Question #1 *Topic 1*

If a user is a member of more than one group that has authorizations on a safe, by default that user is granted___________________.

A. the vault will not allow this situation to occur.

B. only those permissions that exist on the group added to the safe first.

C. only those permissions that exist in all groups to which the user belongs.

D. the cumulative permissions of all the groups to which that user belongs.

Suggested Answer: *D*

Community vote distribution

D (88%) 12%

josephdonalds Highly Voted 3 years, 6 months ago

Selected Answer: D

answer is D, also in the official CyberArk test questions

upvoted 10 times

seiler Highly Voted 3 years, 2 months ago

Selected Answer: D

as in Cyberark test examples

upvoted 5 times

raselrana68 Most Recent 1 year, 2 months ago

Answer D is the correct answer

upvoted 1 times

Sirdick_junior7 1 year, 9 months ago

Answer is D

upvoted 1 times

427243 1 year, 10 months ago

D officially it's should be D

upvoted 1 times

sahilyakup 2 years, 6 months ago

D is correct. It is not only permissions of the first added group. Also, combination of authorizations can be adopted by users who belongs to several groups inside a safe

upvoted 1 times

powertechnet 3 years, 3 months ago

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Managing-Groups.htm?TocPath=Inspect%20User%20Activity%7CManage%20groups%7C_____0

Answer is D

Users who are members of several Groups that own the same Safe, will either have the authorizations of the first group that was added as an Owner to a Safe, or a combination of the authorizations all the groups that they belong to, depending on how the Vault is configured. However, if the user is an independent Owner of the same Safe, his own authorizations will override those of the Group.

upvoted 3 times

Vaibhavk11 3 years, 4 months ago

Ans is D

upvoted 3 times

jairross 3 years, 4 months ago

Selected Answer: B

answer is B

upvoted 2 times

Nes32 3 years, 4 months ago

answer is D

upvoted 4 times

Question #2 *Topic 1*

It is possible to control the hours of the day during which a user may long into the vault.

A. TRUE

B. FALSE

Suggested Answer: *A*

Reference:

https://isecurenet.net/wp-content/uploads/2016/06/user-sb-cyberark_privileged_threat_analytics-030916-final-en-web.pdf

Community vote distribution

A (100%)

raselrana68 1 year, 2 months ago

Answer A

upvoted 1 times

Sirdick_junior7 1 year, 9 months ago

Answer is A

upvoted 1 times

427243 1 year, 10 months ago

The answer is A

upvoted 1 times

Kaustav01 3 years, 1 month ago

Selected Answer: A

https://cyberark-customers.force.com/s/question/0D52J00007KCErmSAH/how-to-control-hours-of-the-day-during-which-a-user-logs-into-the-vaul

upvoted 2 times

Kaustav01 3 years, 1 month ago

A

https://cyberark-customers.force.com/s/question/0D52J00007KCErmSAH/how-to-control-hours-of-the-day-during-which-a-user-logs-into-the-vault

upvoted 1 times

Question #3 *Topic 1*

VAULT authorizations may be granted to ____________________. (Choose all that apply.)

A. Vault Users

B. Vault Groups

C. LDAP Users

D. LDAP Groups

Suggested Answer: *A*

Community vote distribution

A (100%)

lmdroc 1 year, 4 months ago

The answer is: AC

upvoted 1 times

sp00ky84 3 years, 1 month ago

A and C

Vault Authorizations

• Can be assigned only to users (not groups).

• Cannot be inherited via group membership.

• Defined only via the Private Ark Client.

Safe Auth

• Assigned to users and/or groups.

• Can be inherited via group membership.

• Can be defined in the Private Ark Client or PVWA

upvoted 3 times

Paredes32 3 years, 5 months ago

Selected Answer: A

A and C

upvoted 3 times

flawr 3 years, 6 months ago

A and C

upvoted 1 times

seiler 3 years, 8 months ago

Selected Answer: A

A , can shown in privateark client under Tools/Administrative Tools/User and Groups../Select User /Update.. LDAP User can not be updated

upvoted 1 times

powertechnet 3 years, 9 months ago

Answer is correct

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

Users who are listed in an LDAP-compliant enterprise directory can also be managed transparently by the Vault. They can be added as Safe members and given security attributes and authorizations depending on their location in the directory. For more information, refer to .

upvoted 1 times

tuga99 3 years, 11 months ago

A and C

upvoted 3 times

yoontzt 3 years, 11 months ago

Answer : A and C

upvoted 3 times

Question #4 *Topic 1*

What is the purpose of the Interval setting in a CPM policy?

A. To control how often the CPM looks for System Initiated CPM work.

B. To control how often the CPM looks for User Initiated CPM work.

C. To control how long the CPM rests between password changes.

D. To control the maximum amount of time the CPM will wait for a password change to complete.

Suggested Answer: *A*

Community vote distribution

A (100%)

Imdroc 1 year, 4 months ago

Selected Answer: A

Answer is A

upvoted 1 times

Imdroc 1 year, 4 months ago

The answer is: A

upvoted 1 times

NLT 3 years, 1 month ago

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

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASREF/CPM%20Settings%20-%20Introduction.htm

upvoted 2 times

ahmedmostafa 3 years, 3 months ago

i did the exam and i failed on 21 oct non of the questions are exist in the exam .

upvoted 2 times

Kaustav01 3 years, 8 months ago

Selected Answer: A

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASREF/CPM%20Settings%20-%20Introduction.htm

upvoted 2 times

Kaustav01 3 years, 8 months ago

A

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASREF/CPM%20Settings%20-%20Introduction.htm

upvoted 1 times

Question #5 *Topic 1*

All of your Unix root passwords are stored in the safe UnixRoot. Dual control is enabled for some of the accounts in that safe. The members of the AD group
UnixAdmins need to be able to use the show, copy, and connect buttons on those passwords at any time without confirmation. The members of the AD group
OperationsStaff need to be able to use the show, copy and connect buttons on those passwords on an emergency basis, but only with the approval of a member of OperationsManagers. The members of OperationsManagers never need to be able to use the show, copy or connect buttons themselves.
Which safe permissions do you need to grant to OperationsStaff? (Choose all that apply.)

A. Use Accounts

B. Retrieve Accounts

C. List Accounts

D. Authorize Password Requests

E. Access Safe without Authorization

Suggested Answer: *A*

⊟ **Atoure_22** Highly Voted 👍 3 years, 5 months ago

The ensWer is ABC

upvoted 11 times

⊟ **powertechnet** Highly Voted 👍 3 years, 3 months ago

answer A, B , C

List accounts = to show list of accounts in safe

Use accounts = to connect to the target using PSM

retrieve accounts = show and copy passwords

upvoted 6 times

⊟ **ramazana** Most Recent ⏱ 1 year, 5 months ago

the answer is ABC with a request to OperationsManagers

upvoted 2 times

⊟ **dru0pa** 2 years ago

The answer is both A and C. As I have this setup in my lab and have tested this.

upvoted 1 times

⊟ **akik13** 2 years, 3 months ago

The answer is ABC

upvoted 1 times

⊟ **sahilyakup** 2 years, 6 months ago

I think here the answer is A, B, C and D. For connection users must be given Use account permission. Besides, to show and copy the account details, users must have the Retrieve account permission. Finally, if dual control is enabled and users request to use the account, they have to be given the Authorize account request permission in the safe.

upvoted 1 times

⊟ **sahilyakup** 2 years, 6 months ago

One that I forget to write here is that users who are given "Authorize account request" require the ‘List accounts’ authorization to see the Request details of the account requests waiting for their confirmation.

upvoted 1 times

Question #6 *Topic 1*

What is the purpose of the Immediate Interval setting in a CPM policy?

A. To control how often the CPM looks for System Initiated CPM work.

B. To control how often the CPM looks for User Initiated CPM work.

C. To control how long the CPM rests between password changes.

D. To control the maximum amount of time the CPM will wait for a password change to complete.

Suggested Answer: *B*

Community vote distribution

B (100%)

Imdroc 1 year, 4 months ago

Selected Answer: B

Answer is: B

upvoted 1 times

Imdroc 1 year, 4 months ago

Answer is: B

upvoted 1 times

akik13 2 years, 9 months ago

Selected Answer: B

The correct is B

upvoted 2 times

NLT 3 years, 1 month ago

ImmediateInterval - The number of minutes that the CPM waits when the user initiates a Change, Verify or Reconcile task (by clicking the corresponding button on the PVWA).

https://cyberark-customers.force.com/s/article/00000745

upvoted 1 times

Innuendo 3 years, 4 months ago

Selected Answer: B

The number of minutes that will elapse between when the user initiates an account management process and when the process is performed.

upvoted 3 times

harshuthkatta 3 years, 7 months ago

Selected Answer: B

B

is correct

upvoted 4 times

Kaustav01 3 years, 8 months ago

Selected Answer: B

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASREF/Automatic%20Password%20Management%20-%20General.htm?TocPath=Administration%7CReferences%7CConfigure%20the%20System%20through%20PVWA%7CPlatform%20properties%7CAutomatic%20Password%20M

upvoted 4 times

Kaustav01 3 years, 8 months ago

B

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASREF/Automatic%20Password%20Management%20-%20General.htm?TocPath=Administration%7CReferences%7CConfigure%20the%20System%20through%20PVWA%7CPlatform%20properties%7CAutomatic%20Password%20M

upvoted 3 times

rondi 3 years, 8 months ago

A

As per Cyberark Mock Test

upvoted 1 times

Nes32 3 years, 10 months ago

Correct answer : B

On Cyberark doc:

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASREF/Automatic%20Password%20Management%20-%20General.htm?
TocPath=Administration%7CReferences%7CConfigure%20the%20System%20through%20PVWA%7CPlatform%20properties%7CAutomatic%20Password%20M

upvoted 3 times

Nes32 3 years, 10 months ago

Correct answer : B

On Cyberark doc:

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASREF/Automatic%20Password%20Management%20-%20General.htm?
TocPath=Administration%7CReferences%7CConfigure%20the%20System%20through%20PVWA%7CPlatform%20properties%7CAutomatic%20Password%20M

upvoted 1 times

yoontzt 3 years, 11 months ago

Selected Answer: B

Correct Answer : C

upvoted 1 times

Question #7 *Topic 1*

Which utilities could you use to change debugging levels on the vault without having to restart the vault? (Choose all that apply.)

A. PAR Agent

B. PrivateArk Server Central Administration

C. Edit DBParm.ini in a text editor.

D. Setup.exe

Suggested Answer: *A*

Community vote distribution

B (67%) A (33%)

⊟ **yoontzt** Highly Voted 👍 3 years, 11 months ago

Answer : A and B

upvoted 9 times

⊟ **Imdroc** Most Recent ⏲ 1 year, 4 months ago

The Answer is: AB

upvoted 1 times

⊟ **Imdroc** 1 year, 4 months ago

Anwser is A, B.

upvoted 1 times

⊟ **amlal** 2 years, 2 months ago

Selected Answer: A

A & B is correct

upvoted 1 times

⊟ **carloslapa** 2 years, 9 months ago

Selected Answer: B

A resposta é B

upvoted 1 times

⊟ **kllearner** 3 years, 1 month ago

https://cyberark-customers.force.com/s/question/0D52J00007PA3aOSAT/changing-debugging-levels-on-the-vault-without-restarting-the-vault

upvoted 1 times

⊟ **Cyberark** 3 years, 6 months ago

Selected Answer: B

You can't use RCA in the vault.

upvoted 1 times

Question #8 *Topic 1*

A Logon Account can be specified in the Master Policy.

