentityProvider Name" in PVWA saml.config file
- B. IdP "User name" and "SingleSignOnServiceUrl" in PVWA saml.config file
- C. IdP "Audience" and "ServiceProviderName" in the PVWA saml.config file
- D. IdP "Secure hash algorithm" and "Certificate" in the PVWA saml.config file

Suggested Answer: C

Community vote distribution

C (92%)

8%

🗳️ **Cavdog** 4 months, 3 weeks ago

Selected Answer: C

The audience IdP parameter is used to identify the PVWA as a relying party. Therefore the ServiceProviderName on the PVWA must include the same value as it enables the PVWA to identify itself to the IdP.

Therefore the answer is C.

<https://docs.cyberark.com/PAS/Latest/en/Content/PAS%20INST/SAML-Authentication.htm#:~:text=unspecified%20NameID%20format-,Audience,-The%20value%20used>
upvoted 4 times

🗳️ **Fabri59** 8 months, 1 week ago

Selected Answer: C

The answer is C. https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/SAML-Authentication.htm?tocpath=Administrator%7CUser%20Management%7CAuthenticate%20to%20Privileged%20Access%20Manager%20-%20Self-Hosted%7CConfigure%20authentication%20methods%7C___5
upvoted 2 times

🗳️ **penuelaandy** 10 months ago

Selected Answer: A

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/SAML-Authentication.htm#:~:text=The%20value%20used%20by%20the,recommended%20and%20most%20secure%20flow>
upvoted 1 times

🗳️ **penuelaandy** 10 months ago

Sorry, is C

upvoted 2 times

🗳️ **Att84** 10 months, 1 week ago

Selected Answer: C

Audience

The value used by the IdP to identify the PVWA as a relying party.

The value must be identical to the ServiceProvider Name configures in PAM - Self-Hosted.

upvoted 1 times

🗳️ **umesh02** 10 months, 2 weeks ago

Selected Answer: C

Audience is the parameter

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/SAML-Authentication.htm#:~:text=The%20value%20used%20by%20the,recommended%20and%20most%20secure%20flow>
upvoted 4 times

All 80 employees from your satellite Tokyo office are complaining that browsing the PVWA site is very slow; however, your New York headquarters users are not experiencing this. The current PAM solution is:

- 2 distributed Vaults, the primary one in New York and a satellite in Tokyo
- 2 PVWA servers, both in New York with load balancing configured
- 2 PSM servers, both in New York without load balancing configured
- 1 CPM server in New York

All PVWA, PSM, and CPM servers are connected to the primary Vault

Which proposal optimally resolves the performance issue while minimizing the impact to production?

- A. Install two new PVWA servers in Tokyo data center, configure load balancing, connect to the local satellite Vault and provide the URL of new PVWA servers to the local employees.
- B. Install two new PVWA servers in New York data center, configure load balancing and have them connect to the satellite Vault in Tokyo.
- C. Install two new PSM servers in the Tokyo data center, configure load balancing, connect to the local satellite vault, and inform the local employees to browse using the same PVWA URL.
- D. Change the current distributed Vaults architecture, migrate back to a Primary-DR architecture, install two new PVWA servers in the Tokyo data center and configure load balancing. Connect to the local DR Vault and provide the URL of new PVWA servers to the local employees.

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ **Cavdog** 4 months, 3 weeks ago

Selected Answer: A

While there is no direct reference stating that A. is the best course of action it's definitely possible despite the caveats in the references provided and ar

<https://docs.cyberark.com/PAS/11.2/en/Content/PAS%20INST/Installing-PVWA-in-Distributed-Vault-Environment.htm>

<https://cyberark-customers.force.com/s/article/How-to-connect-PVWA-to-a-Satellite-Vault>

<https://docs.cyberark.com/PAS/Latest/en/Content/PAS%20INST/Distributed-Vaults-Components-Features.htm?TocPath=Installation%7CInstall%20PAM%20Hosted%7CCyberArk%20Digital%20Vault%20installation%7CIntroduction%20to%20Digital%20Vault%20installation%7CDistributed%20Vaults%20environment%20Read%20Only%20mode>

upvoted 2 times

🗨️ **Fabri59** 8 months, 1 week ago

Selected Answer: A

The answer is A.

upvoted 1 times

🗨️ **penuelaandy** 10 months ago

Selected Answer: A

A is correct

upvoted 1 times

🗨️ **Att84** 10 months, 1 week ago

Selected Answer: A

A is correct, PVWA and PSM can connect to a satellite vault. a CPM only to a Primary vault.

upvoted 4 times

🗨️ **umesh02** 10 months, 2 weeks ago

Selected Answer: A

I think so correct answer is A

upvoted 1 times

You have been asked to limit a platform called "Windows_Servers" to safes called "WindowsDC1" and "WindowsDC2". The platform must not be assigned to any other safe.

