CyberArk Defender

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.

Answer(s): B

---

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

A. TRUE

B. FALSE

Answer(s): A

---

3. VAULT authorizations may be granted to_____. (Choose all that apply.)

A. Vault Users

B. Vault Groups

C. LDAP Users

D. LDAP Groups

Answer(s): C

4. 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.

Answer(s): A

---

5. 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

Answer(s): A

---

6. 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.

Answer(s): C

---

7. 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

Answer(s): A

---

8. A Logon Account can be specified in the Master Policy.

A. TRUE

B. FALSE

Answer(s): B

---

9. 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.

Answer(s): A

---

10. 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

Answer(s): B

---

11. 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

Answer(s): A

---

12. 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 onboarded 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.

Answer(s): C

---

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

A. TRUE

B. FALSE

Answer(s): B

---

14. 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

Answer(s): C

---

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

A. TRUE

B. FALSE

Answer(s): A

---

16. Platform settings are applied to_____.

A. The entire vault.

B. Network Areas

C. Safes

D. Individual Accounts

Answer(s): C

---

17. 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

Answer(s): B

---

18. 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

Answer(s): D

---

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

A. TRUE

B. FALSE

Answer(s): A

---

20. 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

Answer(s): C