A. TRUE

B. FALSE

Suggested Answer: *B*

Community vote distribution

B (100%)

JohnWick15 Highly Voted 👍 3 years, 11 months ago

B, it will be under Platform settings.

upvoted 5 times

Imdroc Most Recent ⏲ 1 year, 4 months ago

Selected Answer: B

Answer is B - https://docs.cyberark.com/pam-self-hosted/Latest/en/Content/PASIMP/Using-Logon-Accounts-for-SSH-and-Telnet-Connections.htm#Automaticlogonsequence

upvoted 1 times

dru0pa 2 years, 6 months ago

Selected Answer: B

No logon account listed on the page
https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Working-with-Master-Policy-Rules.htm

upvoted 1 times

Hull 3 years, 9 months ago

Selected Answer: B

Nowhere in the master policy can you choose a logon account to use. It wouldn't make sense even, as different logon accounts are used for different systems, and master policy applies to all platforms regardless to which system it is used.

All available master policy settings can be found here:
https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Working-with-Master-Policy-Rules.htm

upvoted 3 times

tuga99 3 years, 11 months ago

answer is A

upvoted 1 times

Atoure_22 3 years, 11 months ago

No the enswer is A, to refer to the sample Exam PAM

upvoted 2 times

Question #9 *Topic 1*

For an account attached to a platform that requires Dual Control based on a Master Policy exception, how would you configure a group of users to access a password without approval?

A. Create an exception to the Master Policy to exclude the group from the workflow process.

B. Edit the master policy rule and modify the advanced 'Access safe without approval' rule to include the group.

C. On the safe in which the account is stored grant the group the 'Access safe without audit' authorization.

D. On the safe in which the account is stored grant the group the 'Access safe without confirmation' authorization.

Suggested Answer: *D*

Community vote distribution

D (100%)

yoontzt Highly Voted 3 years, 11 months ago

Selected Answer: D

Correct Answer : D

upvoted 12 times

Imdroc Most Recent 1 year, 4 months ago

Selected Answer: D

The Answer is: D

upvoted 1 times

Imdroc 1 year, 4 months ago

The Anwer is: D

upvoted 1 times

akik13 2 years, 9 months ago

Selected Answer: D

Correct is D

upvoted 2 times

harshuthkatta 3 years, 7 months ago

Selected Answer: D

D is correct

upvoted 3 times

jairross 3 years, 9 months ago

Selected Answer: D

Correct Answer : d

upvoted 4 times

Question #10 *Topic 1*

As long as you are a member of the Vault Admins group, you can grant any permission on any safe that you have access to.

A. TRUE

B. FALSE

Suggested Answer: *B*

Community vote distribution

B (75%) A (25%)

⊟ **ParameshM** 1 year ago

Selected Answer: B

Even if you are a member of the Vault Admins group, your ability to grant permissions on a safe depends on whether you have the "Manage Safe" permission for that specific safe. Being a Vault Admin grants you elevated privileges, but it does not automatically give you unrestricted access to all safes or the ability to assign permissions without explicit authorization on those safes.

upvoted 1 times

⊟ **Imdroc** 1 year, 4 months ago

Selected Answer: B

Answer is B

upvoted 2 times

⊟ **Imdroc** 1 year, 4 months ago

The answer is: B

upvoted 1 times

⊟ **43aa45a** 1 year, 8 months ago

Selected Answer: A

https://docs.cyberark.com/pam-self-hosted/Latest/en/Content/PASIMP/Predefined-Users-and-Groups.htm#Predefinedgroups

With one condition: (you can grant any permission)
"This group can be added to Safes with all Safe member authorizations." = have it

"that you have access to." - B= Being in Vault admins group only give you access to safes which are created during installation (safe created in installation process) -This is clearly mentioned in documents . - you have access to all safes that you have access with Vault Admins group ;)

upvoted 1 times

⊟ **ShaZZa_Anti_kit** 3 years, 3 months ago

B= Being in Vault admins group only give you access to safes which are created during installation (safe created in installation process) -This is clearly mentioned in documents .

upvoted 2 times

⊟ **Roper** 3 years, 6 months ago

B is correct

upvoted 4 times

Question #11 *Topic 1*

Which report provides a list of accounts stored in the vault?

A. Privileged Accounts Inventory

B. Privileged Accounts Compliance Status

C. Entitlement Report

D. Activity Log

Suggested Answer: *A*

Community vote distribution

A (100%)

Imdroc 1 year, 4 months ago

Selected Answer: A

Answer is A

upvoted 1 times

Imdroc 1 year, 4 months ago

The Answer is: A

upvoted 1 times

akik13 2 years, 9 months ago

Selected Answer: A

Correct is A

upvoted 2 times

Kaustav01 3 years, 8 months ago

Selected Answer: A

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/ReportsInPVWA.htm?TocPath=End%20User%7CReports%20and%20Audits%7C_____1

upvoted 2 times

Kaustav01 3 years, 8 months ago

A

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/ReportsInPVWA.htm?TocPath=End%20User%7CReports%20and%20Audits%7C_____1

upvoted 1 times

rondi 3 years, 8 months ago

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/ReportsInPVWA.htm?TocPath=End%20User%7CReports%20and%20Audits%7C_____1

upvoted 1 times

Question #12 *Topic 1*

When on-boarding account using Accounts Feed, which of the following is true?

A. You must specify an existing Safe where the account will be stored when it is on-boarded to the Vault.

B. You can specify the name of a new safe that will be created where the account will be stored when it is on-boarded to the Vault.

C. You can specify the name of a new Platform that will be created and associated with the account.

D. Any account that is on-boarded can be automatically reconciled regardless of the platform it is associated with.

Suggested Answer: *B*

Community vote distribution

B (100%)

yoontzt Highly Voted 👍 3 years, 11 months ago

Selected Answer: B

Correct Answer : B

upvoted 11 times

Jakub4444 3 years, 4 months ago

Agreed.

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

upvoted 1 times

CarlosAnd1989 Highly Voted 👍 3 years, 6 months ago

Correct answer: A

upvoted 5 times

lmdroc Most Recent 🕓 1 year, 4 months ago

The Answer is: B

upvoted 1 times

Ghost96 2 years, 1 month ago

Correct answer is A

upvoted 1 times

NLT 3 years, 2 months ago

Correct answer is B. We can click "Create Safe" button to create new safe, specify safe name and associated with the account when we add account via Accounts > Ass Account.

upvoted 1 times

Innuendo 3 years, 4 months ago

Selected Answer: B

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.1/en/Content/PASIMP/Onboarding-Accounts-and-SSH-Keys.htm?topath=End%20User%7CPrivileged%20Accounts%7CClassic%20Interface%7CAccounts%20Feed%7C_____4#Onboardi

upvoted 2 times

Question #13 *Topic 1*

Target account platforms can be restricted to accounts that are stored in specific Safes using the AllowedSafes property.

A. TRUE

B. FALSE

Suggested Answer: *A*

Community vote distribution

A (100%)

yoontzt Highly Voted 1 year, 11 months ago

Selected Answer: A

Correct Answer : A

upvoted 9 times

Jakub4444 1 year, 4 months ago

That's correct.

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.3/en/Content/PASIMP/Managing-Target-Service-Account-Platforms.htm

upvoted 1 times

AzDev937 Most Recent 1 year, 1 month ago

A is correct.

upvoted 1 times

NLT 1 year, 2 months ago

YES, we can restrict target account platforms for specific safes via PVWA > Administration > Platform Management > Select 1 Target account platform > Edit > Expand Automatic Password Management > AllowedSafes.

Reference linkhttps://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Limit-Platforms-to-Specific-Safes.htm

upvoted 1 times

fanisx88 1 year, 3 months ago

By default, platform configurations are applied to all Safes. From a security aspect, it is recommended to use the AllowedSafe parameter to enable platforms for specific Safes.

upvoted 1 times

harshuthkatta 1 year, 7 months ago

Selected Answer: A

A is correct

upvoted 1 times

Question #14 *Topic 1*

Which one of the following reports is NOT generated by using the PVWA?

A. Account Inventory

B. Application Inventory

C. Safes List

D. Compliance Status

Suggested Answer: *C*

Community vote distribution

C (100%)

Imdroc 1 year, 4 months ago

Selected Answer: C

Answer is C

upvoted 1 times

NLT 3 years, 2 months ago

Answer C is correct. We can generate the following reports via PVWA:

1.Privileged Accounts Inventory

2.Applications Inventory

3.Privileged Account Compliance Status

4.Entitlement

5.Activity Log

upvoted 3 times

Kaustav01 3 years, 8 months ago

Selected Answer: C

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/ReportsInPVWA.htm?TocPath=End%20User%7CReports%20and%20Audits%7C_____1

upvoted 3 times

Kaustav01 3 years, 8 months ago

C

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/ReportsInPVWA.htm?TocPath=End%20User%7CReports%20and%20Audits%7C_____1

upvoted 3 times

Question #15

Topic 1

PSM captures a record of each command that was executed in Unix.

A. TRUE

B. FALSE

Suggested Answer: *A*

Community vote distribution

A (100%)

Imdroc 1 year, 4 months ago

Selected Answer: A

Answer is A

upvoted 1 times

Kaustav01 3 years, 8 months ago

Selected Answer: A

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Configuring-Recordings-and-Audits-in-PSM.htm?Highlight=Master%20user

upvoted 2 times

Kaustav01 3 years, 8 months ago

A

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Configuring-Recordings-and-Audits-in-PSM.htm?Highlight=Master%20user

upvoted 1 times

Question #16 *Topic 1*

Platform settings are applied to_____________.

A. The entire vault.

B. Network Areas

C. Safes

D. Individual Accounts

Suggested Answer: *D*

Community vote distribution

D (93%) 7%

JohnWick15 Highly Voted 3 years, 11 months ago

D. Individual accounts.

upvoted 7 times

Jakub4444 3 years, 4 months ago

Indeed.

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/manage-platforms.htm?tocpath=Administrator%7CPrivileged%20Accounts%7C_____2

upvoted 1 times

NLT 3 years, 2 months ago

I saw this note "By default, platform configurations are applied to all Safes. Use the AllowedSafe parameter to enable platforms for specific Safes" in your provided link.

Correct answer is C.

upvoted 1 times

jairross Highly Voted 3 years, 9 months ago

Selected Answer: D

D. Individual accounts.

upvoted 5 times

Imdroc Most Recent 1 year, 4 months ago

Selected Answer: C

Safes have Accounts. You add safes to a platform.

By default, platform configurations are applied to all Safes. Use the AllowedSafe parameter to enable platforms for specific Safes.

upvoted 1 times

akik13 2 years, 9 months ago

Selected Answer: D

Correct D

upvoted 1 times

sammikun 2 years, 11 months ago

Selected Answer: D

D is correct. This appears in the official sample exam.

upvoted 1 times

carm8989 3 years, 7 months ago

Selected Answer: D

D:correct

upvoted 2 times

harshuthkatta 3 years, 9 months ago

Selected Answer: D

D is correct

upvoted 4 times

Question #17 *Topic 1*

Customers who have the 'Access Safe without confirmation' safe permission on a safe where accounts are configured for Dual control, still need to request approval to use the account.

A. TRUE

B. FALSE

Suggested Answer: *B*

Community vote distribution

B (100%)

⊟ **Kaustav01** 1 year, 1 month ago

Selected Answer: B

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

upvoted 1 times

⊟ **Kaustav01** 1 year, 2 months ago

B

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

upvoted 1 times

Question #18 *Topic 1*

What is the name of the Platform parameter that controls how long a password will stay valid when One Time Passwords are enabled via the Master Policy?