What is the correct way to accomplish this?

- A. Edit the "Windows_Servers" platform, expand "Automatic Password Management", then select General and modify "AllowedSafes" to be (WindowsDC1)|(WindowsDC2).
- B. Edit the "Windows_Servers" platform, expand "Automatic Password Management", then select Options and modify "AllowedSafes" to be (Win*).
- C. Edit the "WindowsDC1" and "WindowsDC2" safes through Safe Management, Add "Windows_Servers" to the "AllowedPlatforms".
- D. Log in to PrivateArk using an Administrative user, Select File, Server File Categories, Locate the category "WindowsServersAllowedSafes" and specify "WindowsDC1,WindowsDC2".

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ **Cavdog** 4 months, 2 weeks ago

Selected Answer: A

The AllowedSafes parameter can be found in the Platform configuration under Automatic Password Management > General. The field is limited to 700 chars.

<https://docs.cyberark.com/PAS/Latest/en/Content/PASIMP/Limit-Platforms-to-Specific-Safes.htm>

upvoted 3 times

🗨️ **Fabri59** 8 months, 1 week ago

Selected Answer: A

The answer is A. https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PASIMP/Limit-Platforms-to-Specific-Safes.htm?tocpath=End%20user%7CPrivileged%20Accounts%7CClassic%20Interface%7CManage%20platforms%20classic%20interface%7C____7.

upvoted 1 times

🗨️ **penuelaandy** 10 months ago

Selected Answer: A

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Limit-Platforms-to-Specific-Safes.htm#:~:text=In%20the%20list,in%20all%20Safes>.

upvoted 2 times

🗨️ **Att84** 10 months, 1 week ago

Selected Answer: A

AllowedSafes

A regular expression that lists the Safes that this policy can be applied to.

upvoted 1 times

The account used to install a PVWA must have ownership of which safes? (Choose two.)

- A. VaultInternal
- B. PVWAConfig
- C. System
- D. Notification Engine
- E. PVWAReports

Suggested Answer: AD

Community vote distribution

AD (100%)

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

A,D.

[https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/PVWA-install-requirements.htm?](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/PVWA-install-requirements.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PVWA%7C____2)

[tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PVWA%7C____2](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/PVWA-install-requirements.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PVWA%7C____2)

upvoted 8 times

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

Selected Answer: AD

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/PVWA-install-requirements.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PVWA%7C____2#:~:text=The%20user%20performing%20the%20installation%20must%20have%20ownership%20of%20the%20VaultInternal

[#:~:text=The%20user%20performing%20the%20installation%20must%20have%20ownership%20of%20the%20VaultInternal](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/PVWA-install-requirements.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PVWA%7C____2#:~:text=The%20user%20performing%20the%20installation%20must%20have%20ownership%20of%20the%20VaultInternal)

upvoted 6 times

 **Toretto** Most Recent 3 months ago

Selected Answer: AD

Safe ownership

The user performing the installation must have ownership of the VaultInternal and Notification Engine Safes, and the following permissions:

List Files

Retrieve Files


Manage Safe

Manage Safe Owners

View Audit

View Owners

upvoted 1 times

 **Cavdog** 1 year, 4 months ago

Selected Answer: AD

As per Cyberark Documentation the user performing the install must have ownership of the VaultInternal and NotificationEngine safes.

https://docs.cyberark.com/PAS/Latest/en/Content/PAS%20INST/PVWA-install-requirements.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PVWA%7C____2#:~:text=Audit%20Users-,Safe%20ownership,-The%20user%20performing

[#:~:text=Audit%20Users-,Safe%20ownership,-The%20user%20performing](https://docs.cyberark.com/PAS/Latest/en/Content/PAS%20INST/PVWA-install-requirements.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PVWA%7C____2#:~:text=Audit%20Users-,Safe%20ownership,-The%20user%20performing)

upvoted 2 times

 **Fabri59** 1 year, 8 months ago

Selected Answer: AD

The answer are A and D. [https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/PVWA-install-requirements.htm?](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/PVWA-install-requirements.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PVWA%7C____2)

[tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PVWA%7C____2](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/PVWA-install-requirements.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PVWA%7C____2)

upvoted 2 times

DRAG DROP -

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

Answer Area

Unordered Options

Run the PVWAInstallation.ps1 script in PowerShell as Administrator.

Run the PVWA_Prerequisites.ps1 script in Powershell as Administrator.

Run the PVWARegisterComponent.ps1 script with the Vault password and run the PVWA_Hardening.ps1 script in PowerShell as Administrator.



Ordered Response



Suggested Answer:

Ordered Response

Run the PVWA_Prerequisites.ps1 script in Powershell as Administrator.

Run the PVWAInstallation.ps1 script in PowerShell as Administrator.

Run the PVWARegisterComponent.ps1 script with the Vault password and run the PVWA_Hardening.ps1 script in PowerShell as Administrator.

The steps needed to install the Password Vault Web Access (PVWA) should be completed in the following order: PVWA_Prerequisites.ps1, PVWAInstallation.ps1, and

PVWARegisterComponent.ps1 with the Vault password followed by PVWA_Hardening.ps1.

This will ensure that all prerequisites are met before attempting to install and configure PVWA properly. By ensuring these steps are taken in this specific order, it allows for a successful installation of the software on the desired machine or server. After taking these necessary steps in sequence, users can then enjoy their newly installed Password Vault Web Access.

Cavdog 4 months, 3 weeks ago

Pretty self explanatory, run the PVWAPrerequisites.ps1 script, PVWAInstallation.ps1 script, PVWARegisterComponents.ps1 script then PVWA_Hardening.ps1 at the end.

<https://docs.cyberark.com/PAS/Latest/en/Content/PAS%20INST/PVWA-install-preinstall-tasks.htm>

<https://docs.cyberark.com/PAS/Latest/en/Content/PAS%20INST/PVWA-Installation.htm>

<https://docs.cyberark.com/PAS/Latest/en/Content/PAS%20INST/PVWA-hardening-runsript.htm>

upvoted 2 times

Besi2023 6 months, 2 weeks ago

ANS: B, A, C

upvoted 2 times

Which configuration file and Vault utility are used to migrate the server key to an HSM?

- A. DBparm.ini and CAVaultManager.exe
- B. VaultKeys.ini and CAVaultManager.exe
- C. DBparm.ini and ChangeServerKeys.exe
- D. VaultKeys.ini and ChangeServerKeys.exe

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ **Cavdog** 4 months, 3 weeks ago

Selected Answer: A

PKCS11ProviderPath and AllowNonStandard FWAddresses need to be updated in the dbparm.ini and then the CAVaultManager utility can be used to load the key onto the HSM. So answer is A.

AllowNonStandard FWAddresses
upvoted 3 times

🗨️ **Fabri59** 8 months, 1 week ago

Selected Answer: A

The answer is A. https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PASREF/DBParm.ini.htm?tocpath=Administrator%7CReferences%7CConfiguration%20Files%7CCyberArk%20Vault%20Server%20Parameter%20Files%7C____1
upvoted 3 times

🗨️ **penuelaandy** 10 months ago

Selected Answer: A

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASREF/DBParm.ini.htm?tocpath=Administrator%7CReferences%7CConfiguration%20Files%7CCyberArk%20Vault%20Server%20Parameter%20Files%7C____1#:~:text=Server%20ke
upvoted 4 times

🗨️ **ewitkop** 10 months, 3 weeks ago

It is A.
upvoted 3 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.

Suggested Answer: D

Community vote distribution

D (47%)

A (35%)

C (18%)

🗨️ **43aa45a** 3 months, 1 week 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 default or current and the only will change the password within the FromHour to ToHour.

As well in article that someone has put here :

<https://cyberark.my.site.com/s/article/00004112>

upvoted 2 times

🗨️ **Cavdog** 11 months ago

Selected Answer: A

This is a tricky one but I'm inclined to go A. as well, the interval parameter controls how often the CPM looks for system-initiated CPM work. If it is >120 (the CPM sees the trigger and tries to act at 3:01 or later which is outside the window.