A. MinValidityPeriod

B. Interval

C. ImmediateInterval

D. Timeout

Suggested Answer: *A*

Community vote distribution

A (100%)

yoontzt Highly Voted 👍 3 years, 5 months ago

Selected Answer: A

Correct Answer : A

upvoted 9 times

raselrana68 Most Recent 🕒 1 year, 2 months ago

A is correct.

upvoted 1 times

sammikun 2 years, 5 months ago

Selected Answer: A

A is correct. This appears in the official sample exam.

upvoted 1 times

NLT 2 years, 8 months ago

Answer A is correct.

MinValidityPeriod:The number of minutes to wait from the last retrieval of the password until it is replaced. This gives the user a minimum period to be able to use the password before it is replaced. Use -1 to ignore this property. This parameter is also used to release exclusive accounts automatically.

upvoted 3 times

shaan619 3 years, 2 months ago

Selected Answer: A

Correct Answer: A

upvoted 2 times

harshuthkatta 3 years, 3 months ago

Selected Answer: A

A correct

upvoted 2 times

jairross 3 years, 3 months ago

Selected Answer: A

Correct Answer : A

upvoted 2 times

tuga99 3 years, 5 months ago

Selected Answer: A

A is the correct one

upvoted 3 times

Question #19 *Topic 1*

It is possible to leverage DNA to provide discovery functions that are not available with auto-detection.

A. TRUE

B. FALSE

Suggested Answer: *A*

Community vote distribution

A (100%)

Kaustav01 1 year, 1 month ago

Selected Answer: A

https://docs.cyberark.com/Product-Doc/OnlineHelp/PrivCloud/Latest/en/Content/Privilege%20Cloud/PrivCloud-Assess-network.htm#:~:text=CyberArk%20DNA%20is%20a%20discovery,privileged%20and%20non%2Dprivileged%20accounts.

upvoted 1 times

Kaustav01 1 year, 2 months ago

A

https://docs.cyberark.com/Product-Doc/OnlineHelp/PrivCloud/Latest/en/Content/Privilege%20Cloud/PrivCloud-Assess-network.htm#:~:text=CyberArk%20DNA%20is%20a%20discovery,privileged%20and%20non%2Dprivileged%20accounts.

upvoted 1 times

Question #20 *Topic 1*

Which of the following files must be created or configured in order to run Password Upload Utility? (Choose all that apply.)

A. PACli.ini

B. Vault.ini

C. conf.ini

D. A comma delimited upload file

Suggested Answer: *C*

Reference:

https://www.reddit.com/r/CyberARk/comments/84gfsb/password_upload_utility_error/

Nes32 Highly Voted 👍 3 years, 10 months ago

Correct answer : B C D

upvoted 10 times

Imdroc Most Recent ⏲ 1 year, 4 months ago

Answer is: BCD

upvoted 1 times

NLT 3 years, 1 month ago

BCD is correct.

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.4/en/Content/PAS%20INST/Password-Upload-Utility-Installation.htm

upvoted 2 times

Raymond9 3 years, 6 months ago

BCD

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.2/en/Content/PAS%20INST/Password-Upload-Utility-Installation.htm?tocpath=Installation%7CInstall%20PAM%7CInstall%20the%20Vault%20Utilities%7CPassword%20Upload%20Utility%7C_____2

upvoted 3 times

JohnWick15 3 years, 11 months ago

B, C, D

upvoted 4 times

Question #21 *Topic 1*

Users can be restricted through certain CyberArk interfaces (e.g. PVWA or PACLI).

A. TRUE

B. FALSE

Suggested Answer: *A*

Community vote distribution

A (100%)

Imdroc 1 year, 4 months ago

Selected Answer: A

Answer is A

upvoted 1 times

Roper 3 years, 6 months ago

A. TRUE

upvoted 2 times

Question #22 *Topic 1*

What is the purpose of the HeadStartInterval setting in a platform?

A. It determines how far in advance audit data is collected for reports.

B. It instructs the CPM to initiate the password change process X number of days before expiration.

C. It instructs the AIM Provider to 'skip the cache' during the defined time period.

D. It alerts users of upcoming password changes x number of days before expiration.

Suggested Answer: *B*

Community vote distribution

B (100%)

⊟ **Imdroc** 1 year, 4 months ago

Selected Answer: B

Answer is B

upvoted 1 times

⊟ **Kaustav01** 3 years, 8 months ago

Selected Answer: B

https://docs.cyberark.com/Product-Doc/OnlineHelp/PrivCloud/Latest/en/Content/PASREF/Automatic%20Password%20Management%20-%20Password%20Change.htm

upvoted 3 times

⊟ **Kaustav01** 3 years, 8 months ago

B

https://docs.cyberark.com/Product-Doc/OnlineHelp/PrivCloud/Latest/en/Content/PASREF/Automatic%20Password%20Management%20-%20Password%20Change.htm

upvoted 2 times

Question #23 *Topic 1*

It is possible to restrict the time of day, or day of week that a reconcile process can occur.

A. TRUE

B. FALSE

Suggested Answer: *A*

Community vote distribution

A (100%)

⊟ **Hull** Highly Voted 👍 3 years, 4 months ago

Selected Answer: A

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

upvoted 9 times

⊟ **Nes32** Highly Voted 👍 3 years, 4 months ago

A is correct

upvoted 7 times

⊟ **raselrana68** Most Recent 🕒 1 year, 2 months ago

A is the correct answer. It can be restrict in Platform Level

upvoted 1 times

Question #24 *Topic 1*

Which of the following options is not set in the Master Policy?

A. Password Expiration Time

B. Enabling and Disabling of the Connection Through the PSM

C. Password Complexity

D. The use of ג€One-Time-Passwordsג€

Suggested Answer: *C*

Community vote distribution

C (100%)

Imdroc 1 year, 4 months ago

Selected Answer: C

Answer is c

upvoted 1 times

sammikun 2 years, 11 months ago

Selected Answer: C

C. Password complexity is set on the platform level.

upvoted 1 times

Roper 3 years, 6 months ago

A and C

upvoted 1 times

Jakub4444 3 years, 4 months ago

Wrong. Only C.

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

upvoted 2 times

Kaustav01 3 years, 8 months ago

Selected Answer: C

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

upvoted 3 times

Kaustav01 3 years, 8 months ago

C

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

upvoted 1 times

Question #25 *Topic 1*

The primary purpose of exclusive accounts is to ensure non-repudiation (individual accountability).

A. TRUE

B. FALSE

Suggested Answer: *A*

Community vote distribution

A (100%)

Kaustav01 1 year, 1 month ago

Selected Answer: A

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

upvoted 1 times

Kaustav01 1 year, 2 months ago

A

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

upvoted 1 times

Question #26 *Topic 1*

The System safe allows access to the Vault configuration files.

A. TRUE

B. FALSE

Suggested Answer: *A*

Community vote distribution

A (100%)

yoontzt Highly Voted 3 years, 4 months ago

Selected Answer: A

Correct Answer : A

upvoted 7 times

raselrana68 Most Recent 1 year, 2 months ago

A is correct. System Safe consist of DBPARM.ini which is the main configuration file.

upvoted 1 times

Ghost96 1 year, 7 months ago

A is correct

upvoted 1 times

Phalguna_264462 2 years, 10 months ago

Selected Answer: A

Correct Answer : A

upvoted 3 times

Roper 3 years ago

Correct Answer : A

upvoted 2 times

Question #27

Topic 1

You have associated a logon account to one of your UNIX root accounts in the vault. When attempting to change the root account's password the CPM will`¦

A. Log in to the system as root, then change root's password.

B. Log in to the system as the logon account, then change root's password

C. Log in to the system as the logon account, run the su command to log in as root, and then change root's password.

D. None of these.

Suggested Answer: *C*

Community vote distribution

C (100%)

tuga99 Highly Voted 3 years, 11 months ago

Selected Answer: C

C is the correct answer

upvoted 8 times

vyshakv Highly Voted 4 years ago

Selected Answer: C

Once you login using logon account you have elevate the privilege to change passwords
So even CPM will elevate with Sudo command - Answer is C

upvoted 7 times

Imdroc Most Recent 1 year, 4 months ago

The answer is: C

upvoted 1 times

sanathbro 2 years, 4 months ago

Selected Answer: C

C is correct

upvoted 2 times

sammikun 2 years, 11 months ago

Selected Answer: C

C. This appears in the official sample exam.

upvoted 2 times

Sumandorwal 4 years, 1 month ago

correct answer is C

upvoted 5 times

Question #28 *Topic 1*

It is possible to restrict the time of day, or day of week that a verify process can occur.

A. TRUE

B. FALSE

Suggested Answer: *A*

Community vote distribution

A (100%)

Hull Highly Voted 2 years, 10 months ago

Selected Answer: A

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

upvoted 7 times

sanathbro Most Recent 1 year, 4 months ago

Selected Answer: A

It can

upvoted 1 times

harshuthkatta 2 years, 9 months ago

Selected Answer: A

A correct

upvoted 4 times

Question #29 *Topic 1*

Which of the Following can be configured in the Master Policy? (Choose all that apply.)

A. Dual Control

B. One Time Passwords

C. Exclusive Passwords

D. Password Reconciliation

E. Ticketing Integration

F. Required Properties

G. Custom Connection Components

H. Password Aging Rules

Suggested Answer: *ABCH*

Community vote distribution

ABCH (80%) ABH (20%)

hila84 Highly Voted 👍 3 years, 10 months ago

Selected Answer: ABCH

Password reconciliation is in platform settings

upvoted 5 times

Imdroc Most Recent 🕘 1 year, 4 months ago

Selected Answer: ABCH

A B C H

upvoted 1 times

raselrana68 1 year, 8 months ago

Selected Answer: ABCH

upvoted 1 times

AhmedHesham87 1 year, 11 months ago

Selected Answer: ABH

upvoted 1 times

Ivelknievel777 1 year, 11 months ago

ABH ; Exclusive Passwords does not exist. Only exclusive access

upvoted 2 times

Phalguna_264462 3 years, 4 months ago

Selected Answer: ABCH

ABCH is correct

upvoted 2 times

Kaustav01 3 years, 8 months ago

Selected Answer: ABCH

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

upvoted 4 times

Kaustav01 3 years, 8 months ago

ABCH

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

upvoted 3 times

Hull 3 years, 9 months ago

Selected Answer: ABH

Password reconciliation is most definitely not something you can set in master policy.

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Working-with-Master-Policy-Rules.htm

upvoted 3 times

⊟ **Jakub4444** 3 years, 4 months ago

You should add C - exclusive passwords too

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

upvoted 2 times

Question #30 *Topic 1*

If a password is changed manually on a server, bypassing the CPM, how would you configure the account so that the CPM could resume management automatically?

A. Configure the Provider to change the password to match the Vault's Password

B. Associate a reconcile account and configure the platform to reconcile automatically.

C. Associate a logon account and configure the platform to reconcile automatically.

D. Run the correct auto detection process to rediscover the password.

Suggested Answer: *B*

Community vote distribution

B (100%)

Benny_On 1 year, 2 months ago

Two options for this case:

1) Reconcile automatically

2) Change Vault's password match current password on target server at PVWA then verify

--> B is an answer

upvoted 1 times

Kaustav01 1 year, 8 months ago

Selected Answer: B

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.4/en/Content/PASIMP/Reconciling-Passwords.htm

upvoted 2 times

Kaustav01 1 year, 8 months ago

B

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.4/en/Content/PASIMP/Reconciling-Passwords.htm

upvoted 1 times

Question #31 *Topic 1*

What is the maximum number of levels of authorizations you can set up in Dual Control?