[https://docs.cyberark.com/PAS/13.2/en/Content/PASREF/Automatic%20Password%20Management%20-%20General.htm?](https://docs.cyberark.com/PAS/13.2/en/Content/PASREF/Automatic%20Password%20Management%20-%20General.htm?tocpath=Administrator%7CReferences%7CConfigure%20the%20system%20through%20PVWA%7CPlatform%20properties%7CAutomatic%20Password%20M)

[The%20number%20of](https://docs.cyberark.com/PAS/13.2/en/Content/PASREF/Automatic%20Password%20Management%20-%20General.htm?tocpath=Administrator%7CReferences%7CConfigure%20the%20system%20through%20PVWA%7CPlatform%20properties%7CAutomatic%20Password%20M)

upvoted 1 times

🗨️ **Cavdog** 10 months, 3 weeks ago

It's also worth noting that for versions up to v9.10 there was a formula issued by CyberArk to calculate the value of this parameter when used in conjunction with FromHour and ToHour: $(\text{Timeframe of FromHour ToHour in minutes}/2)-1=\text{Interval}$. For example if set from 2 to 4 am, it would be have been $(120/2)-1=59$.

<https://cyberark-customers.force.com/s/article/00004112>

upvoted 1 times

🗨️ **rlam** 1 year ago

Selected Answer: D

After having checked on lab, there's no DaysToRun parameter, only ExecutionDays.

So C is not the correct answer as the parameter invoked doesn't exist.

D is the right answer.

upvoted 3 times

🗨️ **Fabri59** 1 year, 2 months ago

The most likely cause of the issue is that the DaysToRun setting for the platform is incorrect So the correct answer probably is C or D.

upvoted 1 times

🗨️ **laternak26** 1 year, 3 months ago

Selected Answer: A

Interval - The number of minutes after which the Central Policy Manager re-reads the list of platforms, to handle new platforms or remove deleted ones.

So the interval must be less than 120 minutes to make sure that CPM will change password within that 2 hour window.

upvoted 2 times

🗨️ **TraciG** 1 year, 3 months ago

Selected Answer: A

The interval setting is to control how often the CPM looks for system-initiated CPM work. If it is >120 say 121 - the trigger happens at 01:00, CPM sees the trigger and tries to act at 3:01. It's outside the window, so it can't change the password.

upvoted 3 times

🗨️ **penuelaandy** 1 year, 4 months ago

Selected Answer: C

Interval is the number of minutes after which the Central Policy Manager re-reads the list of platforms.

ImmediateInterval determines the number of minutes it takes before the first rotation attempt.

HeadStartInterval is the number of days before the password expires.

DaysToRun doesn't exist. ExecuteDays is the answer. I think is the parameter should appear in the exam and maybe is the parameter the autor meant

upvoted 3 times

🗨️ **Att84** 1 year, 4 months ago

good point, but how about: "however, this does not work consistently" apparently it does work but not always..

upvoted 3 times

🗨️ **penuelaandy** 1 year, 4 months ago

Maybe. Yes.

Because if HeadStartInterval = 0 means the password will be change the same expiration day. If not equal 0, the password can change before Sat or Sun and other weeks/months can fix that desired days...

Good observation.

upvoted 1 times

🗨️ **Att84** 1 year, 4 months ago

Selected Answer: D

DaystoRun setting does not exists, HeadStartinterval default is 0..

So I think it must be D

upvoted 3 times

What must you do to synchronize a new Vault server with an organization's NTP server?

- A. Configure an AllowNonStandardFWAddresses rule for the organization's NTP server in DBParm.ini on the Vault server.
- B. Use the Windows Firewall console to configure a rule on the Vault server which allows communication with the organization's NTP server.
- C. Ensure the organization's NTP server is installed in the same location as the Vault server requiring synchronization.
- D. Update the AutoSyncExternalObjects configuration in DBParm.ini on the Vault server to schedule regular synchronization.

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ **Fabri59** 2 months ago

Selected Answer: A

The answer is A. https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/following-vault-Installation.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CCyberArk%20Digital%20Vault%20installation%7CInstall%20a%20Primary-DR%20Environment%7C___7

upvoted 4 times

🗨️ **penuelaandy** 4 months ago

Selected Answer: A

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/following-vault-Installation.htm#:~:text=ln%20C%3A%5CProgram,123%3Aoutbound/udp>

upvoted 2 times

🗨️ **Att84** 4 months ago

Selected Answer: A

A Firewall rule must be added to the DBPARM.INI file, to allow NTP communication with the Time Server. As with all changes to the DBPARM.INI, a restart of the PrivateArk Server service is required.