A. 1

B. 2

C. 3

D. 4

Suggested Answer: *B*

Community vote distribution

B (100%)

JSOC_DXB 1 year, 3 months ago

Answer B:

If the advanced Require multi-level password access approval setting was enabled:

After each confirmation or denial, a notification is sent to all authorized users at the confirmation level of the user who has just confirmed it.
After the first level of authorized users have confirmed a request, a notification about the request is sent to the second level of authorized users.
After the final confirmation, a notification is sent to both levels of authorized users.

upvoted 1 times

Imdroc 1 year, 4 months ago

Selected Answer: B

2 levels

upvoted 1 times

sunnyajmera 2 years, 11 months ago

Shouldn't this be C, 3.

upvoted 2 times

Kaustav01 3 years, 8 months ago

Selected Answer: B

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/PVWA-Dual-Control.htm?tocpath=Administrator%7CComponents%7CPVWA%7CConfigure%20the%20PVWA%7C_____7

upvoted 2 times

Kaustav01 3 years, 8 months ago

B

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/PVWA-Dual-Control.htm?tocpath=Administrator%7CComponents%7CPVWA%7CConfigure%20the%20PVWA%7C_____7

upvoted 1 times

Question #32 *Topic 1*

As long as you are a member of the Vault Admins group you can grant any permission on any safe.

A. TRUE

B. FALSE

Suggested Answer: *B*

Community vote distribution

B (100%)

JustTheUserCA 4 weeks, 1 day ago

Selected Answer: B

B - you need to add vault admins to a safe using the master account

upvoted 1 times

Imdroc 1 year, 4 months ago

Selected Answer: B

Clearly B

upvoted 1 times

raselrana68 1 year, 8 months ago

it should be A

upvoted 1 times

NLT 3 years, 1 month ago

I think the answer is TRUE.

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

The Vault Admins group is a group of Vault administrators. This group can be added to Safes with all Safe member authorizations. This group is added automatically to the following Safes.

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

upvoted 1 times

Question #33 *Topic 1*

In accordance with best practice, SSH access is denied for root accounts on UNIXLINUX system.
What is the BEST way to allow CPM to manage root accounts?

A. Create a privileged account on the target server. Allow this account the ability to SSH directly from the CPM machine. Configure this account of the target server's root account.

B. Create a non-privileged account on the target server. Allow this account the ability to SSH directly from the CPM machine. Configure this account as the Logon account of the target server's root account.

C. Configure the Unix system to allow SSH logins.

D. Configure the CPM to allow SSH logins.

Suggested Answer: *B*

Community vote distribution

B (100%)

Kaustav01 1 year, 1 month ago

Selected Answer: B

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Using-Logon-Accounts-for-SSH-and-Telnet-Connections.htm?Highlight=logon%20account

upvoted 3 times

Kaustav01 1 year, 1 month ago

B

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Using-Logon-Accounts-for-SSH-and-Telnet-Connections.htm?Highlight=logon%20account

upvoted 1 times

Question #34 *Topic 1*

Which of the following statements are NOT true when enabling PSM recording for a target Windows server? (Choose all that apply.)

A. The PSM software must be installed on the target server.

B. PSM must be enabled in the Master Policy (either directly, or through exception).

C. PSMConnect must be added as a local user on the target server.

D. RDP must be enabled on the target server.

Suggested Answer: *C*

tuga99 Highly Voted 3 years, 5 months ago

correct answers are A and C

upvoted 13 times

raselrana68 Most Recent 1 year, 2 months ago

correct answers are A and C

upvoted 2 times

Phalguna_264462 2 years, 10 months ago

correct answers are A and C

upvoted 3 times

Question #35 *Topic 1*

The Password upload utility can be used to create safes.

A. TRUE

B. FALSE

Suggested Answer: *A*

Community vote distribution

A (100%)

Imdroc 1 year, 4 months ago

Selected Answer: A

Answer is A

upvoted 1 times

Imdroc 1 year, 4 months ago

The Answer is: A

upvoted 1 times

xruinoiua 2 years, 10 months ago

Selected Answer: A

The answer is A

upvoted 2 times

Kaustav01 3 years, 8 months ago

Selected Answer: A

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Password-Upload-Utility.htm

upvoted 2 times

> **Jakub4444** 3 years, 4 months ago
>
> The answer is correct, but link seems to have expired. New one:
> https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.2/en/Content/PAS%20INST/Password-Upload-Utility-Installation-Considerations.htm?tocpath=Installation%7CInstall%20PAM%7CInstall%20the%20Vault%20Utilities%7CPassword%20Upload%20Utility%7C_____1
>
> upvoted 1 times

Kaustav01 3 years, 8 months ago

A

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Password-Upload-Utility.htm

upvoted 1 times

Question #36 *Topic 1*

Which CyberArk components products can be used to discover Windows Services or Scheduled Tasks that use privileged accounts? (Choose all that apply.)

A. Discovery and Audit (DNA)

B. Auto Detection (AD)

C. Export Vault Data (EVD)

D. On Demand Privileges manager (OPM)

E. Accounts Discovery

Suggested Answer: *AE*

Community vote distribution

AB (100%)

tuga99 Highly Voted 3 years, 11 months ago

Correct answer is : A,B,E

upvoted 10 times

lmdroc Most Recent 1 year, 4 months ago

The answer is: ABE

upvoted 1 times

raselrana68 1 year, 8 months ago

A, B, E

upvoted 1 times

xruinoiua 2 years, 10 months ago

Selected Answer: AB

A,B, E

upvoted 1 times

NLT 3 years, 1 month ago

DNA, Account Discovery and Auto-detection are correct anwers.

https://cyberark-customers.force.com/s/article/What-are-the-differences-between-Auto-Detection-and-Accounts-Discovery

upvoted 2 times

jojo2323 3 years, 3 months ago

the right answer is A & E, my boy Spenser told me so

upvoted 2 times

Question #37 *Topic 1*

A Reconcile Account can be specified in the Master Policy.

A. TRUE

B. FALSE

Suggested Answer: *B*

Community vote distribution

B (100%)

Imdroc 1 year, 4 months ago

Selected Answer: B

Answer is B

upvoted 1 times

Kaustav01 3 years, 8 months ago

Selected Answer: B

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

upvoted 4 times

Kaustav01 3 years, 8 months ago

B

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

upvoted 2 times

Question #38 Topic 1

In order to connect to a target device through PSM, the account credentials used for the connection must be stored in the vault?

A. True.

B. False. Because the user can also enter credentials manually using Secure Connect.

C. False. Because if credentials are not stored in the vault, the PSM will log into the target device as PSMConnect.

D. False. Because if credentials are not stored in the vault, the PSM will prompt for credentials.

Suggested Answer: *B*

Community vote distribution

B (100%)

Kaustav01 Highly Voted 3 years, 8 months ago

Selected Answer: B

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.3/en/Content/PASIMP/Configuring-Secure-Connect.htm

upvoted 5 times

Jakub4444 3 years, 4 months ago

Agreed. Slightly newer version of the documentation: https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/latest/en/Content/PASIMP/Configuring-Secure-Connect.htm#:~:text=In%20the%20PVWA%2C%20click%20Administration,Secure%20Connect%20User%20or%20Group.

upvoted 1 times

Jakub4444 3 years, 3 months ago

And I believe it's called ad hoc connections now.

upvoted 4 times

lmdroc Most Recent 1 year, 4 months ago

Selected Answer: B

ad hoc connections

upvoted 1 times

lmdroc 1 year, 4 months ago

Answer is: B

upvoted 1 times

xruinoiua 2 years, 10 months ago

Selected Answer: B

Stored in Vault or Secure Connect ad-hoc

upvoted 2 times

Question #39 *Topic 1*

SAFE Authorizations may be granted to _______________. (Choose all that apply.)

A. Vault Users

B. Vault Groups

C. LDAP Users

D. LDAP Groups

Suggested Answer: *A*

Community vote distribution

A (100%)

tuga99 Highly Voted 3 years, 11 months ago

correct answer is A B C D

upvoted 10 times

Imdroc Most Recent 1 year, 4 months ago

Answer is: ABCD

upvoted 1 times

Imdroc 1 year, 4 months ago

Answer is: ABCD

upvoted 1 times

raselrana68 1 year, 8 months ago

answer is A B C D

upvoted 1 times

dummy521 3 years, 1 month ago

Selected Answer: A

ABCD

is correct

upvoted 2 times

NLT 3 years, 1 month ago

Users who have access to safes are called Safe members. A Safe member can be a single user or a group.

https://docs.cyberark.com/Product-Doc/OnlineHelp/PrivCloud/Latest/en/Content/Privilege%20Cloud/privCloud-manage-safe-members.htm?topath=Administrators%7CAccess%20control%7C_____2

upvoted 1 times

Kaustav01 3 years, 8 months ago

ABCD

https://docs.cyberark.com/Product-Doc/OnlineHelp/PrivCloud/Latest/en/Content/Privilege%20Cloud/privCloud-manage-safe-members.htm?topath=Administrators%7CAccess%20control%7C_____2

upvoted 4 times

rondi 3 years, 8 months ago

Yes, ABCD are correct

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Adding-and-Managing-Safe-Members.htm?Highlight=safe%20permissions

upvoted 2 times

Question #40 *Topic 1*

Secure Connect provides the following features. (Choose all that apply.)

A. PSM connections to target devices that are not managed by CyberArk.

B. Session Recording.

C. real-time live session monitoring.

D. PSM connections from a terminal without the need to login to the PVWA.

Suggested Answer: *ABC*

Community vote distribution

ABC (100%)

Kaustav01 Highly Voted 3 years, 8 months ago

Selected Answer: ABC

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Connecting-with-Secure-Connect.htm

upvoted 7 times

Imdroc Most Recent 1 year, 4 months ago

Selected Answer: ABC

Answer is: ABC

upvoted 1 times

Imdroc 1 year, 4 months ago

Answer is: ABC

upvoted 1 times

xruinoiua 2 years, 10 months ago

Selected Answer: ABC

A, B, C

upvoted 2 times

NLT 3 years, 1 month ago

A,B,C are correct answers.
You can connect to any machine through PSM using any account, including those that are not managed in the CyberArk Vault.

Ad Hoc Connections connection refers to connecting to non-managed, or non-defined,machines by entering the target machine's credentials. Ad hoc connection sessions benefit from the standard PSM features, including session recording, detailed auditing, and standard audit records. In addition, authorized users can monitor active sessions in real time, assume control, and terminate them when necessary.

upvoted 2 times

Kaustav01 3 years, 8 months ago

ABC

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Connecting-with-Secure-Connect.htm

upvoted 2 times

Question #41 *Topic 1*

Which onboarding method would you use to integrate CyberArk with your accounts provisioning process?

A. Accounts Discovery

B. Auto Detection

C. Onboarding RestAPI functions

D. PTA Rules

Suggested Answer: *C*

Community vote distribution

C (100%)

Imdroc 1 year, 4 months ago

Selected Answer: C

Answer is C

upvoted 1 times

sanathbro 2 years, 4 months ago

Selected Answer: C

CA exam has similar question

upvoted 1 times

akik13 2 years, 9 months ago

Selected Answer: C

I think correct is C, i saw similar question in the mock exam

upvoted 1 times

sunnyajmera 2 years, 11 months ago

C, I think I have seen this question in the CyberArk Defender Sample Question too.

upvoted 2 times

duracell 3 years, 4 months ago

I guess the correct answer today would be Accounts Feed.

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Provisioning-Accounts-Automatically.htm?TocPath=End%20User%7CPrivileged%20Accounts%7CClassic%20Interface%7CAccount%20Management%7C_____4

upvoted 1 times

Kaustav01 3 years, 8 months ago

B?

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Provisioning-Accounts-Automatically.htm

upvoted 2 times

Question #42 *Topic 1*

What is the purpose of a linked account?