AllowNonStandardFWAddresses=[X.X.X.X,Y.Y.Y.Z.Z.Z.Z],Yes,123:outbound/udp

upvoted 4 times

You need to add a new PSM server to an existing CyberArk environment.

What is the best way to determine the sizing of this server?

- A. Review the "Recommended Server Specifications" for PSMs in the CyberArk Documents website.
- B. Use the specifications of any existing PSM and request a server of the same size.
- C. Use the CyberArk Support Knowledgebase, search for "PSM Sizing" and locate the Knowledgebase article related to sizing.
- D. Refer to the Microsoft Windows website, determine the minimum specifications required for the Operating System you are installing, and then add 4 Gb of RAM and 20 GB of disk.

Suggested Answer: A

Community vote distribution

A (93%)

7%

🗳️ 👤 **Cavdog** 4 months, 2 weeks ago

Selected Answer: A

The logical answer is to consult the recommended server specifications provided by CyberArk with special consideration being given to storage requirements for recordings based on the formula in the PSM Installation considerations doco.

<https://docs.cyberark.com/PAS/13.2/en/Content/PAS%20SysReq/System%20Requirements%20-%20PSM.htm>

<https://docs.cyberark.com/PAS/13.2/en/Content/PAS%20INST/Considerations-Before-Installing-PSM.htm>

upvoted 4 times

🗳️ 👤 **Fabri59** 8 months, 1 week ago

Selected Answer: A

The best way to determine the sizing of a new PSM server in an existing CyberArk environment would be to review the "Recommended Server Specifications" for PSMs in the CyberArk Documents website. So the correct answer would be option A.

upvoted 3 times

🗳️ 👤 **TraciG** 10 months ago

Selected Answer: A

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20SysReq/Recommended%20Server%20Specifications.htm>

upvoted 2 times

🗳️ 👤 **penuelaandy** 10 months ago

Selected Answer: A

I think A is the logic answer.

B doesn't make much sense, cuz maybe existing PSM Servers doesn't meet the trully requirement, and maybe the administrator have to install 2 new PSM Servers if follow the same specification of current servers.

And C and D don't make sense.

upvoted 4 times

🗳️ 👤 **umesh02** 10 months, 2 weeks ago

Selected Answer: B

think so its B

upvoted 1 times


Which file must you edit to ensure the PSM for SSH server is not hardened automatically after installation?

- A. vault.ini
- B. user.cred
- C. psmpparms
- D. psmgw.config

Suggested Answer: C

Community vote distribution

C (100%)

 **Cavdog** 4 months, 3 weeks ago

Selected Answer: C

It's definitely C. the psmpparms file.


https://docs.cyberark.com/PAS/13.2/en/Content/PAS%20INST/Before-Installing-PSMP.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PSM%20for%20SSH%7C____1#:~:text=completing%20the%20registration-,Create%20the%20PSM%20for%20SSH%20parameters%20Create%20the%20PSM
upvoted 2 times

 **vikramanmca** 6 months ago

Selected Answer: C

C is correct

upvoted 1 times

 **Fabri59** 8 months, 1 week ago


Selected Answer: C

The answer is C. https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/Installing-the-PSMP.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PSM%20for%20SSH%7C____2
upvoted 1 times

 **penuelaandy** 10 months ago


Selected Answer: C

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PrivCloud/Latest/en/Content/Privilege%20Cloud/privCloud-prerequ-PSM-SSH.htm#CreatethePSMforSSHparametersfile>
upvoted 3 times

 **Bulu1988** 10 months, 2 weeks ago

C is correct answer

upvoted 2 times

 **WadeLee** 10 months, 2 weeks ago

C

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PrivCloud/Latest/en/Content/Privilege%20Cloud/privCloud-prerequ-PSM-SSH.htm>
upvoted 3 times

When integrating a Vault with HSM, which file is uploaded to the HSM device?

- A. server.key
- B. recpub.key
- C. recprv.key
- D. mdbase.dat

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ **Cavdog** 4 months, 2 weeks ago

Selected Answer: A

In accordance with CyberArk best practices and the documented process the server.key file can be stored a HSM device as a secure way of storing it while making it more easily available in the even of planned restarts et. Than storing it in a physical safe.

<https://docs.cyberark.com/PAS/13.2/en/Content/PAS%20INST/configuring-HSM-Key-Management.htm>

upvoted 2 times

🗨️ **Fabri59** 8 months, 1 week ago

Selected Answer: A

The answer is A. <https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.2/en/Content/PAS%20INST/configuring-HSM-Key-Management.htm>

upvoted 3 times

🗨️ **penuelaandy** 10 months ago

Selected Answer: A

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.2/en/Content/PAS%20INST/configuring-HSM-Key-Management.htm#_Ref242158975:~:text=CyberArk%20Vault%20operations.,Generate%20the%20server%20key%20in%20the%20HSM,-Make%20sure%20that

upvoted 3 times

🗨️ **Att84** 10 months, 1 week ago

Selected Answer: A

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.2/en/Content/PAS%20INST/configuring-HSM-Key-Management.htm>

upvoted 4 times

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

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

Suggested Answer: B

Community vote distribution

B (100%)

 **Att84** Highly Voted 1 year, 4 months ago

Selected Answer: B

B is correct, this is de first step:

Configure RADIUS Authentication

To configure the RADIUS authentication, you need to prepare by collecting the required information, then configure an organization SSL certificate for the Vault server. After you configure the certificate, you need to place the RADIUS secret in a Safe.

Preparation

In the RADIUS server, define the CyberArk Vault as a RADIUS client/agent. For more information, refer to your vendor's RADIUS server documentation.

upvoted 5 times

 **penuelaandy** 1 year, 4 months ago

Is correct. B s is the prerequisite and the answer of this particular question.

Option D is part of the configuration of RADIUS auth on Cyberark.

upvoted 3 times

 **JM_Olympus** Most Recent 2 months ago

B

<https://docs.cyberark.com/pam-self-hosted/13.2/en/Content/PAS%20INST/RADIUS-Authentication.htm#ConfigureRADIUSAuthentication>

upvoted 1 times

 **Cavdog** 11 months ago

Selected Answer: B

As per the doco the firststep in preparing for the installation is defining the Vault as a RADIUS client/agent under "Preparation". So the answer is B.

https://docs.cyberark.com/PAS/13.2/en/Content/PAS%20INST/RADIUS-Authentication.htm?tocpath=Administrator%7CUser%20Management%7CAuthenticate%20to%20Privileged%20Access%20Manager%20-%20Self-Hosted%7CConfigure%20authentication%20methods%7C___4#:~:text=to%20255%20characters.,Configure%20RADIUS%20Authentication,-To%20configure%20the

upvoted 3 times

 **cyb01** 1 year ago

Prerequisite is B, D is the actual config to use the radius. Correct answer B.

upvoted 3 times

 **Fabri59** 1 year, 2 months ago

Selected Answer: B

Before CyberArk can be configured to support RADIUS authentication, a prerequisite step is to define the CyberArk Vault as a RADIUS client/agent in the RADIUS server. So the correct answer would be option B. This will allow the RADIUS server to recognize and authenticate requests coming from the CyberArk Vault. <https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/RADIUS-Authentication.htm>

toopath=Administrator%7CUser%20Management%7CAuthenticate%20to%20Privileged%20Access%20Manager%20-%20Self-Hosted%7CConfigure%20authentication%20methods%7C____4

upvoted 3 times

  **marcosneves** 1 year, 3 months ago

Selected Answer: B

If you pay attention to the documentation, the first step for Radius integration is described in answer B.

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/RADIUS-Authentication.htm>

Preparation:

1. In the RADIUS server, define the CyberArk Vault as a RADIUS client/agent. For more information, refer to your vendor's RADIUS server documentation.

2. Gather the following information from the RADIUS server:

RADIUS server hostname, FQDN, or IP address

RADIUS server Port

Host name of the RADIUS client (Vault machine). This name must be identical to the name

you entered for the RADIUS client/agent.

Password secret

upvoted 4 times

  **FastSloth** 1 year, 4 months ago

D

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/RADIUS-Authentication.htm>

upvoted 1 times

  **WadeLee** 1 year, 4 months ago

Correct answer is D

upvoted 1 times

A customer wants to store PSM recordings for 100 days and estimates they will have 10 Windows sessions per day for 100 minutes each. What is the minimum storage required for the Vault and PAReplicate for the PSM recordings?