A. To ensure that a particular collection of accounts all have the same password.

B. To ensure a particular set of accounts all change at the same time.

C. To connect the CPNI to a target system.

D. To allow more than one account to work together as part of a password management process.

Suggested Answer: *D*

Community vote distribution

D (100%)

Imdroc 1 year, 4 months ago

Selected Answer: D

Answer is D

upvoted 1 times

Imdroc 1 year, 4 months ago

Answer is: D

upvoted 1 times

Kaustav01 3 years, 8 months ago

Selected Answer: D

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Linked-Accounts.htm?TocPath=End%20User%7CPrivileged%20Accounts%7CClassic%20Interface%7CManage%20platforms%20classic%20interface%7C_____8

upvoted 4 times

Kaustav01 3 years, 8 months ago

D

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Linked-Accounts.htm?TocPath=End%20User%7CPrivileged%20Accounts%7CClassic%20Interface%7CManage%20platforms%20classic%20interface%7C_____8

upvoted 1 times

Question #43 *Topic 1*

Which of the following PTA detections are included in the Core PAS offering?

A. Suspected Credential Theft

B. Over-Pass-The Hash

C. Golden Ticket

D. Unmanaged Privileged Access

Suggested Answer: *A*

Community vote distribution

A (100%)

Hull Highly Voted 3 years, 10 months ago

Selected Answer: A

Core PAS offers both A and D

upvoted 11 times

lmdroc Most Recent 1 year, 4 months ago

The answer is: AD

upvoted 1 times

akashbaots 2 years, 7 months ago

A and D

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

upvoted 1 times

carm8989 3 years, 7 months ago

answer: A,B

upvoted 1 times

> **Jakub4444** 3 years, 4 months ago
>
> Not correct. Should be A and D. This was mentioned in the official CyberArk mock exam.
>
> upvoted 5 times

Question #44 *Topic 1*

One can create exceptions to the Master Policy based on __________________.

A. Safes

B. Platforms

C. Policies

D. Accounts

Suggested Answer: *B*

Community vote distribution

B (100%)

tuga99 Highly Voted 3 years, 11 months ago

Selected Answer: B

B - Platforms

upvoted 11 times

Imdroc Most Recent 1 year, 4 months ago

Selected Answer: B

Answer is B

upvoted 1 times

Kaustav01 3 years, 8 months ago

Selected Answer: B

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Exceptions.htm?topath=Administrator%7CPrivileged%20Accounts%7CSecurity%20Policy%7C_____3

upvoted 4 times

Kaustav01 3 years, 8 months ago

B

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Exceptions.htm?topath=Administrator%7CPrivileged%20Accounts%7CSecurity%20Policy%7C_____3

upvoted 2 times

Question #45 *Topic 1*

The vault supports Role Based Access Control.

A. TRUE

B. FALSE

Suggested Answer: *A*

Community vote distribution

A (100%)

amlal 1 year, 2 months ago

Selected Answer: A

It is outrageous to pay so much but all the answers are wrong

upvoted 1 times

akik13 1 year, 9 months ago

Selected Answer: A

the correct is A. Role can be an auditor so it supports.

upvoted 1 times

Innuendo 2 years, 4 months ago

The Vault (PAM) itself does not support RBAC. Role base access controls could be deployed using an external directory (LDAP)

upvoted 1 times

Jakub4444 2 years, 4 months ago

Agreed - A. How come the 'reveal solution' never gives the correct answer?

upvoted 4 times

Kaustav01 2 years, 8 months ago

Selected Answer: A

https://docs.cyberark.com/Product-Doc/OnlineHelp/Idaptive/Latest/en/Content/CoreServices/GetStarted/Create-Roles.htm

upvoted 2 times

> **Innuendo** 2 years, 4 months ago
>
> But that info belongs to CyberArk Identity producto, it is not part of Cyberark PAM-Vault. Could you please, clarify?
>
> upvoted 1 times

Kaustav01 2 years, 8 months ago

A

https://docs.cyberark.com/Product-Doc/OnlineHelp/Idaptive/Latest/en/Content/CoreServices/GetStarted/Create-Roles.htm

upvoted 2 times

tuga99 2 years, 11 months ago

Selected Answer: A

Correct answer: A

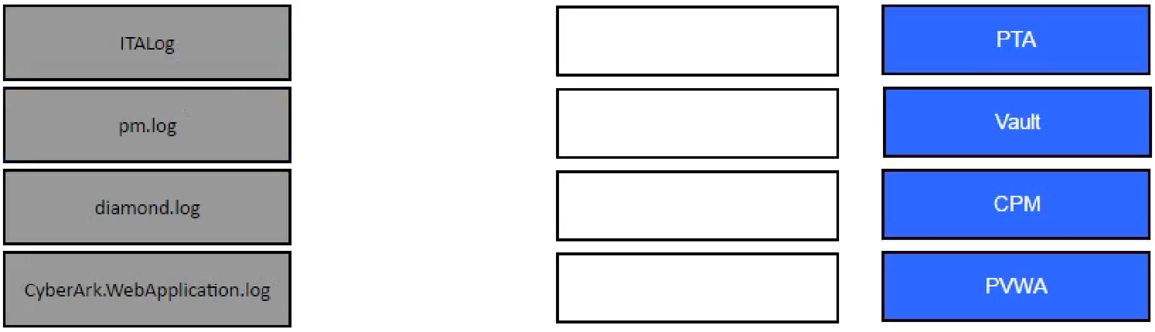
upvoted 4 times

Question #46 *Topic 1*

DRAG DROP -

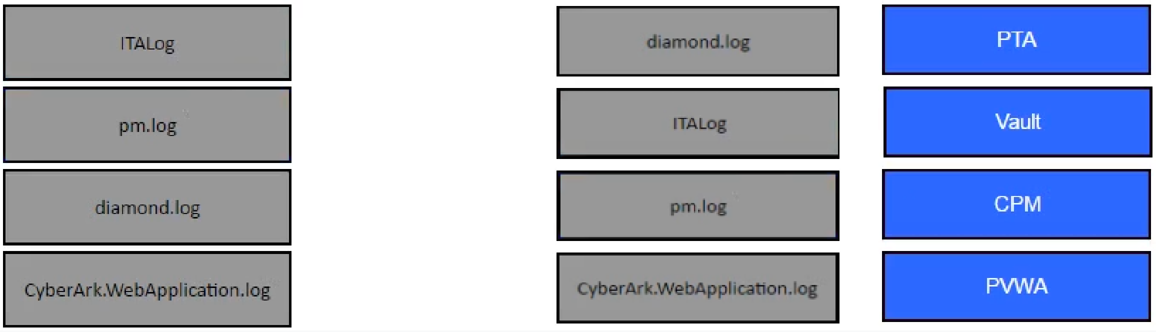
Match the log file name with the CyberArk Component that generates the log.

Select and Place:



ITALog		PTA
pm.log		Vault
diamond.log		CPM
CyberArk.WebApplication.log		PVWA

Suggested Answer:



ITALog	diamond.log	PTA
pm.log	ITALog	Vault
diamond.log	pm.log	CPM
CyberArk.WebApplication.log	CyberArk.WebApplication.log	PVWA

Reference:

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

Jony22 Highly Voted 1 year, 6 months ago

PTA - diamond.log

Vault - ITALog

CPM - pm.log

PVWA - CyberArk.WebApplication.log

upvoted 8 times

Question #47 *Topic 1*

Can the 'Connect' button be used to initiate an SSH connection, as root, to a Unix system when SSH access for root is denied?

A. Yes, when using the connect button, CyberArk uses the PMTerminal.exe process which bypasses the root SSH restriction.

B. Yes, only if a logon account is associated with the root account and the user connects through the PSM-SSH connection component.

C. Yes, if a logon account is associated with the root account.

D. No, it is not possible.

Suggested Answer: *C*

Community vote distribution

C (65%) B (35%)

⊟ **Hull** Highly Voted 3 years, 10 months ago

Selected Answer: C

You don't need to use PSM-SSH, this works over PVWA as well

upvoted 6 times

⊟ **Imdroc** Most Recent 1 year, 4 months ago

Selected Answer: C

Answer is C

upvoted 1 times

⊟ **dru0pa** 2 years, 6 months ago

Selected Answer: C

C

As the PSM for Windows can also do ssh connection to the Linux\Unix host as it makes use of Putty which is installed on the PSM for Windows.

upvoted 1 times

⊟ **Shivani_Goyal** 2 years, 8 months ago

Selected Answer: B

PSM for SSH works only with the PSMP-SSH connection component to perform SSH connections to targets. The configurations in the PSMP-SSH connection component affect all connections made with PSM for SSH. To change the configuration for some accounts, override the PSMP-SSH settings at platform level.

For example, you can configure the PSMP-SSH connection component with a setting for SSH connections, such as an AutomaticLogonSequenceWithLogonAccount for SSH. To define this setting for Telnet, create a platform for Telnet connections that overrides AutomaticLogonSequenceWithLogonAccount with a value suitable for Telnet connections.

upvoted 1 times

⊟ **xruinoiua** 2 years, 10 months ago

Selected Answer: C

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Using-Logon-Accounts-for-SSH-and-Telnet-Connections.htm?Highlight=logon%20account

upvoted 1 times

⊟ **Benny_On** 3 years, 1 month ago

Selected Answer: C

Not only PSM-SSH but also PSMP can also be used

https://cyberark-customers.force.com/s/article/PSM-SSH-Access-for-root-user

upvoted 1 times

⊟ **NLT** 3 years, 1 month ago

PSM-SSH and PSMP are the same though.

upvoted 1 times

⊟ **Innuendo** 3 years, 4 months ago

Selected Answer: C

You can use EVP Transparent Connection, directly, without PSM

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PASREF/Options%20-%20Connection%20Components.htm?

tocpath=Administrator%7CReferences%7CConfigure%20the%20system%20through%20PVWA%7COptions%7C_____19

upvoted 1 times

⊟ **carm8989** 3 years, 7 months ago

Selected Answer: B

ANS: B

upvoted 2 times

⊟ **Kaustav01** 3 years, 8 months ago

Selected Answer: B

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Using-Logon-Accounts-for-SSH-and-Telnet-Connections.htm?Highlight=logon%20account

upvoted 3 times

⊟ **Kaustav01** 3 years, 8 months ago

B

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Using-Logon-Accounts-for-SSH-and-Telnet-Connections.htm?Highlight=logon%20account

upvoted 1 times

Question #48 *Topic 1*

A user with administrative privileges to the vault can only grant other users privileges that he himself has.

A. TRUE

B. FALSE

Suggested Answer: *A*

Community vote distribution

A (92%) 8%

yoontzt Highly Voted 3 years, 10 months ago

Selected Answer: A

Correct Answer : A

upvoted 9 times

lmdroc Most Recent 1 year, 4 months ago

The answer is: A

upvoted 1 times

dru0pa 2 years, 6 months ago

Selected Answer: B

the limitation is you can not assign yourself administration privileges to a safe, you can grant others any privileges on any safe. this includes any you do not have access to. That is why when the administrator is left off from having access to a safe they are not able to add themselves to the safe by another user (Admin user) that can see the safe

upvoted 1 times

Benny_On 3 years, 2 months ago

Selected Answer: A

If user A administrative privileges have D,E,F role, so A can grand full D,E,F role to user B or less.

--> I think A is correct.

upvoted 2 times

Question #49 *Topic 1*

By default, members of which built-in groups will be able to view and configure Automatic Remediation and Session Analysis and Response in the PVWA?