- A. 25 GB
- B. 250 GB
- C. 500 GB
- D. 5 GB

Suggested Answer: A

Community vote distribution

A (55%)

B (45%)

 **Fabri59** Highly Voted 1 year, 8 months ago

Selected Answer: A

The answer is A

The estimated storage requirement for PSM recordings is approximately 50-250 KB for each minute of a recording session. The recording size is affected by the type of session recording (console vs. GUI recording) as well as by the type and number of activities that are performed during the session.

In this case, the customer wants to store PSM recordings for 100 days and estimates they will have 10 Windows sessions per day for 100 minutes each. This means that the total number of minutes of recording will be 100 days * 10 sessions/day * 100 minutes/session = 100,000 minutes.

At the high end of the estimated storage requirement, this would require 100,000 minutes * 250 KB/minute = 25 GB of storage.

However, the customer may be able to get away with less storage if they use a lower quality recording setting or if they only record certain types of sessions.

upvoted 8 times

 **Pascal_57** Most Recent 5 months, 3 weeks ago

Why adding 20 Gb to the only formula provided by official documentations and then ending with 250 gb instead of 25 Gb?

upvoted 1 times

 **venkatesh24** 7 months, 2 weeks ago

Selected Answer: B

It is option B

upvoted 1 times

 **MaheswaraReddy** 11 months ago

Ans 25GB

Recording 250KB/Min

And exp

1Day -> 10*100= 1000Min/Day

100Days -> 1000*100= 100000 Min


1MB = 1000KB

1GB = 1000MB= 1000*1000KB= 1000000KB

1KB = 1/1000000 GB

Total GB = 100000*250/1000000= 25GB

upvoted 3 times

 **hyuraki** 1 year, 2 months ago

Selected Answer: B

After exhausting calculation, the best answer is the B.

First of all, we need to understand the minimum quality possible it is 100 KB/s

100 x 10 x 100 x 100 KB + 20 GB.

after we need to convert the value of session KB to GB:

$100 \times 10 \times 100 \times 0,0001 + 20 \text{ GB} = 30 \text{ GB}$

upvoted 1 times

🗨️ **Cavdog** 1 year, 4 months ago

Selected Answer: B

Another trick question, based on the formula provided by CyberArk: $100(\text{retention}) \times 10(\# \text{ of sessions}) \times 100(\text{minutes each}) \times 250 (\text{kb/min}) + 20\text{GB} = 45\text{GB}$ therefore the next smallest size is 250GB so I'd be inclined to agree that the answer is in fact B.

https://docs.cyberark.com/PAS/13.2/en/Content/PAS%20INST/Considerations-Before-Installing-PSM.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PSM%7C___1#:~:text=of%20your%20implementation.,Planning%20capacity,-Determine%20the%20amount

upvoted 2 times

🗨️ **Riaan_M** 1 year, 9 months ago

Selected Answer: A

$[(100 \text{ min}) \times (10 \text{ sessions})] \times (100 \text{ days}) \times 250(\text{kb/min}) = 25000000\text{kb} = 25 \text{ GB}$. The answer should be A.

upvoted 3 times

🗨️ **TraciG** 1 year, 10 months ago

$((100 \text{ days}) \times (10 \text{ sessions/day}) \times (100 \text{ minutes/session}) \times (250 \text{ kb/min})) = 25 \text{ GB}$

upvoted 3 times

🗨️ **Att84** 1 year, 9 months ago

it's $(S_{PSM}) = (C_{session})(t_{session})(R_{(session \text{ recording})}) + 20\text{GB}$

so is $25 \text{ gb} + 20\text{gb} = 45 \text{ gb}$. So minimum is 250 GB

upvoted 1 times

🗨️ **penuelaandy** 1 year, 10 months ago

Selected Answer: B

$[(100 \text{ min}) \times (10 \text{ sessions})] \times (100 \text{ days}) \times 250(\text{kb/min})$

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/Considerations-Before-Installing-PSM.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PSM%7C___1#Planningcapacity

upvoted 2 times

🗨️ **Riaan_M** 1 year, 9 months ago

$[(100 \text{ min}) \times (10 \text{ sessions})] \times (100 \text{ days}) \times 250(\text{kb/min}) = 25000000\text{kb} = 25 \text{ GB}$. So according to the way you calculated, the answer should be A.

upvoted 1 times

🗨️ **Att84** 1 year, 10 months ago

Selected Answer: B

$(100 \text{ days}) \times (10 \text{ sessions/day}) \times (100 \text{ minutes/session}) + 20\text{GB} = 100 \text{ 020 (100 GB)}$

minimum is 250 GB

upvoted 3 times

🗨️ **Att84** 1 year, 9 months ago

$*100 \text{ GB} + 20 \text{ Gb} = 120 \text{ GB}$

upvoted 1 times

🗨️ **1a6559f** 3 months, 2 weeks ago

In the question, we're asked to identify the size for PSM Recordings and PARecplicate. if you have a Primary and DR vault, you need to store two copies of the recordings (one in each Vault) so you have to double the storage

$120\text{GB} \times 2 = 240 \text{ GB}$

upvoted 1 times

🗨️ **Att84** 1 year, 9 months ago

the correct calculation:

it's $(S_{PSM}) = (C_{session})(t_{session})(R_{(session \text{ recording})}) + 20\text{GB}$

so is $25 \text{ gb} + 20\text{gb} = 45 \text{ gb}$. So minimum is 250 GB

upvoted 1 times

In large-scale environments, it is important to enable the CPM to focus its search operations on specific Safes instead of scanning all Safes it sees in the Vault.

How is this accomplished?

- A. Administration Options > CPM Settings
- B. AllowedSafe Parameter on each platform policy
- C. MaxConcurrentConnection parameter on each platform policy
- D. Administration > Options > CPM Scanner

Suggested Answer: B

Community vote distribution

B (100%)

🗨️ **Cavdog** 4 months, 3 weeks ago

Selected Answer: B

Definitely B. for this one.

<https://docs.cyberark.com/PAS/Latest/en/Content/PASIMP/Limit-Platforms-to-Specific-Safes.htm#:~:text=In%20large%2Dscale%20environments%2C%20it%20is%20very%20important%20to%20enable%20the%20CPM%20to%20focus%20its%20>

upvoted 3 times

🗨️ **Fabri59** 8 months ago

Selected Answer: B

The answer is B. [https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PASIMP/Limit-Platforms-to-Specific-Safes.htm?](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PASIMP/Limit-Platforms-to-Specific-Safes.htm?tocpath=End%20user%7CPrivileged%20Accounts%7CClassic%20Interface%7CManage%20platforms%20classic%20interface%7C____7)

tocpath=End%20user%7CPrivileged%20Accounts%7CClassic%20Interface%7CManage%20platforms%20classic%20interface%7C____7

upvoted 2 times

🗨️ **penuelaandy** 10 months ago

B is correct

upvoted 2 times

🗨️ **Att84** 10 months, 1 week ago

Selected Answer: B

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Limit-Platforms-to-Specific-Safes.htm>

upvoted 3 times

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

- A. performs IIS hardening
- B. configures all group policy settings
- C. renames the local Administrator Account
- D. configures Windows Firewall
- E. imports the CyberArk INF configuration

Suggested Answer: AE

Community vote distribution

AE (100%)

 **JM_Olympus** 2 months ago

AE

<https://docs.cyberark.com/pam-self-hosted/Latest/en/Content/PAS%20INST/PVWA-hardening-runscript.htm#Overview>

inf file is imported first. Do not be misled by order of possible answers

upvoted 1 times


 **Cavdog** 11 months ago

Selected Answer: AE

Another sneaky one, the script performs alot of IIS hardening so A. is definitely one however while it makes changes to the local policy it doesn't do anything with "group policy" and it also doesn't do anything with the firewall or the built in administrator account but as per the reference the first thing it does is import the INF configuration for MMC so answers are A. and E.

<https://docs.cyberark.com/PAS/Latest/en/Content/PAS%20INST/PVWA-hardening-task-descriptions.htm>

upvoted 2 times

 **Fabri59** 1 year, 2 months ago

Selected Answer: AE

The answers are A and E. https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PAS%20INST/PVWA-hardening-runscript.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PVWA%7CPVWA%20Hardening%7CHarden%20the%20PVWA%20server%7C____0

upvoted 3 times

 **penuelaandy** 1 year, 4 months ago

Selected Answer: AE

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/PVWA-hardening-runscript.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PVWA%7CPVWA%20Hardening%7CHarden%20the%20PVWA%20server%7C____0#Overview

upvoted 4 times

 **FastSloth** 1 year, 4 months ago

AE is Correct.

upvoted 4 times

 **WadeLee** 1 year, 4 months ago

Correct answer is AE

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/PVWA-hardening-runscript.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PVWA%7CPVWA%20Hardening%7CHarden%20the%20PVWA%20server%7C____0

upvoted 4 times