A. Vault Admins

B. Security Admins

C. Security Operators

D. Auditors

Suggested Answer: *B*
Reference:
https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PTA/Security-Configuration.htm

Imdroc 1 year, 4 months ago
The question is Groups, so A and B
upvoted 1 times

> **Imdroc** 1 year, 4 months ago
> GroupS
> upvoted 1 times

Imdroc 1 year, 4 months ago
Answer is: AB
upvoted 1 times

dummy521 3 years, 1 month ago
A and B Correct answer
upvoted 2 times

NLT 3 years, 1 month ago
Users in the Vault Admins and Security Admins groups can configure the security rules and remediation actions.

You can update the groups in the SecurityConfigurationsAuthorizationGroups parameter, found in Administration > Options > General.
https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PTA/Security-Configuration.htm
upvoted 3 times

Chanez_22 3 years, 7 months ago
Correct answer A,B
upvoted 1 times

Kaustav01 3 years, 8 months ago
AB
https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PTA/Security-Configuration.htm
upvoted 3 times

tuga99 3 years, 11 months ago
Correct answer is A and B
upvoted 4 times

Question #50 *Topic 1*

CyberArk implements license limits by controlling the number and types of users that can be provisioned in the vault.

A. TRUE

B. FALSE

Suggested Answer: *A*

Reference:

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Managing-the-CyberArk-License.htm

Community vote distribution

A (100%)

Imdroc 1 year, 4 months ago

Selected Answer: A

Answer is A

upvoted 1 times

Kaustav01 3 years, 8 months ago

Selected Answer: A

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Managing-the-CyberArk-License.htm

upvoted 1 times

Question #51 *Topic 1*

Assuming a safe has been configured to be accessible during certain hours of the day, a Vault Admin may still access that safe outside of those hours.

A. TRUE

B. FALSE

Suggested Answer: *B*

Reference:

https://www.freshers360.com/wp-content/uploads/2019/05/Privileged-Account-Security-Implementation-Guide.pdf

Community vote distribution

B (100%)

Imdroc 1 year, 4 months ago

Selected Answer: B

Answer is B

upvoted 1 times

sunnyajmera 2 years, 11 months ago

I tested it too, B is the answer

upvoted 2 times

Benny_On 3 years, 2 months ago

I tested on my LAB --> B

upvoted 3 times

Question #52 *Topic 1*

The Accounts Feed contains:

A. Accounts that were discovered by CyberArk in the last 30 days

B. Accounts that were discovered by CyberArk that have not yet been onboarded

C. All accounts added to the vault in the last 30 days

D. All users added to CyberArk in the last 30 days

Suggested Answer: *B*

Community vote distribution

B (100%)

tuga99 Highly Voted 3 years, 11 months ago

Selected Answer: B

B is correct

upvoted 13 times

Imdroc Most Recent 1 year, 4 months ago

Selected Answer: B

The answer is: B

upvoted 1 times

Imdroc 1 year, 4 months ago

The answer is: B

upvoted 1 times

Azdender 3 years, 2 months ago

Selected Answer: B

B is in the test exam

upvoted 3 times

Benny_On 3 years, 2 months ago

Selected Answer: B

"All the detected accounts are displayed in the Pending Accounts page in the PVWA, where you can view them and onboard them, based on various criteria that you can define."
https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Accounts-Feed.htm?TocPath=End%20user%7CPrivileged%20Accounts%7CClassic%20Interface%7CAccounts%20Feed%7C_____0

upvoted 3 times

Question #53

Topic 1

PSM for Windows (previously known as `RDP Proxy`) supports connections to the following target systems

A. Windows

B. UNIX

C. Oracle

D. All of the above

Suggested Answer: *D*

Community vote distribution

D (100%)

⊟ **tuga99** Highly Voted 👍 1 year, 11 months ago

Selected Answer: D

D. All of the above

upvoted 6 times

⊟ **Azdender** Most Recent 🕘 1 year, 2 months ago

Selected Answer: D

Response D

upvoted 1 times

Question #54 *Topic 1*

What is the primary purpose of One Time Passwords?

A. Reduced risk of credential theft

B. More frequent password changes

C. Non-repudiation (individual accountability)

D. To force a 'collusion to commit' fraud ensuring no single actor may use a password without authorization.

Suggested Answer: *A*

Community vote distribution

A (75%) B (25%)

Jakub4444 Highly Voted 3 years, 5 months ago

Based on answers provided by CyberArk PAM Defender Mock exam - it's A

upvoted 9 times

Imdroc Most Recent 1 year, 4 months ago

The answer is: A

upvoted 1 times

uswarrior 2 years, 6 months ago

Selected Answer: A

The answer should be A.

upvoted 3 times

diyemop 3 years, 3 months ago

A cf Defender training

upvoted 4 times

Kaustav01 3 years, 8 months ago

Selected Answer: B

https://cyberark-customers.force.com/s/article/Understanding-the-possible-One-Time-Password-Exclusive-and-Allow-Manual-Change-combinations

upvoted 1 times

Kaustav01 3 years, 1 month ago

The correct answer is A. It's included in the official PAM Defender sample questions list.

upvoted 1 times

Question #55 *Topic 1*

The vault supports Subnet Based Access Control.

A. TRUE

B. FALSE

Suggested Answer: *A*

Community vote distribution

A (100%)

Kaustav01 1 year, 1 month ago

Selected Answer: A

In the official sample questions.

upvoted 1 times

Question #56 Topic 1

Ad-Hoc Access (formerly Secure Connect) provides the following features. (Choose all that apply.)

A. PSM connections to target devices that are not managed by CyberArk.

B. Session Recording.

C. Real-time live session monitoring.

D. PSM connections from a terminal without the need to login to the PVWA.

Suggested Answer: *ABC*

Community vote distribution

ABC (100%)

uswarrior 1 year, 6 months ago

Selected Answer: ABC

ABC is correct.

upvoted 1 times

Kaustav01 2 years, 8 months ago

Selected Answer: ABC

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Connecting-with-Secure-Connect.htm?TocPath=End%20User%7CConnect%20to%20Accounts%7C_____2

upvoted 2 times

Question #57 Topic 1

When a group is granted the 'Authorize Account Requests' permission on a safe Dual Control requests must be approved by

A. Any one person from that group

B. Every person from that group

C. The number of persons specified by the Master Policy

D. That access cannot be granted to groups

Suggested Answer: *C*

Community vote distribution

C (100%)

Imdroc 1 year, 4 months ago

Selected Answer: C

C is correct

upvoted 1 times

Imdroc 1 year, 4 months ago

The answer is: C

upvoted 1 times

amlal 2 years, 2 months ago

Selected Answer: C

The request is confirmed or rejected by the authorized user: Through the notification, authorized users can access the request and view its details. Based on these details, authorized users either confirm or reject the request. The number of authorized users who are required to confirm requests is defined in the Master Policy. Confirm requests from the PVWA (see Confirm requests in PVWA) or from the CyberArk Mobile app (see Confirm requests in CyberArk Mobile App).

upvoted 2 times

Kaustav01 3 years, 8 months ago

Selected Answer: C

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

upvoted 2 times

Question #58 Topic 1

When managing SSH keys, the CPM stores the Private Key

A. In the Vault

B. On the target server

C. A & B

D. Nowhere because the private key can always be generated from the public key.

Suggested Answer: *A*

Community vote distribution

A (100%)

⊟ **Kaustav01** Highly Voted 👍 1 year, 1 month ago

Selected Answer: A

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/SSHKM/Managing%20SSH%20Keys.htm

upvoted 6 times

Question #59 *Topic 1*

When managing SSH keys, the CPM stores the Public Key

A. In the Vault

B. On the target server

C. A & B

D. Nowhere because the public key can always be generated from the private key.

Suggested Answer: *B*

Community vote distribution

B (78%) 11% 11%

⊟ **amlal** 1 year, 2 months ago

Selected Answer: B

Public Key file

The path of the public key on the target machine. The default value is ~/.ssh/authorized_keys.

Note: If this path does not exist, the SSH Key Manager creates it automatically with the following permissions:

.ssh folder – 700
authorized_keys file – 600

https://docs.cyberark.com/PAS/Latest/en/Content/SSHKM/Managing%20SSH%20Keys.htm

upvoted 2 times

⊟ **Raymond9** 2 years, 5 months ago

Selected Answer: B

A single SSH Key can be used to access multiple target systems. The same public key is distributed to each target system where a privileged account can be authenticated using the same SSH Key.

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/SSHKM/Managing%20SSH%20Keys.htm

upvoted 2 times

⊟ **Jakub4444** 2 years, 4 months ago

This is true as per official CyberArk PAM mock exam too.

upvoted 2 times

⊟ **Chanez_22** 2 years, 7 months ago

B IS correct

upvoted 1 times

⊟ **harshuthkatta** 2 years, 7 months ago

Selected Answer: B

B is correct

upvoted 1 times

⊟ **carm8989** 2 years, 7 months ago

Selected Answer: A

correct answer A
https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/SSHKM/Managing %20SSH%20Keys.htm

upvoted 1 times

⊟ **Kaustav01** 2 years, 8 months ago

Selected Answer: B

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/SSHKM/Managing%20SSH%20Keys.htm

upvoted 2 times

⊟ **hila84** 2 years, 10 months ago

Selected Answer: D

Answer is D

upvoted 1 times

Question #60 *Topic 1*

Accounts Discovery allows secure connections to domain controllers.

A. TRUE

B. FALSE

Suggested Answer: *A*

Community vote distribution

A (86%) 14%

frodo1791 Highly Voted 👍 2 years, 11 months ago

Answer is A. True. Regarding PAM Exam.

upvoted 9 times

uswarrior Most Recent ⏲ 1 year, 6 months ago

Selected Answer: B

The question is not very clear.

The account discovery can discover accounts on domain controllers securely (using encryption)? The answer is Yes (A).

Account discovery allows (is used) to secure connections to domain controllers ? Not really. That's not its primary function. In this case, I would vote for B.

upvoted 1 times

EnjoyExam 2 years, 4 months ago

Selected Answer: A

Answer is A. True.

upvoted 2 times

Kaustav01 2 years, 8 months ago

Selected Answer: A

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Supported-Target-Machines.htm#_Ref453156095

upvoted 4 times

Question #61 *Topic 1*

Which parameter controls how often the CPM looks for Soon-to-be-expired Passwords that need to be changed?

A. HeadStartInterval

B. Interval

C. ImmediateInterval

D. The CPM does not change the password under this circumstance

Suggested Answer: *B*

Community vote distribution

B (75%) A (25%)

yoontzt Highly Voted 3 years, 10 months ago

Selected Answer: B

Correct Answer : B (from cyberark defender sample question)

upvoted 9 times

Kaustav01 Highly Voted 3 years, 8 months ago

Selected Answer: A

https://docs.cyberark.com/Product-Doc/OnlineHelp/PrivCloud/Latest/en/Content/PASREF/Automatic%20Password%20Management%20-%20Password%20Change.htm

upvoted 5 times

Imdroc Most Recent 1 year, 4 months ago

Selected Answer: B

Answer is B

upvoted 1 times

Imdroc 1 year, 4 months ago

Correct Answer : B

upvoted 1 times

amlal 2 years, 2 months ago

Selected Answer: A

Es ist A und nicht B da der Parameter von Interval sich unter General befindet und auf minuten basiert.
Interval

The number of minutes that the CPM waits between loops when processing accounts associated with this platform.

Acceptable values: Number

Default value: 1440
Hier der link zu Interval: https://docs.cyberark.com/PrivCloud/Latest/en/Content/PASREF/Automatic%20Password%20Management%20-%20General.htm?tocpath=Administrators%7CManage%20platforms%7CPlatform%20configuration%20and%20settings%7CAutomatic%20Password%20Management%7C_____1

Und hier zu Antwort A:
https://docs.cyberark.com/PrivCloud/Latest/en/Content/PASREF/Automatic%20Password%20Management%20-%20Password%20Change.htm?tocpath=Administrators%7CManage%20platforms%7CPlatform%20configuration%20and%20settings%7CAutomatic%20Password%20Management%7C_____4

upvoted 1 times

uswarrior 2 years, 6 months ago

Selected Answer: B

The correct answer is B.

* Interval: The number of minutes that the CPM waits between loops when processing accounts associated with this platform (Frequency of password validation check by CPM)
* HeadStartInterval: The number of days before the password expires that the CPM will initiate a password change process (minimum days before

password expiration that CPM must wait before initiating password change)
* ImmediateInterval: The number of minutes that will elapse between when the user initiates an account management process and when the process is performed. (Amout of time in minutes between when the user initiates password change and when the change is actually performed by CPM)

upvoted 1 times

Love_kesh28 3 years, 1 month ago

C is correct one

upvoted 1 times

Innuendo 3 years, 4 months ago

Selected Answer: B

....control HOW OFTEN: it is related to a cycle or loop, so, appliying logic it is related to Interval , not HeadInterval that only is a "advancement" of the real password expiration

upvoted 3 times

Raymond9 3 years, 5 months ago

A?

HeadStartInterval
The number of days before the password expires (according to the ExpirationPeriod parameter) that the CPM will initiate a password change process. This parameter is not relevant if the policy will be applied to a member of an account group.

Interval
The number of minutes that the Central Policy Manager waits between running periodic searches for the platform. Note: It is recommended to leave the default value of 1440. If a change/verify policy has been configured, the Central Policy Manager will automatically align the periodic searches with the start of the defined timeframes.

ImmediateInterval
The minimal time, in minutes, that will elapse from the last search performed by the Central Policy Manager for this platform until it processes the account. When OneTimePassword is used, it is recommended to set an immediate interval that is as short as possible, so that associated accounts are affected more quickly.

upvoted 4 times

Chanez_22 3 years, 7 months ago

Answer A

upvoted 1 times

harshuthkatta 3 years, 7 months ago

Selected Answer: B

B IS CORRECT

upvoted 4 times

Question #62 *Topic 1*

Vault admins must manually add the auditors group to newly created safes so auditors will have sufficient access to run reports.

A. TRUE

B. FALSE

Suggested Answer: *B*

Community vote distribution

B (100%)

⊟ **Kaustav01** Highly Voted 👍 3 years, 8 months ago

Selected Answer: B

Official CyberArk sample question

upvoted 5 times

⊟ **lmdroc** Most Recent ⏲ 1 year, 4 months ago

The answer is: B

upvoted 1 times

⊟ **uswarrior** 2 years, 6 months ago

Selected Answer: B

False. They can just update the LDAP group.

upvoted 1 times

Question #63 *Topic 1*

Which of the following Privileged Session Management solutions provide a detailed audit log of session activities?

A. PSM (i.e., launching connections by clicking on the "Connect" button in the PVWA)

B. PSM for Windows (previously known as RDP Proxy)

C. PSM for SSH (previously known as PSM SSH Proxy)

D. All of the above

Suggested Answer: *D*

Community vote distribution

D (100%)

tuga99 Highly Voted 👍 1 year, 5 months ago

Selected Answer: D

D is the correct answer

upvoted 8 times

Kaustav01 Most Recent 🕘 1 year, 1 month ago

Selected Answer: D

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.3/en/Content/PASIMP/Configuring-Recordings-and-Audits-in-PSM.htm

upvoted 3 times

Question #64 *Topic 1*

What is the primary purpose of Dual Control?

A. Reduced risk of credential theft

B. More frequent password changes

C. Non-repudiation (individual accountability)

D. To force a 'collusion to commit' fraud ensuring no single actor may use a password without authorization.

Suggested Answer: *D*

Community vote distribution

D (100%)

updates7777 1 year, 6 months ago

Selected Answer: D

D as per Defender mock exam questions

upvoted 1 times

sunnyajmera 1 year, 11 months ago

Answer is A

upvoted 1 times

Kaustav01 2 years, 8 months ago

Selected Answer: D

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

upvoted 4 times

Question #65 *Topic 1*

Time of day or day of week restrictions on when password verifications can occur configured in ____________________.

A. The Master Policy

B. The Platform settings

C. The Safe settings

D. The Account Details

Suggested Answer: *B*

Reference:

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

Community vote distribution

B (100%)

Imdroc 1 year, 4 months ago

Selected Answer: B

Answer is B

upvoted 1 times

ShaZZa_Anti_kit 3 years, 3 months ago

Answer B

upvoted 2 times

Chanez_22 3 years, 7 months ago

Answer B

Automatic password verification is determined by the following:

- The Master Policy defines how frequently passwords will be verified.

-Platform settings applied to the account determine how verification is initiated and the hours during which the verification process will take place.

upvoted 3 times

Question #66 *Topic 1*

Which parameter controls how often the CPM looks for accounts that need to be changed from recently completed Dual control requests?

A. HeadStartInterval

B. Interval

C. ImmediateInterval

D. The CPM does not change the password under this circumstance

Suggested Answer: *D*

Community vote distribution

D (82%) A (18%)

yoontzt Highly Voted 3 years, 10 months ago

Selected Answer: D

Correct Answer : D (from Cyberark Defender Sample Ques)

upvoted 8 times

Imdroc Most Recent 1 year, 4 months ago

Selected Answer: D

Answer is D

upvoted 1 times

Imdroc 1 year, 4 months ago

The answer is: D

upvoted 1 times

Chanez_22 3 years, 7 months ago

Answer D

upvoted 4 times

Kaustav01 3 years, 8 months ago

Selected Answer: A

https://docs.cyberark.com/Product-Doc/OnlineHelp/PrivCloud/Latest/en/Content/PASREF/Automatic%20Password%20Management%20-%20Password%20Change.htm

upvoted 2 times

Question #67 *Topic 1*

According to the DEFAULT Web Options settings, which group grants access to the REPORTS page?

A. PVWAUsers

B. Vault Admins

C. Auditors

D. PVWAMonitor

Suggested Answer: *D*

Community vote distribution

D (100%)

Imdroc 1 year, 4 months ago

Selected Answer: D

Answer is: D

upvoted 1 times

Imdroc 1 year, 4 months ago

Answer is: D

upvoted 1 times

updates7777 2 years, 6 months ago

Selected Answer: D

D as per CyberArk sample questions

upvoted 2 times

Chanez_22 3 years, 7 months ago

Answer D

PVWAMonitor

upvoted 2 times

Kaustav01 3 years, 8 months ago

Selected Answer: D

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

upvoted 3 times

Question #68 *Topic 1*

Which Master Policy Setting must be active in order to have an account checked-out by one user for a pre-determined amount of time?

A. Require dual control password access Approval

B. Enforce check-in/check-out exclusive access

C. Enforce one-time password access

D. Enforce check-in/check-out exclusive access & Enforce one-time password access

Suggested Answer: *D*

Community vote distribution

D (100%)

frodo1791 Highly Voted 3 years, 11 months ago

Answer is D regarding PAM Exam.

upvoted 13 times

Imdroc Most Recent 1 year, 4 months ago

Selected Answer: D

Answer is D

upvoted 1 times

sahilyakup 3 years ago

D is correct. Here the key point is to know that using one-time password restricts access to a single user. And the question asks for one user which has the same meaning.

upvoted 3 times

Raymond9 3 years, 5 months ago

Selected Answer: D

To achieve automatic release of locked passwords and full personal accountability, enable this rule along with the Enforce one-time password access rule.

https://docs.cyberark.com/Product-Doc/OnlineHelp/PrivCloud/Latest/en/Content/Privilege%20Cloud/privCloud-master-policy-rules.htm#Enforce

upvoted 3 times

MohdAnis 3 years, 7 months ago

Correct Answer is D according to CyberArk Defender Sample exam.

upvoted 4 times

Chanez_22 3 years, 7 months ago

Answer D

upvoted 3 times

Question #69 *Topic 1*

The password upload utility must run from the CPM server

A. TRUE

B. FALSE

Suggested Answer: *B*

Reference:

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Password-Upload-Utility.htm

Community vote distribution

B (100%)

Imdroc 1 year, 4 months ago

Selected Answer: B

Answer is B

upvoted 1 times

KHKH2021 2 years, 5 months ago

B is correct

upvoted 1 times

Chanez_22 3 years, 7 months ago

Answer B

upvoted 1 times

> **Jakub4444** 3 years, 4 months ago
>
> Agreed.
>
> https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.2/en/Content/PAS%20INST/Password-Upload-Utility-Installation.htm?tocpath=Installation%7CInstall%20PAM%7CInstall%20the%20Vault%20Utilities%7CPassword%20Upload%20Utility%7C_____2
>
> upvoted 1 times

Kaustav01 3 years, 7 months ago

Selected Answer: B

Easy one

upvoted 1 times

Question #70 Topic 1

For a safe with Object Level Access enabled you can turn off Object Level Access Control when it no longer needed on the safe.

A. TRUE

B. FALSE

Suggested Answer: *B*

Community vote distribution

B (100%)

Imdroc 1 year, 4 months ago

Selected Answer: B

Answer is B

upvoted 1 times

Kaustav01 3 years, 7 months ago

Selected Answer: B

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.1/en/Content/PASIMP/Object-Level-Access-Control.htm#:~:text=The%20Privileged%20Access%20Security%20solution,of%20Safe%20level%20member%20authorizations.

upvoted 4 times

Question #71 *Topic 1*

When creating an onboarding rule, it will be executed upon ___________________.

A. All accounts in the pending accounts list

B. Any future accounts discovered by a discovery process

C. Both ג€All accounts in the pending accounts listג€ and ג€Any future accounts discovered by a discovery processג€

Suggested Answer: *B*

Community vote distribution

B (100%)

Kaustav01 Highly Voted 3 years, 7 months ago

Selected Answer: B

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/automatic_onboarding_rules.htm?TocPath=End%20User%7CPrivileged%20Accounts%7CVersion%2010%20Interface%7C_____12

upvoted 5 times

lmdroc Most Recent 1 year, 4 months ago

Selected Answer: B

Answer is B

upvoted 1 times

lmdroc 1 year, 4 months ago

The answer is: B

upvoted 1 times

KHKH2021 2 years, 5 months ago

answer is B

upvoted 1 times

Question #72 *Topic 1*

How does the Vault administrator apply a new license file?

A. Upload the license.xml file to the system Safe and restart the PrivateArk Server service

B. Upload the license.xml file to the system Safe

C. Upload the license.xml file to the Vault Internal Safe and restart the PrivateArk Server service

D. Upload the license.xml file to the Vault Internal Safe

Suggested Answer: *B*

Community vote distribution

B (79%) A (21%)

Kaustav01 Highly Voted 3 years, 7 months ago

Selected Answer: B

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Managing-the-CyberArk-License.htm

upvoted 9 times

JSOC_DXB Most Recent 1 year, 3 months ago

The question is badly asked, but if you're going to use the vault admin to update it you need to use the PrivateArk client, in which case you do not need to restart the service.

If you were going to add the file manually in the OS, then you would use the local administrator user, and would need to restart the service.

Answer B

upvoted 1 times

Imdroc 1 year, 4 months ago

Selected Answer: B

Answer is B

upvoted 1 times

KHKH2021 2 years, 5 months ago

ansver is B

upvoted 2 times

uswarrior 2 years, 6 months ago

Selected Answer: B

When uploading to system safe via private ark client, no need to restart privateark service.

upvoted 1 times

rabznet 2 years, 11 months ago

Answer is B

Two methods of adding license

1. Via PrivateArk Server - safes no needs to restart

2. Copying the license straight into Conf folder - there is a need to PrivateArk Server service

upvoted 2 times

JAD159 3 years ago

Selected Answer: A

You need restart the service.

Reference: https://cyberark-customers.force.com/s/article/00002945

upvoted 3 times

Chanez_22 3 years, 7 months ago

Answer B

upvoted 2 times

Question #73 *Topic 1*

When Dual Control is enabled a user must first submit a request in the Password Vault Web Access (PVWA) and receive approval before being able to launch a secure connection via PSM for Windows (previously known as RDP Proxy).

A. True

B. False, a user can submit the request after the connection has already been initiated via the PSM for Windows

Suggested Answer: *A*

Community vote distribution

A (100%)

Hull Highly Voted 3 years, 10 months ago

Selected Answer: A

If a user must request access, then there is no way for user to access the target system with requested account before getting the approval, as that would make dual control useless. There is an option to get access and bypass dual control even when it is enabled, as per https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/DualControlV10.htm#Dualcontroloptions

But that's not what it is asked here

upvoted 8 times

Imdroc Most Recent 1 year, 4 months ago

Selected Answer: A

Answer is A

upvoted 1 times

Chanez_22 3 years, 7 months ago

Answer A

upvoted 3 times

Kaustav01 3 years, 7 months ago

Selected Answer: A

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Dual-Control.htm#_Ref232742832

upvoted 4 times

Question #74 *Topic 1*

Which of the following PTA detections require the deployment of a Network Sensor or installing the PTA Agent on the domain controller?

A. Suspected credential theft

B. Over-Pass-The-Hash

C. Golden Ticket

D. Unmanaged privileged access

Suggested Answer: *B*

Community vote distribution

B (100%)

⊟ **Hull** Highly Voted 👍 3 years, 10 months ago

Selected Answer: B

It is B and C

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

upvoted 10 times

⊟ **frodo1791** Highly Voted 👍 3 years, 11 months ago

I think answer is B and C.

upvoted 6 times

⊟ **Imdroc** Most Recent 🕐 1 year, 4 months ago

The answer is: BC

upvoted 1 times

⊟ **KHKH2021** 2 years, 5 months ago

B and C

upvoted 3 times

⊟ **[Removed]** 3 years, 2 months ago

Selected Answer: B

B and C, Sample Exam

upvoted 3 times

⊟ **Jaheim** 3 years, 2 months ago

ACD - From Sample Exam

upvoted 1 times

Question #75 *Topic 1*

Via Password Vault Web Access (PVWA), a user initiates a PSM connection to the target Linux machine using RemoteApp. When the client's machine makes an
RDP connection to the PSM server, which user will be utilized?

A. Credentials stored in the Vault for the target machine

B. Shadowuser

C. PSMConnect

D. PSMAdminConnect

Suggested Answer: *C*

Community vote distribution

C (100%)

Kaustav01 Highly Voted 👍 3 years, 7 months ago

Selected Answer: C

PSMConnect is the main user that connects to the PSM.
PSMAdminConnect is the user that is used for Live Monitoring

upvoted 7 times

Imdroc Most Recent 1 year, 4 months ago

Selected Answer: C

Answer is C

upvoted 1 times

Imdroc 1 year, 4 months ago

The answer is: C

upvoted 1 times

EnjoyExam 3 years, 4 months ago

Selected Answer: C

C is correct

upvoted 3 times

Question #76 *Topic 1*

Which report shows the accounts that are accessible to each user?

A. Activity report

B. Entitlement report

C. Privileged Accounts Compliance Status report

D. Applications Inventory report

Suggested Answer: *B*

Community vote distribution

B (100%)

Imdroc 1 year, 4 months ago

Selected Answer: B

Answer is B

upvoted 1 times

Chanez_22 3 years, 7 months ago

Answer B

upvoted 3 times

Kaustav01 3 years, 7 months ago

Selected Answer: B

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

upvoted 3 times

Question #77 *Topic 1*

The Vault administrator can change the Vault license by uploading the new license to the system Safe.

A. True

B. False

Suggested Answer: *A*

Community vote distribution

A (100%)

Imdroc 1 year, 4 months ago

Selected Answer: A

answer is A

upvoted 1 times

KHKH2021 2 years, 5 months ago

Answer is A

upvoted 1 times

EnjoyExam 3 years, 4 months ago

Selected Answer: A

A is correct

upvoted 3 times

Chanez_22 3 years, 7 months ago

Answer A

upvoted 4 times

Question #78 *Topic 1*

A Vault administrator have associated a logon account to one of their Unix root accounts in the vault. When attempting to verify the root account's password the
Central Policy Manager (CPM) will:

A. ignore the logon account and attempt to log in as root

B. prompt the end user with a dialog box asking for the login account to use

C. log in first with the logon account, then run the SU command to log in as root using the password in the Vault

D. none of these

Suggested Answer: *C*

Community vote distribution

C (100%)

frodo1791 Highly Voted 3 years, 11 months ago

Answer shoud be C.

upvoted 9 times

Hull Highly Voted 3 years, 10 months ago

Selected Answer: C

Answer is C, password verification and login for linux root is done in the same way

upvoted 8 times

Imdroc Most Recent 1 year, 4 months ago

Selected Answer: C

Answer is C

upvoted 1 times

Question #79 *Topic 1*

Which is the primary purpose of exclusive accounts?

A. Reduced risk of credential theft

B. More frequent password changes

C. Non-repudiation (individual accountability)

D. To force a 'collusion to commit' fraud ensuring no single actor may use a password without authorization

Suggested Answer: *C*

Community vote distribution

C (100%)

Imdroc 1 year, 4 months ago

Selected Answer: C

Answer is C

upvoted 1 times

KHKH2021 2 years, 5 months ago

ansver C

upvoted 1 times

Innuendo 3 years, 4 months ago

Answer C

upvoted 3 times

Chanez_22 3 years, 7 months ago

Answer C

upvoted 2 times

Kaustav01 3 years, 7 months ago

Selected Answer: C

https://docs.cyberark.com/Product-Doc/OnlineHelp/AAM-DAP/Latest/en/Content/CP%20and%20ASCP/cv_Using-One-time-Passwords-Exclusive-Accounts.htm

upvoted 2 times

Question #80 *Topic 1*

What is the chief benefit of PSM?

A. Privileged session isolation

B. Automatic password management

C. Privileged session recording

D. 'Privileged session isolation' and 'Privileged session recording'

Suggested Answer: *D*

Community vote distribution

D (100%)

Hull Highly Voted 👍 3 years, 10 months ago

Selected Answer: D

As per CyberArk PAM Admin course, Privileged Session Management provides three main benefits :
Isolation
Monitoring
Recording

So, answer is D

upvoted 7 times

Imdroc Most Recent ◷ 1 year, 4 months ago

Selected Answer: D

Answer is D

upvoted 1 times

Question #81 *Topic 1*

A Simple Mail Transfer Protocol (SMTP) integration is critical for monitoring Vault activity and facilitating workflow processes, such as Dual Control.

A. True

B. False

Suggested Answer: *A*

Community vote distribution

A (100%)

Atoure_22 Highly Voted 👍 3 years, 11 months ago

Answer A to refer to sample exam PAM

upvoted 10 times

Imdroc Most Recent 🕓 1 year, 4 months ago

Selected Answer: A

Answer is A

upvoted 1 times

EnjoyExam 3 years, 4 months ago

Selected Answer: A

A is correct

upvoted 2 times

hila84 3 years, 10 months ago

Selected Answer: A

Answer is A

upvoted 3 times

Question #82 *Topic 1*

CyberArk recommends implementing object level access control on all Safes.

A. True

B. False

Suggested Answer: *B*

Community vote distribution

B (100%)

Imdroc 1 year, 4 months ago

Selected Answer: B

Answer is B

upvoted 1 times

KHKH2021 2 years, 5 months ago

answer is B

upvoted 1 times

ShaZZa_Anti_kit 3 years, 3 months ago

Answer B

upvoted 1 times

Question #83 Topic 1

Which of the following logs contains information about errors related to PTA?

A. ITAlog.log

B. diamond.log

C. pm_error.log

D. WebApplication.log

Suggested Answer: *B*

Community vote distribution

B (100%)

lmdroc 1 year, 4 months ago

Selected Answer: B

Answer is B

upvoted 1 times

dummy521 3 years, 1 month ago

B is answer

upvoted 2 times

Question #84 *Topic 1*

An auditor initiates a live monitoring session to PSM server to view an ongoing live session. When the auditor's machine makes an RDP connection the PSM server, which user will be used?

A. PSMAdminConnect

B. Shadowuser

C. PSMConnect

D. Credentials stored in the Vault for the target machine

Suggested Answer: *A*

Community vote distribution

A (100%)

Imdroc 1 year, 4 months ago

Selected Answer: A

Answer is A

upvoted 1 times

Kaustav01 3 years, 7 months ago

Selected Answer: A

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/Optional-Moving-the-PSMConnec-and-PSMAdminConnect-users-to-your-Domain.htm#ConfiguretheRemoteDesktopSessiononthePSM

upvoted 2 times

Question #85 *Topic 1*

Which keys are required to be present in order to start the PrivateArk Server service?

A. Recovery public key

B. Recovery private key

C. Server key

D. Safe key

Suggested Answer: *AC*

Community vote distribution

AC (100%)

Kaustav01 Highly Voted 3 years, 7 months ago

Selected Answer: AC

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Server-Keys.htm?
TocPath=Administrator%7CComponents%7CDigital%20Vault%7CAdvanced%20Digital%20Vault%20Environment%7CCyberArk%20Vault%20Structure%7C_____

upvoted 5 times

Imdroc Most Recent 1 year, 4 months ago

Selected Answer: AC

Differently Answser is AC

upvoted 1 times

Imdroc 1 year, 4 months ago

The answer is: AC

upvoted 1 times

Question #86 *Topic 1*

Which of the following Privileged Session Management (PSM) solutions support live monitoring of active sessions?

A. PSM (i.e., launching connections by clicking on the connect button in the Password Vault Web Access (PVWA)

B. PSM for Windows (previously known as RDP Proxy)

C. PSM for SSH (previously known as PSM-SSH Proxy)

D. All of the above

Suggested Answer: *D*

Community vote distribution

D (100%)

Kaustav01 Highly Voted 3 years, 7 months ago

Selected Answer: D

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Monitoring-Privileged-Sessions.htm?tocpath=End%20user%7CMonitor%20Sessions%7CClassic%20Interface%7C_____1

upvoted 5 times

Imdroc Most Recent 1 year, 4 months ago

Selected Answer: D

Answer is D

upvoted 1 times

Imdroc 1 year, 4 months ago

The answer is: D

upvoted 1 times

frodo1791 3 years, 11 months ago

Answer is A and B. There is no live monitoring for PSMP.

upvoted 2 times

Benny_On 3 years, 1 month ago

v12.6 has live monitoring (keystroke live monitoring) for PSMP

upvoted 1 times

Jakub4444 3 years, 4 months ago

That's not correct, sir. Answer is D.

upvoted 1 times

Question #87 *Topic 1*

Within the Vault each password is encrypted by:

A. the server key

B. the recovery public key

C. the recovery private key

D. its own unique key

Suggested Answer: *D*

Community vote distribution

D (100%)

Imdroc 1 year, 4 months ago

Selected Answer: D

Answer is D

upvoted 1 times

Kaustav01 3 years, 7 months ago

Selected Answer: D

CyberArk sample question

upvoted 4 times